UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CORRECT TRANSMISSION, LLC	§	
	§	
Plaintiff,	§	Case No. 2:22-cv-00343
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
NOKIA CORPORATION, NOKIA	§	
SOLUTIONS AND NETWORKS OY, AND	§	
NOKIA OF AMERICA CORPORATION,	§	
	§	
Defendants.		

COMPLAINT FOR PATENT INFRINGEMENT

Correct Transmission, LLC ("Correct Transmission" or "Plaintiff"), by and through its attorneys, for its Complaint for patent infringement against Nokia of America Corporation, Nokia Solutions and Networks Oy, and Nokia of America Corporation ("Nokia" or "Defendants"), and demanding trial by jury, hereby alleges, on information and belief with regard to the actions of Defendants and on knowledge with regard to its own actions, as follows:

I. NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 271, et seq., to enjoin and obtain damages resulting from Defendants' unauthorized use, sale, and offer to sell in the United States, of products, methods, processes, services and/or systems that infringe Plaintiff's United States patents, as described herein.

2. Defendants manufacture, provide, use, sell, offer for sale, import, and/or distribute infringing products and services, and encourages others to use its products and services in an infringing manner, as set forth herein.

3. Plaintiff seeks past and future damages and prejudgment and post-judgment interest for Defendants' infringement of the Asserted Patents, as defined below.

II. PARTIES

4. Plaintiff Correct Transmission is a limited liability company organized and existing under the law of the State of Delaware, with its principal place of business located at 825 Watter's Creek Boulevard, Building M, Suite 250, Allen, TX 75013.

5. Correct Transmission is the owner of the entire right, title, and interest of the Asserted Patents, as defined below.

6. Defendant Nokia Corporation ("Nokia Corp.") is a Finnish corporation with its principal place of business at Karaportti 3, FI-02610 Espoo, Finland. Upon information and belief, Alcatel-Lucent S.A. ("Alcatel-Lucent") was merged into Nokia Corp.'s "Nokia Networks" division in 2016.

7. Defendant Nokia Solutions and Networks Oy is a corporation organized and existing under the laws of Finland with its principal place of business at Karaportti 3, 02610 Espoo, Finland. On information and belief, Nokia Solutions and Networks Oy is a wholly owned subsidiary of Nokia Corp.

8. Nokia of America Corporation is a Delaware corporation with its U.S. Headquarters in Dallas, Texas. Nokia may be served through its registered agent Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, Texas 78701. On information and belief, Nokia is registered to do business in the State of Texas and has been since at least December 29, 1995.

9. On information and belief, Nokia of America Corporation is an indirect wholly owned subsidiary of Nokia Corporation and Nokia Solutions and Networks Oy.

10. Nokia Corp., Nokia Solutions and Networks Oy, and Nokia of America are collectively referred to as "Nokia."

11. The Nokia Defendants hold themselves out as a single "Nokia" company, exemplified in the company's website, www.nokia.com. Nokia offers for sale and sells the accused products, through that website.

12. Nokia conducts business operations within the Eastern District of Texas, including its offices located at 2525 Highway 121, Lewisville, Texas 75056 and 601 Data Drive, Plano, Texas 75075. Nokia has offices in the Eastern District of Texas where it sells and/or markets its products, including its offices in Lewisville and Plano, Texas.

13. Nokia maintains additional offices throughout Texas including its U.S. headquarters in Dallas and office in this district.

III. JURISDICTION AND VENUE

14. This is an action for patent infringement which arises under the patent laws of the United States, in particular, 35 U.S.C. §§ 271, 281, 283, 284, and 285.

15. This Court has exclusive jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

16. This Court has personal jurisdiction over Nokia in this action because Nokia has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Nokia would not offend traditional notions of fair play and substantial justice. Defendants Nokia, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the Asserted Patents. Moreover, Nokia is registered to do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

17. Venue is proper in this district under 28 U.S.C. §§ 1391(b)–(d) and 1400(b). Defendant Nokia of America Corporation is registered to do business in the State of Texas, has offices in the State of Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas. Nokia of America Corporation maintains a regular and established place of business in the Eastern District of Texas, including offices located at 2525 Highway 121, Lewisville, Texas 75056 and 601 Data Drive, Plano, Texas 75075. Nokia has operated the Plano office as a "NokiaEDU Training Center," which it describes as "the company's premiere learning organization serving customers, partners and employees worldwide . . . . to deliver[] a top-quality learning experience tailored to our customers' specific requirements and preferences." https://learningstore.nokia.com/locations/files/US-Plano.pdf.

18. Venue is proper as to Nokia Corp. under 28 U.S.C. § 1391(c)(3) as a corporation that is not resident in the United States.

19. Venue is proper as to Nokia Solutions and Networks Oy under 28 U.S.C. § 1391(c)(3) as a corporation that is not resident in the United States.

IV. COUNTS OF PATENT INFRINGEMENT

20. Plaintiff alleges that Defendants have infringed and continue to infringe the following United States patents (collectively the "Asserted Patents"):

United States Patent No. 6,876,669 (the "'669 Patent") (Exhibit A)
United States Patent No. 7,127,523 (the "'523 Patent") (Exhibit B)
United States Patent No. 7,283,465 (the "'465 Patent") (Exhibit C)
United States Patent No. 7,768,928 (the "'928 Patent") (Exhibit D)
United States Patent No. 7,983,150 (the "'150 Patent") (Exhibit E)

COUNT ONE
INFRINGEMENT OF U.S. PATENT 6,876,669

21. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-20 as if fully set forth herein.

22. The ’669 Patent, entitled “PACKET FRAGMENTATION WITH NESTED INTERRUPTIONS,” was filed on January 8, 2001 and issued on April 5, 2005.

23. Plaintiff is the assignee and owner of all rights, title and interest to the ’669 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

24. On May 19, 2021, IPR2021-00984 was filed on the ‘669 Patent challenging claims 1 – 27. On November 19, 2021, the Patent Trial and Appeal Board (“PTAB”) denied institution of IPR2021-00984.

Technical Description

25. The ’669 Patent addresses problems in the prior art of fragmentation, including that a prior art data transmission method “cannot stop until the entire packet has been sent” “once the transmitter has begun sending fragments of a given packet.” (col. 3, ll. 6-10). “Thus, the only way that a high-priority packet can be "assured immediate transmission is by discarding any low-priority packets whose transmission is in progress.” (col. 3, ll. 10-13).

26. The ’669 Patent provides a technical solution to prior art problems by applying a “multi-priority approach,” which “allows the transmitter to stop sending the low-priority packet in the middle, and then to complete the transmission after high-priority requirements have been serviced.” Indeed, in a preferred embodiment, any number of increasingly high-priority packets may interrupt transmission of earlier commenced transmissions of lower-priority

packets, using "nested" packet interruptions, "without compromising the ability of the receiver to reassemble all of the packets." (col. 3, ll. 14-30).

Direct Infringement

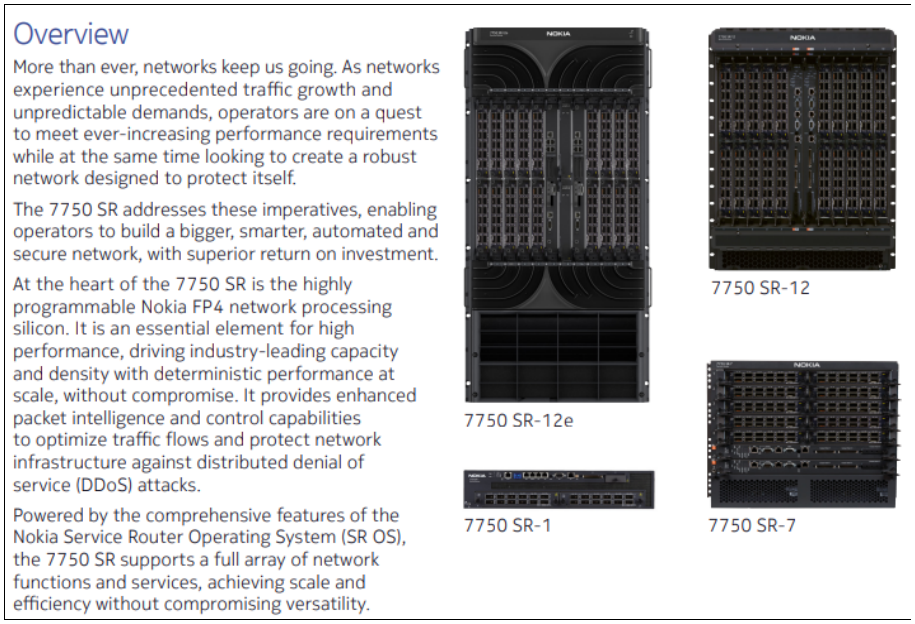
27. Defendants, without authorization or license from Plaintiff, have been and are directly infringing the '669 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale telecommunications equipment that infringes one or more claims of the '669 Patent. Defendants develop, designs, manufacture, and distribute telecommunications equipment that infringes one or more claims of the '669 Patent. Defendants further provide services that practice methods that infringe one or more claims of the '669 Patent. Defendants are thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Defendants' Nokia 7750 Service Router and all other substantially similar products (collectively the "'669 Accused Products").

28. Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendants' infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '669 Accused Products.

29. Defendants are liable for direct infringement pursuant to 35 U.S.C. § 271 for the manufacture, sale, offer for sale, importation, or distribution of Defendants' 7750 Service Router.

30. Defendants' 7750 Service Router is a non-limiting example of an apparatus that meets all limitations of claim 1 of the '669 Patent, either literally or equivalently.

31. The 7750 Service Router comprises a method for transmitting data over a channel.



Overview

More than ever, networks keep us going. As networks experience unprecedented traffic growth and unpredictable demands, operators are on a quest to meet ever-increasing performance requirements while at the same time looking to create a robust network designed to protect itself.

The 7750 SR addresses these imperatives, enabling operators to build a bigger, smarter, automated and secure network, with superior return on investment.

At the heart of the 7750 SR is the highly programmable Nokia FP4 network processing silicon. It is an essential element for high performance, driving industry-leading capacity and density with deterministic performance at scale, without compromise. It provides enhanced packet intelligence and control capabilities to optimize traffic flows and protect network infrastructure against distributed denial of service (DDoS) attacks.

Powered by the comprehensive features of the Nokia Service Router Operating System (SR OS), the 7750 SR supports a full array of network functions and services, achieving scale and efficiency without compromising versatility.

7750 SR-12e

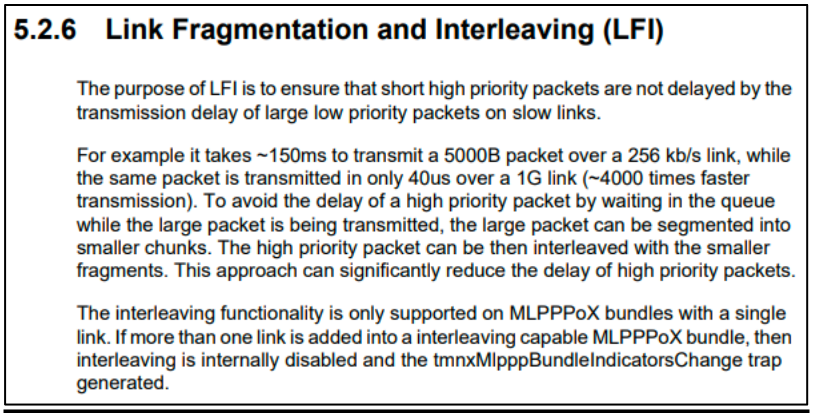
7750 SR-12

7750 SR-1

7750 SR-7

https://resources.nokia.com/asset/164728?_ga=2.188290280.1557979830.1638603790-478191956.1631863234 **(Page 1 of PDF)**

32. The 7750 Service Router receives a first datagram for transmission at a first priority.



5.2.6 Link Fragmentation and Interleaving (LFI)

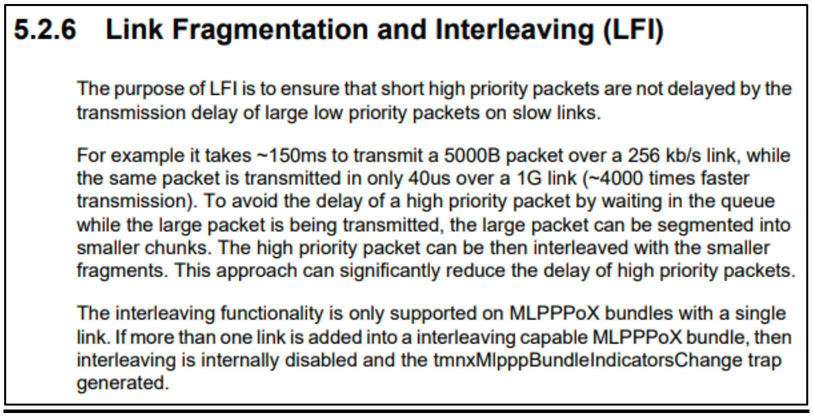
The purpose of LFI is to ensure that short high priority packets are not delayed by the transmission delay of large low priority packets on slow links.

For example it takes ~150ms to transmit a 5000B packet over a 256 kb/s link, while the same packet is transmitted in only 40us over a 1G link (~4000 times faster transmission). To avoid the delay of a high priority packet by waiting in the queue while the large packet is being transmitted, the large packet can be segmented into smaller chunks. The high priority packet can be then interleaved with the smaller fragments. This approach can significantly reduce the delay of high priority packets.

The interleaving functionality is only supported on MLPPPoX bundles with a single link. If more than one link is added into a interleaving capable MLPPPoX bundle, then interleaving is internally disabled and the tmnxMlpppBundleIndicatorsChange trap generated.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf **(Page 182 of PDF)**

33. The 7750 Service Router receives a second datagram for transmission at a second priority, higher than the first priority, before the transmission of the first datagram is completed.



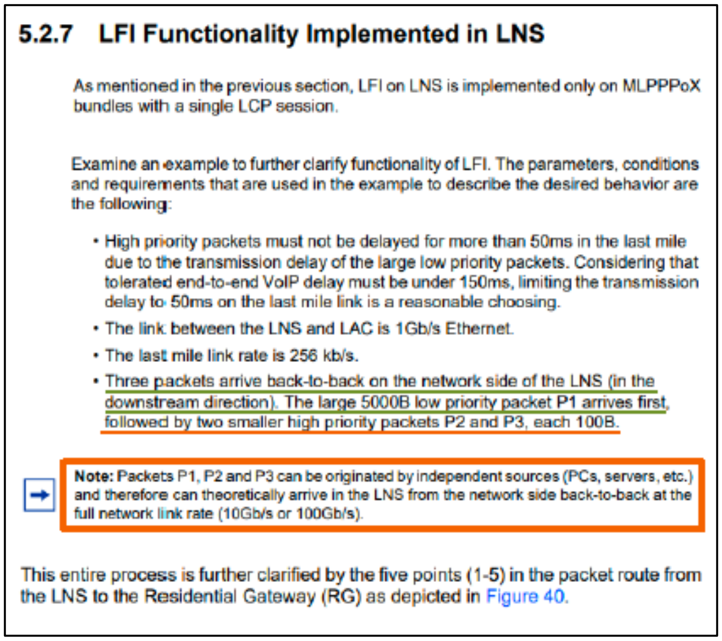
5.2.6 Link Fragmentation and Interleaving (LFI)

The purpose of LFI is to ensure that short high priority packets are not delayed by the transmission delay of large low priority packets on slow links.

For example it takes ~150ms to transmit a 5000B packet over a 256 kb/s link, while the same packet is transmitted in only 40us over a 1G link (~4000 times faster transmission). To avoid the delay of a high priority packet by waiting in the queue while the large packet is being transmitted, the large packet can be segmented into smaller chunks. The high priority packet can be then interleaved with the smaller fragments. This approach can significantly reduce the delay of high priority packets.

The interleaving functionality is only supported on MLPPPoX bundles with a single link. If more than one link is added into a interleaving capable MLPPPoX bundle, then interleaving is internally disabled and the tmnxMlpppBundleIndicatorsChange trap generated.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Page 182 of PDF**)



5.2.7 LFI Functionality Implemented in LNS

As mentioned in the previous section, LFI on LNS is implemented only on MLPPPoX bundles with a single LCP session.

Examine an example to further clarify functionality of LFI. The parameters, conditions and requirements that are used in the example to describe the desired behavior are the following:

- High priority packets must not be delayed for more than 50ms in the last mile due to the transmission delay of the large low priority packets. Considering that tolerated end-to-end VoIP delay must be under 150ms, limiting the transmission delay to 50ms on the last mile link is a reasonable choosing.
- The link between the LNS and LAC is 1Gb/s Ethernet.
- The last mile link rate is 256 kb/s.
- Three packets arrive back-to-back on the network side of the LNS (in the downstream direction). The large 5000B low priority packet P1 arrives first, followed by two smaller high priority packets P2 and P3, each 100B.

Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

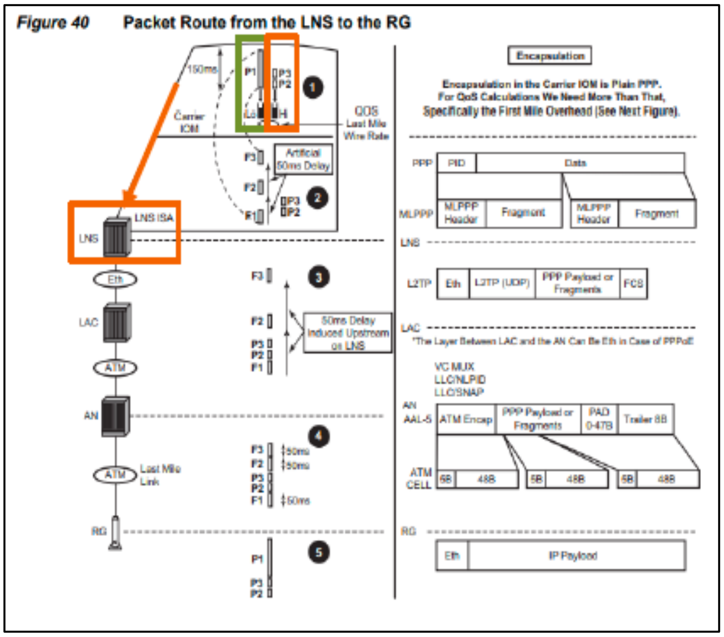
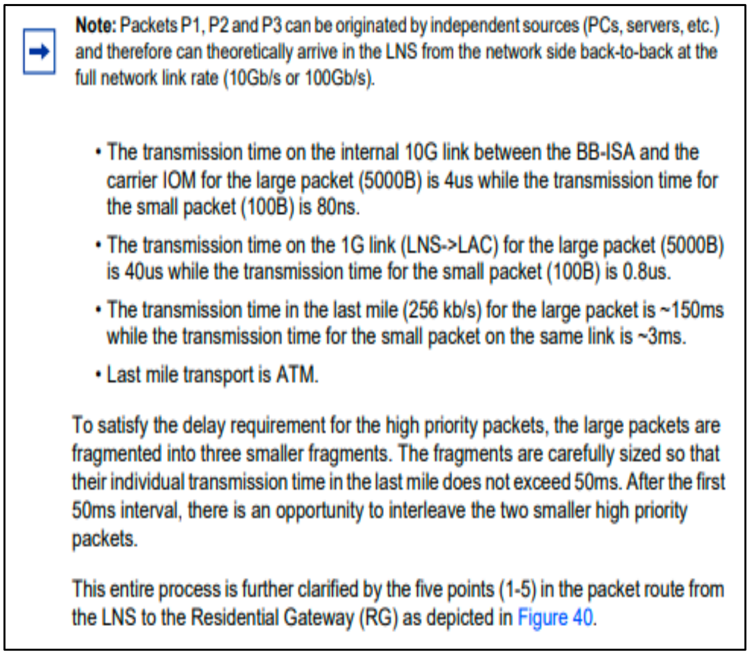


Figure 40 Packet Route from the LNS to the RG

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf **(Pages 184-186 of PDF)**

34. The 7750 Service Router responsive to receiving the second datagram, deciding to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.



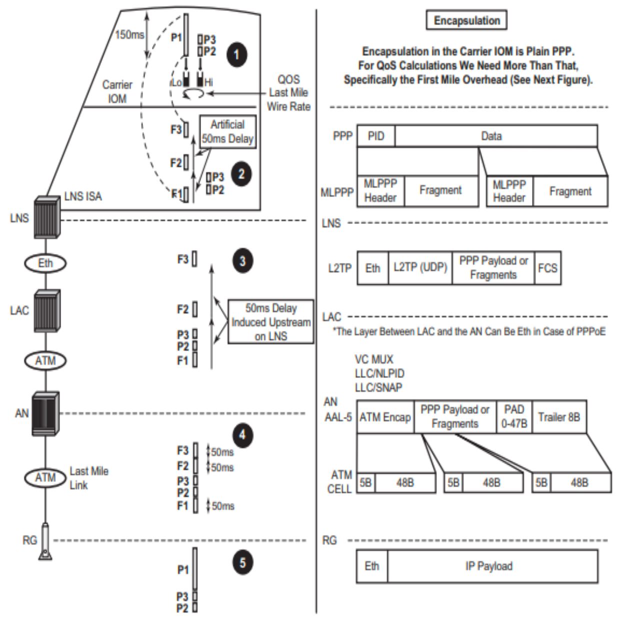
Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

- The transmission time on the internal 10G link between the BB-ISA and the carrier IOM for the large packet (5000B) is 4us while the transmission time for the small packet (100B) is 80ns.
- The transmission time on the 1G link (LNS->LAC) for the large packet (5000B) is 40us while the transmission time for the small packet (100B) is 0.8us.
- The transmission time in the last mile (256 kb/s) for the large packet is ~150ms while the transmission time for the small packet on the same link is ~3ms.
- Last mile transport is ATM.

To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

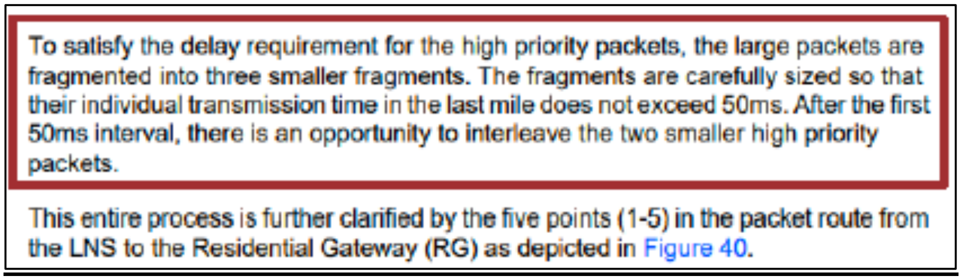
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 184-186 of PDF**)

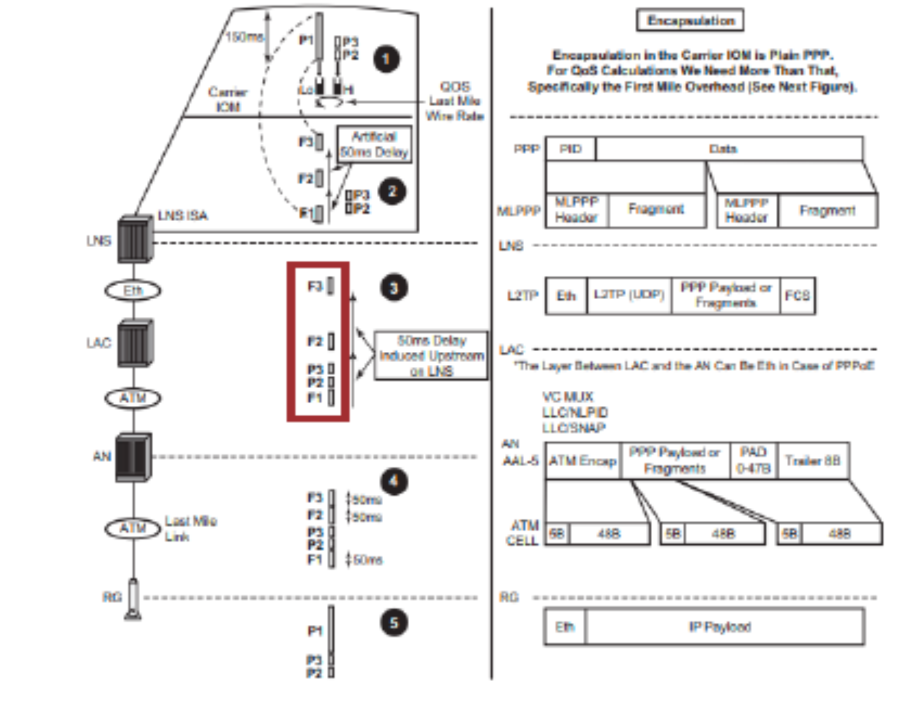
35. The 7750 Service Router transmits the fragments of the first datagram over the channel, beginning with the first fragment.



To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

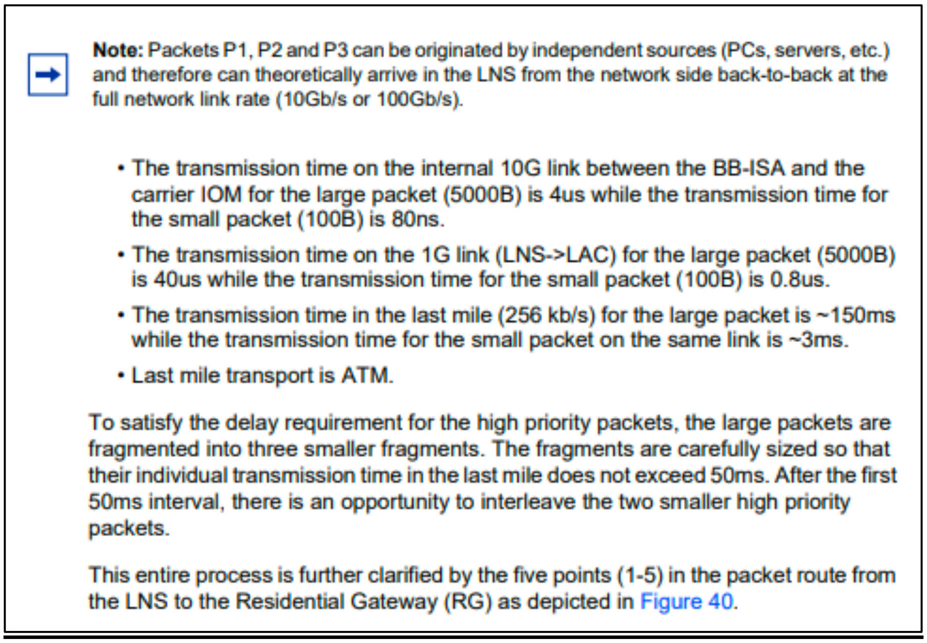
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 185 and 186 of PDF**)

36. The 7750 Service Router transmits at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram**.**



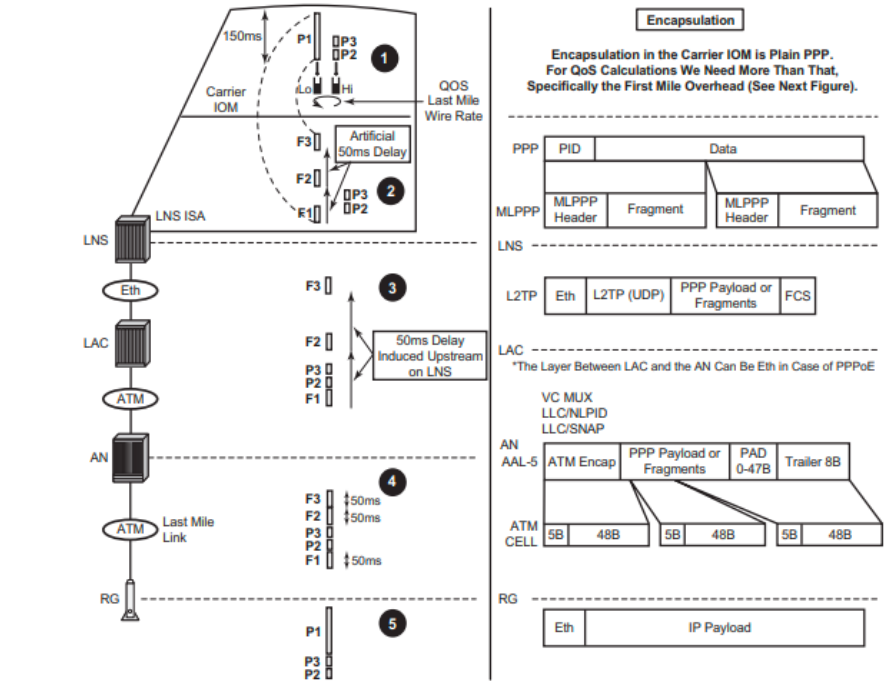
Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

- The transmission time on the internal 10G link between the BB-ISA and the carrier IOM for the large packet (5000B) is 4us while the transmission time for the small packet (100B) is 80ns.
- The transmission time on the 1G link (LNS->LAC) for the large packet (5000B) is 40us while the transmission time for the small packet (100B) is 0.8us.
- The transmission time in the last mile (256 kb/s) for the large packet is ~150ms while the transmission time for the small packet on the same link is ~3ms.
- Last mile transport is ATM.

To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

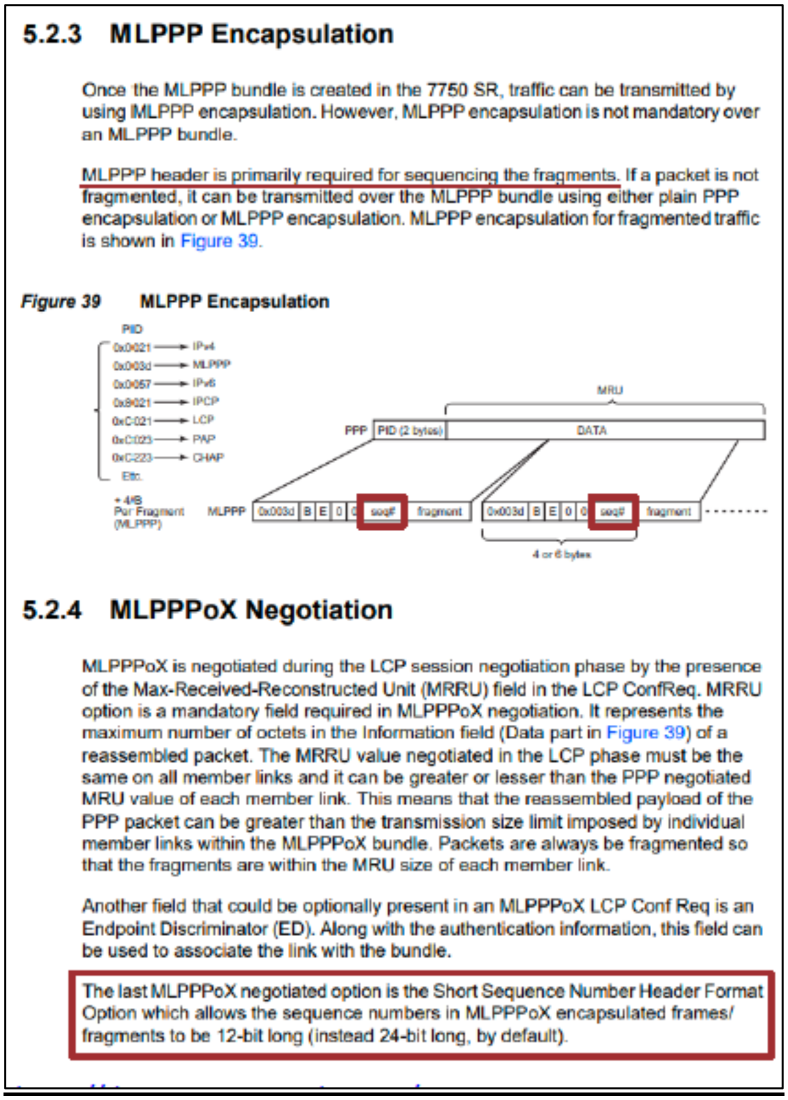
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf **(Pages 184-186 of PDF)**

37. The 7750 Service Router wherein transmitting at least the fragment of the second datagram comprises interrupting transmission of a number of datagrams, including at least the first datagram, in order to transmit at least the fragment of the second datagram, and adding a field to the fragment indicating the number of datagrams whose transmission has been interrupted.



5.2.3 MLPPP Encapsulation

Once the MLPPP bundle is created in the 7750 SR, traffic can be transmitted by using MLPPP encapsulation. However, MLPPP encapsulation is not mandatory over an MLPPP bundle.

MLPPP header is primarily required for sequencing the fragments. If a packet is not fragmented, it can be transmitted over the MLPPP bundle using either plain PPP encapsulation or MLPPP encapsulation. MLPPP encapsulation for fragmented traffic is shown in Figure 39.

Figure 39 **MLPPP Encapsulation**

5.2.4 MLPPPoX Negotiation

MLPPPoX is negotiated during the LCP session negotiation phase by the presence of the Max-Received-Reconstructed Unit (MRRU) field in the LCP ConfReq. MRRU option is a mandatory field required in MLPPPoX negotiation. It represents the maximum number of octets in the Information field (Data part in Figure 39) of a reassembled packet. The MRRU value negotiated in the LCP phase must be the same on all member links and it can be greater or lesser than the PPP negotiated MRU value of each member link. This means that the reassembled payload of the PPP packet can be greater than the transmission size limit imposed by individual member links within the MLPPPoX bundle. Packets are always be fragmented so that the fragments are within the MRU size of each member link.

Another field that could be optionally present in an MLPPPoX LCP Conf Req is an Endpoint Discriminator (ED). Along with the authentication information, this field can be used to associate the link with the bundle.

The last MLPPPoX negotiated option is the Short Sequence Number Header Format Option which allows the sequence numbers in MLPPPoX encapsulated frames/ fragments to be 12-bit long (instead 24-bit long, by default).

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 179 and 180 of PDF**)

Willful Infringement

38. Defendants have had actual knowledge of the ’669 Patent and its infringement thereof at least as of service of Plaintiff’s Complaint.

39. Defendants’ risk of infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendants.

40. Notwithstanding this knowledge, Defendants have knowingly or with reckless disregard willfully infringed the ’669 Patent. Defendants have thus had actual notice of the infringement of the ’669 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

41. This objective risk was either known or so obvious that it should have been known to Defendants. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

42. Defendants have induced and is knowingly inducing its customers and/or end users to directly infringe the ’669 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

43. Defendants have knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the ’669 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

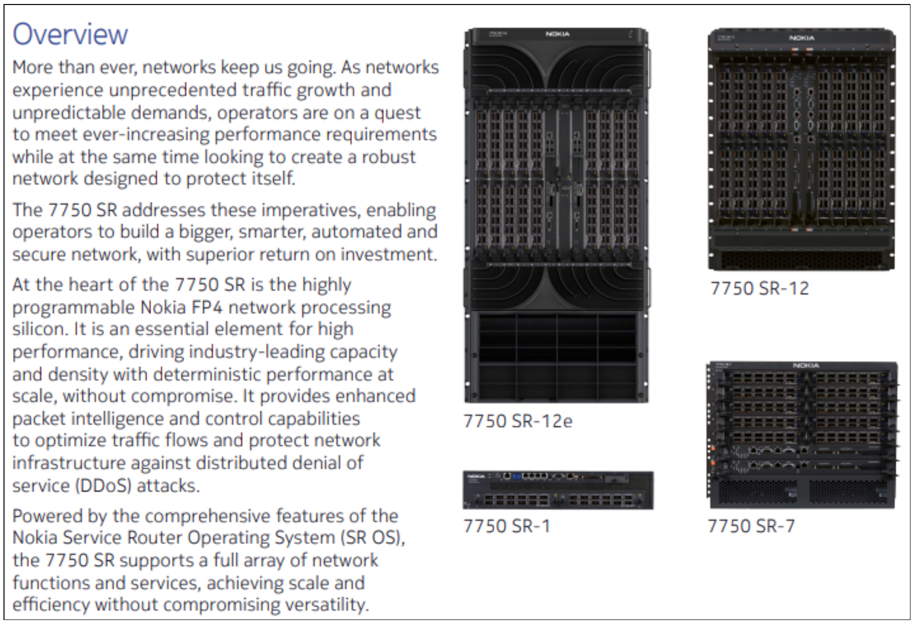
44. Defendants' indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '669 Patent.

45. Defendants' indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendants' indirect infringement further includes providing application notes instructing its customers on infringing uses of the accused products. The '669 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '669 Patent, either literally or equivalently. Defendants know and intend that customers who purchase the '669 Accused Products will use those products for their intended purpose. For example, Defendants' United States website: https://www.nokia.com, instructs customers to use the '669 Accused Products in numerous infringing applications. Furthermore, Defendants provide instructions and other resources via its "Doc Center" (https://documentation.nokia.com), "Nokia Service Routing Certification" and training courses from its "NokiaEDU Training Centers" (https://www.nokia.com/networks/training/src/courses/#open-enrollment), and elsewhere on using the '669 Accused Products. Defendants' customers directly infringe the '669 patent when they follow Defendants' provided instructions on website, videos, and elsewhere. Defendants' customers who follow Defendants' provided instructions directly infringe claims of the '669 Patent.

46. In addition, Defendants specifically intend that its customers, such as United States distributors, retailers and customers, will import, use, configure and sell infringing products in the United States to serve and develop the United States market for Defendants' infringing products. Defendants know following its instructions directly infringes claims of the '669 Patent, including for example Claim 1.

47. Defendants' customers who follow Defendants' provided instructions directly infringe the method of Claim 1 of the '669 Patent.

48. Defendants instruct its customers to use the 7750 Service Router in a method for transmitting data over a channel:



Overview

More than ever, networks keep us going. As networks experience unprecedented traffic growth and unpredictable demands, operators are on a quest to meet ever-increasing performance requirements while at the same time looking to create a robust network designed to protect itself.

The 7750 SR addresses these imperatives, enabling operators to build a bigger, smarter, automated and secure network, with superior return on investment.

At the heart of the 7750 SR is the highly programmable Nokia FP4 network processing silicon. It is an essential element for high performance, driving industry-leading capacity and density with deterministic performance at scale, without compromise. It provides enhanced packet intelligence and control capabilities to optimize traffic flows and protect network infrastructure against distributed denial of service (DDoS) attacks.

Powered by the comprehensive features of the Nokia Service Router Operating System (SR OS), the 7750 SR supports a full array of network functions and services, achieving scale and efficiency without compromising versatility.

7750 SR-12e

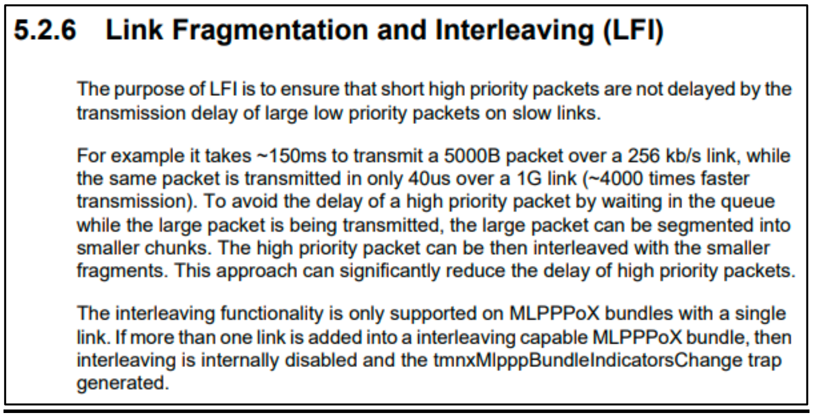
7750 SR-12

7750 SR-1

7750 SR-7

https://resources.nokia.com/asset/164728?_ga=2.188290280.1557979830.1638603790-478191956.1631863234 **(Page 1 of PDF)**

49. Defendants instruct its customers to use the 7750 Service Router to receive a first datagram for transmission at a first priority.



5.2.6 Link Fragmentation and Interleaving (LFI)

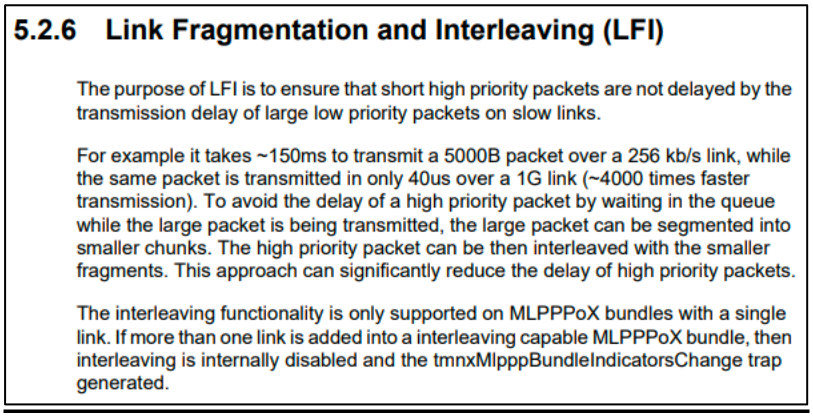
The purpose of LFI is to ensure that short high priority packets are not delayed by the transmission delay of large low priority packets on slow links.

For example it takes ~150ms to transmit a 5000B packet over a 256 kb/s link, while the same packet is transmitted in only 40us over a 1G link (~4000 times faster transmission). To avoid the delay of a high priority packet by waiting in the queue while the large packet is being transmitted, the large packet can be segmented into smaller chunks. The high priority packet can be then interleaved with the smaller fragments. This approach can significantly reduce the delay of high priority packets.

The interleaving functionality is only supported on MLPPPoX bundles with a single link. If more than one link is added into a interleaving capable MLPPPoX bundle, then interleaving is internally disabled and the tmnxMlpppBundleIndicatorsChange trap generated.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Page 182 of PDF**)

50. Defendants instruct its customers to use the 7750 Service Router to receive a second datagram for transmission at a second priority, higher than the first priority, before the transmission of the first datagram is completed.



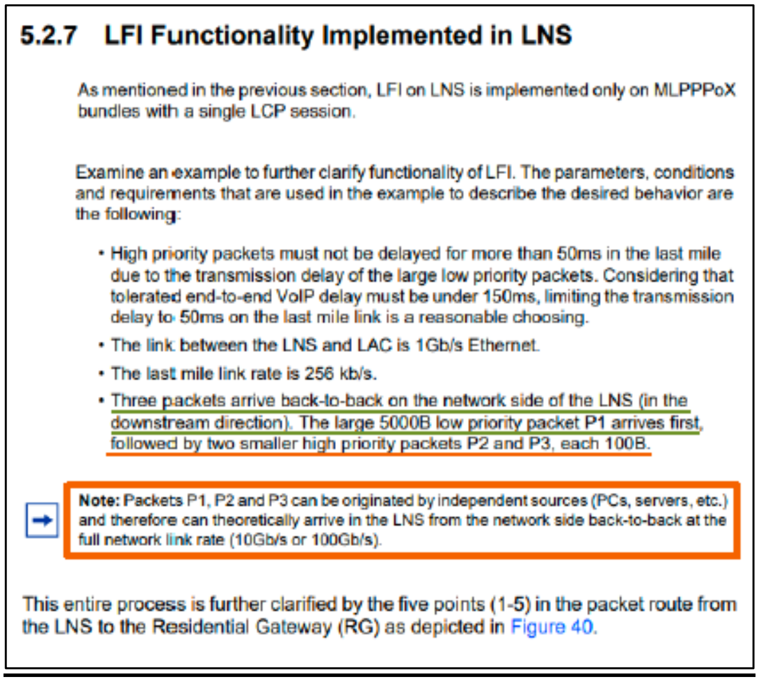
5.2.6 Link Fragmentation and Interleaving (LFI)

The purpose of LFI is to ensure that short high priority packets are not delayed by the transmission delay of large low priority packets on slow links.

For example it takes ~150ms to transmit a 5000B packet over a 256 kb/s link, while the same packet is transmitted in only 40us over a 1G link (~4000 times faster transmission). To avoid the delay of a high priority packet by waiting in the queue while the large packet is being transmitted, the large packet can be segmented into smaller chunks. The high priority packet can be then interleaved with the smaller fragments. This approach can significantly reduce the delay of high priority packets.

The interleaving functionality is only supported on MLPPPoX bundles with a single link. If more than one link is added into a interleaving capable MLPPPoX bundle, then interleaving is internally disabled and the tmnxMlpppBundleIndicatorsChange trap generated.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Page 182 of PDF**)



5.2.7 LFI Functionality Implemented in LNS

As mentioned in the previous section, LFI on LNS is implemented only on MLPPPoX bundles with a single LCP session.

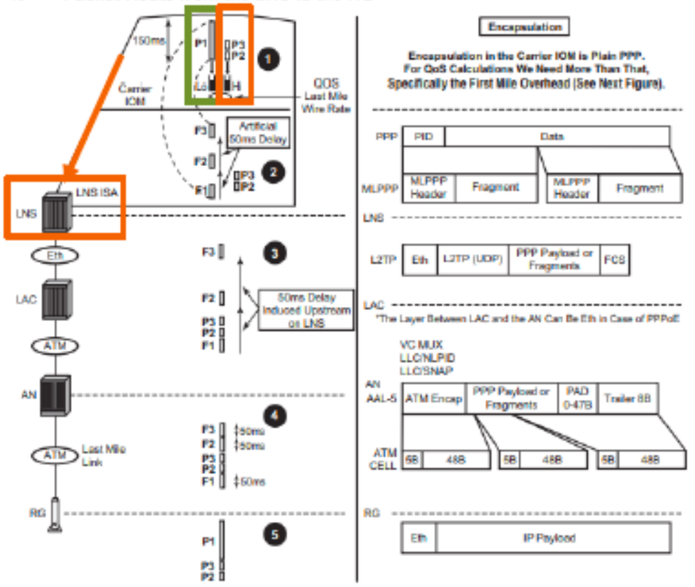
Examine an example to further clarify functionality of LFI. The parameters, conditions and requirements that are used in the example to describe the desired behavior are the following:

- High priority packets must not be delayed for more than 50ms in the last mile due to the transmission delay of the large low priority packets. Considering that tolerated end-to-end VoIP delay must be under 150ms, limiting the transmission delay to 50ms on the last mile link is a reasonable choosing.
- The link between the LNS and LAC is 1Gb/s Ethernet.
- The last mile link rate is 256 kb/s.
- Three packets arrive back-to-back on the network side of the LNS (in the downstream direction). The large 5000B low priority packet P1 arrives first, followed by two smaller high priority packets P2 and P3, each 100B.

Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

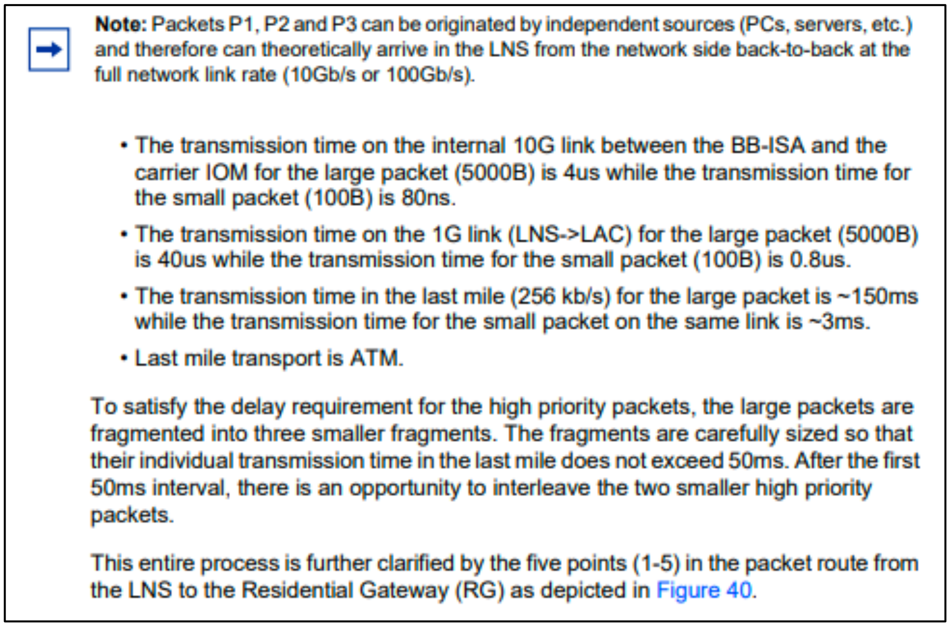
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf **(Pages 184-186 of PDF)**

51. Defendants instruct its customers to use the 7750 Service Router which responsive to receiving the second datagram, deciding to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.



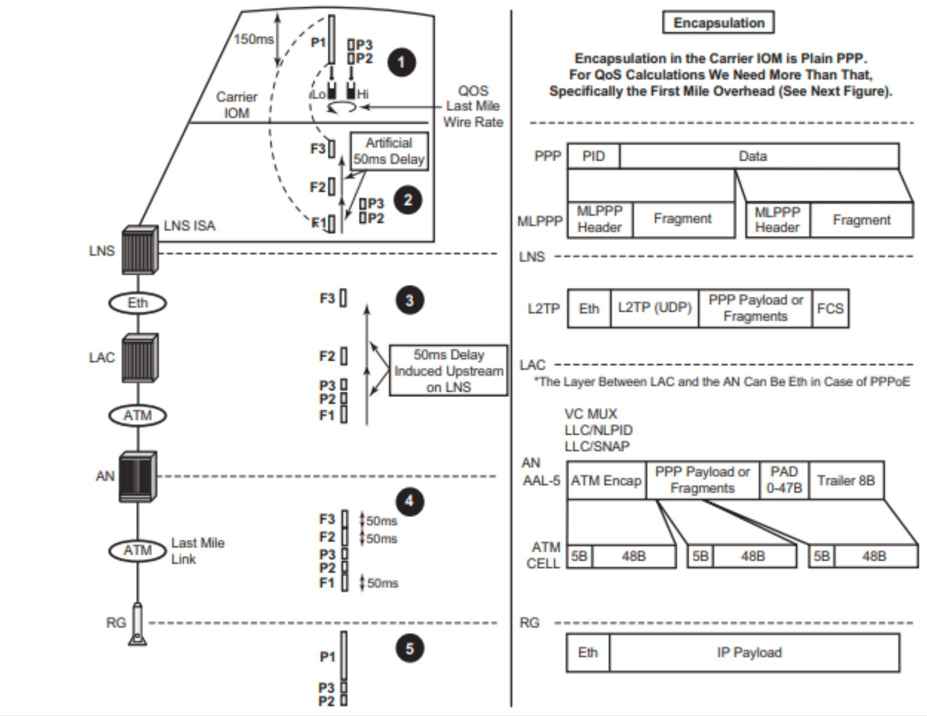
Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

- The transmission time on the internal 10G link between the BB-ISA and the carrier IOM for the large packet (5000B) is 4us while the transmission time for the small packet (100B) is 80ns.
- The transmission time on the 1G link (LNS->LAC) for the large packet (5000B) is 40us while the transmission time for the small packet (100B) is 0.8us.
- The transmission time in the last mile (256 kb/s) for the large packet is ~150ms while the transmission time for the small packet on the same link is ~3ms.
- Last mile transport is ATM.

To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

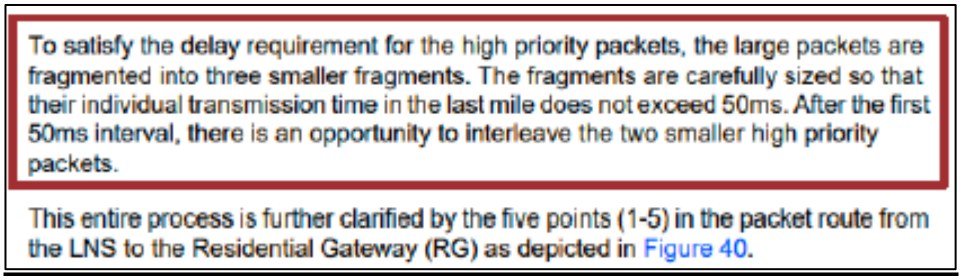
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 184-186 of PDF**)

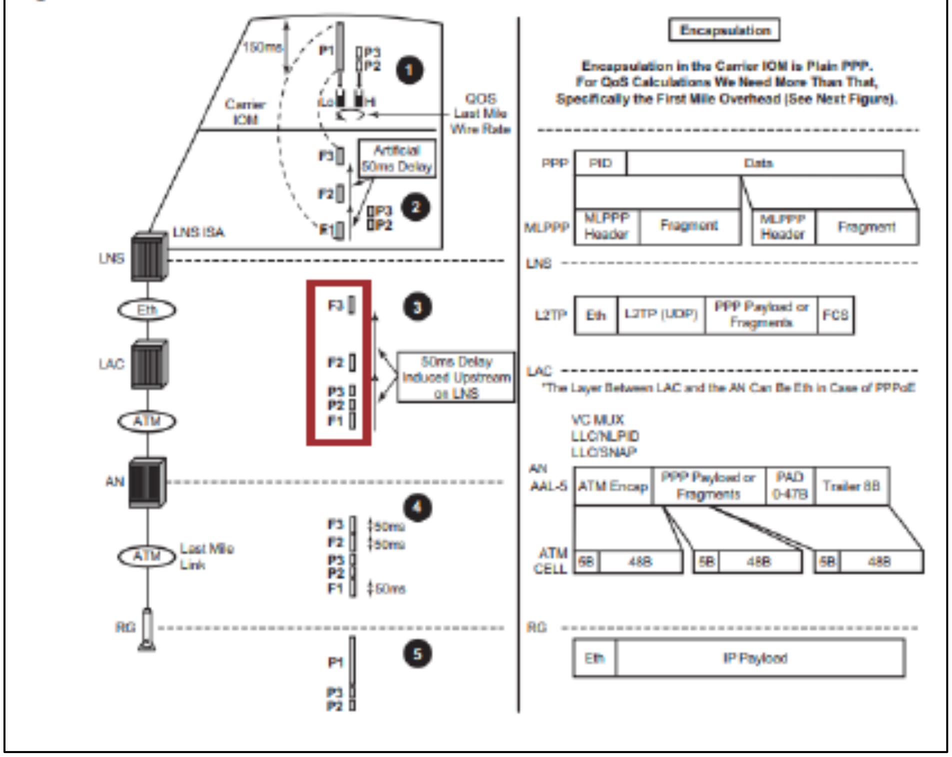
52. Defendants instruct its customers to use the 7750 Service Router to transmit the fragments of the first datagram over the channel, beginning with the first fragment.



To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

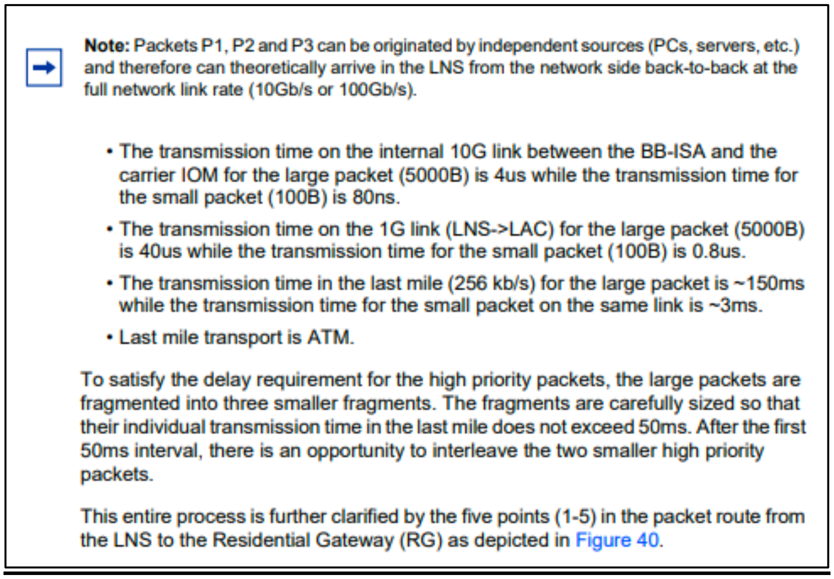
This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20SR%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 185 and 186 of PDF**)

53. Defendants instruct its customers to use the 7750 Service Router to transmit at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram.



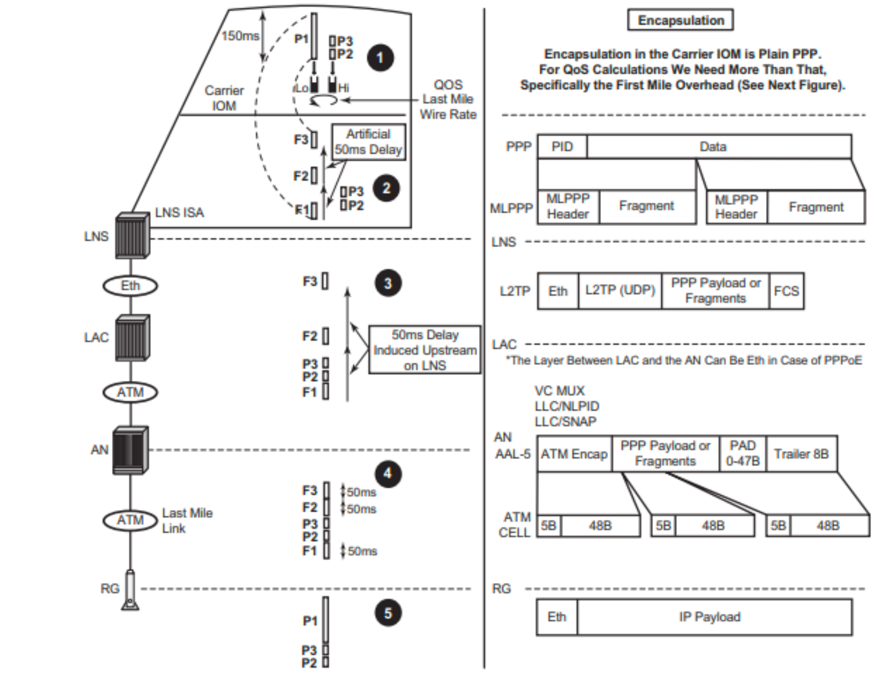
Note: Packets P1, P2 and P3 can be originated by independent sources (PCs, servers, etc.) and therefore can theoretically arrive in the LNS from the network side back-to-back at the full network link rate (10Gb/s or 100Gb/s).

- The transmission time on the internal 10G link between the BB-ISA and the carrier IOM for the large packet (5000B) is 4us while the transmission time for the small packet (100B) is 80ns.
- The transmission time on the 1G link (LNS->LAC) for the large packet (5000B) is 40us while the transmission time for the small packet (100B) is 0.8us.
- The transmission time in the last mile (256 kb/s) for the large packet is ~150ms while the transmission time for the small packet on the same link is ~3ms.
- Last mile transport is ATM.

To satisfy the delay requirement for the high priority packets, the large packets are fragmented into three smaller fragments. The fragments are carefully sized so that their individual transmission time in the last mile does not exceed 50ms. After the first 50ms interval, there is an opportunity to interleave the two smaller high priority packets.

This entire process is further clarified by the five points (1-5) in the packet route from the LNS to the Residential Gateway (RG) as depicted in Figure 40.

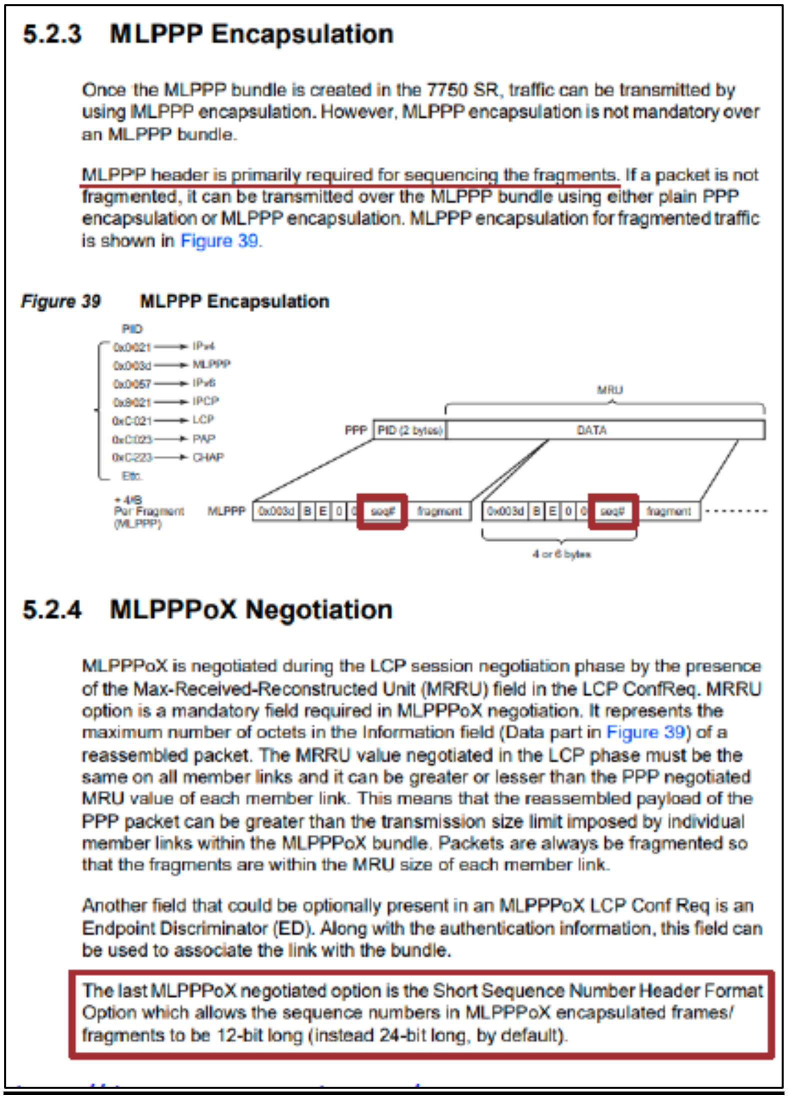
Figure 40 **Packet Route from the LNS to the RG**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20S

R%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 184-186 of PDF**)

54. Defendants instruct its customers to use the 7750 Service Router wherein transmitting at least the fragment of the second datagram comprises interrupting transmission of a number of datagrams, including at least the first datagram, in order to transmit at least the fragment of the second datagram, and adding a field to the fragment indicating the number of datagrams whose transmission has been interrupted.



5.2.3 MLPPP Encapsulation

Once the MLPPP bundle is created in the 7750 SR, traffic can be transmitted by using MLPPP encapsulation. However, MLPPP encapsulation is not mandatory over an MLPPP bundle.

MLPPP header is primarily required for sequencing the fragments. If a packet is not fragmented, it can be transmitted over the MLPPP bundle using either plain PPP encapsulation or MLPPP encapsulation. MLPPP encapsulation for fragmented traffic is shown in Figure 39.

Figure 39 **MLPPP Encapsulation**

5.2.4 MLPPPoX Negotiation

MLPPPoX is negotiated during the LCP session negotiation phase by the presence of the Max-Received-Reconstructed Unit (MRRU) field in the LCP ConfReq. MRRU option is a mandatory field required in MLPPPoX negotiation. It represents the maximum number of octets in the Information field (Data part in Figure 39) of a reassembled packet. The MRRU value negotiated in the LCP phase must be the same on all member links and it can be greater or lesser than the PPP negotiated MRU value of each member link. This means that the reassembled payload of the PPP packet can be greater than the transmission size limit imposed by individual member links within the MLPPPoX bundle. Packets are always be fragmented so that the fragments are within the MRU size of each member link.

Another field that could be optionally present in an MLPPPoX LCP Conf Req is an Endpoint Discriminator (ED). Along with the authentication information, this field can be used to associate the link with the bundle.

The last MLPPPoX negotiated option is the Short Sequence Number Header Format Option which allows the sequence numbers in MLPPPoX encapsulated frames/fragments to be 12-bit long (instead 24-bit long, by default).

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17164AAADTQZZA01_V1_7450%20ESS%207750%20S

R%20and%20VSR%20Triple%20Play%20Service%20Delivery%20Architecture%20Guide%2021.10.R1.pdf (**Pages 179 and 180 of PDF**)

55. As a result of Defendants' infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT TWO
INFRINGEMENT OF U.S. PATENT 7,127,523

56. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-20 as if fully set forth herein.

57. The '523 Patent, entitled "SPANNING TREE PROTOCOL TRAFFIC IN A TRANSPARENT LAN" was filed on January 25, 2002 and issued on October 24, 2006.

58. Plaintiff is the assignee and owner of all rights, title and interest to the '523 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

59. On February 22, 2021, IPR2021-00571 was filed on the '523 Patent challenging claims 1-6 and 10-15. On August 30, 2021, the Patent Trial and Appeal Board ("PTAB") denied institution of IPR2021-00571.

60. On March 17, 2022, a Request for Ex Parte Reexamination was filed on the '523 Paten requesting reexamination of claims 1-6, 10-15, and 19. On August 3, 2022, the USPTO confirmed claims 1-6, 10-15, and 19 and terminated the Reexam.

Technical Description

61. The '523 Patent addresses problems in the prior art of local-area-network (LAN) technology, including prior-art attempts to prevent problematic data-packet-communication loops

in transparent LAN services (TLS). Prior attempts were "costly and difficult to maintain," had "security and reliability drawbacks," were "excessively complex to configure," and/or were largely theoretical, failing to account for issues stemming from the "separation of provider and user domains." (col. 4, l. 61 – col. 5, l. 15)

62. The '523 Patent provides a solution to the prior art problems by disclosing improved equipment and an improved method "for preventing loops in a TLS network." (col. 5, ll. 63-64) In preferred embodiments, "STP [spanning tree protocol] frames are sent through the same tunnels as the user traffic, but are distinguished from the user data frames by a special STP label. Loop removal is carried out in this way for each one of the TLSs, so that each TLS has its own loop-free topology. Using this method, the TLS network operator is able to ensure that there are no loops in the core network, irrespective of loops that users b add when they connect their own equipment to the network." (col. 6, ll. 2-9).

Direct Infringement

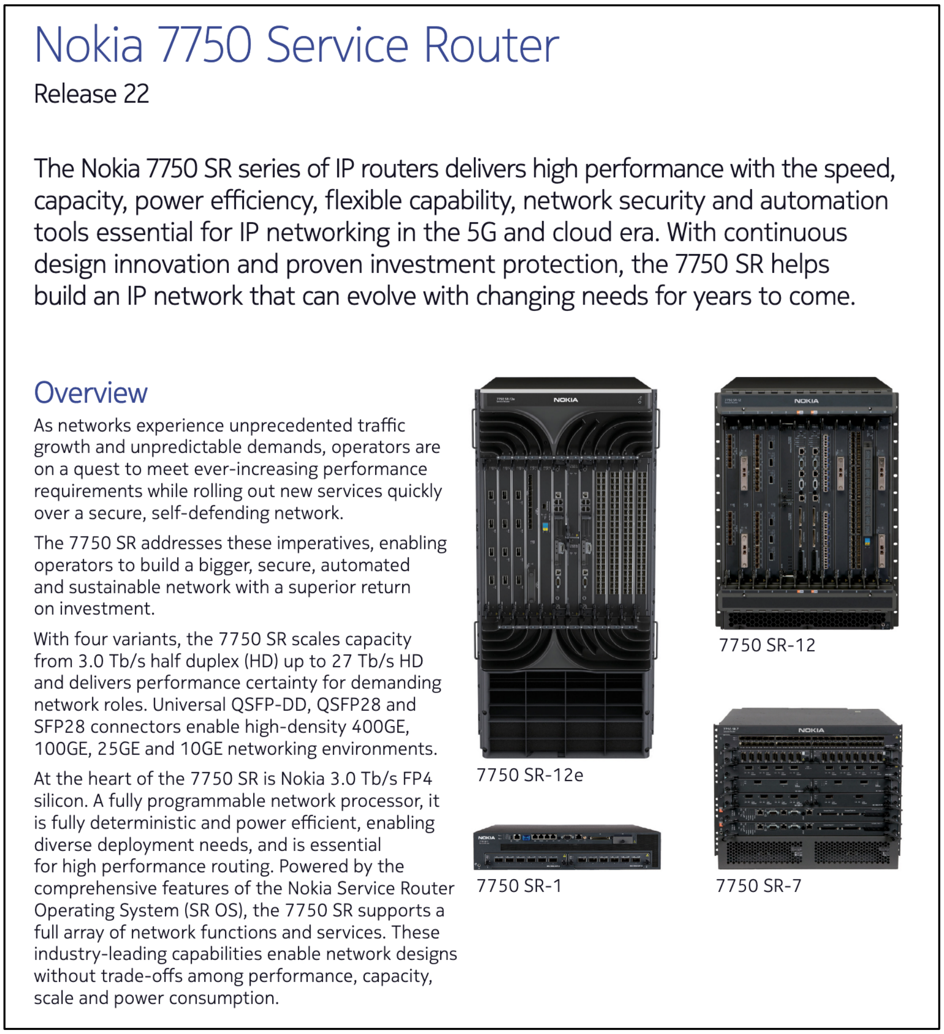
63. Defendants, without authorization or license from Plaintiff, have been and is directly infringing the '523 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '523 Patent. Defendants develop, design, manufacture, and distribute telecommunications equipment that infringes one or more claims of the '523 Patent. Defendants further provides services that practice methods that infringe one or more claims of the '523 Patent. Defendants are thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Nokia 7750 Service Router, and all other substantially similar products (collectively the "'523 Accused Products").

64. Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendants' infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '523 Accused Products.

65. Defendants are liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendants' 7750 Service Router.

66. Defendants' 7750 Service Router is a non-limiting example of a router that meets all limitations of claim 10 of the '523 Patent, either literally or equivalently.

67. Defendants' 7750 Service Router is a communication device for operation as one of a plurality of label-switched routers (LSRs) in a transparent local area network service (TLS), which includes a system of label-switched tunnels between the label-switched routers (LSRs) through a communication network, the TLS having at least first and second endpoints to which first and second user equipment is connected so that the TLS acts as a virtual bridge between the first and second user equipment:



Nokia 7750 Service Router

Release 22

The Nokia 7750 SR series of IP routers delivers high performance with the speed, capacity, power efficiency, flexible capability, network security and automation tools essential for IP networking in the 5G and cloud era. With continuous design innovation and proven investment protection, the 7750 SR helps build an IP network that can evolve with changing needs for years to come.

Overview

As networks experience unprecedented traffic growth and unpredictable demands, operators are on a quest to meet ever-increasing performance requirements while rolling out new services quickly over a secure, self-defending network.

The 7750 SR addresses these imperatives, enabling operators to build a bigger, secure, automated and sustainable network with a superior return on investment.

With four variants, the 7750 SR scales capacity from 3.0 Tb/s half duplex (HD) up to 27 Tb/s HD and delivers performance certainty for demanding network roles. Universal QSFP-DD, QSFP28 and SFP28 connectors enable high-density 400GE, 100GE, 25GE and 10GE networking environments.

At the heart of the 7750 SR is Nokia 3.0 Tb/s FP4 silicon. A fully programmable network processor, it is fully deterministic and power efficient, enabling diverse deployment needs, and is essential for high performance routing. Powered by the comprehensive features of the Nokia Service Router Operating System (SR OS), the 7750 SR supports a full array of network functions and services. These industry-leading capabilities enable network designs without trade-offs among performance, capacity, scale and power consumption.

7750 SR-12e

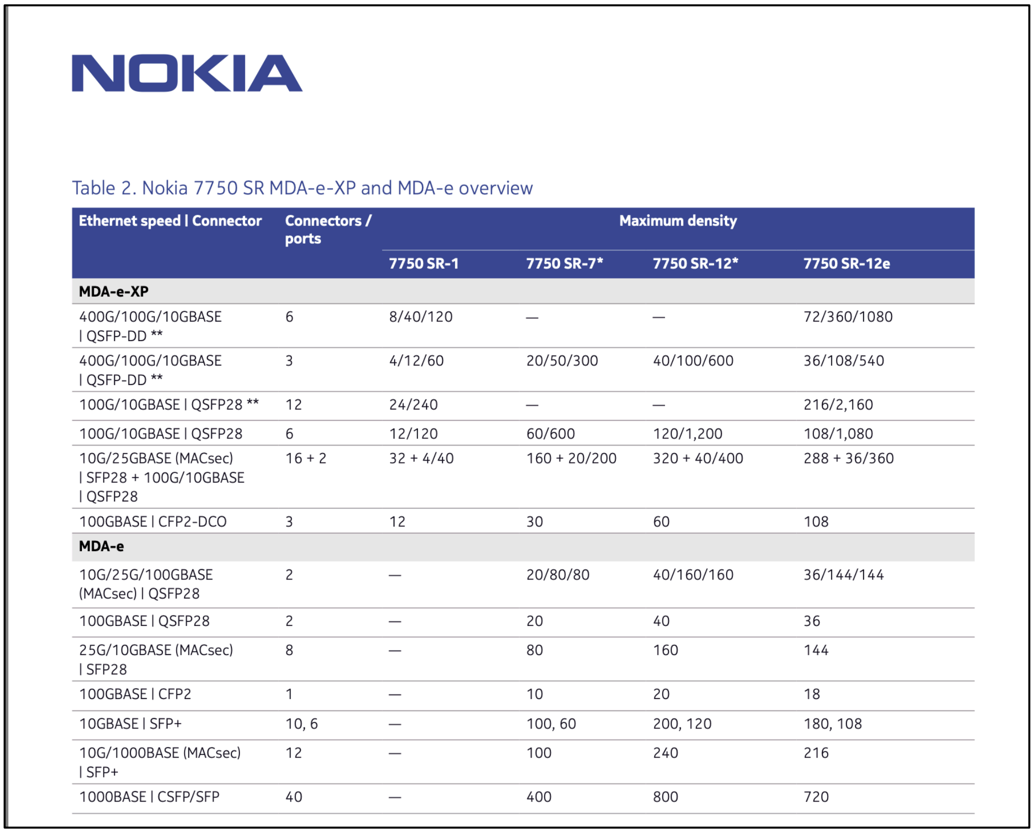
7750 SR-12

7750 SR-1

7750 SR-7

https://onestore.nokia.com/asset/164728?_ga=2.188290280.1557979830.1638603790-478191956.1631863234

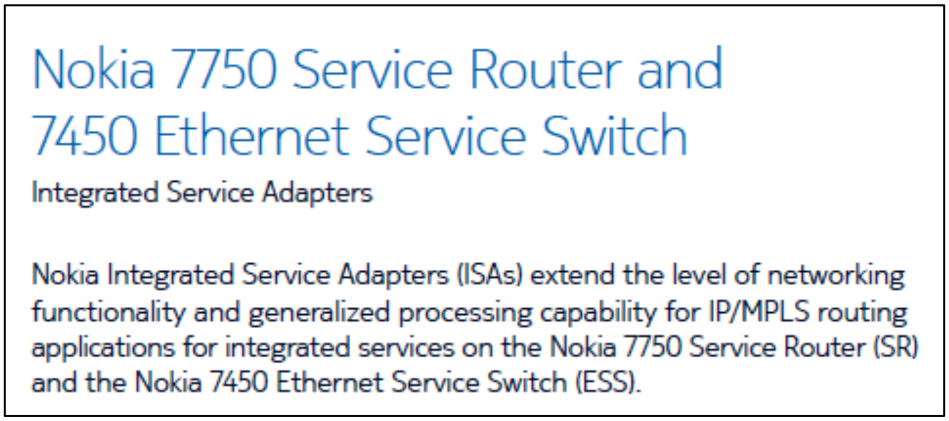
68. Defendants' 7750 Service Router is a communication device comprising one or more ports, adapted to send and receive traffic via the label-switched tunnels:



NOKIA

Table 2. Nokia 7750 SR MDA-e-XP and MDA-e overview

Ethernet speed | Connector	Connectors / ports	Maximum density			
		7750 SR-1	7750 SR-7*	7750 SR-12*	7750 SR-12e
MDA-e-XP					
400G/100G/10GBASE | QSFP-DD **	6	8/40/120	—	—	72/360/1080
400G/100G/10GBASE | QSFP-DD **	3	4/12/60	20/50/300	40/100/600	36/108/540
100G/10GBASE | QSFP28 **	12	24/240	—	—	216/2,160
100G/10GBASE | QSFP28	6	12/120	60/600	120/1,200	108/1,080
10G/25GBASE (MACsec) | SFP28 + 100G/10GBASE | QSFP28	16 + 2	32 + 4/40	160 + 20/200	320 + 40/400	288 + 36/360
100GBASE | CFP2-DCO	3	12	30	60	108
MDA-e					
10G/25G/100GBASE (MACsec) | QSFP28	2	—	20/80/80	40/160/160	36/144/144
100GBASE | QSFP28	2	—	20	40	36
25G/10GBASE (MACsec) | SFP28	8	—	80	160	144
100GBASE | CFP2	1	—	10	20	18
10GBASE | SFP+	10, 6	—	100, 60	200, 120	180, 108
10G/1000BASE (MACsec) | SFP+	12	—	100	240	216
1000BASE | CSFP/SFP	40	—	400	800	720



Nokia 7750 Service Router and 7450 Ethernet Service Switch

Integrated Service Adapters

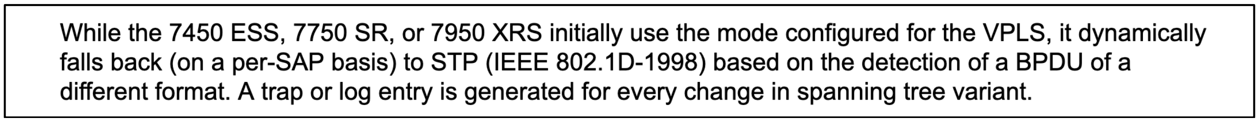
Nokia Integrated Service Adapters (ISAs) extend the level of networking functionality and generalized processing capability for IP/MPLS routing applications for integrated services on the Nokia 7750 Service Router (SR) and the Nokia 7450 Ethernet Service Switch (ESS).

https://onestore.nokia.com/asset/157673?_ga=2.111614212.1016918459.1649964251-16661628.1649964251

69. Defendants' 7750 Service Router is a communication device comprising a traffic processor which is coupled to the one or more ports, and is adapted to transmit control frames to the LSRs in the TLS via the label-switched tunnels, each control frame comprising a control traffic label and a bridge protocol data unit (BPDU) in accordance with a spanning tree protocol (STP),

the control traffic label indicating to the LSRs that the STP is to be executed by the LSRs without transmission of the BPDU to the user equipment, wherein the traffic processor is further adapted, upon receiving the control frames, to process the BPDU, responsively to the control traffic label, so as to remove loops in a topology of the TLS irrespective of the user equipment:

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17148AAADTQZZA01_V1_7450%20ESS%207750%20SR%207950%20XRS%20and%20VSR%20Layer%202%20Services%20and%20EVPN%20Guide:%20VLL%20VPLS%20PBB%20and%20EVPN%2021.10.R1.pdf **(page 197)**



While the 7450 ESS, 7750 SR, or 7950 XRS initially use the mode configured for the VPLS, it dynamically falls back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

***Id.* at 198.**

Id. at 201-202.

https://documentation.nokia.com/html/0_add-h-f/93-0076-10-01/7750_SR_OS_Services_Guide/Service-VPLS-CLI.pdf **(page 5).**

Willful Infringement

70. Defendants have had actual knowledge of the '523 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated February 27, 2017.

71. Defendants have had actual knowledge of the '523 Patent and its infringement thereof at least as of service of Plaintiff's Complaint.

72. Defendants' risk of infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendants.

73. Notwithstanding this knowledge, Defendants have knowingly or with reckless disregard willfully infringed the '523 Patent. Defendants have thus had actual notice of the infringement of the '523 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff's valid patent rights, either literally or equivalently.

74. This objective risk was either known or so obvious that it should have been known to Defendants. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

75. Defendants have induced and is knowingly inducing its customers and/or end users to directly infringe the '523 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

76. Defendants have knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the '523 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

77. Defendants' indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '523 Patent.

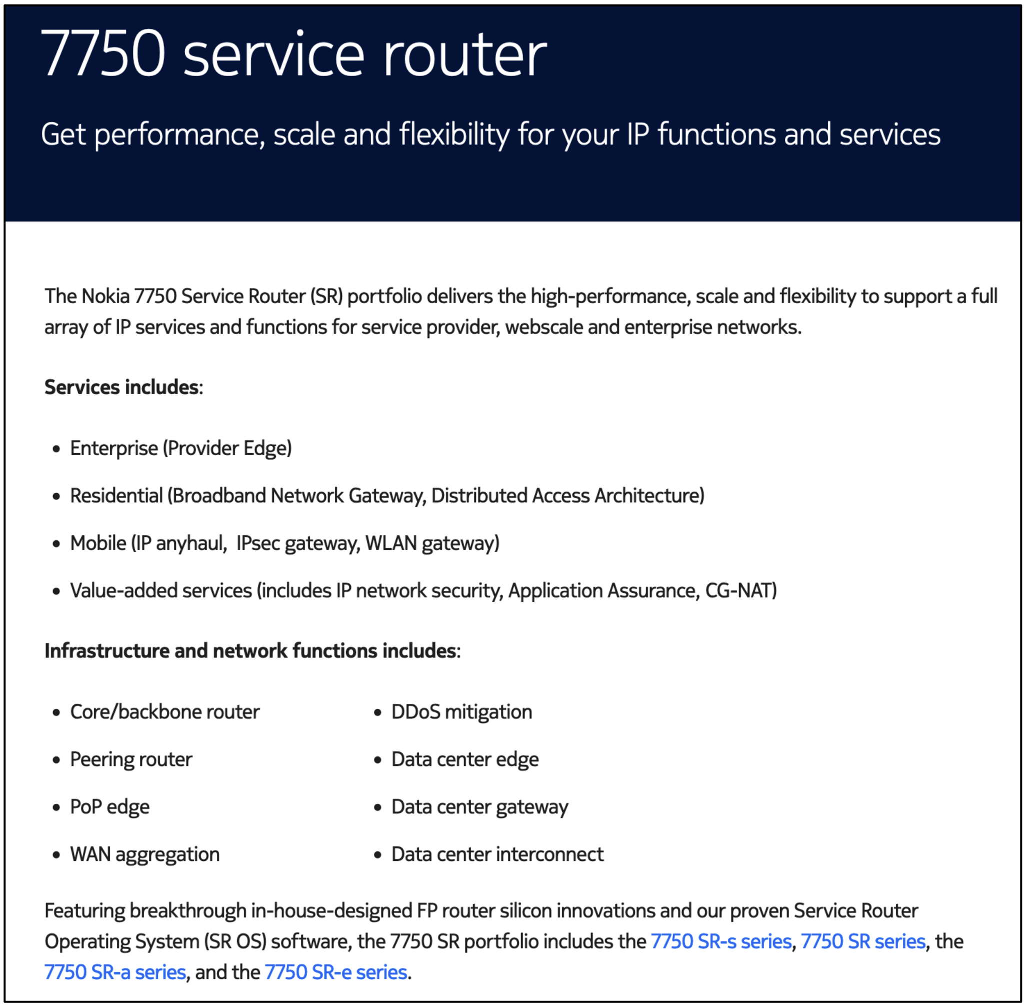
78. Defendants' indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendants' indirect infringement further includes

providing application notes instructing its customers on infringing uses of the accused products. The ’523 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the ’523 Patent, either literally or equivalently. Defendants know and intend that customers who purchase the ’523 Accused Products will use those products for their intended purpose. For example, Defendants’ United States website: https://www.nokia.com, instructs customers to use the ’523 Accused Products in numerous infringing applications. Furthermore, Defendants provide instructions and other resources via its “Doc Center” (https://documentation.nokia.com), “Nokia Service Routing Certification” and training courses from its “NokiaEDU Training Centers” (https://www.nokia.com/networks/training/src/courses/#open-enrollment), and elsewhere on using the ’523 Accused Products. Defendants’ customers directly infringe the ’523 patent when they follow Defendants’ provided instructions on website, videos, and elsewhere. Defendants’ customers who follow Defendants’ provided instructions directly infringe claims of the ’523 Patent.

79. In addition, Defendants specifically intend that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendants’ infringing products. Defendants know following its instructions directly infringes claims of the ’523 Patent, including for example Claim 1.

80. Defendants’ customers who follow Defendants’ provided instructions directly infringe the method of Claim 1 of the ’523 Patent.

81. Defendants instruct its customers use the 7750 Service Router in a method for communication:



7750 service router

Get performance, scale and flexibility for your IP functions and services

The Nokia 7750 Service Router (SR) portfolio delivers the high-performance, scale and flexibility to support a full array of IP services and functions for service provider, webscale and enterprise networks.

Services includes:

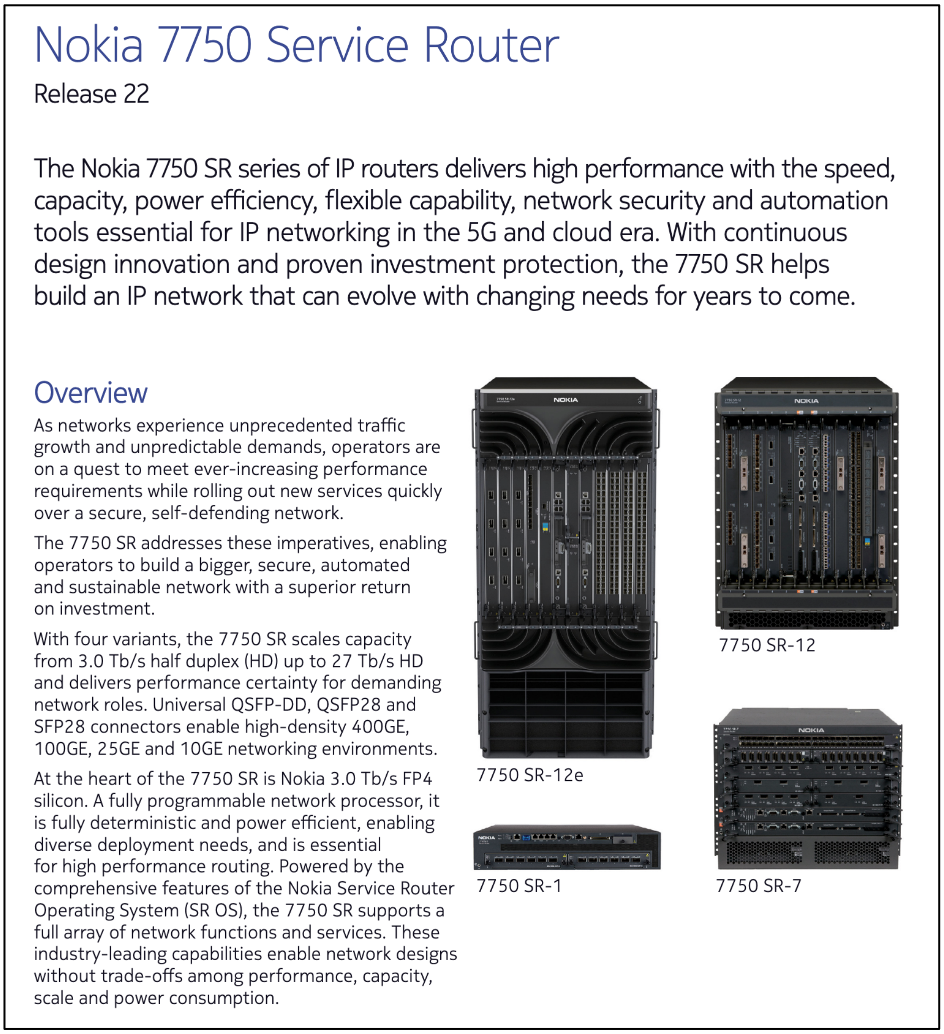
- Enterprise (Provider Edge)
- Residential (Broadband Network Gateway, Distributed Access Architecture)
- Mobile (IP anyhaul, IPsec gateway, WLAN gateway)
- Value-added services (includes IP network security, Application Assurance, CG-NAT)

Infrastructure and network functions includes:

- Core/backbone router
- Peering router
- PoP edge
- WAN aggregation
- DDoS mitigation
- Data center edge
- Data center gateway
- Data center interconnect

Featuring breakthrough in-house-designed FP router silicon innovations and our proven Service Router Operating System (SR OS) software, the 7750 SR portfolio includes the 7750 SR-s series, 7750 SR series, the 7750 SR-a series, and the 7750 SR-e series.

https://www.nokia.com/networks/products/7750-service-router/



Nokia 7750 Service Router

Release 22

The Nokia 7750 SR series of IP routers delivers high performance with the speed, capacity, power efficiency, flexible capability, network security and automation tools essential for IP networking in the 5G and cloud era. With continuous design innovation and proven investment protection, the 7750 SR helps build an IP network that can evolve with changing needs for years to come.

Overview

As networks experience unprecedented traffic growth and unpredictable demands, operators are on a quest to meet ever-increasing performance requirements while rolling out new services quickly over a secure, self-defending network.

The 7750 SR addresses these imperatives, enabling operators to build a bigger, secure, automated and sustainable network with a superior return on investment.

With four variants, the 7750 SR scales capacity from 3.0 Tb/s half duplex (HD) up to 27 Tb/s HD and delivers performance certainty for demanding network roles. Universal QSFP-DD, QSFP28 and SFP28 connectors enable high-density 400GE, 100GE, 25GE and 10GE networking environments.

At the heart of the 7750 SR is Nokia 3.0 Tb/s FP4 silicon. A fully programmable network processor, it is fully deterministic and power efficient, enabling diverse deployment needs, and is essential for high performance routing. Powered by the comprehensive features of the Nokia Service Router Operating System (SR OS), the 7750 SR supports a full array of network functions and services. These industry-leading capabilities enable network designs without trade-offs among performance, capacity, scale and power consumption.

7750 SR-12e

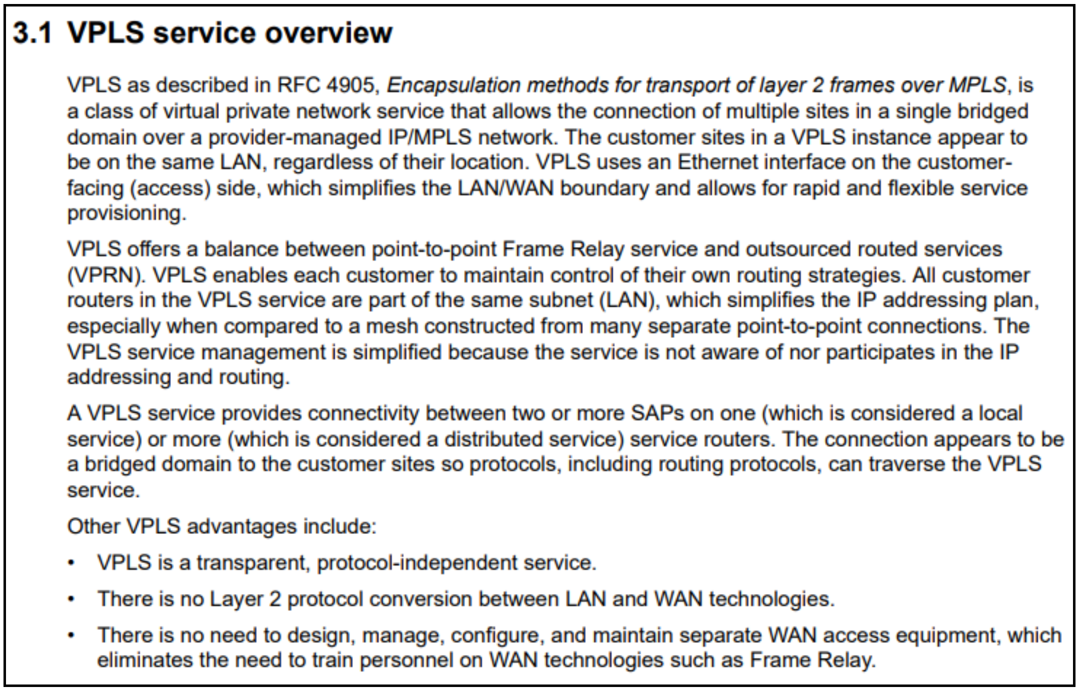
7750 SR-12

7750 SR-1

7750 SR-7

https://onestore.nokia.com/asset/164728?_ga=2.188290280.1557979830.1638603790-478191956.1631863234

82. Defendants instruct its customers use the 7750 Service Router to define a topology of a transparent local area network service (TLS), comprising a system of label-switched tunnels between label-switched routers (LSRs) through a communication network, the TLS having at least first and second endpoints to which first and second user equipment is connected so that the TLS acts as a virtual bridge between the first and second user equipment:



3.1 VPLS service overview

VPLS as described in RFC 4905, *Encapsulation methods for transport of layer 2 frames over MPLS*, is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side, which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning.

VPLS offers a balance between point-to-point Frame Relay service and outsourced routed services (VPRN). VPLS enables each customer to maintain control of their own routing strategies. All customer routers in the VPLS service are part of the same subnet (LAN), which simplifies the IP addressing plan, especially when compared to a mesh constructed from many separate point-to-point connections. The VPLS service management is simplified because the service is not aware of nor participates in the IP addressing and routing.

A VPLS service provides connectivity between two or more SAPs on one (which is considered a local service) or more (which is considered a distributed service) service routers. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the VPLS service.

Other VPLS advantages include:

- VPLS is a transparent, protocol-independent service.
- There is no Layer 2 protocol conversion between LAN and WAN technologies.
- There is no need to design, manage, configure, and maintain separate WAN access equipment, which eliminates the need to train personnel on WAN technologies such as Frame Relay.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17148AAADTQZZA01_V1_7450%20ESS%207750%20SR%207950%20XRS%20and%20VSR%20Layer%202%20Services%20and%20EVPN%20Guide:%20VLL%20VPLS%20PBB%20and%20EVPN%2021.10.R1.pdf **(page 173)**

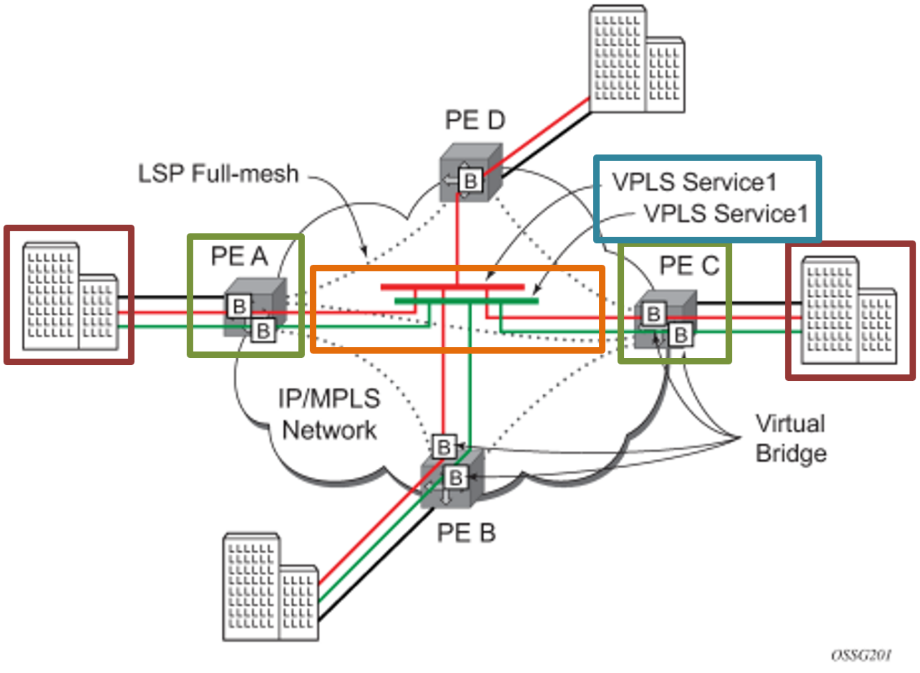
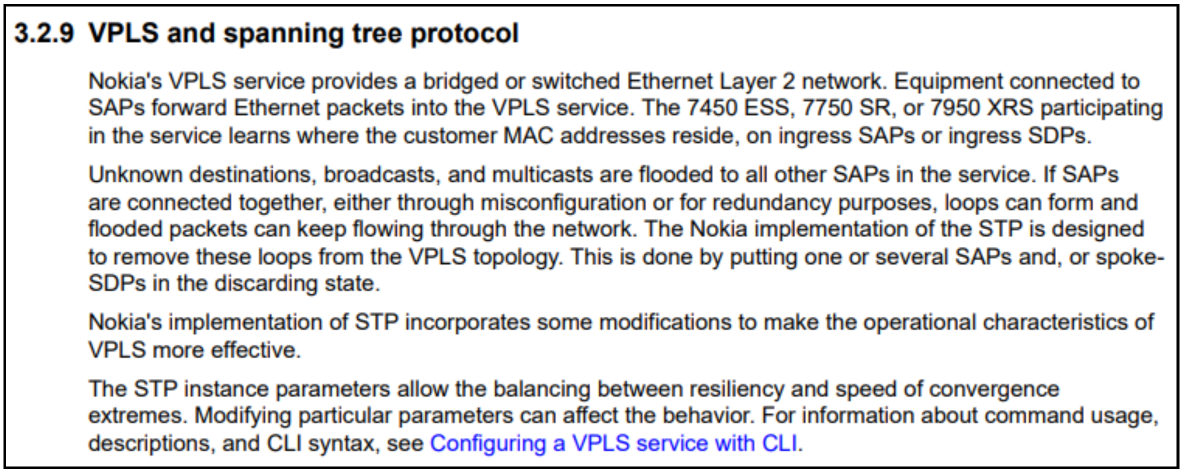


Figure 56: VPLS service architecture

Id. **at 174.**



3.2.9 VPLS and spanning tree protocol

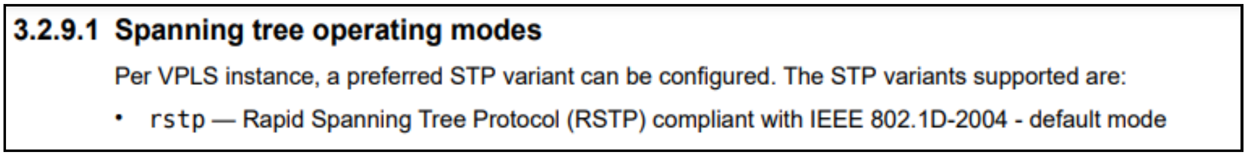
Nokia's VPLS service provides a bridged or switched Ethernet Layer 2 network. Equipment connected to SAPs forward Ethernet packets into the VPLS service. The 7450 ESS, 7750 SR, or 7950 XRS participating in the service learns where the customer MAC addresses reside, on ingress SAPs or ingress SDPs.

Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and flooded packets can keep flowing through the network. The Nokia implementation of the STP is designed to remove these loops from the VPLS topology. This is done by putting one or several SAPs and, or spoke-SDPs in the discarding state.

Nokia's implementation of STP incorporates some modifications to make the operational characteristics of VPLS more effective.

The STP instance parameters allow the balancing between resiliency and speed of convergence extremes. Modifying particular parameters can affect the behavior. For information about command usage, descriptions, and CLI syntax, see Configuring a VPLS service with CLI.

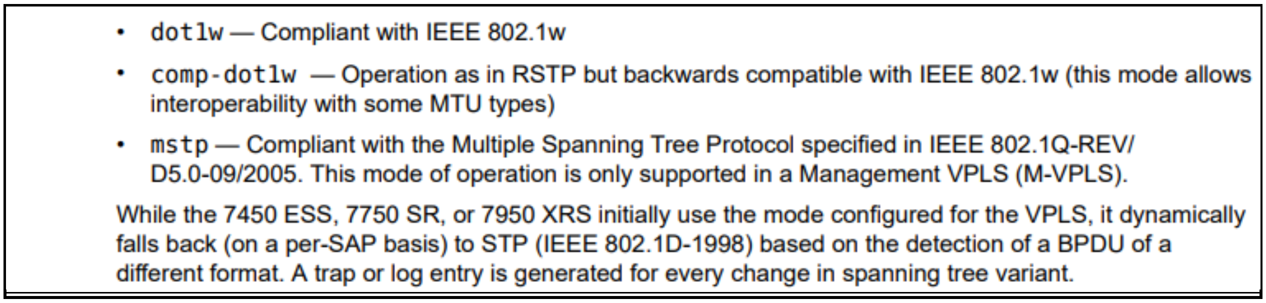
Id. **at 197.**



3.2.9.1 Spanning tree operating modes

Per VPLS instance, a preferred STP variant can be configured. The STP variants supported are:

- `rstp` — Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode

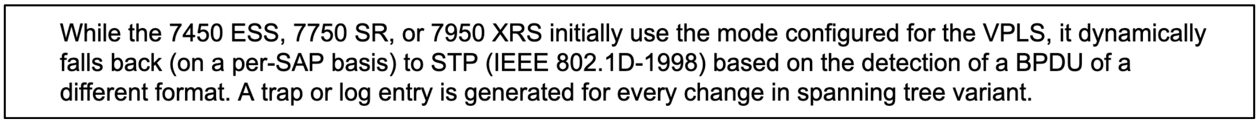


- `dot1w` — Compliant with IEEE 802.1w
- `comp-dot1w` — Operation as in RSTP but backwards compatible with IEEE 802.1w (this mode allows interoperability with some MTU types)
- `mstp` — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q-REV/D5.0-09/2005. This mode of operation is only supported in a Management VPLS (M-VPLS).

While the 7450 ESS, 7750 SR, or 7950 XRS initially use the mode configured for the VPLS, it dynamically falls back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

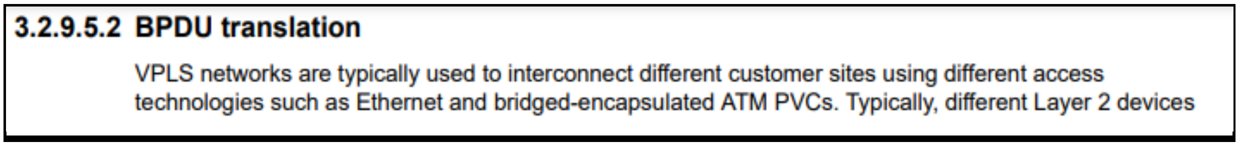
Id. **at 197-198.**

83. Defendants instruct its customers use the 7750 Service Router to transmit control frames among the LSRs in the TLS via the label-switched tunnels, each control frame comprising a control traffic label and a bridge protocol data unit (BPDU) in accordance with a spanning tree protocol (STP), the control traffic label indicating to the LSRs that the STP is to be executed by the LSRs without transmission of the BPDU to the user equipment:



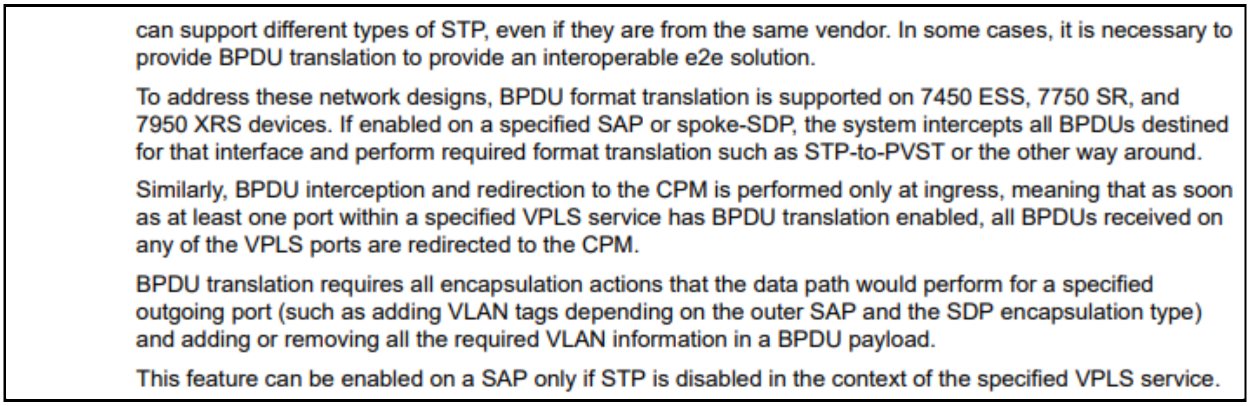
While the 7450 ESS, 7750 SR, or 7950 XRS initially use the mode configured for the VPLS, it dynamically falls back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

***Id.* at 198.**



3.2.9.5.2 BPDU translation

VPLS networks are typically used to interconnect different customer sites using different access technologies such as Ethernet and bridged-encapsulated ATM PVCs. Typically, different Layer 2 devices



can support different types of STP, even if they are from the same vendor. In some cases, it is necessary to provide BPDU translation to provide an interoperable e2e solution.

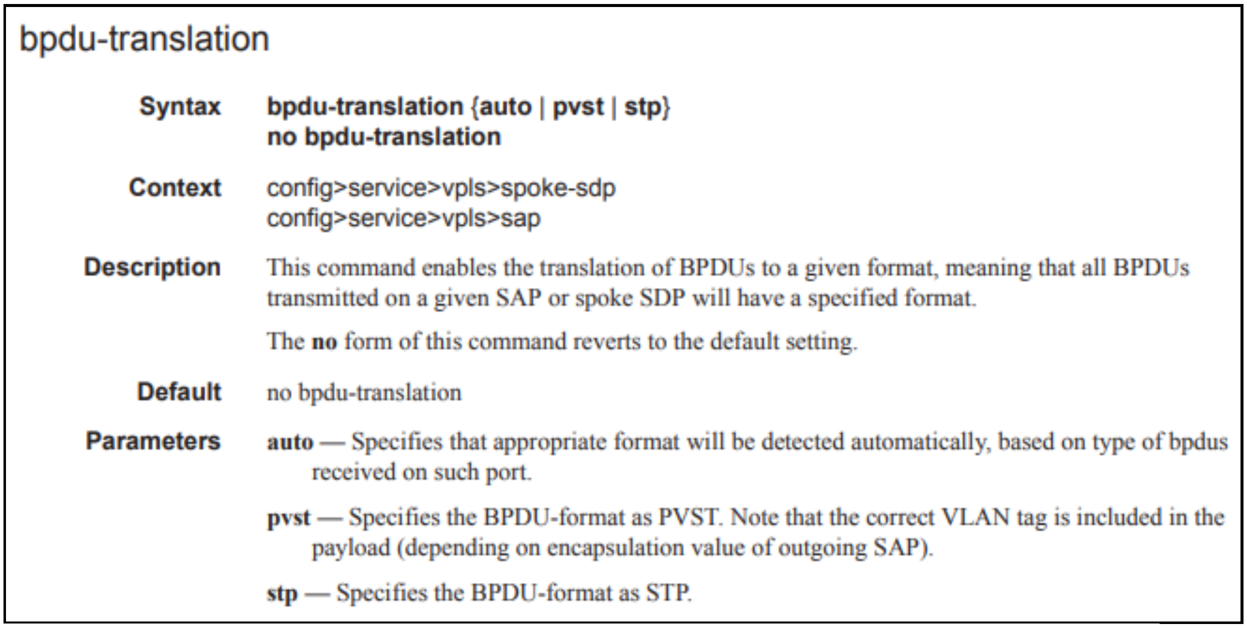
To address these network designs, BPDU format translation is supported on 7450 ESS, 7750 SR, and 7950 XRS devices. If enabled on a specified SAP or spoke-SDP, the system intercepts all BPDUs destined for that interface and perform required format translation such as STP-to-PVST or the other way around.

Similarly, BPDU interception and redirection to the CPM is performed only at ingress, meaning that as soon as at least one port within a specified VPLS service has BPDU translation enabled, all BPDUs received on any of the VPLS ports are redirected to the CPM.

BPDU translation requires all encapsulation actions that the data path would perform for a specified outgoing port (such as adding VLAN tags depending on the outer SAP and the SDP encapsulation type) and adding or removing all the required VLAN information in a BPDU payload.

This feature can be enabled on a SAP only if STP is disabled in the context of the specified VPLS service.

Id. at 201-202.



bpdu-translation

Syntax **bpdu-translation** {**auto** | **pvst** | **stp**}
no bpdu-translation

Context config>service>vpls>spoke-sdp
config>service>vpls>sap

Description This command enables the translation of BPDUs to a given format, meaning that all BPDUs transmitted on a given SAP or spoke SDP will have a specified format.

The **no** form of this command reverts to the default setting.

Default no bpdu-translation

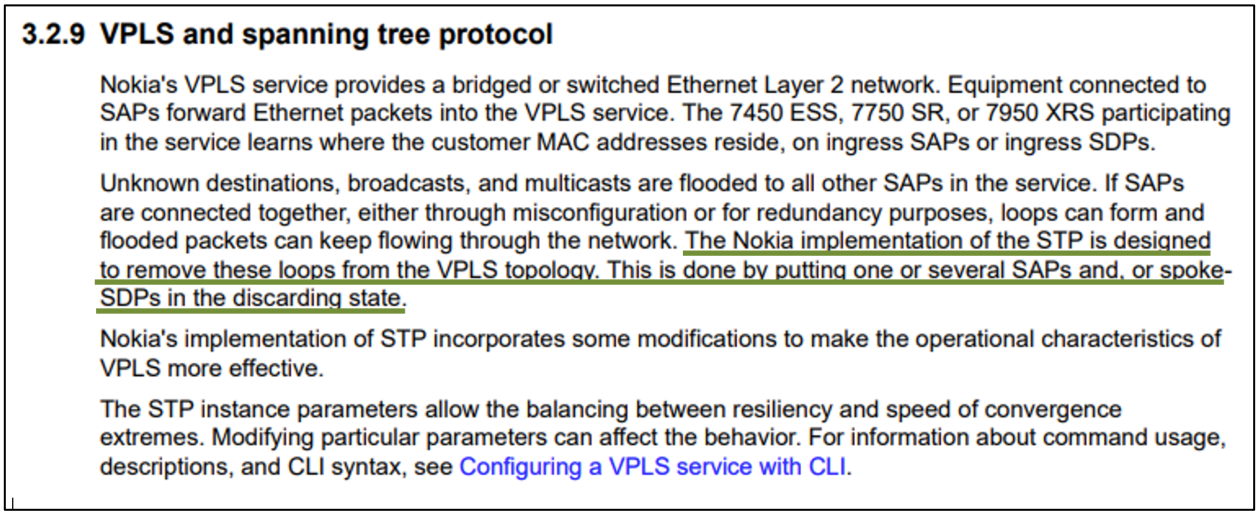
Parameters **auto** — Specifies that appropriate format will be detected automatically, based on type of bpdus received on such port.

pvst — Specifies the BPDU-format as PVST. Note that the correct VLAN tag is included in the payload (depending on encapsulation value of outgoing SAP).

stp — Specifies the BPDU-format as STP.

https://documentation.nokia.com/html/0_add-h-f/93-0076-10-01/7750_SR_OS_Services_Guide/Service-VPLS-CLI.pdf **(page 5).**

84. Defendants instruct its customers use the 7750 Service Router, upon receiving the control frames at the LSRs, to process the BPDU, responsively to the control traffic label, so as to remove loops in the topology of the TLS irrespective of the user equipment:



3.2.9 VPLS and spanning tree protocol

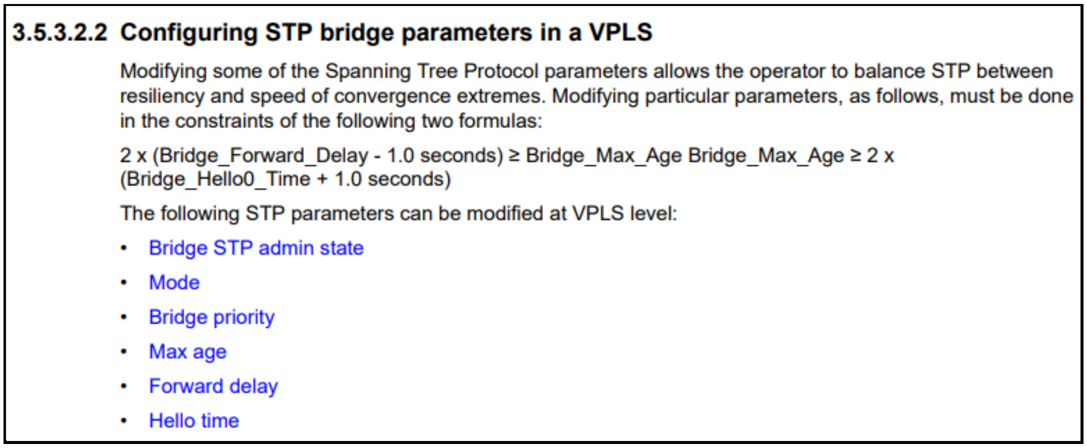
Nokia's VPLS service provides a bridged or switched Ethernet Layer 2 network. Equipment connected to SAPs forward Ethernet packets into the VPLS service. The 7450 ESS, 7750 SR, or 7950 XRS participating in the service learns where the customer MAC addresses reside, on ingress SAPs or ingress SDPs.

Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and flooded packets can keep flowing through the network. The Nokia implementation of the STP is designed to remove these loops from the VPLS topology. This is done by putting one or several SAPs and, or spoke-SDPs in the discarding state.

Nokia's implementation of STP incorporates some modifications to make the operational characteristics of VPLS more effective.

The STP instance parameters allow the balancing between resiliency and speed of convergence extremes. Modifying particular parameters can affect the behavior. For information about command usage, descriptions, and CLI syntax, see Configuring a VPLS service with CLI.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17148AAADTQZZA01_V1_7450%20ESS%207750%20SR%207950%20XRS%20and%20VSR%20Layer%202%20Services%20and%20EVPN%20Guide:%20VLL%20VPLS%20PBB%20and%20EVPN%2021.10.R1.pdf **(page 197).**



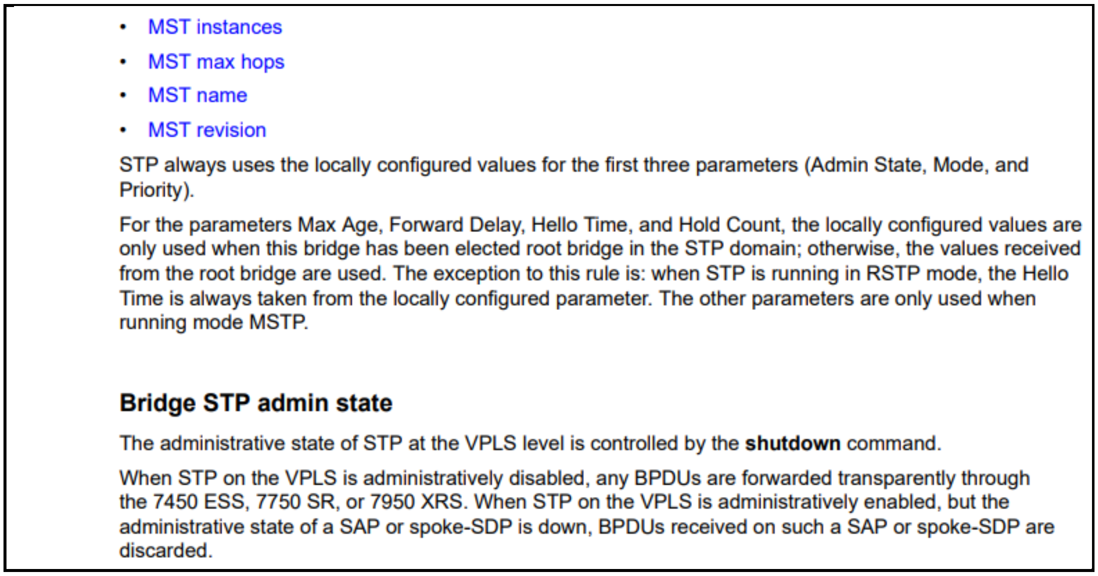
3.5.3.2.2 Configuring STP bridge parameters in a VPLS

Modifying some of the Spanning Tree Protocol parameters allows the operator to balance STP between resiliency and speed of convergence extremes. Modifying particular parameters, as follows, must be done in the constraints of the following two formulas:

2 x (Bridge_Forward_Delay - 1.0 seconds) ≥ Bridge_Max_Age Bridge_Max_Age ≥ 2 x (Bridge_Hello0_Time + 1.0 seconds)

The following STP parameters can be modified at VPLS level:

- Bridge STP admin state
- Mode
- Bridge priority
- Max age
- Forward delay
- Hello time



- MST instances
- MST max hops
- MST name
- MST revision

STP always uses the locally configured values for the first three parameters (Admin State, Mode, and Priority).

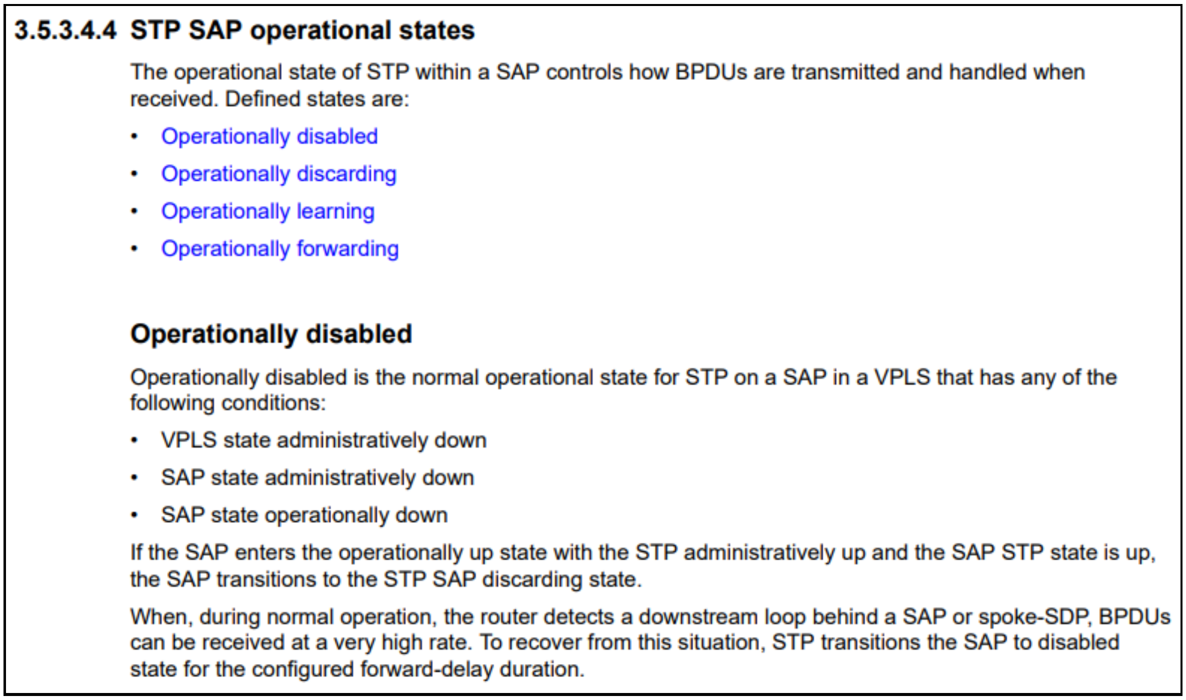
For the parameters Max Age, Forward Delay, Hello Time, and Hold Count, the locally configured values are only used when this bridge has been elected root bridge in the STP domain; otherwise, the values received from the root bridge are used. The exception to this rule is: when STP is running in RSTP mode, the Hello Time is always taken from the locally configured parameter. The other parameters are only used when running mode MSTP.

Bridge STP admin state

The administrative state of STP at the VPLS level is controlled by the **shutdown** command.

When STP on the VPLS is administratively disabled, any BPDUs are forwarded transparently through the 7450 ESS, 7750 SR, or 7950 XRS. When STP on the VPLS is administratively enabled, but the administrative state of a SAP or spoke-SDP is down, BPDUs received on such a SAP or spoke-SDP are discarded.

***Id.* at 270-271.**



3.5.3.4.4 STP SAP operational states

The operational state of STP within a SAP controls how BPDUs are transmitted and handled when received. Defined states are:

- Operationally disabled
- Operationally discarding
- Operationally learning
- Operationally forwarding

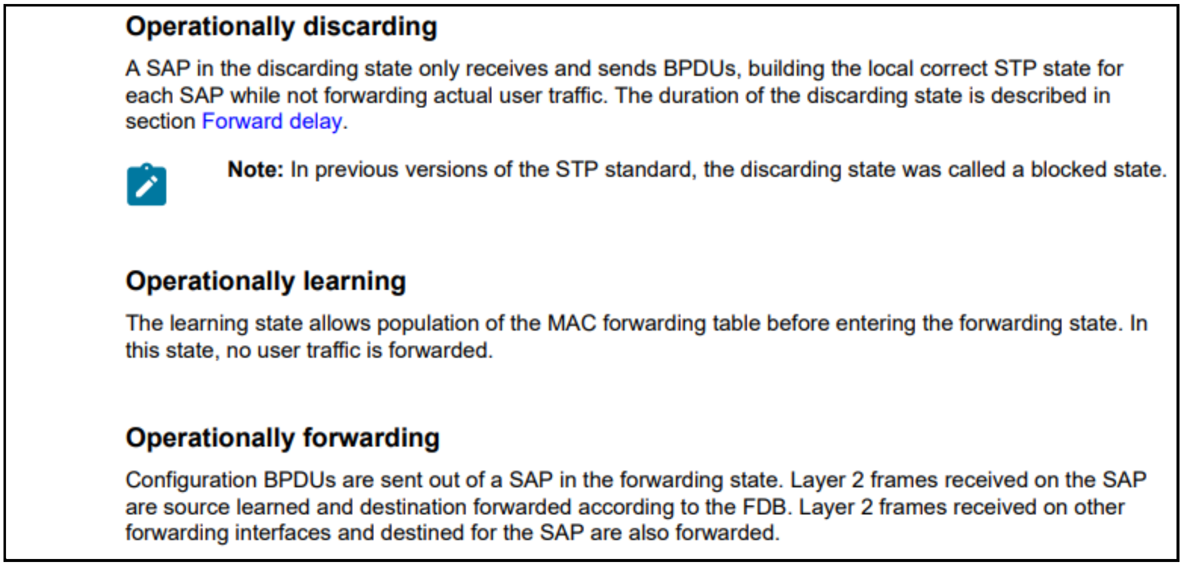
Operationally disabled

Operationally disabled is the normal operational state for STP on a SAP in a VPLS that has any of the following conditions:

- VPLS state administratively down
- SAP state administratively down
- SAP state operationally down

If the SAP enters the operationally up state with the STP administratively up and the SAP STP state is up, the SAP transitions to the STP SAP discarding state.

When, during normal operation, the router detects a downstream loop behind a SAP or spoke-SDP, BPDUs can be received at a very high rate. To recover from this situation, STP transitions the SAP to disabled state for the configured forward-delay duration.



Operationally discarding

A SAP in the discarding state only receives and sends BPDUs, building the local correct STP state for each SAP while not forwarding actual user traffic. The duration of the discarding state is described in section Forward delay.

Note: In previous versions of the STP standard, the discarding state was called a blocked state.

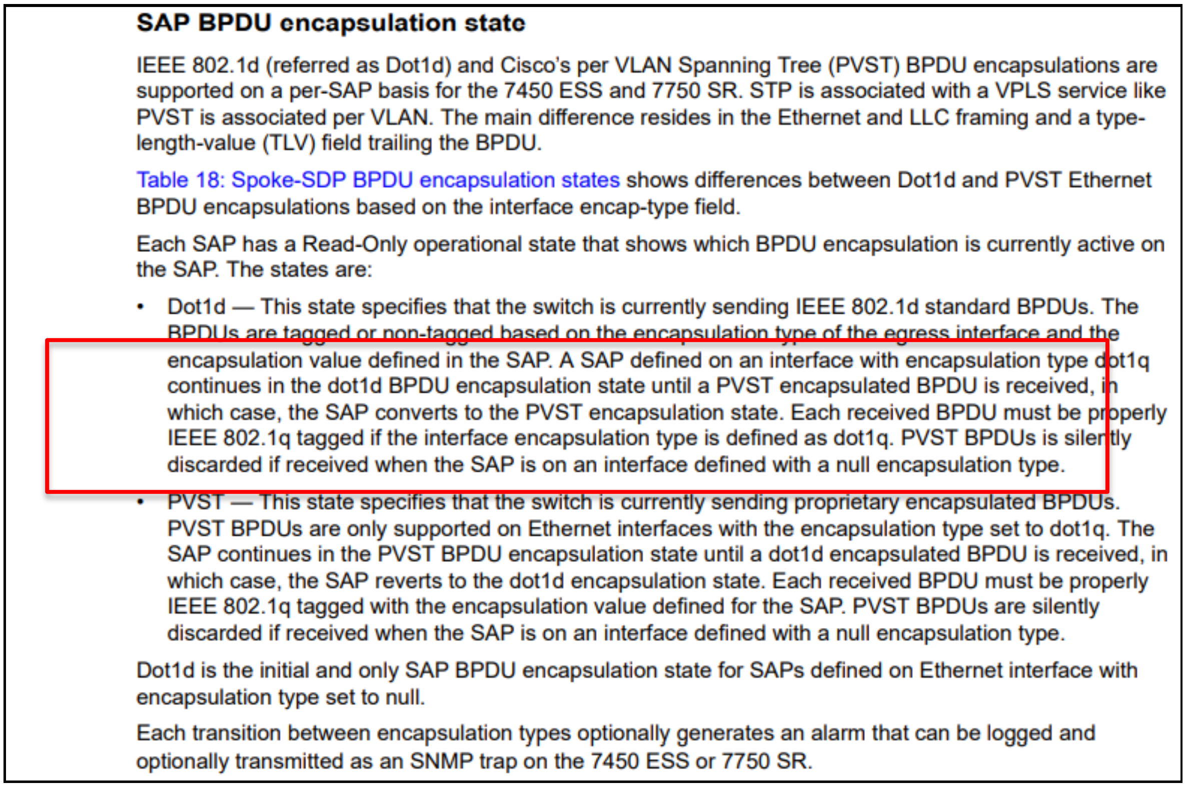
Operationally learning

The learning state allows population of the MAC forwarding table before entering the forwarding state. In this state, no user traffic is forwarded.

Operationally forwarding

Configuration BPDUs are sent out of a SAP in the forwarding state. Layer 2 frames received on the SAP are source learned and destination forwarded according to the FDB. Layer 2 frames received on other forwarding interfaces and destined for the SAP are also forwarded.

***Id.* at 280-281.**



SAP BPDU encapsulation state

IEEE 802.1d (referred as Dot1d) and Cisco's per VLAN Spanning Tree (PVST) BPDU encapsulations are supported on a per-SAP basis for the 7450 ESS and 7750 SR. STP is associated with a VPLS service like PVST is associated per VLAN. The main difference resides in the Ethernet and LLC framing and a type-length-value (TLV) field trailing the BPDU.

Table 18: Spoke-SDP BPDU encapsulation states shows differences between Dot1d and PVST Ethernet BPDU encapsulations based on the interface encap-type field.

Each SAP has a Read-Only operational state that shows which BPDU encapsulation is currently active on the SAP. The states are:

- Dot1d — This state specifies that the switch is currently sending IEEE 802.1d standard BPDUs. The BPDUs are tagged or non-tagged based on the encapsulation type of the egress interface and the encapsulation value defined in the SAP. A SAP defined on an interface with encapsulation type dot1q continues in the dot1d BPDU encapsulation state until a PVST encapsulated BPDU is received, in which case, the SAP converts to the PVST encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged if the interface encapsulation type is defined as dot1q. PVST BPDUs is silently discarded if received when the SAP is on an interface defined with a null encapsulation type.
- PVST — This state specifies that the switch is currently sending proprietary encapsulated BPDUs. PVST BPDUs are only supported on Ethernet interfaces with the encapsulation type set to dot1q. The SAP continues in the PVST BPDU encapsulation state until a dot1d encapsulated BPDU is received, in which case, the SAP reverts to the dot1d encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged with the encapsulation value defined for the SAP. PVST BPDUs are silently discarded if received when the SAP is on an interface defined with a null encapsulation type.

Dot1d is the initial and only SAP BPDU encapsulation state for SAPs defined on Ethernet interface with encapsulation type set to null.

Each transition between encapsulation types optionally generates an alarm that can be logged and optionally transmitted as an SNMP trap on the 7450 ESS or 7750 SR.

***Id.* at 281.**

85. As a result of Defendants' infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT THREE
<u>INFRINGEMENT OF U.S. PATENT 7,283,465</u>

86. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-20 as if fully set forth herein.

87. The '465 Patent, entitled "HIERARCHICAL VIRTUAL PRIVATE LAN SERVICE PROTECTION SCHEME" was filed on January 7, 2003 and issued on October 16, 2007.

88. Plaintiff is the assignee and owner of all rights, title and interest to the '465 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

<u>Technical Description</u>

89. The '465 Patent addresses technical problems in the prior art of LAN networks that may result from failures in network nodes. Existing failure protection systems may use "backup point-to-point PWs between each edge node and an additional core node. The backup PW connection is in addition to the standard PW connection already existing between the edge node and another code node. Thus, if a VC between an edge node and a core node fails, a backup 'protection path' through another core node can be used to provide access between the edge node and the rest of the network." (col. 4, ll. 18-33). Such systems however suffer from "long period[s] of traffic outage if a virtual connection fails between an edge node and a core node, or if a code

node fails. In most cases, initiation of failure protection depends on MAC address aging and learning schemes, which are slow." *Id*. Further, there are no provisions for handling multiple failures at once and the need to handle both standard connections (to edge nodes and other core nodes) and backup protection connections (to edge nodes) complicates the design of the core nodes and the network as a whole. *Id*.

90. The '465 Patent "seeks to provide improved mechanisms for protection from failure in virtual private networks (VPNs)" by using a network comprising primary core nodes and standby core nodes having the same topology as a corresponding primary core node which it protects. (col. 4, l. 50-col. 5, l. 39). "[I]f the "primary core node fails, the remaining nodes in the network simply redirect all connections from the failed primary core node to the corresponding standby core node. Since the standby core node has the same topology as the failed primary core node, the remaining nodes in the network do not need to re-learn MAC table addresses, and are thus able to recover quickly from the failure. In addition, there is no need to clear the MAC tables, so that packet flooding is reduced significantly." *Id*.

Direct Infringement

91. Defendants, without authorization or license from Plaintiff, have been and are directly infringing the '465 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '465 Patent. Defendants develop, design, manufacture, and distribute telecommunications equipment that infringes one or more claims of the '465 Patent. Defendants further provide services that practice methods that infringe one or more claims of the '465 Patent. Defendants are thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities

include Nokia 7705 Service Aggregation Router, and all other substantially similar products (collectively the "'465 Accused Products").

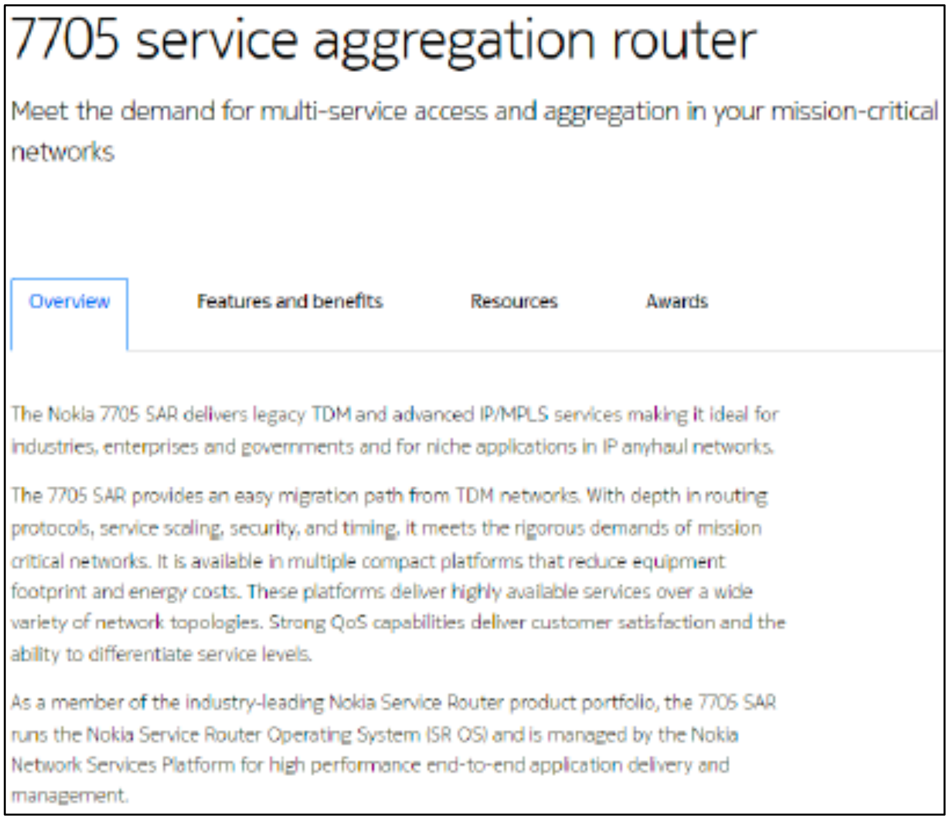
92. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendants' infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '465 Accused Products.

93. Defendants are liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendants' 7705 Service Aggregation Router.

94. Defendants' 7705 Service Aggregation Router are non-limiting examples of ethernet switches that meet all limitations of claim 1 of the '465 Patent, either literally or equivalently.

95. Defendants' 7705 Service Aggregation Router is configured to comprise a data communication network.

96. Defendants' 7705 Service Aggregation Routers are configured to comprise a plurality of primary virtual bridges, interconnected by primary virtual connections so as to transmit and receive data packets over the network to and from edge devices connected thereto.



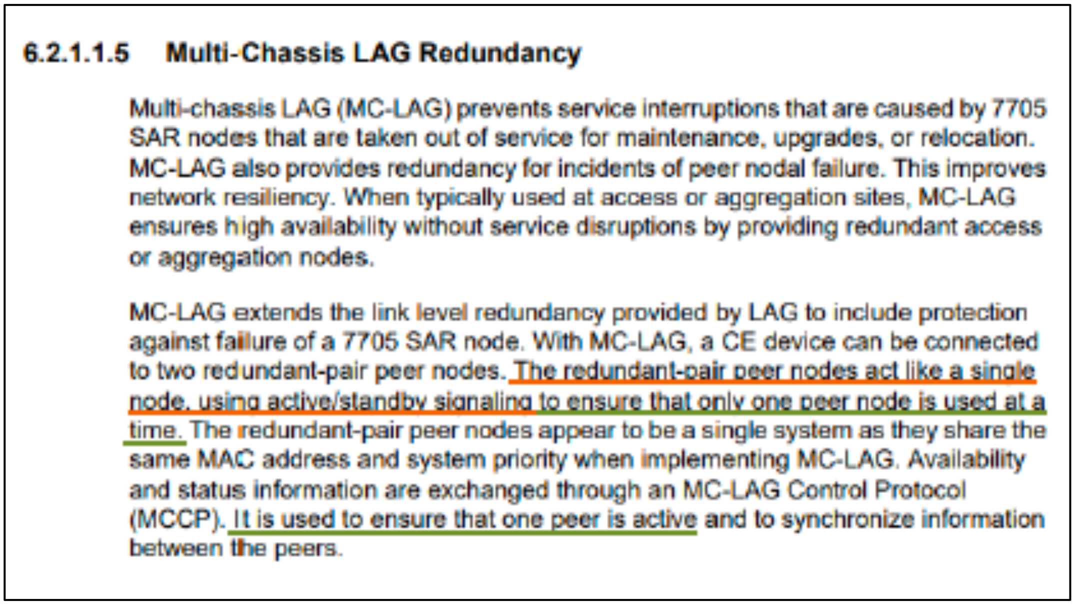
7705 service aggregation router

Meet the demand for multi-service access and aggregation in your mission-critical networks

The Nokia 7705 SAR delivers legacy TDM and advanced IP/MPLS services making it ideal for industries, enterprises and governments and for niche applications in IP anyhaul networks.

The 7705 SAR provides an easy migration path from TDM networks. With depth in routing protocols, service scaling, security, and timing, it meets the rigorous demands of mission critical networks. It is available in multiple compact platforms that reduce equipment footprint and energy costs. These platforms deliver highly available services over a wide variety of network topologies. Strong QoS capabilities deliver customer satisfaction and the ability to differentiate service levels.

As a member of the industry-leading Nokia Service Router product portfolio, the 7705 SAR runs the Nokia Service Router Operating System (SR OS) and is managed by the Nokia Network Services Platform for high performance end-to-end application delivery and management.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

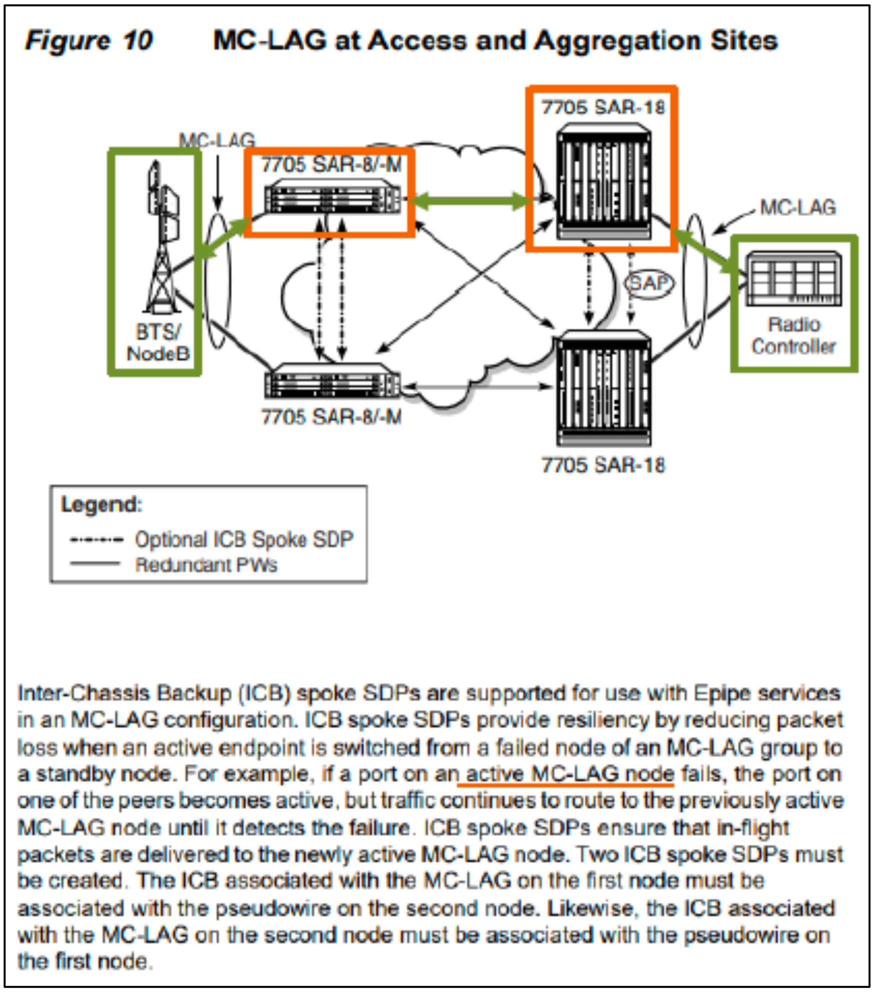
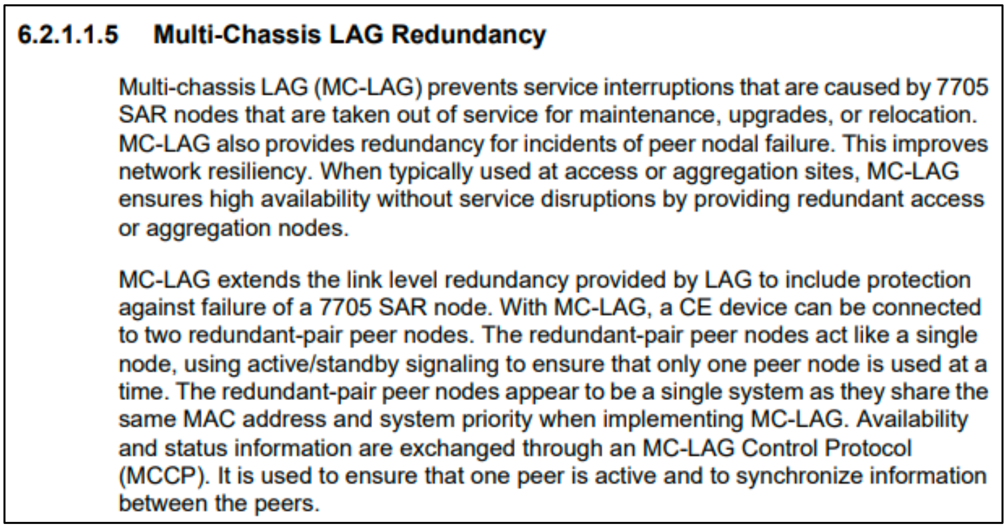


Figure 10 **MC-LAG at Access and Aggregation Sites**

Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf (**Pages 240 and 241 of PDF**)

97. Defendants' 7705 Service Aggregation Routers are configured to comprise a plurality of backup virtual bridges, each such backup virtual bridge being paired with a corresponding one of the primary virtual bridges and connected by secondary virtual connections to the other primary virtual bridges.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

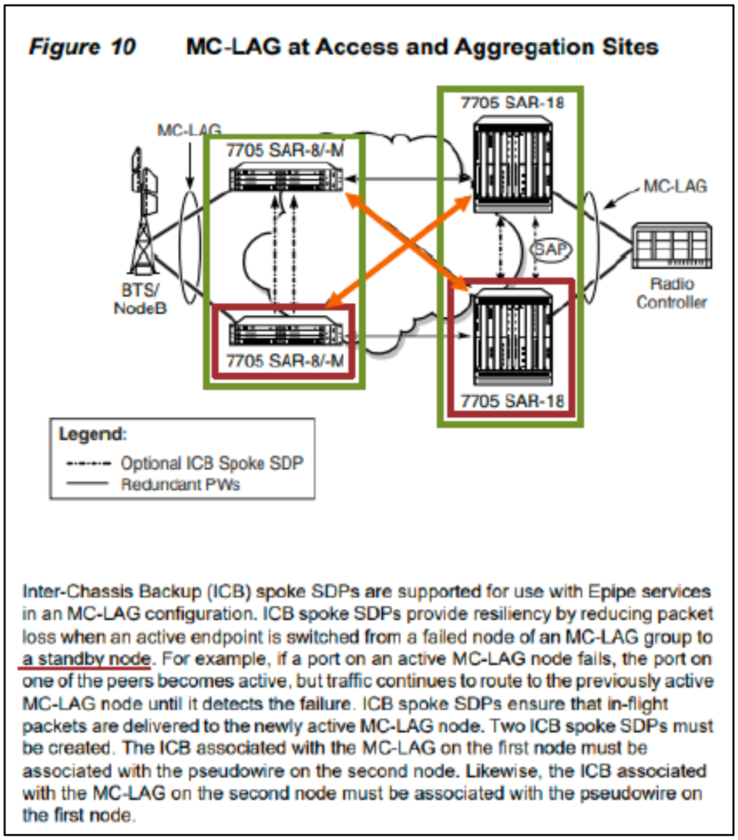


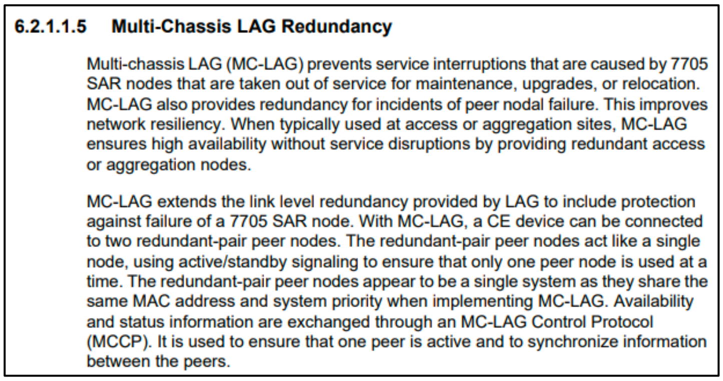
Figure 10 **MC-LAG at Access and Aggregation Sites**

Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf (**Pages 240 and 241 of PDF**)

98. Defendants' 7705 Service Aggregation Routers are configured wherein the primary virtual connections define a respective primary topology image for each of the primary virtual

bridges, and wherein each of the backup virtual bridges is connected to the other primary virtual bridges by secondary virtual connections that are identical to the primary virtual connections of the corresponding one of the primary virtual bridges, thus defining a respective secondary topology image that is identical to the respective primary topology image of the corresponding one of the primary virtual bridges.

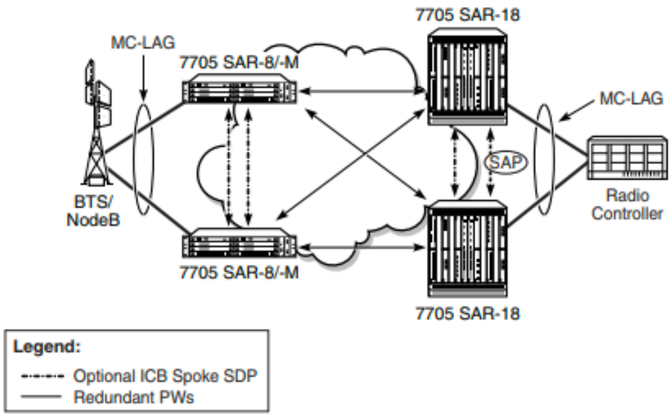


6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

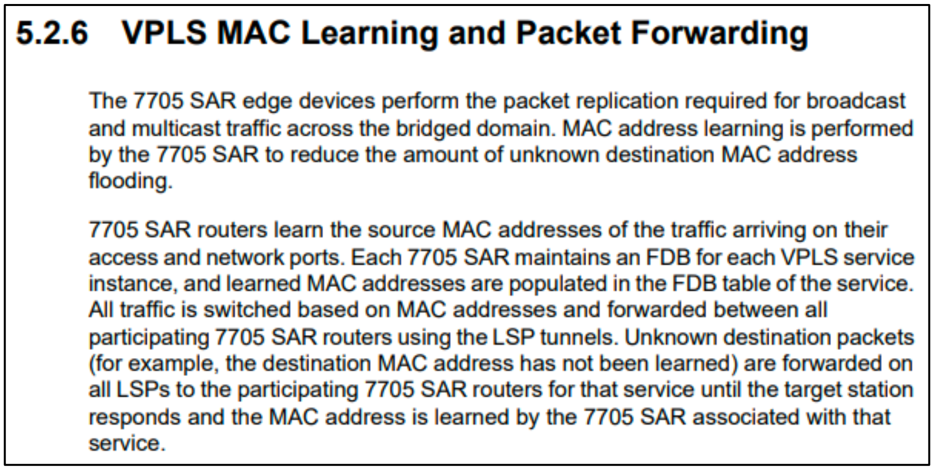
Figure 10 **MC-LAG at Access and Aggregation Sites**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

99. Defendants’ 7705 Service Aggregation Routers are configured wherein each of the primary and backup virtual bridges is adapted to maintain a respective forwarding table, and to forward the data packets in accordance with entries in the respective forwarding table, and wherein each of the backup virtual bridges is adapted to periodically synchronize its forwarding table by

copying contents of the forwarding table of the corresponding one of the primary virtual bridges with which it is paired.

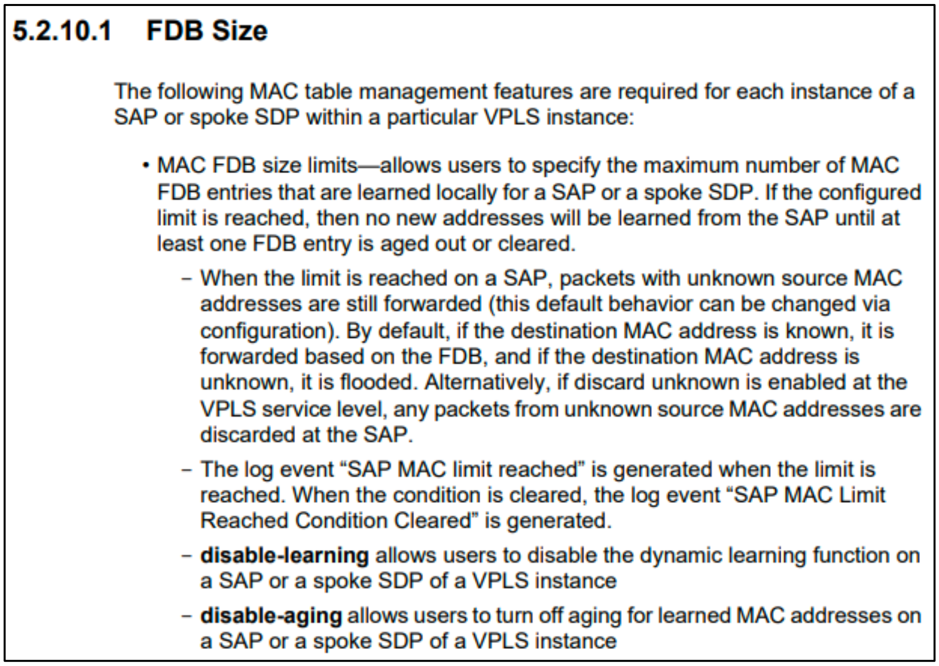


5.2.6 VPLS MAC Learning and Packet Forwarding

The 7705 SAR edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed by the 7705 SAR to reduce the amount of unknown destination MAC address flooding.

7705 SAR routers learn the source MAC addresses of the traffic arriving on their access and network ports. Each 7705 SAR maintains an FDB for each VPLS service instance, and learned MAC addresses are populated in the FDB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating 7705 SAR routers using the LSP tunnels. Unknown destination packets (for example, the destination MAC address has not been learned) are forwarded on all LSPs to the participating 7705 SAR routers for that service until the target station responds and the MAC address is learned by the 7705 SAR associated with that service.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE16308AAAATQZZA01_V1_7705%20SAR%20Services%20Guide%2020.4.R1.pdf **(Page 573 of PDF)**

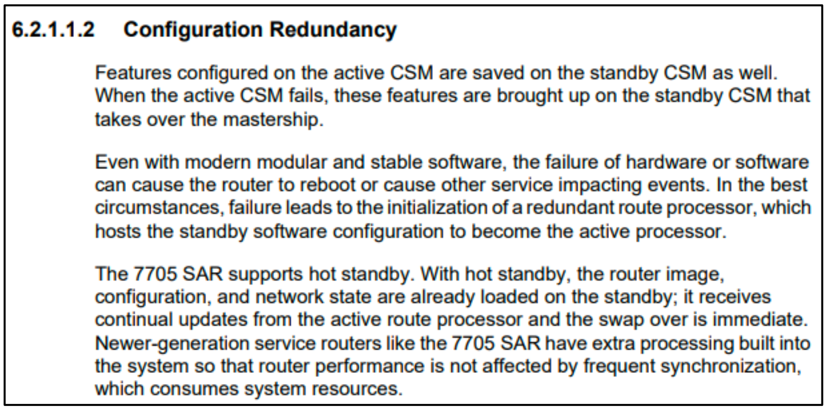


5.2.10.1 FDB Size

The following MAC table management features are required for each instance of a SAP or spoke SDP within a particular VPLS instance:

- MAC FDB size limits—allows users to specify the maximum number of MAC FDB entries that are learned locally for a SAP or a spoke SDP. If the configured limit is reached, then no new addresses will be learned from the SAP until at least one FDB entry is aged out or cleared.
  - When the limit is reached on a SAP, packets with unknown source MAC addresses are still forwarded (this default behavior can be changed via configuration). By default, if the destination MAC address is known, it is forwarded based on the FDB, and if the destination MAC address is unknown, it is flooded. Alternatively, if discard unknown is enabled at the VPLS service level, any packets from unknown source MAC addresses are discarded at the SAP.
  - The log event “SAP MAC limit reached” is generated when the limit is reached. When the condition is cleared, the log event “SAP MAC Limit Reached Condition Cleared” is generated.
  - **disable-learning** allows users to disable the dynamic learning function on a SAP or a spoke SDP of a VPLS instance
  - **disable-aging** allows users to turn off aging for learned MAC addresses on a SAP or a spoke SDP of a VPLS instance

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE16308AAAATQZZA01_V1_7705%20SAR%20Services%20Guide%2020.4.R1.pdf **(Page 576 of PDF)**

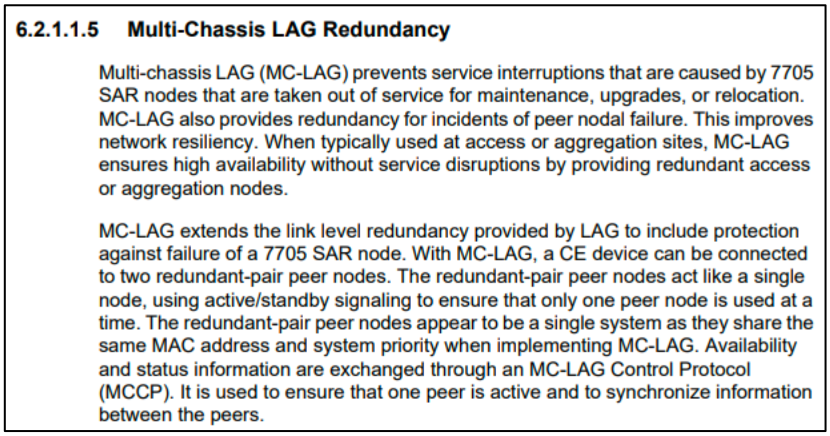


6.2.1.1.2 Configuration Redundancy

Features configured on the active CSM are saved on the standby CSM as well. When the active CSM fails, these features are brought up on the standby CSM that takes over the mastership.

Even with modern modular and stable software, the failure of hardware or software can cause the router to reboot or cause other service impacting events. In the best circumstances, failure leads to the initialization of a redundant route processor, which hosts the standby software configuration to become the active processor.

The 7705 SAR supports hot standby. With hot standby, the router image, configuration, and network state are already loaded on the standby; it receives continual updates from the active route processor and the swap over is immediate. Newer-generation service routers like the 7705 SAR have extra processing built into the system so that router performance is not affected by frequent synchronization, which consumes system resources.



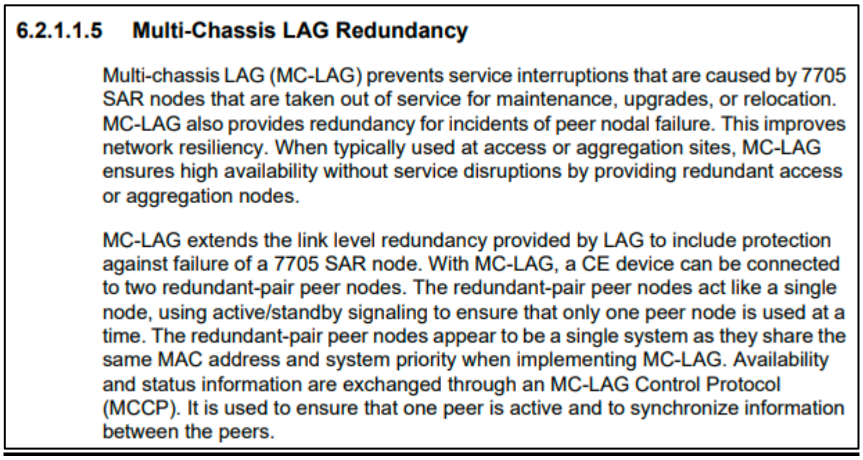
6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf (**Pages 239 and 240 of PDF**)

100. Defendants' 7705 Service Aggregation Routers are configured whereby upon a failure of the corresponding one of the primary virtual bridges, each of the backup virtual bridge forwards and receives the data packets over the network via the secondary virtual connections, in accordance with the synchronized forwarding table, in place of the corresponding one of the primary virtual bridges.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

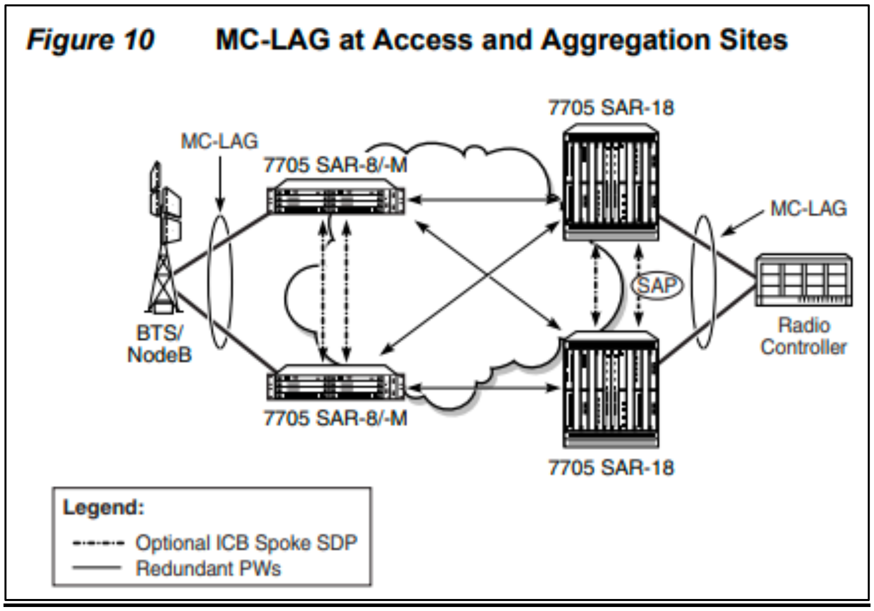
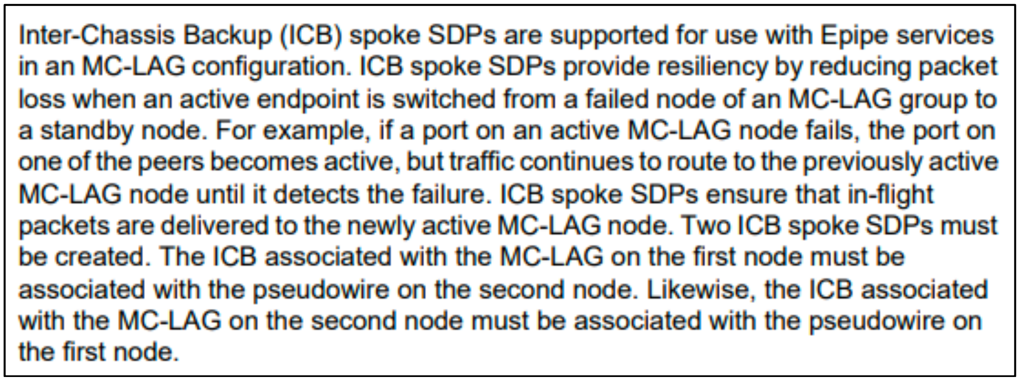


Figure 10 **MC-LAG at Access and Aggregation Sites**



Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

Willful Infringement

101. Defendants have had actual knowledge of the ’465 Patent and its infringement thereof at least as of service of Plaintiff’s Complaint.

102. Defendants’ risk of infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendants.

103. Notwithstanding this knowledge, Defendants have knowingly or with reckless disregard willfully infringed the ’465 Patent. Defendants have thus had actual notice of the infringement of the ’465 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

104. This objective risk was either known or so obvious that it should have been known to Defendants. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

105. Defendants have induced and is knowingly inducing its customers and/or end users to directly infringe the ’465 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

106. Defendants have knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the ’465 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

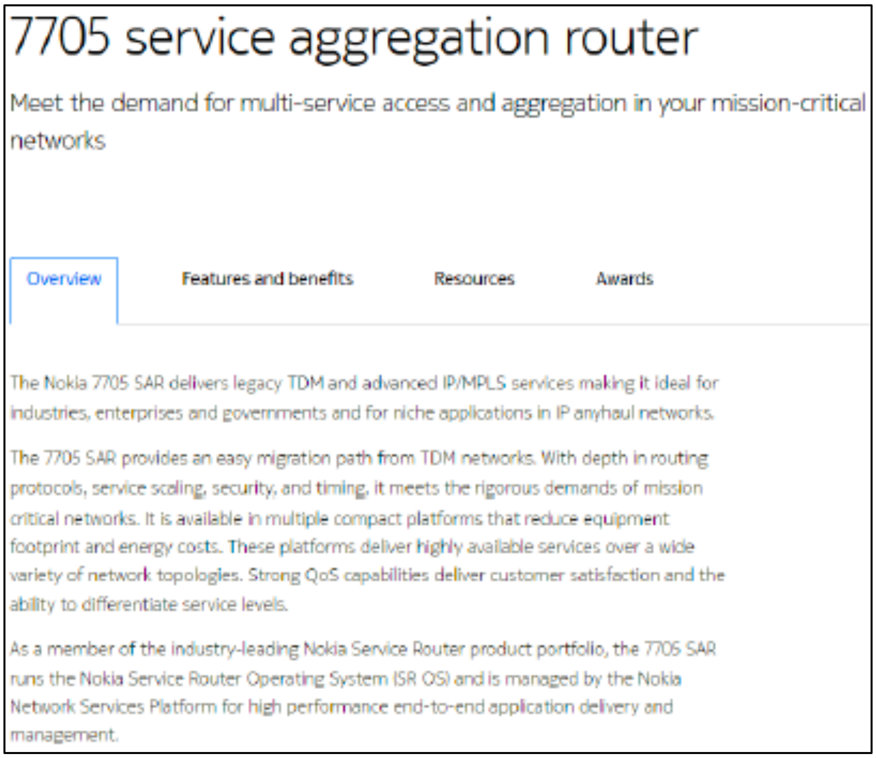
107. Defendants' indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '465 Patent.

108. Defendants' indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendants' indirect infringement further includes providing application notes instructing its customers on infringing uses of the '465 Accused Products. The '465 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '465 Patent, either literally or equivalently. Defendants know and intend that customers who purchase the '465 Accused Products will use those products for their intended purpose. For example, Defendants' United States website: https://www.nokia.com, instructs customers to use the '465 Accused Products in numerous infringing applications. Furthermore, Defendants provide instructions and other resources via its "Doc Center" (https://documentation.nokia.com), "Nokia Service Routing Certification" and training courses from its "NokiaEDU Training Centers" (https://www.nokia.com/networks/training/src/courses/#open-enrollment), and elsewhere on using the '465 Accused Products. Defendants' customers directly infringe the '465 patent when they follow Defendants' provided instructions on website, videos, and elsewhere. Defendants' customers who follow Defendants' provided instructions directly infringe claims of the '465 Patent.

109. In addition, Defendants specifically intend that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendants' infringing products. Defendants know following its instructions directly infringes claims of the '465 Patent, including for example Claim 16.

110. Defendants' customers who follow Defendants' provided instructions directly infringe the method of claim 16 of the '465 Patent.

111. Defendants instruct its customers to use the 7750 Service Router in a method for data communication. communication network.



7705 service aggregation router

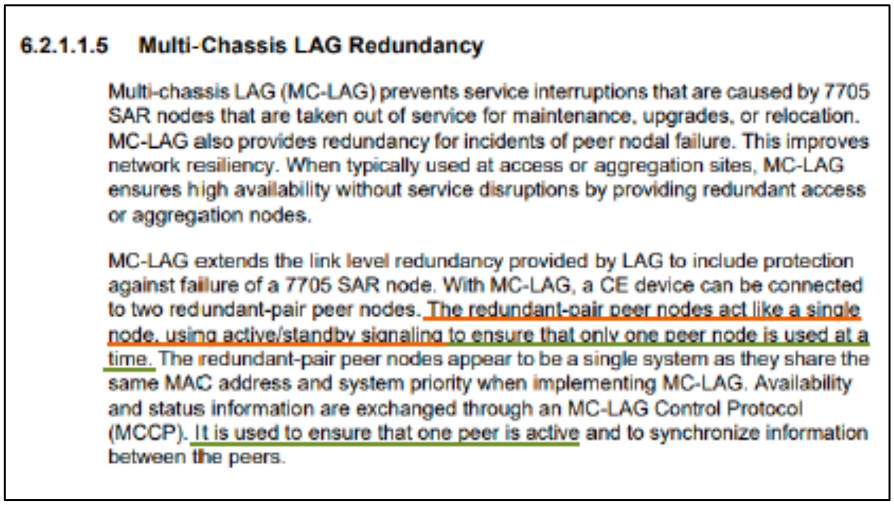
Meet the demand for multi-service access and aggregation in your mission-critical networks

The Nokia 7705 SAR delivers legacy TDM and advanced IP/MPLS services making it ideal for industries, enterprises and governments and for niche applications in IP anyhaul networks.

The 7705 SAR provides an easy migration path from TDM networks. With depth in routing protocols, service scaling, security, and timing, it meets the rigorous demands of mission critical networks. It is available in multiple compact platforms that reduce equipment footprint and energy costs. These platforms deliver highly available services over a wide variety of network topologies. Strong QoS capabilities deliver customer satisfaction and the ability to differentiate service levels.

As a member of the industry-leading Nokia Service Router product portfolio, the 7705 SAR runs the Nokia Service Router Operating System (SR OS) and is managed by the Nokia Network Services Platform for high performance end-to-end application delivery and management.

112. Defendants instruct its customers to configure Defendants' 7705 Service Aggregation Routers to comprise a plurality of primary virtual bridges, interconnected by primary virtual connections so as to transmit and receive data packets over the network to and from edge devices connected thereto.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

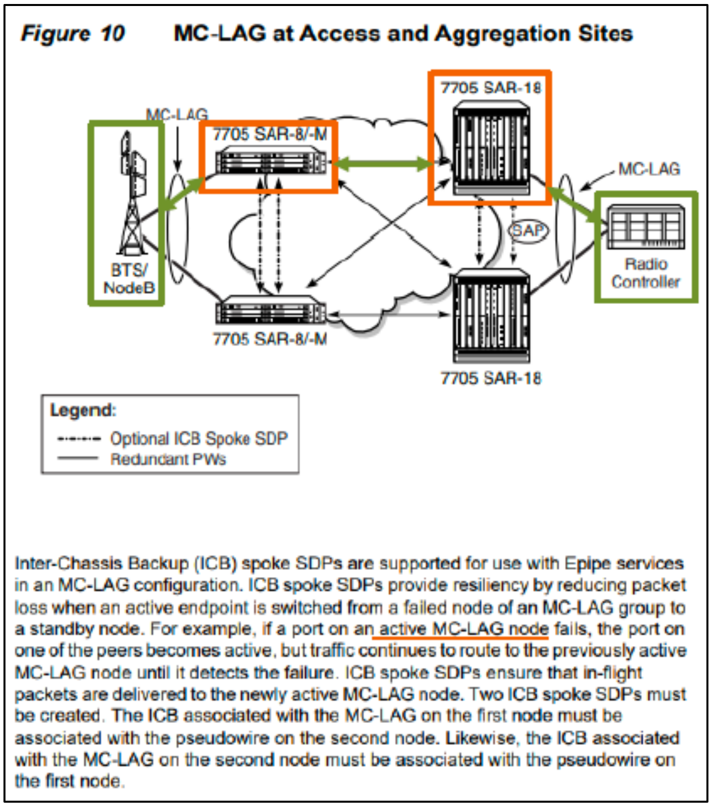


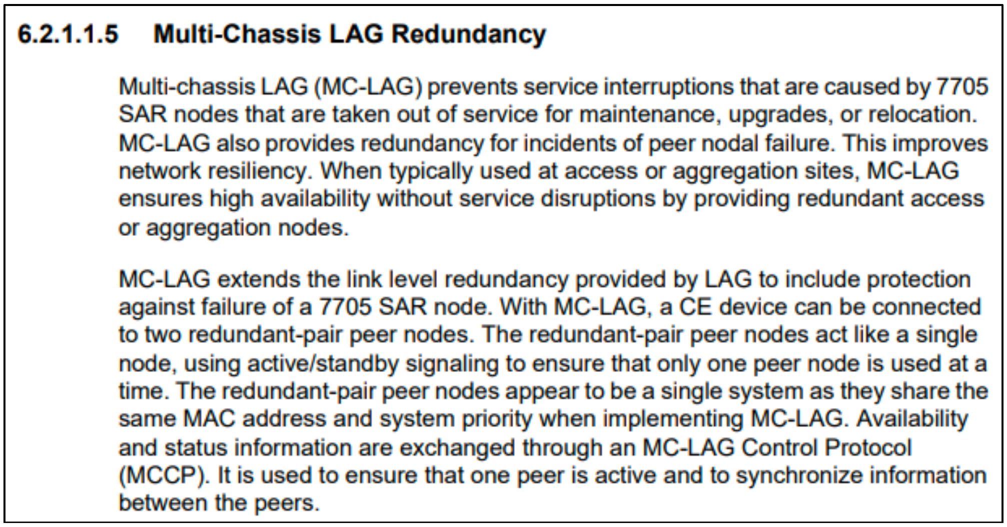
Figure 10 MC-LAG at Access and Aggregation Sites

Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

113. Defendants instruct its customers to configure Defendants' 7705 Service Aggregation Routers to comprise a plurality of backup virtual bridges, each such backup virtual

bridge being paired with a corresponding one of the primary virtual bridges and connected by secondary virtual connections to the other primary virtual bridges.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

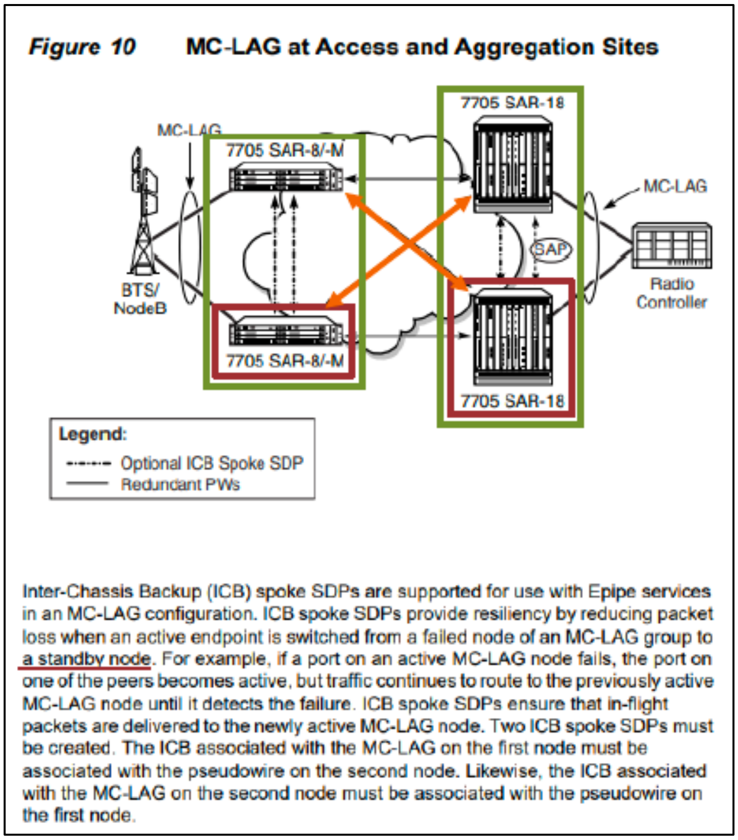
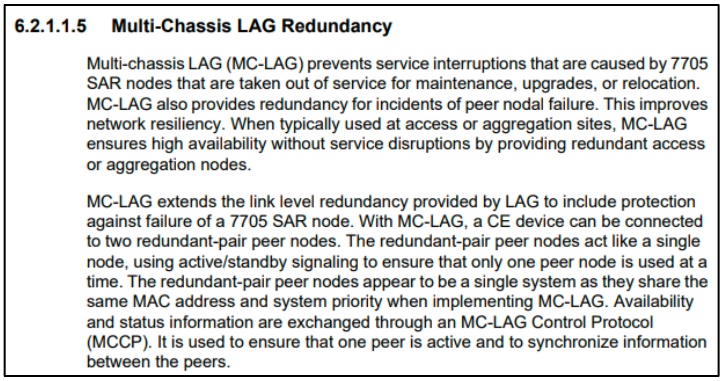


Figure 10 **MC-LAG at Access and Aggregation Sites**

Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

114. Defendants instruct its customers to configure Defendants' 7705 Service Aggregation Routers wherein the primary virtual connections define a respective primary topology image for each of the primary virtual bridges, and wherein each of the backup virtual bridges is connected to the other primary virtual bridges by secondary virtual connections that are identical to the primary virtual connections of the corresponding one of the primary virtual bridges, thus defining a respective secondary topology image that is identical to the respective primary topology image of the corresponding one of the primary virtual bridges.

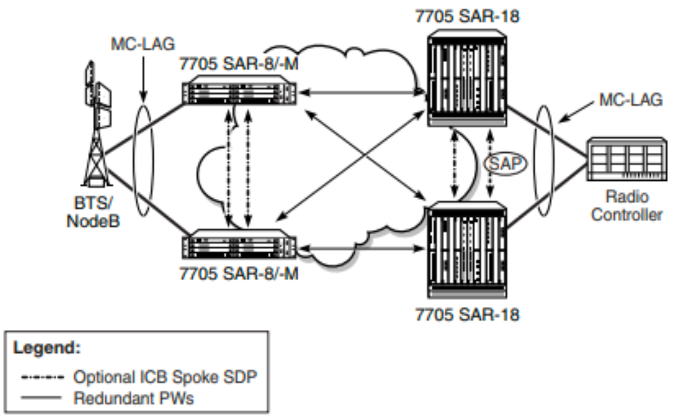


6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

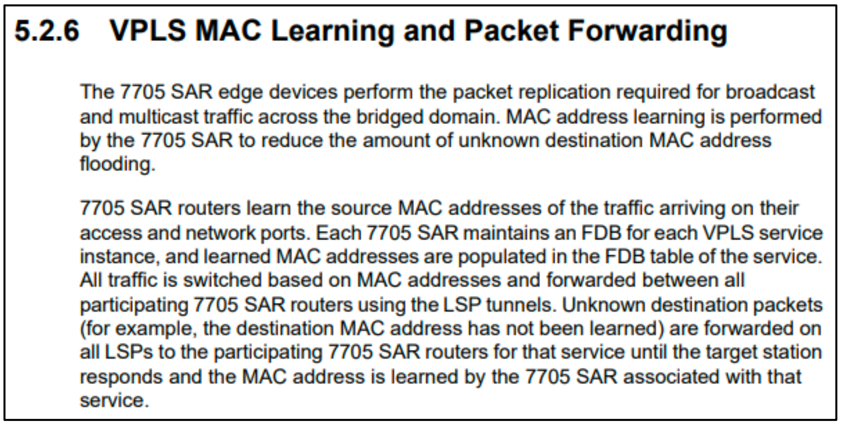
MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

Figure 10 **MC-LAG at Access and Aggregation Sites**



https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

115. Defendants instruct its customers to configure Defendants' 7705 Service Aggregation Routers wherein each of the primary and backup virtual bridges is adapted to maintain a respective forwarding table, and to forward the data packets in accordance with entries in the respective forwarding table, and wherein each of the backup virtual bridges is adapted to periodically synchronize its forwarding table by copying contents of the forwarding table of the corresponding one of the primary virtual bridges with which it is paired.

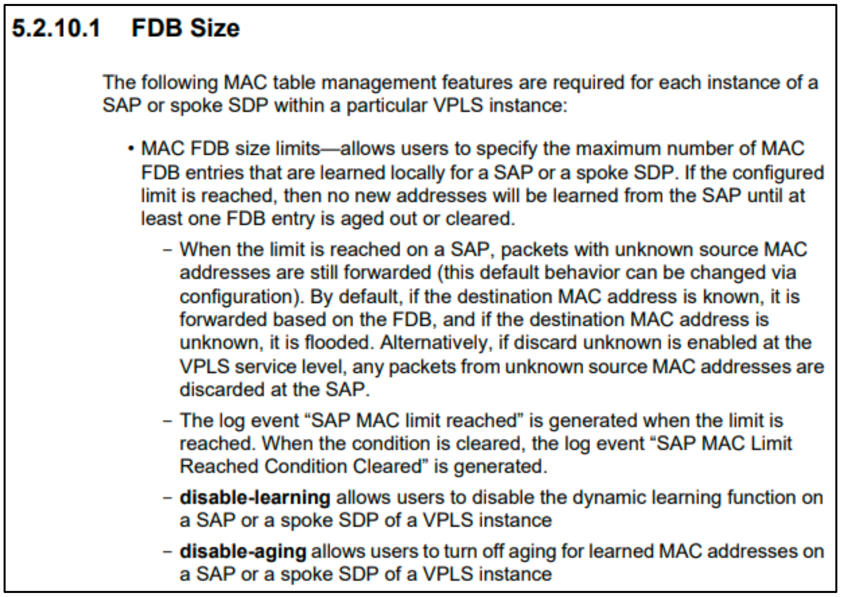


5.2.6 VPLS MAC Learning and Packet Forwarding

The 7705 SAR edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed by the 7705 SAR to reduce the amount of unknown destination MAC address flooding.

7705 SAR routers learn the source MAC addresses of the traffic arriving on their access and network ports. Each 7705 SAR maintains an FDB for each VPLS service instance, and learned MAC addresses are populated in the FDB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating 7705 SAR routers using the LSP tunnels. Unknown destination packets (for example, the destination MAC address has not been learned) are forwarded on all LSPs to the participating 7705 SAR routers for that service until the target station responds and the MAC address is learned by the 7705 SAR associated with that service.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE16308AAAATQZZA01_V1_7705%20SAR%20Services%20Guide%2020.4.R1.pdf **(Page 573 of PDF)**

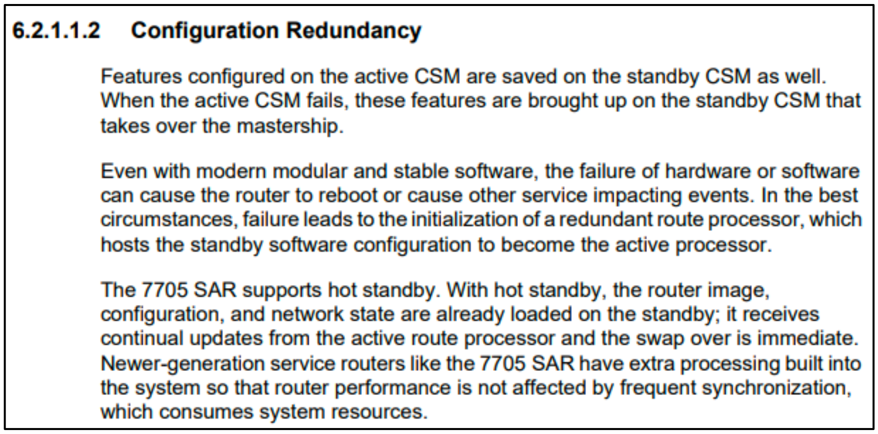


5.2.10.1 FDB Size

The following MAC table management features are required for each instance of a SAP or spoke SDP within a particular VPLS instance:

- MAC FDB size limits—allows users to specify the maximum number of MAC FDB entries that are learned locally for a SAP or a spoke SDP. If the configured limit is reached, then no new addresses will be learned from the SAP until at least one FDB entry is aged out or cleared.
  - When the limit is reached on a SAP, packets with unknown source MAC addresses are still forwarded (this default behavior can be changed via configuration). By default, if the destination MAC address is known, it is forwarded based on the FDB, and if the destination MAC address is unknown, it is flooded. Alternatively, if discard unknown is enabled at the VPLS service level, any packets from unknown source MAC addresses are discarded at the SAP.
  - The log event "SAP MAC limit reached" is generated when the limit is reached. When the condition is cleared, the log event "SAP MAC Limit Reached Condition Cleared" is generated.
  - **disable-learning** allows users to disable the dynamic learning function on a SAP or a spoke SDP of a VPLS instance
  - **disable-aging** allows users to turn off aging for learned MAC addresses on a SAP or a spoke SDP of a VPLS instance

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE16308AAAATQZZA01_V1_7705%20SAR%20Services%20Guide%2020.4.R1.pdf **(Page 576 of PDF)**

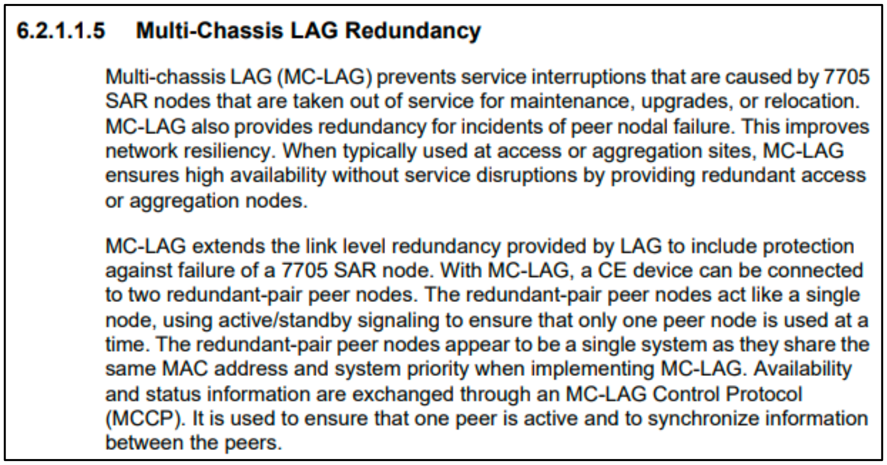


6.2.1.1.2 Configuration Redundancy

Features configured on the active CSM are saved on the standby CSM as well. When the active CSM fails, these features are brought up on the standby CSM that takes over the mastership.

Even with modern modular and stable software, the failure of hardware or software can cause the router to reboot or cause other service impacting events. In the best circumstances, failure leads to the initialization of a redundant route processor, which hosts the standby software configuration to become the active processor.

The 7705 SAR supports hot standby. With hot standby, the router image, configuration, and network state are already loaded on the standby; it receives continual updates from the active route processor and the swap over is immediate. Newer-generation service routers like the 7705 SAR have extra processing built into the system so that router performance is not affected by frequent synchronization, which consumes system resources.



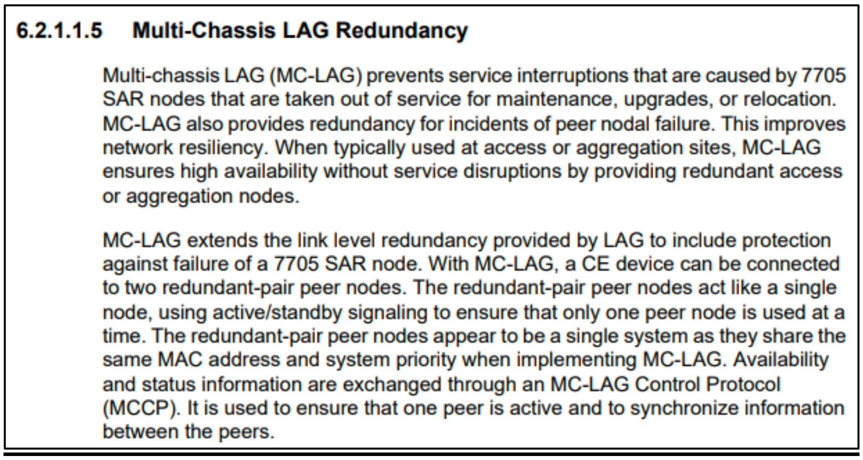
6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 239 and 240 of PDF)**

116. Defendants instruct its customers to configure Defendants' 7705 Service Aggregation Routers whereby upon a failure of the corresponding one of the primary virtual bridges, each of the backup virtual bridge forwards and receives the data packets over the network via the secondary virtual connections, in accordance with the synchronized forwarding table, in place of the corresponding one of the primary virtual bridges.



6.2.1.1.5 Multi-Chassis LAG Redundancy

Multi-chassis LAG (MC-LAG) prevents service interruptions that are caused by 7705 SAR nodes that are taken out of service for maintenance, upgrades, or relocation. MC-LAG also provides redundancy for incidents of peer nodal failure. This improves network resiliency. When typically used at access or aggregation sites, MC-LAG ensures high availability without service disruptions by providing redundant access or aggregation nodes.

MC-LAG extends the link level redundancy provided by LAG to include protection against failure of a 7705 SAR node. With MC-LAG, a CE device can be connected to two redundant-pair peer nodes. The redundant-pair peer nodes act like a single node, using active/standby signaling to ensure that only one peer node is used at a time. The redundant-pair peer nodes appear to be a single system as they share the same MAC address and system priority when implementing MC-LAG. Availability and status information are exchanged through an MC-LAG Control Protocol (MCCP). It is used to ensure that one peer is active and to synchronize information between the peers.

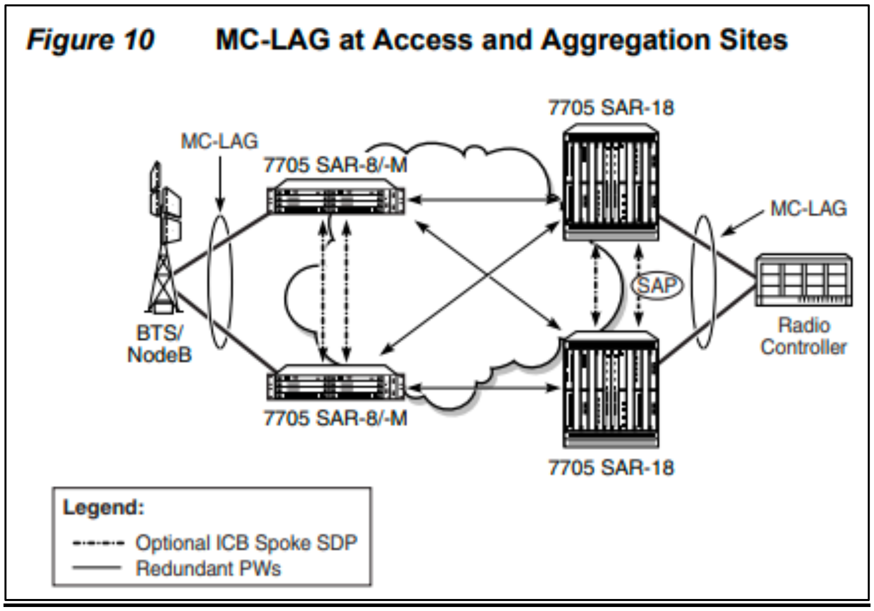
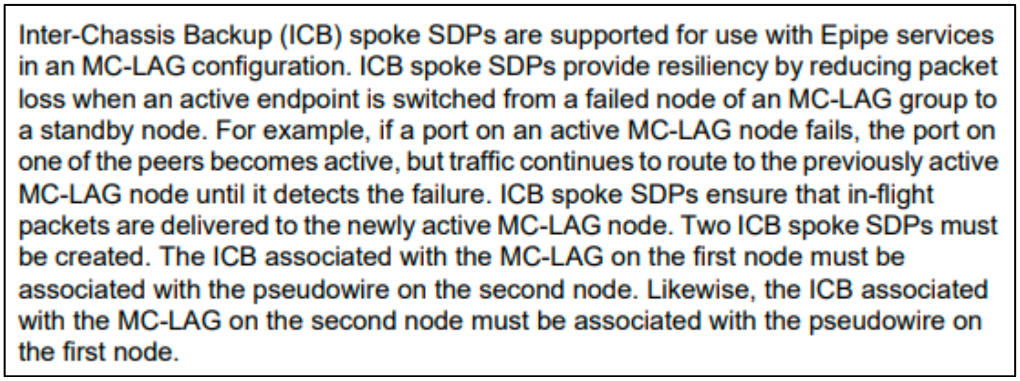


Figure 10 **MC-LAG at Access and Aggregation Sites**



Inter-Chassis Backup (ICB) spoke SDPs are supported for use with Epipe services in an MC-LAG configuration. ICB spoke SDPs provide resiliency by reducing packet loss when an active endpoint is switched from a failed node of an MC-LAG group to a standby node. For example, if a port on an active MC-LAG node fails, the port on one of the peers becomes active, but traffic continues to route to the previously active MC-LAG node until it detects the failure. ICB spoke SDPs ensure that in-flight packets are delivered to the newly active MC-LAG node. Two ICB spoke SDPs must be created. The ICB associated with the MC-LAG on the first node must be associated with the pseudowire on the second node. Likewise, the ICB associated with the MC-LAG on the second node must be associated with the pseudowire on the first node.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE17547AAABTQZZA01_V1_7705%20SAR%20Basic%20System%20Configuration%20Guide%2021.10.R1.pdf **(Pages 240 and 241 of PDF)**

117. As a result of Defendants' infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT FOUR
INFRINGEMENT OF U.S. PATENT 7,768,928

118. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-20 as if fully set forth herein.

119. The '928 Patent, entitled "CONNECTIVITY FAULT MANAGEMENT (CFM) IN NETWORKS WITH LINK AGGREGATION GROUP CONNECTIONS" was filed on July 11, 2006 and issued on August 3, 2010.

120. Plaintiff is the assignee and owner of all rights, title and interest to the '928 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

121. On April 16, 2021, IPR2021-00814 was filed on the '928 Patent challenging claims 1–3, 6, 7, 9–15, 18–24, 26, 27, and 30–32. On October 22, 2021, the Patent Trial and Appeal Board ("PTAB") denied institution of IPR2021-00814.

Technical Description

122. The '928 Patent addresses problems in the prior art of Ethernet service network maintenance, including that prior art CFM systems and techniques "cannot detect certain malfunctions" because "[w]hen a certain network such as a local area network (LAN) or a virtual-LAN (V-LAN) employs LAG interfaces, some of the connectivity fault management functions as currently specified by the IEEE 802.1ag Standard and ITU-T Recommendation Y.1731 cannot be utilized." (col. 2, ll. 31–36). When LAG interfaces are used, packets, which are forwarded from

one entity to another, are not sent via a known single fixed network link but via a set of aggregated output links that comprise a single logical port or link. *Id*. The packets are distributed among the links and therefore "the path of each packet cannot be predicted by the originating ME that initiates the CFM function. This could affect the reception of reply messages and performance results such as frame delay variation." *Id*.

123. The '928 Patent provides a solution to the problems in the prior art by providing "a system for implementing fault management functions in networks with LAG connections which are devoid of the above limitations." (col. 3, ll. 1–3). Specifically, the '928 Patent provides a technical solution to the problem by using a "maintenance entity operable in an Ethernet Connectivity Fault Management (CFM) domain. The maintenance entity comprises a port definer module and a connection configured to be connected to a group of aggregated links. The port definer module is configured to examine a designated link of the group by forwarding at least one CFM message via the designated link." (col. 3, ll. 5–14). "The port definer module is configured for allowing the separate examination of a designated link of the group of LAG members. The examination is done by facilitating the forwarding of CFM messages via the probed designated link." (col. 6, ll. 20–33).

Direct Infringement

124. Defendants, without authorization or license from Plaintiff, have been and are directly infringing the '928 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '928 Patent. Defendants develop, design, manufacture, and distribute telecommunications equipment that infringes one or more claims of the '928 Patent. Defendants further provides services that

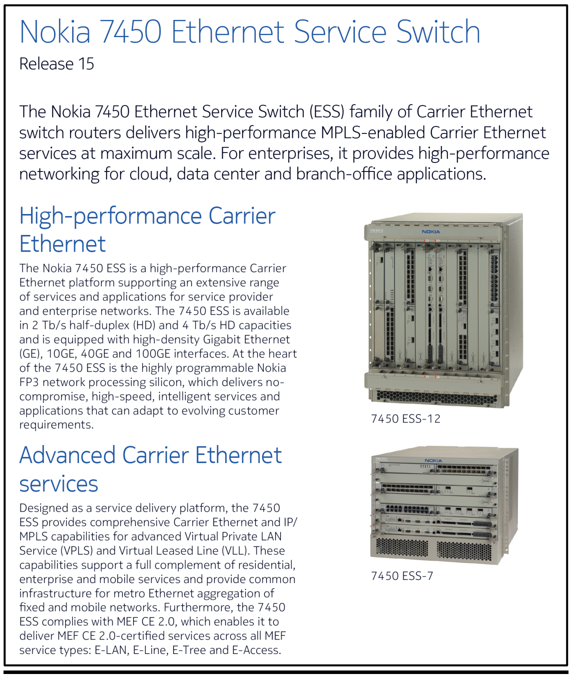
practice methods that infringe one or more claims of the ’928 Patent. Defendants are thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include 7450 Ethernet Service Switch, and all other substantially similar products (collectively the “’928 Accused Products”).

125. Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendants’ infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of ’928 Accused Products.

126. Defendants are liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, important, or distribution of Defendants’ 7450 Ethernet Service Switch.

127. Defendants’ 7450 Ethernet Service Switch is a non-limiting example of an apparatus that meets all limitations of claim 14 of the ’928 Patent, either literally or equivalently.

128. Defendants’ 7450 Ethernet Service Switch is a system for using Connectivity Fault Management (CFM) functions to examine aggregated link connections:



Nokia 7450 Ethernet Service Switch

Release 15

The Nokia 7450 Ethernet Service Switch (ESS) family of Carrier Ethernet switch routers delivers high-performance MPLS-enabled Carrier Ethernet services at maximum scale. For enterprises, it provides high-performance networking for cloud, data center and branch-office applications.

High-performance Carrier Ethernet

The Nokia 7450 ESS is a high-performance Carrier Ethernet platform supporting an extensive range of services and applications for service provider and enterprise networks. The 7450 ESS is available in 2 Tb/s half-duplex (HD) and 4 Tb/s HD capacities and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces. At the heart of the 7450 ESS is the highly programmable Nokia FP3 network processing silicon, which delivers no-compromise, high-speed, intelligent services and applications that can adapt to evolving customer requirements.

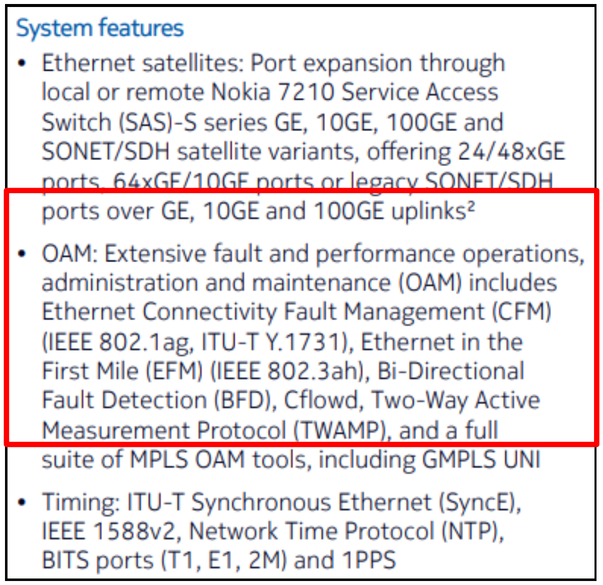
7450 ESS-12

Advanced Carrier Ethernet services

Designed as a service delivery platform, the 7450 ESS provides comprehensive Carrier Ethernet and IP/MPLS capabilities for advanced Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL). These capabilities support a full complement of residential, enterprise and mobile services and provide common infrastructure for metro Ethernet aggregation of fixed and mobile networks. Furthermore, the 7450 ESS complies with MEF CE 2.0, which enables it to deliver MEF CE 2.0-certified services across all MEF service types: E-LAN, E-Line, E-Tree and E-Access.

7450 ESS-7

https://onestore.nokia.com/asset/164727 **(page 1)**

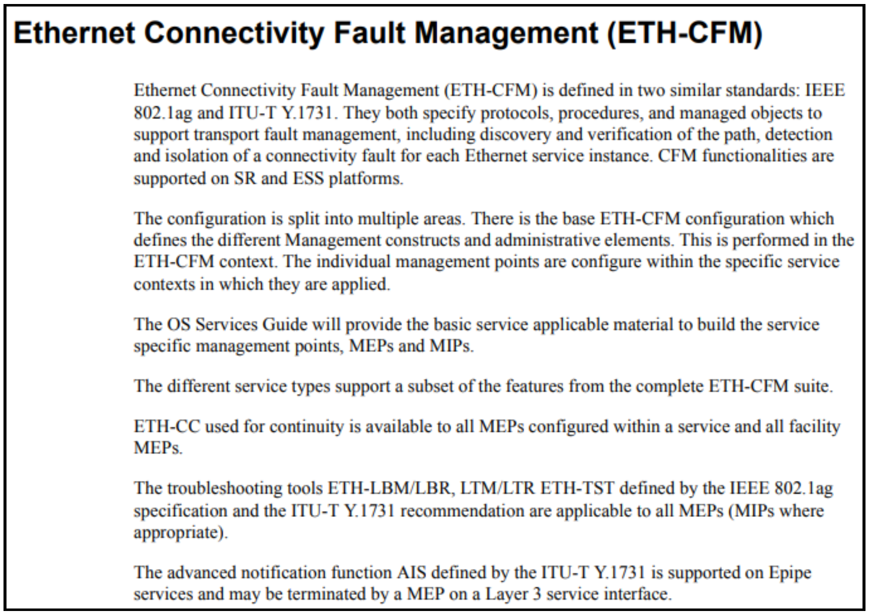


System features

- Ethernet satellites: Port expansion through local or remote Nokia 7210 Service Access Switch (SAS)-S series GE, 10GE, 100GE and SONET/SDH satellite variants, offering 24/48xGE ports, 64xGE/10GE ports or legacy SONET/SDH ports over GE, 10GE and 100GE uplinks[2]
- OAM: Extensive fault and performance operations, administration and maintenance (OAM) includes Ethernet Connectivity Fault Management (CFM) (IEEE 802.1ag, ITU-T Y.1731), Ethernet in the First Mile (EFM) (IEEE 802.3ah), Bi-Directional Fault Detection (BFD), Cflowd, Two-Way Active Measurement Protocol (TWAMP), and a full suite of MPLS OAM tools, including GMPLS UNI
- Timing: ITU-T Synchronous Ethernet (SyncE), IEEE 1588v2, Network Time Protocol (NTP), BITS ports (T1, E1, 2M) and 1PPS

https://onestore.nokia.com/asset/164727 **(page 6)**

129. Defendants' 7450 Ethernet Service Switch comprises a plurality of maintenance entities connected to a CFM domain, each one of said maintenance entities comprising a port definer module:



Ethernet Connectivity Fault Management (ETH-CFM)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in two similar standards: IEEE 802.1ag and ITU-T Y.1731. They both specify protocols, procedures, and managed objects to support transport fault management, including discovery and verification of the path, detection and isolation of a connectivity fault for each Ethernet service instance. CFM functionalities are supported on SR and ESS platforms.

The configuration is split into multiple areas. There is the base ETH-CFM configuration which defines the different Management constructs and administrative elements. This is performed in the ETH-CFM context. The individual management points are configure within the specific service contexts in which they are applied.

The OS Services Guide will provide the basic service applicable material to build the service specific management points, MEPs and MIPs.

The different service types support a subset of the features from the complete ETH-CFM suite.

ETH-CC used for continuity is available to all MEPs configured within a service and all facility MEPs.

The troubleshooting tools ETH-LBM/LBR, LTM/LTR ETH-TST defined by the IEEE 802.1ag specification and the ITU-T Y.1731 recommendation are applicable to all MEPs (MIPs where appropriate).

The advanced notification function AIS defined by the ITU-T Y.1731 is supported on Epipe services and may be terminated by a MEP on a Layer 3 service interface.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 102)**

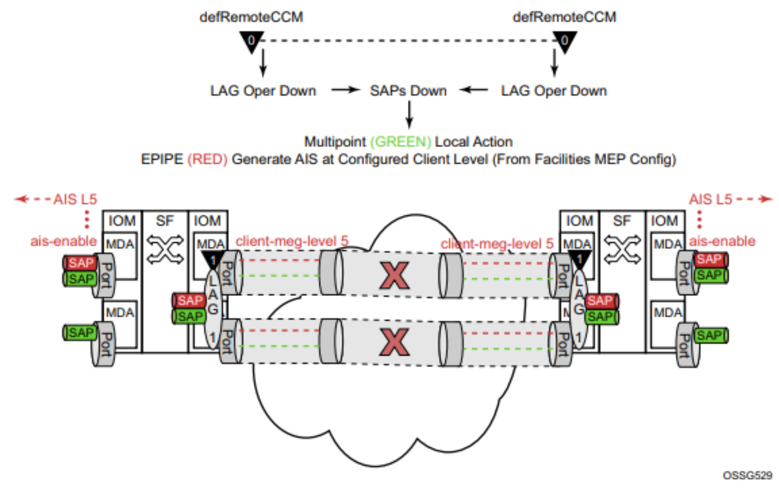


Figure 29: Fault Handling LAG MEP

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 120-121)**

130. Defendants' 7450 Ethernet Service Switch comprises at least one group of aggregated physical links comprising a single logical link, configured for connecting a first and a second of said plurality of maintenance entities:

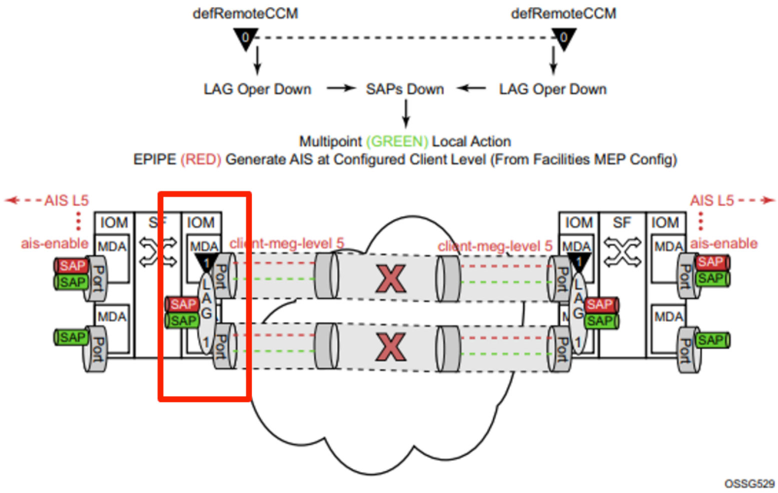
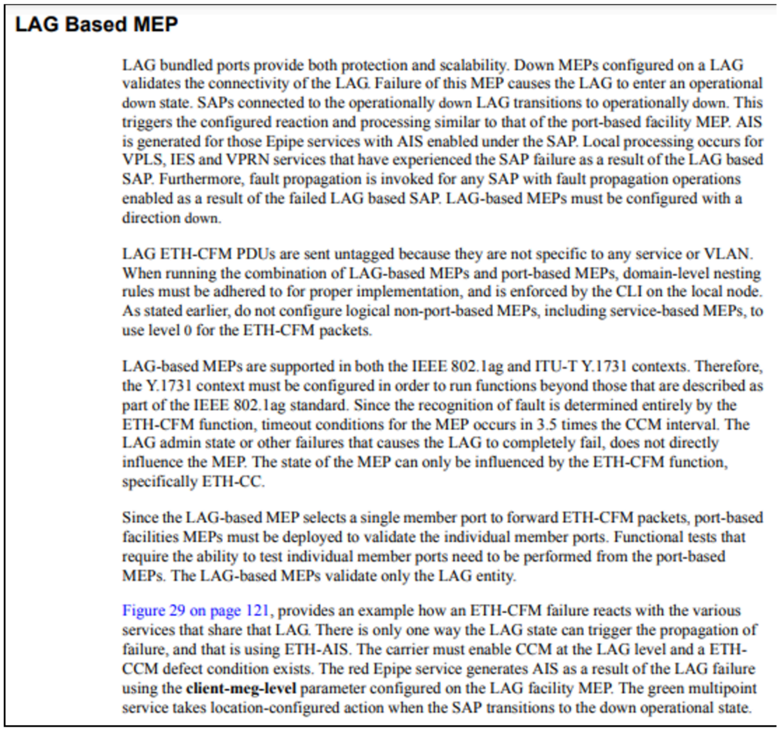


Figure 29: Fault Handling LAG MEP

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 120)**



LAG Based MEP

LAG bundled ports provide both protection and scalability. Down MEPs configured on a LAG validates the connectivity of the LAG. Failure of this MEP causes the LAG to enter an operational down state. SAPs connected to the operationally down LAG transitions to operationally down. This triggers the configured reaction and processing similar to that of the port-based facility MEP. AIS is generated for those Epipe services with AIS enabled under the SAP. Local processing occurs for VPLS, IES and VPRN services that have experienced the SAP failure as a result of the LAG based SAP. Furthermore, fault propagation is invoked for any SAP with fault propagation operations enabled as a result of the failed LAG based SAP. LAG-based MEPs must be configured with a direction down.

LAG ETH-CFM PDUs are sent untagged because they are not specific to any service or VLAN. When running the combination of LAG-based MEPs and port-based MEPs, domain-level nesting rules must be adhered to for proper implementation, and is enforced by the CLI on the local node. As stated earlier, do not configure logical non-port-based MEPs, including service-based MEPs, to use level 0 for the ETH-CFM packets.

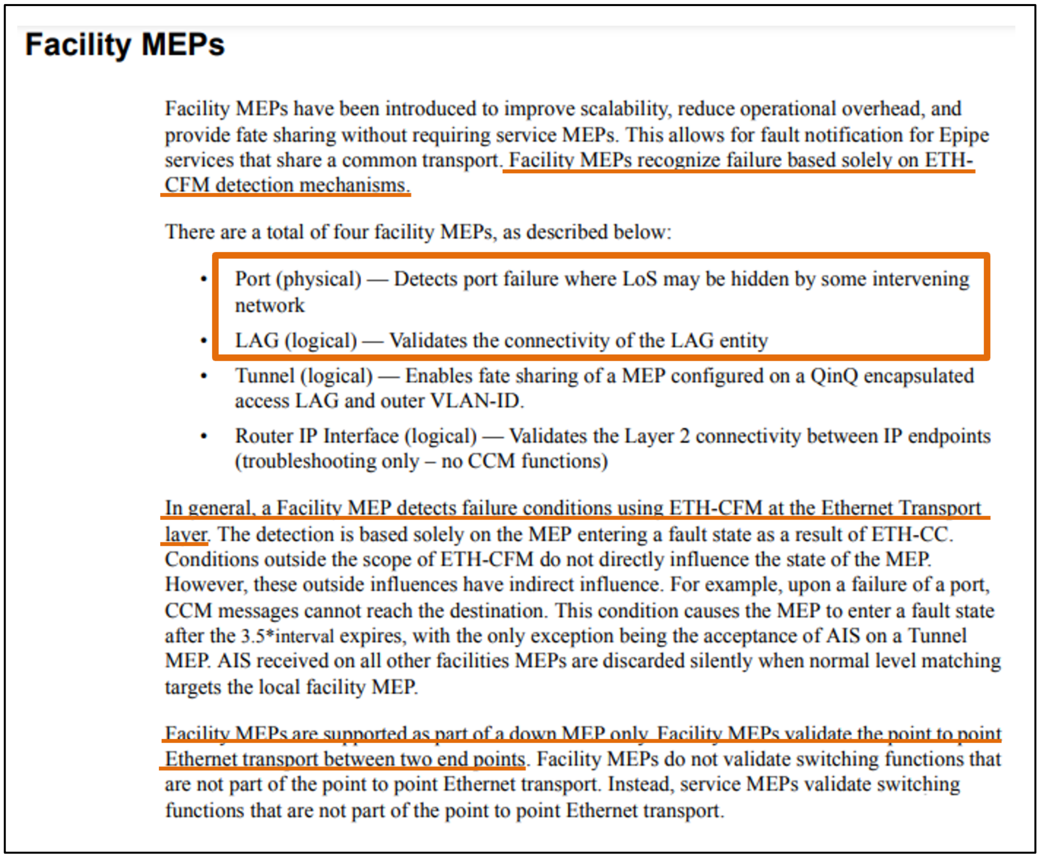
LAG-based MEPs are supported in both the IEEE 802.1ag and ITU-T Y.1731 contexts. Therefore, the Y.1731 context must be configured in order to run functions beyond those that are described as part of the IEEE 802.1ag standard. Since the recognition of fault is determined entirely by the ETH-CFM function, timeout conditions for the MEP occurs in 3.5 times the CCM interval. The LAG admin state or other failures that causes the LAG to completely fail, does not directly influence the MEP. The state of the MEP can only be influenced by the ETH-CFM function, specifically ETH-CC.

Since the LAG-based MEP selects a single member port to forward ETH-CFM packets, port-based facilities MEPs must be deployed to validate the individual member ports. Functional tests that require the ability to test individual member ports need to be performed from the port-based MEPs. The LAG-based MEPs validate only the LAG entity.

Figure 29 on page 121, provides an example how an ETH-CFM failure reacts with the various services that share that LAG. There is only one way the LAG state can trigger the propagation of failure, and that is using ETH-AIS. The carrier must enable CCM at the LAG level and a ETH-CCM defect condition exists. The red Epipe service generates AIS as a result of the LAG failure using the **client-meg-level** parameter configured on the LAG facility MEP. The green multipoint service takes location-configured action when the SAP transitions to the down operational state.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 121)**

131. Defendants' 7450 Ethernet Service Switch comprises the port definer module of said first maintenance entity being configured to designate any physical link as required of said single logical link, and examine said designated link of said single logical link by forwarding at least one CFM message to said second maintenance entity via said logical link in such a way that said CFM message is passed specifically via said designated physical link, thereby to allow examination of any physical link of said single logical link:



Facility MEPs

Facility MEPs have been introduced to improve scalability, reduce operational overhead, and provide fate sharing without requiring service MEPs. This allows for fault notification for Epipe services that share a common transport. Facility MEPs recognize failure based solely on ETH-CFM detection mechanisms.

There are a total of four facility MEPs, as described below:

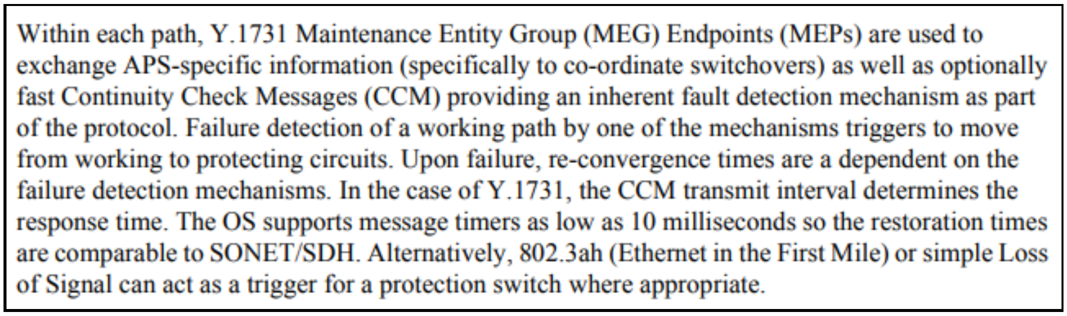
- Port (physical) — Detects port failure where LoS may be hidden by some intervening network
- LAG (logical) — Validates the connectivity of the LAG entity
- Tunnel (logical) — Enables fate sharing of a MEP configured on a QinQ encapsulated access LAG and outer VLAN-ID.
- Router IP Interface (logical) — Validates the Layer 2 connectivity between IP endpoints (troubleshooting only – no CCM functions)

In general, a Facility MEP detects failure conditions using ETH-CFM at the Ethernet Transport layer. The detection is based solely on the MEP entering a fault state as a result of ETH-CC. Conditions outside the scope of ETH-CFM do not directly influence the state of the MEP. However, these outside influences have indirect influence. For example, upon a failure of a port, CCM messages cannot reach the destination. This condition causes the MEP to enter a fault state after the 3.5*interval expires, with the only exception being the acceptance of AIS on a Tunnel MEP. AIS received on all other facilities MEPs are discarded silently when normal level matching targets the local facility MEP.

Facility MEPs are supported as part of a down MEP only. Facility MEPs validate the point to point Ethernet transport between two end points. Facility MEPs do not validate switching functions that are not part of the point to point Ethernet transport. Instead, service MEPs validate switching functions that are not part of the point to point Ethernet transport.

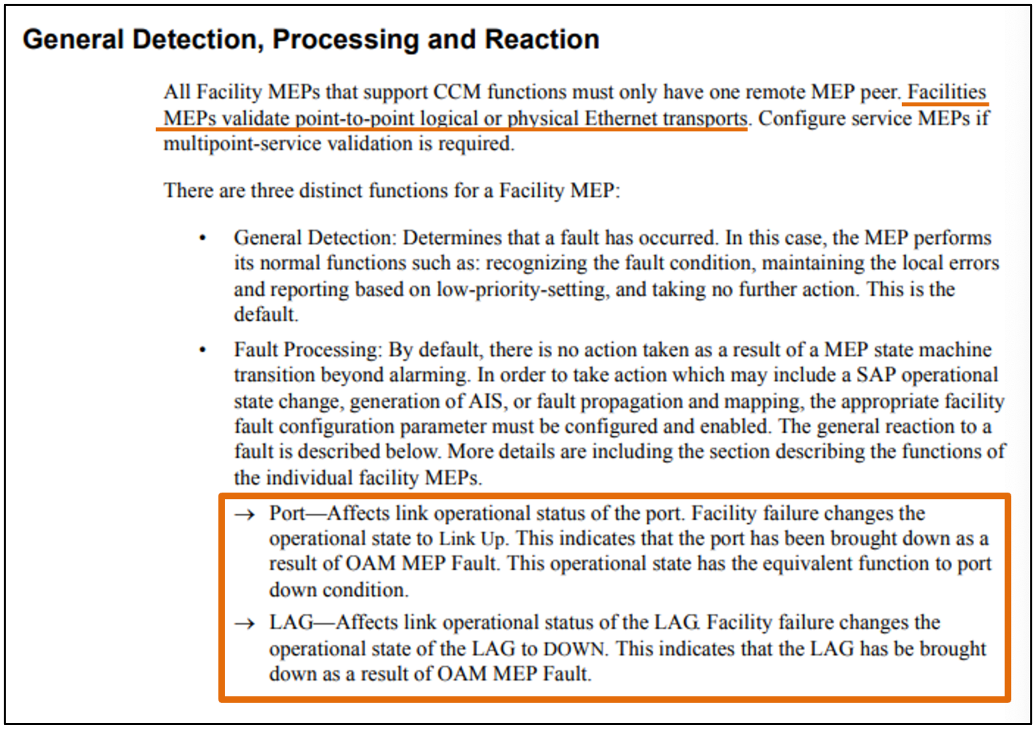
https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 106)**

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 110)**



Within each path, Y.1731 Maintenance Entity Group (MEG) Endpoints (MEPs) are used to exchange APS-specific information (specifically to co-ordinate switchovers) as well as optionally fast Continuity Check Messages (CCM) providing an inherent fault detection mechanism as part of the protocol. Failure detection of a working path by one of the mechanisms triggers to move from working to protecting circuits. Upon failure, re-convergence times are a dependent on the failure detection mechanisms. In the case of Y.1731, the CCM transmit interval determines the response time. The OS supports message timers as low as 10 milliseconds so the restoration times are comparable to SONET/SDH. Alternatively, 802.3ah (Ethernet in the First Mile) or simple Loss of Signal can act as a trigger for a protection switch where appropriate.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 64)**



General Detection, Processing and Reaction

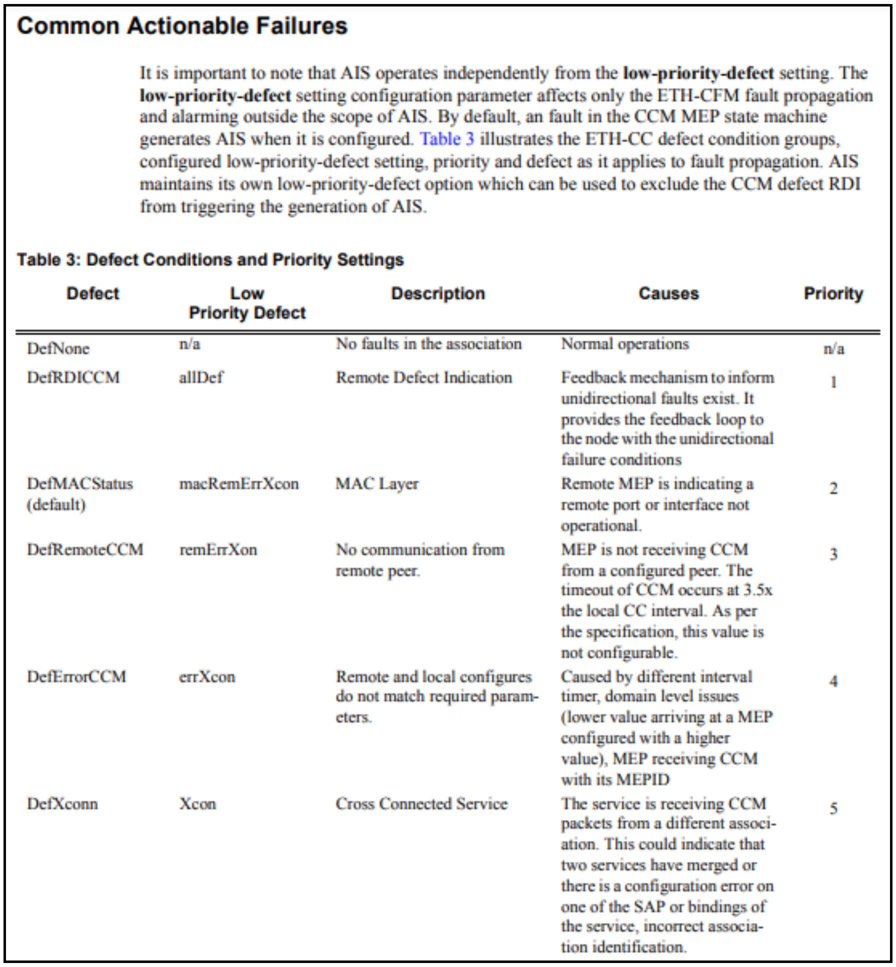
All Facility MEPs that support CCM functions must only have one remote MEP peer. Facilities MEPs validate point-to-point logical or physical Ethernet transports. Configure service MEPs if multipoint-service validation is required.

There are three distinct functions for a Facility MEP:

- General Detection: Determines that a fault has occurred. In this case, the MEP performs its normal functions such as: recognizing the fault condition, maintaining the local errors and reporting based on low-priority-setting, and taking no further action. This is the default.
- Fault Processing: By default, there is no action taken as a result of a MEP state machine transition beyond alarming. In order to take action which may include a SAP operational state change, generation of AIS, or fault propagation and mapping, the appropriate facility fault configuration parameter must be configured and enabled. The general reaction to a fault is described below. More details are including the section describing the functions of the individual facility MEPs.

→ Port—Affects link operational status of the port. Facility failure changes the operational state to Link Up. This indicates that the port has been brought down as a result of OAM MEP Fault. This operational state has the equivalent function to port down condition.

→ LAG—Affects link operational status of the LAG. Facility failure changes the operational state of the LAG to DOWN. This indicates that the LAG has be brought down as a result of OAM MEP Fault.



Common Actionable Failures

It is important to note that AIS operates independently from the **low-priority-defect** setting. The **low-priority-defect** setting configuration parameter affects only the ETH-CFM fault propagation and alarming outside the scope of AIS. By default, an fault in the CCM MEP state machine generates AIS when it is configured. Table 3 illustrates the ETH-CC defect condition groups, configured low-priority-defect setting, priority and defect as it applies to fault propagation. AIS maintains its own low-priority-defect option which can be used to exclude the CCM defect RDI from triggering the generation of AIS.

Table 3: Defect Conditions and Priority Settings

Defect	Low Priority Defect	Description	Causes	Priority
DefNone	n/a	No faults in the association	Normal operations	n/a
DefRDICCM	allDef	Remote Defect Indication	Feedback mechanism to inform unidirectional faults exist. It provides the feedback loop to the node with the unidirectional failure conditions	1
DefMACStatus (default)	macRemErrXcon	MAC Layer	Remote MEP is indicating a remote port or interface not operational.	2
DefRemoteCCM	remErrXon	No communication from remote peer.	MEP is not receiving CCM from a configured peer. The timeout of CCM occurs at 3.5x the local CC interval. As per the specification, this value is not configurable.	3
DefErrorCCM	errXcon	Remote and local configures do not match required parameters.	Caused by different interval timer, domain level issues (lower value arriving at a MEP configured with a higher value), MEP receiving CCM with its MEPID	4
DefXconn	Xcon	Cross Connected Service	The service is receiving CCM packets from a different association. This could indicate that two services have merged or there is a configuration error on one of the SAP or bindings of the service, incorrect association identification.	5

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 108)**

Willful Infringement

132. Defendants have had actual knowledge the ’928 Patent and its infringement thereof at least as of receipt of Plaintiff’s notice letter dated February 27, 2017.

133. Defendants have had actual knowledge of the ’928 Patent and its infringement thereof at least as of service of Plaintiff’s Complaint.

134. Defendants’ risk of infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendants.

135. Notwithstanding this knowledge, Defendants have knowingly or with reckless disregard willfully infringed the ’928 Patent. Defendants have thus had actual notice of the infringement of the ’928 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

136. This objective risk was either known or so obvious that it should have been known to Defendants. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

137. Defendants have induced and is knowingly inducing its customers and/or end users to directly infringe the ’928 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

138. Defendants have knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the ’928 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

139. Defendants’ indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe ’928 Patent.

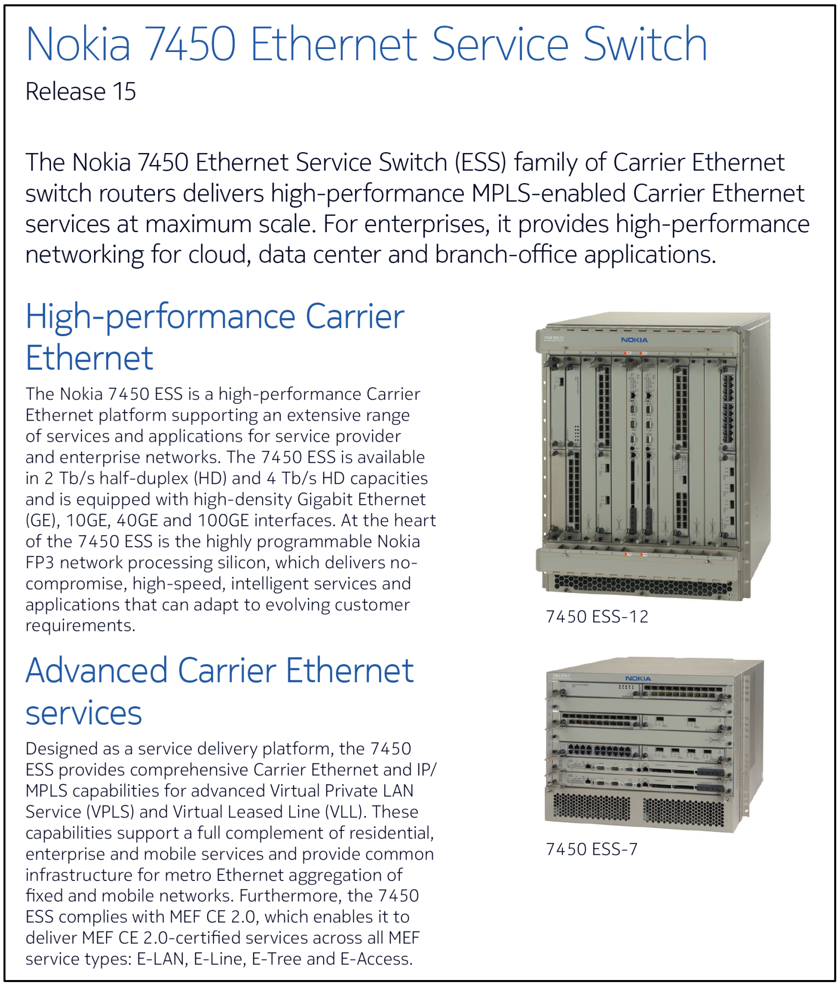
140. Defendants’ indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendants’ indirect infringement further includes providing application notes instructing its customers on infringing uses of the ’928 Accused Products. The ’928 Accused Products are designed in such a way that when they are used for their

intended purpose, the user infringes the ’928 Patent, either literally or equivalently. Defendants know and intend that customers who purchase the ’928 Accused Products will use those products for their intended purpose. For example, Defendants’ United States website: https://www.nokia.com, instructs customers to use the ’928 Accused Products in numerous infringing applications. Furthermore, Defendants provide instructions and other resources via its “Doc Center” (https://documentation.nokia.com), “Nokia Service Routing Certification” and training courses from its “NokiaEDU Training Centers” (https://www.nokia.com/networks/training/src/courses/#open-enrollment), and elsewhere on using the ’928 Accused Products. Defendants’ customers directly infringe the ’928 patent when they follow Defendants’ provided instructions on website, videos, and elsewhere. Defendants’ customers who follow Defendants’ provided instructions directly infringe claims of the ’928 Patent.

141. In addition, Defendants specifically intend that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendants’ infringing products. Defendants know following its instructions directly infringes claims of the ’928 Patent, including for example Claim 22.

142. Defendants’ customers who follow Defendants’ provided instructions directly infringe the method of claim 22 of the ’928 Patent.

143. Defendants instruct its customers use the 7450 Ethernet Service Switch to implement connectivity fault management (CFM) functions in a network.



Nokia 7450 Ethernet Service Switch

Release 15

The Nokia 7450 Ethernet Service Switch (ESS) family of Carrier Ethernet switch routers delivers high-performance MPLS-enabled Carrier Ethernet services at maximum scale. For enterprises, it provides high-performance networking for cloud, data center and branch-office applications.

High-performance Carrier Ethernet

The Nokia 7450 ESS is a high-performance Carrier Ethernet platform supporting an extensive range of services and applications for service provider and enterprise networks. The 7450 ESS is available in 2 Tb/s half-duplex (HD) and 4 Tb/s HD capacities and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces. At the heart of the 7450 ESS is the highly programmable Nokia FP3 network processing silicon, which delivers no-compromise, high-speed, intelligent services and applications that can adapt to evolving customer requirements.

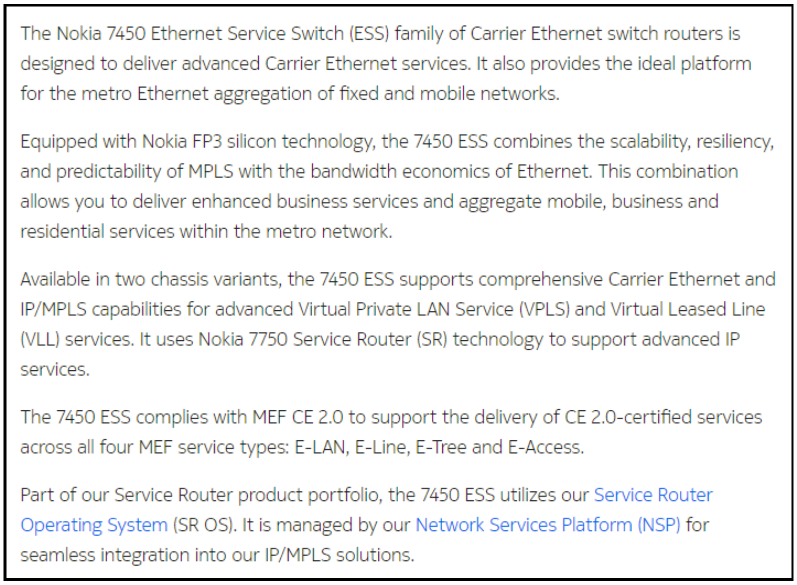
7450 ESS-12

Advanced Carrier Ethernet services

Designed as a service delivery platform, the 7450 ESS provides comprehensive Carrier Ethernet and IP/MPLS capabilities for advanced Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL). These capabilities support a full complement of residential, enterprise and mobile services and provide common infrastructure for metro Ethernet aggregation of fixed and mobile networks. Furthermore, the 7450 ESS complies with MEF CE 2.0, which enables it to deliver MEF CE 2.0-certified services across all MEF service types: E-LAN, E-Line, E-Tree and E-Access.

7450 ESS-7

https://onestore.nokia.com/asset/164727 **(page 1)**



The Nokia 7450 Ethernet Service Switch (ESS) family of Carrier Ethernet switch routers is designed to deliver advanced Carrier Ethernet services. It also provides the ideal platform for the metro Ethernet aggregation of fixed and mobile networks.

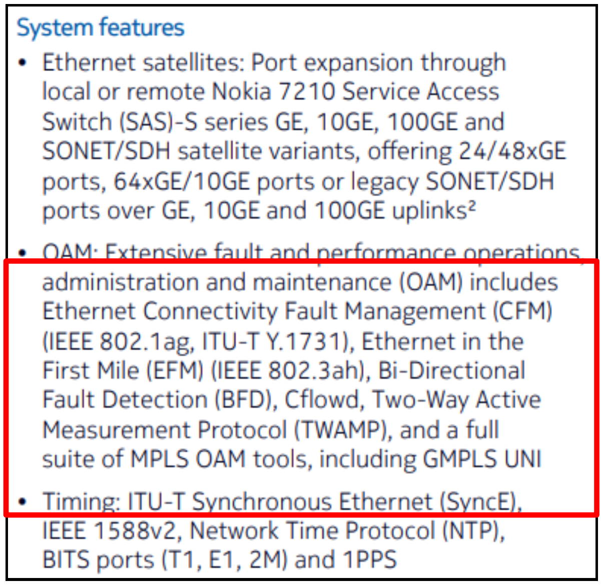
Equipped with Nokia FP3 silicon technology, the 7450 ESS combines the scalability, resiliency, and predictability of MPLS with the bandwidth economics of Ethernet. This combination allows you to deliver enhanced business services and aggregate mobile, business and residential services within the metro network.

Available in two chassis variants, the 7450 ESS supports comprehensive Carrier Ethernet and IP/MPLS capabilities for advanced Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL) services. It uses Nokia 7750 Service Router (SR) technology to support advanced IP services.

The 7450 ESS complies with MEF CE 2.0 to support the delivery of CE 2.0-certified services across all four MEF service types: E-LAN, E-Line, E-Tree and E-Access.

Part of our Service Router product portfolio, the 7450 ESS utilizes our Service Router Operating System (SR OS). It is managed by our Network Services Platform (NSP) for seamless integration into our IP/MPLS solutions.

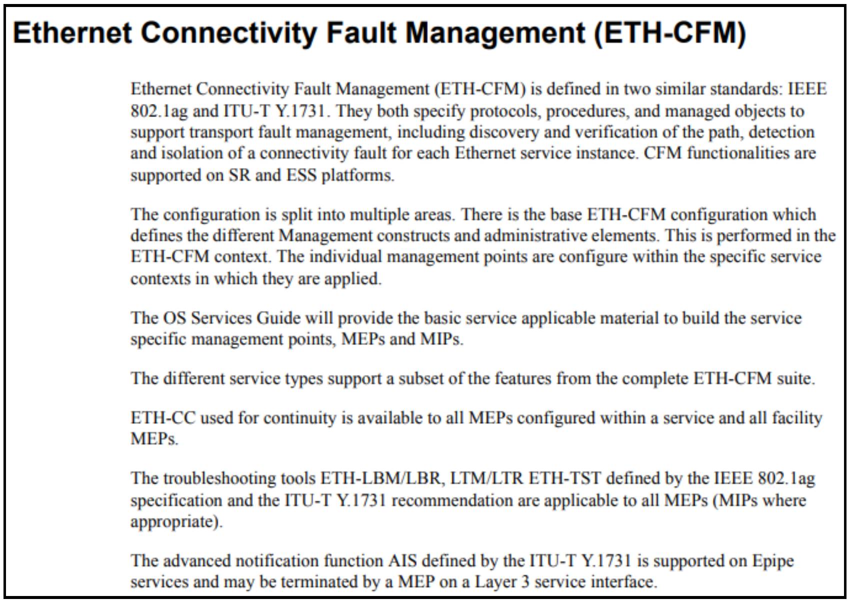
https://www.nokia.com/networks/products/7450-ethernet-service-switch/



System features

- Ethernet satellites: Port expansion through local or remote Nokia 7210 Service Access Switch (SAS)-S series GE, 10GE, 100GE and SONET/SDH satellite variants, offering 24/48xGE ports, 64xGE/10GE ports or legacy SONET/SDH ports over GE, 10GE and 100GE uplinks[2]
- OAM: Extensive fault and performance operations, administration and maintenance (OAM) includes Ethernet Connectivity Fault Management (CFM) (IEEE 802.1ag, ITU-T Y.1731), Ethernet in the First Mile (EFM) (IEEE 802.3ah), Bi-Directional Fault Detection (BFD), Cflowd, Two-Way Active Measurement Protocol (TWAMP), and a full suite of MPLS OAM tools, including GMPLS UNI
- Timing: ITU-T Synchronous Ethernet (SyncE), IEEE 1588v2, Network Time Protocol (NTP), BITS ports (T1, E1, 2M) and 1PPS

https://onestore.nokia.com/asset/164727 **(page 6)**



Ethernet Connectivity Fault Management (ETH-CFM)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in two similar standards: IEEE 802.1ag and ITU-T Y.1731. They both specify protocols, procedures, and managed objects to support transport fault management, including discovery and verification of the path, detection and isolation of a connectivity fault for each Ethernet service instance. CFM functionalities are supported on SR and ESS platforms.

The configuration is split into multiple areas. There is the base ETH-CFM configuration which defines the different Management constructs and administrative elements. This is performed in the ETH-CFM context. The individual management points are configure within the specific service contexts in which they are applied.

The OS Services Guide will provide the basic service applicable material to build the service specific management points, MEPs and MIPs.

The different service types support a subset of the features from the complete ETH-CFM suite.

ETH-CC used for continuity is available to all MEPs configured within a service and all facility MEPs.

The troubleshooting tools ETH-LBM/LBR, LTM/LTR ETH-TST defined by the IEEE 802.1ag specification and the ITU-T Y.1731 recommendation are applicable to all MEPs (MIPs where appropriate).

The advanced notification function AIS defined by the ITU-T Y.1731 is supported on Epipe services and may be terminated by a MEP on a Layer 3 service interface.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 102)**

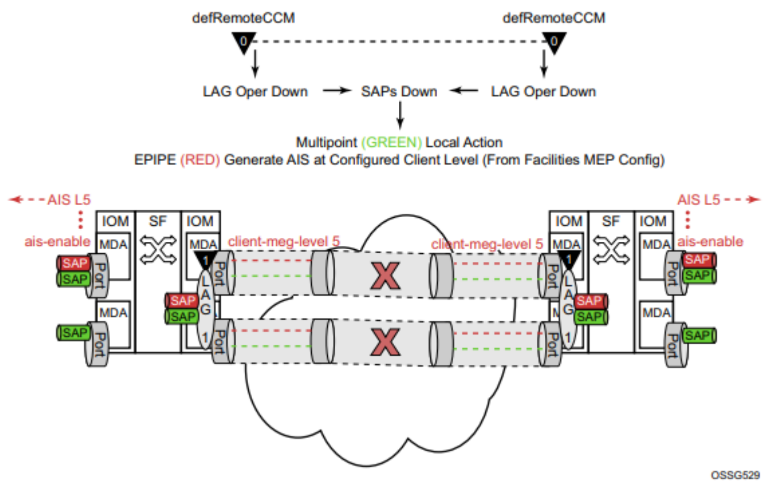
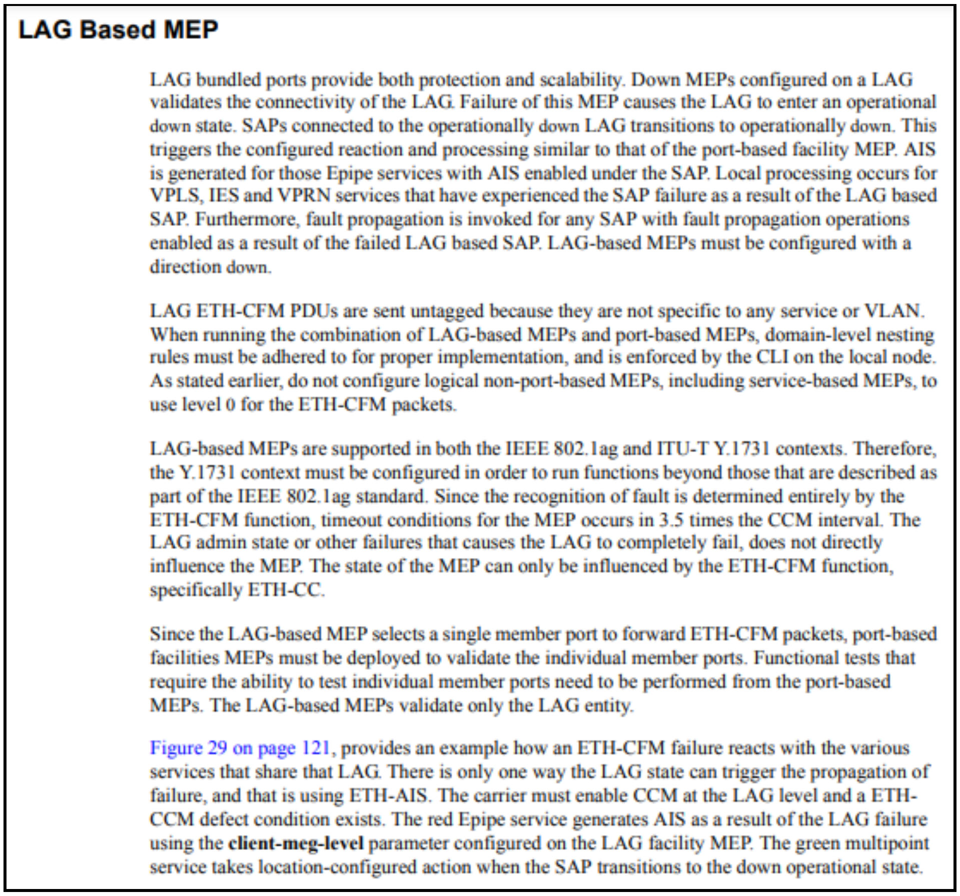


Figure 29: Fault Handling LAG MEP

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 120-121)**

144. Defendants instruct its customers use the 7450 Ethernet Service Switch to connect first and second maintenance entities via a link aggregation group (LAG), said LAG comprising a single logical link made up of a plurality of physical links:



LAG Based MEP

LAG bundled ports provide both protection and scalability. Down MEPs configured on a LAG validates the connectivity of the LAG. Failure of this MEP causes the LAG to enter an operational down state. SAPs connected to the operationally down LAG transitions to operationally down. This triggers the configured reaction and processing similar to that of the port-based facility MEP. AIS is generated for those Epipe services with AIS enabled under the SAP. Local processing occurs for VPLS, IES and VPRN services that have experienced the SAP failure as a result of the LAG based SAP. Furthermore, fault propagation is invoked for any SAP with fault propagation operations enabled as a result of the failed LAG based SAP. LAG-based MEPs must be configured with a direction down.

LAG ETH-CFM PDUs are sent untagged because they are not specific to any service or VLAN. When running the combination of LAG-based MEPs and port-based MEPs, domain-level nesting rules must be adhered to for proper implementation, and is enforced by the CLI on the local node. As stated earlier, do not configure logical non-port-based MEPs, including service-based MEPs, to use level 0 for the ETH-CFM packets.

LAG-based MEPs are supported in both the IEEE 802.1ag and ITU-T Y.1731 contexts. Therefore, the Y.1731 context must be configured in order to run functions beyond those that are described as part of the IEEE 802.1ag standard. Since the recognition of fault is determined entirely by the ETH-CFM function, timeout conditions for the MEP occurs in 3.5 times the CCM interval. The LAG admin state or other failures that causes the LAG to completely fail, does not directly influence the MEP. The state of the MEP can only be influenced by the ETH-CFM function, specifically ETH-CC.

Since the LAG-based MEP selects a single member port to forward ETH-CFM packets, port-based facilities MEPs must be deployed to validate the individual member ports. Functional tests that require the ability to test individual member ports need to be performed from the port-based MEPs. The LAG-based MEPs validate only the LAG entity.

Figure 29 on page 121, provides an example how an ETH-CFM failure reacts with the various services that share that LAG. There is only one way the LAG state can trigger the propagation of failure, and that is using ETH-AIS. The carrier must enable CCM at the LAG level and a ETH-CCM defect condition exists. The red Epipe service generates AIS as a result of the LAG failure using the **client-meg-level** parameter configured on the LAG facility MEP. The green multipoint service takes location-configured action when the SAP transitions to the down operational state.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 120)**

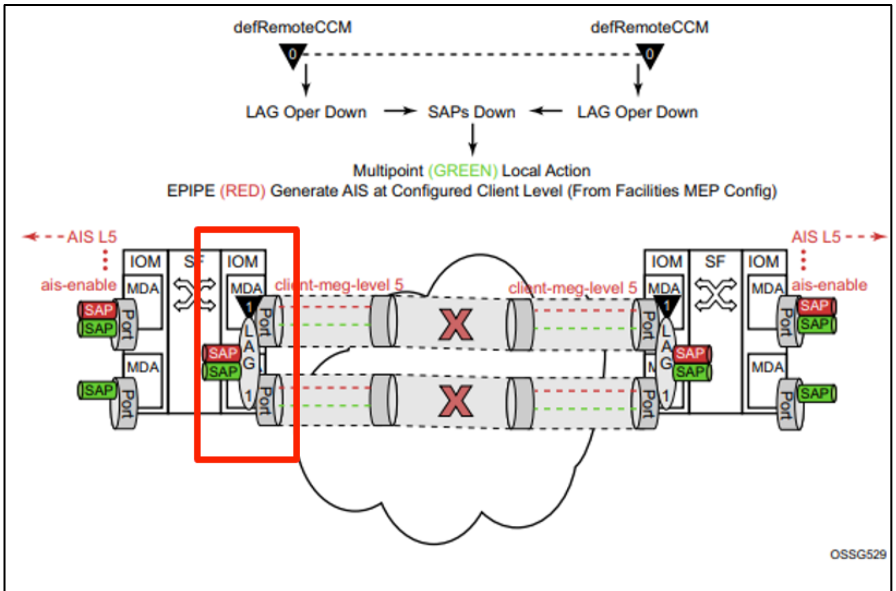
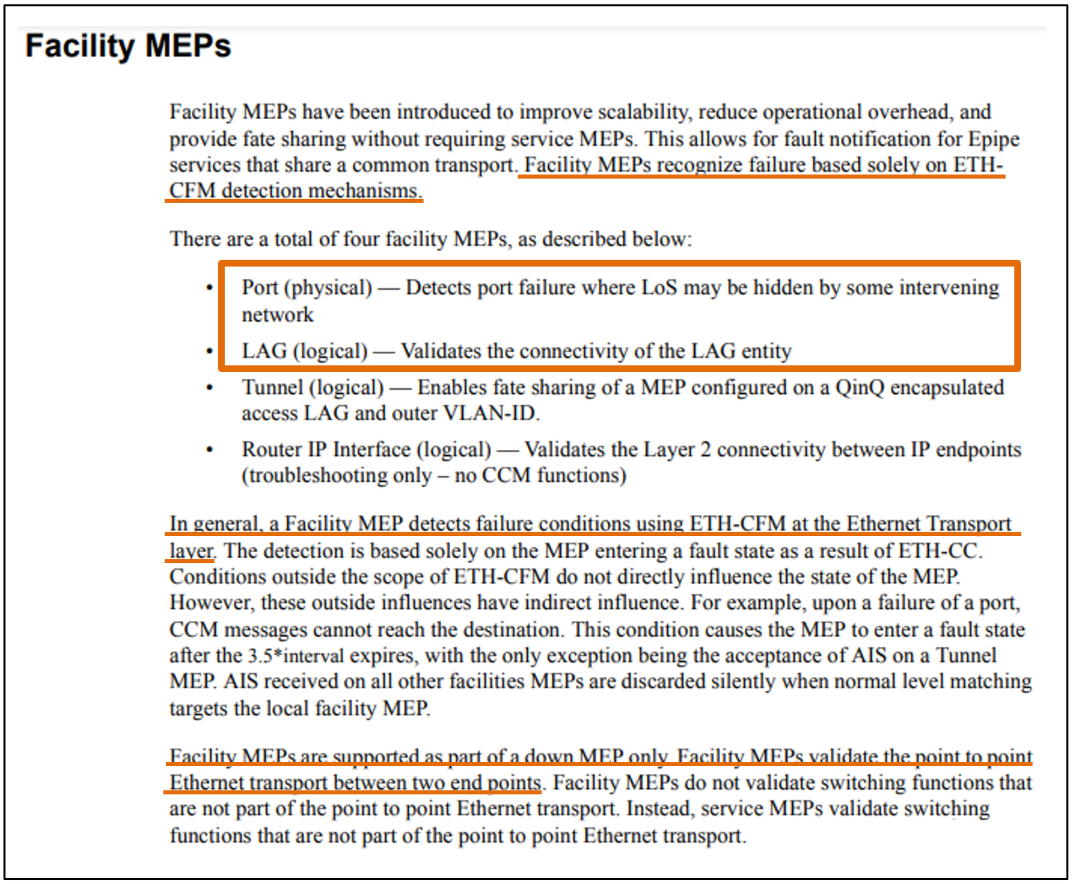


Figure 29: Fault Handling LAG MEP

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 121)**

145. Defendants instruct its customers use the 7450 Ethernet Service Switch to use said first maintenance entity to select one of said physical links as a designated link for forwarding a CFM message via a designated link of said LAG:



Facility MEPs

Facility MEPs have been introduced to improve scalability, reduce operational overhead, and provide fate sharing without requiring service MEPs. This allows for fault notification for Epipe services that share a common transport. Facility MEPs recognize failure based solely on ETH-CFM detection mechanisms.

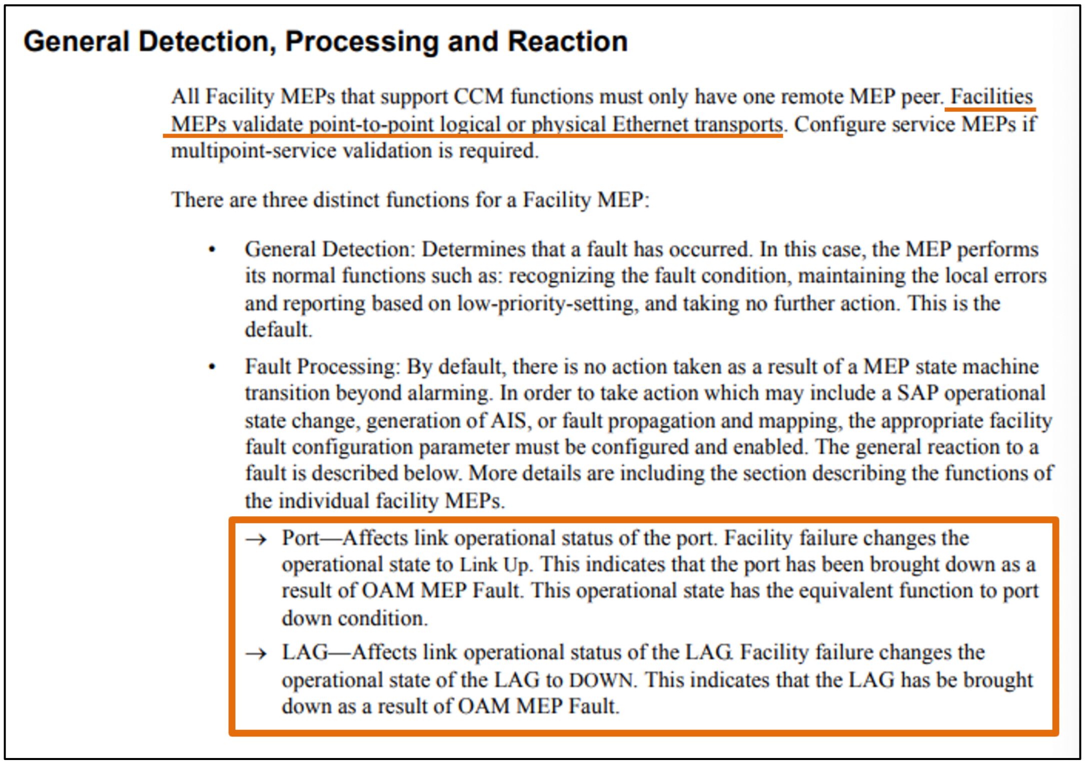
There are a total of four facility MEPs, as described below:

- Port (physical) — Detects port failure where LoS may be hidden by some intervening network
- LAG (logical) — Validates the connectivity of the LAG entity
- Tunnel (logical) — Enables fate sharing of a MEP configured on a QinQ encapsulated access LAG and outer VLAN-ID.
- Router IP Interface (logical) — Validates the Layer 2 connectivity between IP endpoints (troubleshooting only – no CCM functions)

In general, a Facility MEP detects failure conditions using ETH-CFM at the Ethernet Transport layer. The detection is based solely on the MEP entering a fault state as a result of ETH-CC. Conditions outside the scope of ETH-CFM do not directly influence the state of the MEP. However, these outside influences have indirect influence. For example, upon a failure of a port, CCM messages cannot reach the destination. This condition causes the MEP to enter a fault state after the 3.5*interval expires, with the only exception being the acceptance of AIS on a Tunnel MEP. AIS received on all other facilities MEPs are discarded silently when normal level matching targets the local facility MEP.

Facility MEPs are supported as part of a down MEP only. Facility MEPs validate the point to point Ethernet transport between two end points. Facility MEPs do not validate switching functions that are not part of the point to point Ethernet transport. Instead, service MEPs validate switching functions that are not part of the point to point Ethernet transport.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 106)**



General Detection, Processing and Reaction

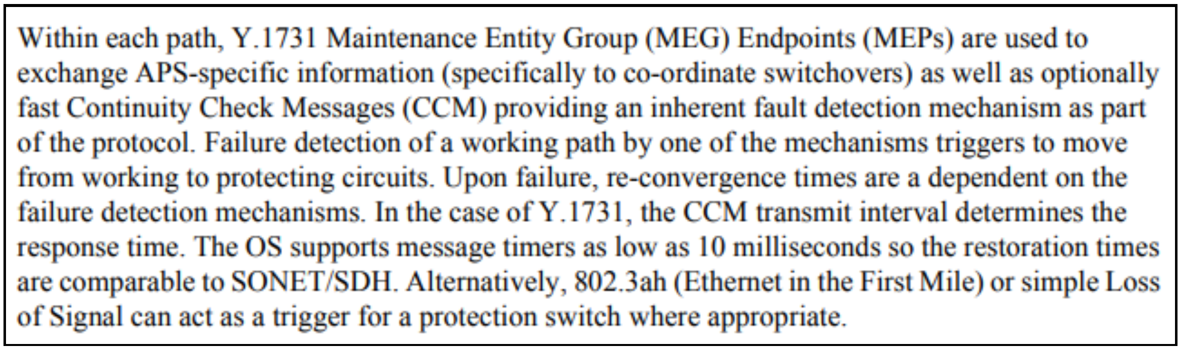
All Facility MEPs that support CCM functions must only have one remote MEP peer. Facilities MEPs validate point-to-point logical or physical Ethernet transports. Configure service MEPs if multipoint-service validation is required.

There are three distinct functions for a Facility MEP:

- General Detection: Determines that a fault has occurred. In this case, the MEP performs its normal functions such as: recognizing the fault condition, maintaining the local errors and reporting based on low-priority-setting, and taking no further action. This is the default.
- Fault Processing: By default, there is no action taken as a result of a MEP state machine transition beyond alarming. In order to take action which may include a SAP operational state change, generation of AIS, or fault propagation and mapping, the appropriate facility fault configuration parameter must be configured and enabled. The general reaction to a fault is described below. More details are including the section describing the functions of the individual facility MEPs.
  - → Port—Affects link operational status of the port. Facility failure changes the operational state to Link Up. This indicates that the port has been brought down as a result of OAM MEP Fault. This operational state has the equivalent function to port down condition.
  - → LAG—Affects link operational status of the LAG. Facility failure changes the operational state of the LAG to DOWN. This indicates that the LAG has be brought down as a result of OAM MEP Fault.

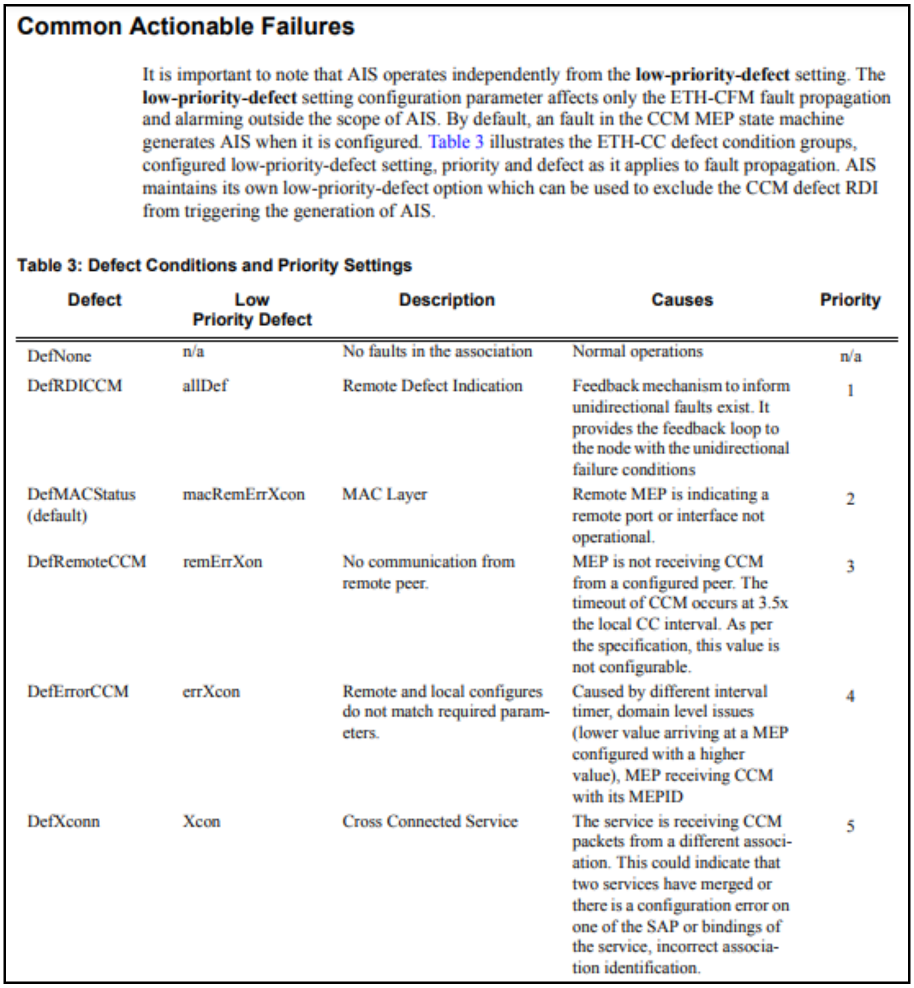
https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 110)**

146. Defendants instruct its customers use the 7450 Ethernet Service Switch to verify the functioning of said designated link by analyzing the outcome of said forwarding, each of said physical links being selectable as said designated link, thereby to provide for examination as required for any physical link of said group comprising said single logical link:



Within each path, Y.1731 Maintenance Entity Group (MEG) Endpoints (MEPs) are used to exchange APS-specific information (specifically to co-ordinate switchovers) as well as optionally fast Continuity Check Messages (CCM) providing an inherent fault detection mechanism as part of the protocol. Failure detection of a working path by one of the mechanisms triggers to move from working to protecting circuits. Upon failure, re-convergence times are a dependent on the failure detection mechanisms. In the case of Y.1731, the CCM transmit interval determines the response time. The OS supports message timers as low as 10 milliseconds so the restoration times are comparable to SONET/SDH. Alternatively, 802.3ah (Ethernet in the First Mile) or simple Loss of Signal can act as a trigger for a protection switch where appropriate.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 64)**



Common Actionable Failures

It is important to note that AIS operates independently from the **low-priority-defect** setting. The **low-priority-defect** setting configuration parameter affects only the ETH-CFM fault propagation and alarming outside the scope of AIS. By default, an fault in the CCM MEP state machine generates AIS when it is configured. Table 3 illustrates the ETH-CC defect condition groups, configured low-priority-defect setting, priority and defect as it applies to fault propagation. AIS maintains its own low-priority-defect option which can be used to exclude the CCM defect RDI from triggering the generation of AIS.

Table 3: Defect Conditions and Priority Settings

Defect	Low Priority Defect	Description	Causes	Priority
DefNone	n/a	No faults in the association	Normal operations	n/a
DefRDICCM	allDef	Remote Defect Indication	Feedback mechanism to inform unidirectional faults exist. It provides the feedback loop to the node with the unidirectional failure conditions	1
DefMACStatus (default)	macRemErrXcon	MAC Layer	Remote MEP is indicating a remote port or interface not operational.	2
DefRemoteCCM	remErrXon	No communication from remote peer.	MEP is not receiving CCM from a configured peer. The timeout of CCM occurs at 3.5x the local CC interval. As per the specification, this value is not configurable.	3
DefErrorCCM	errXcon	Remote and local configures do not match required parameters.	Caused by different interval timer, domain level issues (lower value arriving at a MEP configured with a higher value), MEP receiving CCM with its MEPID	4
DefXconn	Xcon	Cross Connected Service	The service is receiving CCM packets from a different association. This could indicate that two services have merged or there is a configuration error on one of the SAP or bindings of the service, incorrect association identification.	5

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301071102_V1_7450%20ESS%20OS%20Services%20Guide%2012.0.R4.pdf **(page 108)**

147. As a result of Defendants' infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT FIVE
INFRINGEMENT OF U.S. PATENT 7,983,150

148. Plaintiff incorporates by reference the allegations in all preceding paragraphs as if fully set forth herein.

149. The ’150 Patent, entitled “VPLS FAILURE PROTECTION IN RING NETWORKS” was filed on January 18, 2006 and issued on July 19, 2011.

150. Plaintiff is the assignee and owner of all rights, title and interest to the ’150 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

151. On January 26, 2021, IPR2021-00469 was filed on the ‘150 Patent challenging claims 1–5, 8–15, and 18–20. On August 8, 2022, the Patent Trial and Appeal Board (“PTAB”) in a final written decision upheld the patentability of claims 1–5, 8–15, and 18–20.

Technical Description

152. The ’150 Patent addresses technical problems in the prior art of virtual private networks, including that prior art failure protection mechanisms in bi-directional ring networks “do not adequately protect against all failure scenarios that may occur in a VPLS that is provisioned over the ring.” (col. 2, ll. 40‒42).

153. The ’150 Patent provides a technical solution to the prior art problems by providing “failure protection mechanisms that can respond to and overcome these sorts of VPLS failure scenarios quickly and efficiently.” (col. 2, ll. 51‒53).

154. The ’150 Patent discloses the use of standby connection termination points (CTPs) in a virtual private LAN service. “Each CTP connects the respective node to a network external to the ring network. In the absence of a network failure, these standby CTPs are blocked. When a failure occurs, the nodes in the ring network exchange topology messages and inform one another

of the failure. Based on these messages, the nodes may determine that the VPLS has been segmented. In this case, the nodes choose one or more of the standby CTPs to be activated in order to overcome the segmentation." (col. 2, ll. 56–64).

Direct Infringement

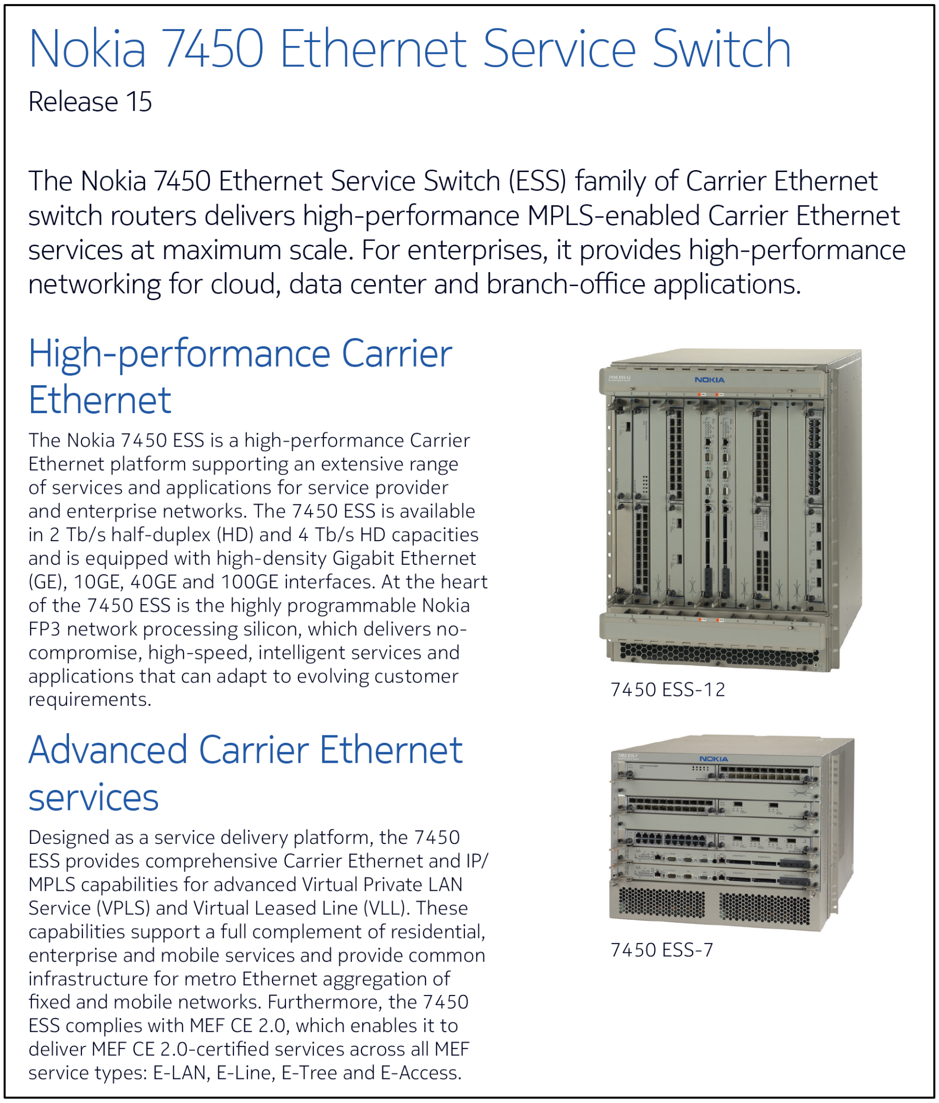
155. Defendants, without authorization or license from Plaintiff, have been and are directly infringing the '150 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), selling and offering for sale apparatus and methods infringing one or more claims of the '150 Patent. Defendants develop, design, manufacture, and distribute telecommunications equipment that infringe one or more claims of the '150 Patent. Defendants further provide services that practice methods that infringe one or more claims of the '150 Patent. Defendants are thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Nokia 7450 Ethernet Service Switch, and all other substantially similar products (collectively the "'150 Accused Products").

156. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendants' infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '150 Accused Products.

157. Defendants are liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendants' 7450 Ethernet Service Switch.

158. Defendants' 7450 Ethernet Service Switch is a non-limiting example of switches that operate to meet all limitations of claim 11 of the '150 Patent, either literally or equivalently.

159. Defendants' 7450 Ethernet Service Switch is a system for communication comprising nodes connected by spans so as to define a bi-directional ring network, over which a virtual private local area network service (VPLS) is provisioned to serve users:



Nokia 7450 Ethernet Service Switch

Release 15

The Nokia 7450 Ethernet Service Switch (ESS) family of Carrier Ethernet switch routers delivers high-performance MPLS-enabled Carrier Ethernet services at maximum scale. For enterprises, it provides high-performance networking for cloud, data center and branch-office applications.

High-performance Carrier Ethernet

The Nokia 7450 ESS is a high-performance Carrier Ethernet platform supporting an extensive range of services and applications for service provider and enterprise networks. The 7450 ESS is available in 2 Tb/s half-duplex (HD) and 4 Tb/s HD capacities and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces. At the heart of the 7450 ESS is the highly programmable Nokia FP3 network processing silicon, which delivers no-compromise, high-speed, intelligent services and applications that can adapt to evolving customer requirements.

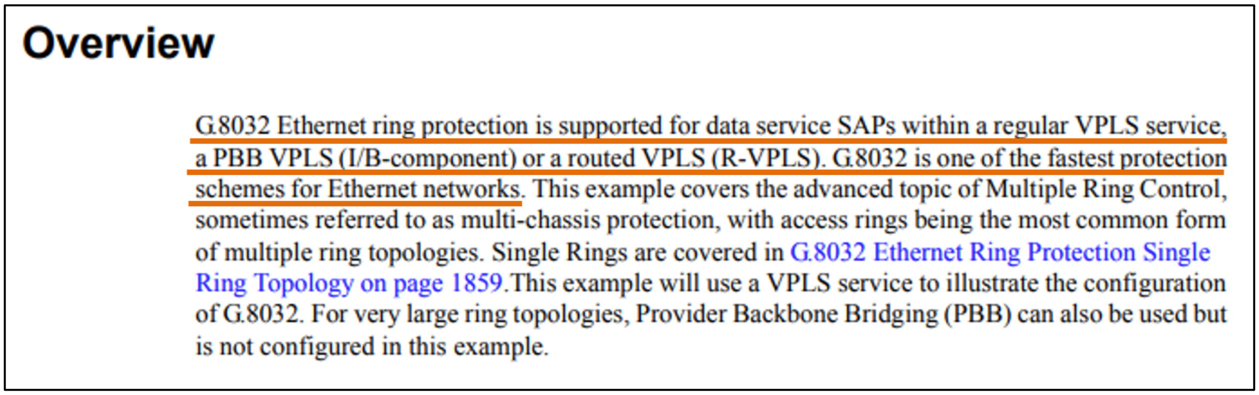
7450 ESS-12

Advanced Carrier Ethernet services

Designed as a service delivery platform, the 7450 ESS provides comprehensive Carrier Ethernet and IP/MPLS capabilities for advanced Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL). These capabilities support a full complement of residential, enterprise and mobile services and provide common infrastructure for metro Ethernet aggregation of fixed and mobile networks. Furthermore, the 7450 ESS complies with MEF CE 2.0, which enables it to deliver MEF CE 2.0-certified services across all MEF service types: E-LAN, E-Line, E-Tree and E-Access.

7450 ESS-7

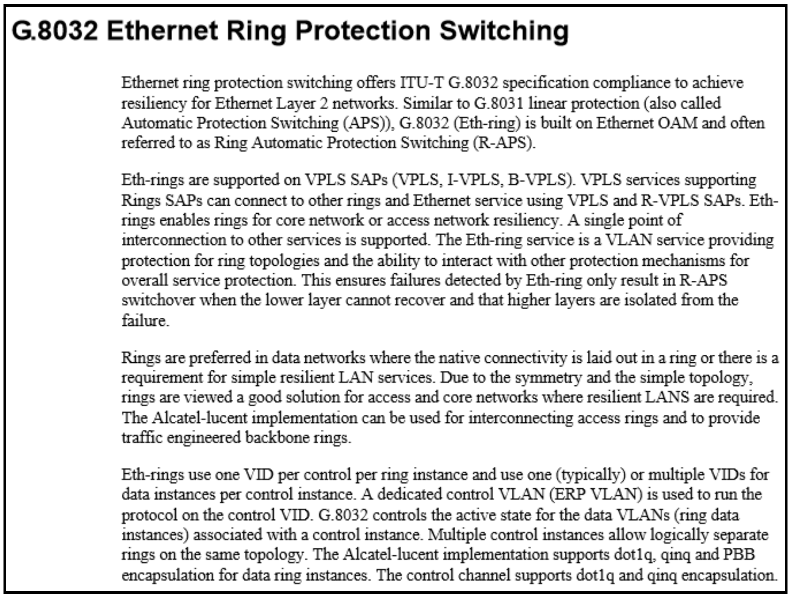
https://onestore.nokia.com/asset/164727 **(page 1)**



Overview

G.8032 Ethernet ring protection is supported for data service SAPs within a regular VPLS service, a PBB VPLS (I/B-component) or a routed VPLS (R-VPLS). G.8032 is one of the fastest protection schemes for Ethernet networks. This example covers the advanced topic of Multiple Ring Control, sometimes referred to as multi-chassis protection, with access rings being the most common form of multiple ring topologies. Single Rings are covered in G.8032 Ethernet Ring Protection Single Ring Topology on page 1859.This example will use a VPLS service to illustrate the configuration of G.8032. For very large ring topologies, Provider Backbone Bridging (PBB) can also be used but is not configured in this example.

https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/G8032-MultiRing.pdf **(page 5)**



G.8032 Ethernet Ring Protection Switching

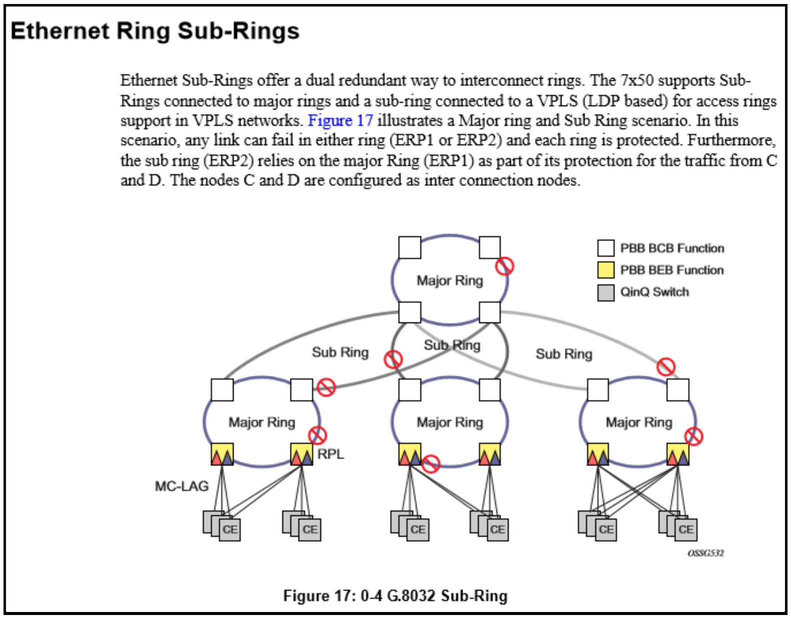
Ethernet ring protection switching offers ITU-T G.8032 specification compliance to achieve resiliency for Ethernet Layer 2 networks. Similar to G.8031 linear protection (also called Automatic Protection Switching (APS)), G.8032 (Eth-ring) is built on Ethernet OAM and often referred to as Ring Automatic Protection Switching (R-APS).

Eth-rings are supported on VPLS SAPs (VPLS, I-VPLS, B-VPLS). VPLS services supporting Rings SAPs can connect to other rings and Ethernet service using VPLS and R-VPLS SAPs. Eth-rings enables rings for core network or access network resiliency. A single point of interconnection to other services is supported. The Eth-ring service is a VLAN service providing protection for ring topologies and the ability to interact with other protection mechanisms for overall service protection. This ensures failures detected by Eth-ring only result in R-APS switchover when the lower layer cannot recover and that higher layers are isolated from the failure.

Rings are preferred in data networks where the native connectivity is laid out in a ring or there is a requirement for simple resilient LAN services. Due to the symmetry and the simple topology, rings are viewed a good solution for access and core networks where resilient LANS are required. The Alcatel-lucent implementation can be used for interconnecting access rings and to provide traffic engineered backbone rings.

Eth-rings use one VID per control per ring instance and use one (typically) or multiple VIDs for data instances per control instance. A dedicated control VLAN (ERP VLAN) is used to run the protocol on the control VID. G.8032 controls the active state for the data VLANs (ring data instances) associated with a control instance. Multiple control instances allow logically separate rings on the same topology. The Alcatel-lucent implementation supports dot1q, qinq and PBB encapsulation for data ring instances. The control channel supports dot1q and qinq encapsulation.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301070804_V1_7450%20ESS%20OS%20Services%20Guide%209.0R4.pdf **(page 57)**



Ethernet Ring Sub-Rings

Ethernet Sub-Rings offer a dual redundant way to interconnect rings. The 7x50 supports Sub-Rings connected to major rings and a sub-ring connected to a VPLS (LDP based) for access rings support in VPLS networks. Figure 17 illustrates a Major ring and Sub Ring scenario. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Furthermore, the sub ring (ERP2) relies on the major Ring (ERP1) as part of its protection for the traffic from C and D. The nodes C and D are configured as inter connection nodes.

Figure 17: 0-4 G.8032 Sub-Ring

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301070804_V1_7450%20ESS%20OS%20Services%20Guide%209.0R4.pdf **(page 63)**

160. Defendants' 7450 Ethernet Service Switch is communication system in which the VPLS comprising connection termination points provisioned respectively on a plurality of the nodes so as to connect each of the plurality of nodes to a second network external to the ring network:

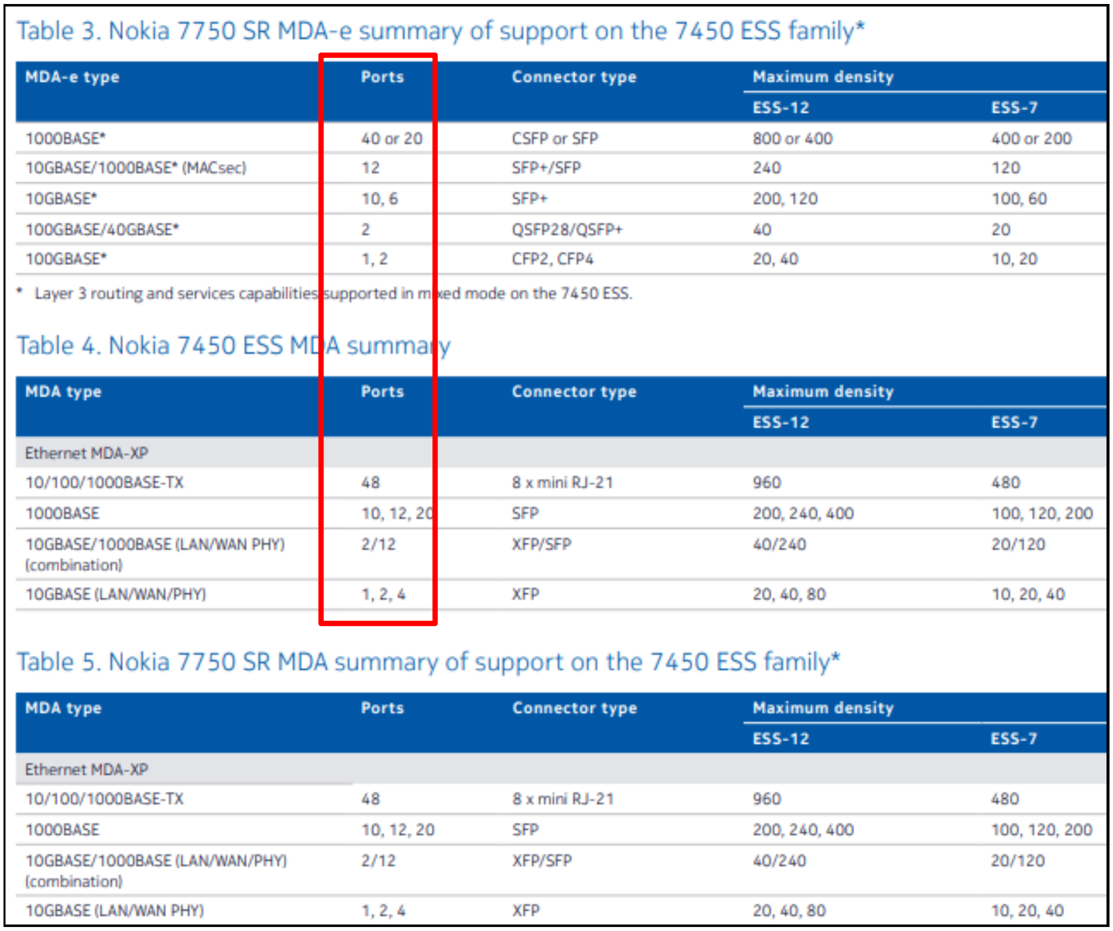


Table 3. Nokia 7750 SR MDA-e summary of support on the 7450 ESS family*

MDA-e type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
1000BASE*	40 or 20	CSFP or SFP	800 or 400	400 or 200
10GBASE/1000BASE* (MACsec)	12	SFP+/SFP	240	120
10GBASE*	10, 6	SFP+	200, 120	100, 60
100GBASE/40GBASE*	2	QSFP28/QSFP+	40	20
100GBASE*	1, 2	CFP2, CFP4	20, 40	10, 20

* Layer 3 routing and services capabilities supported in mixed mode on the 7450 ESS.

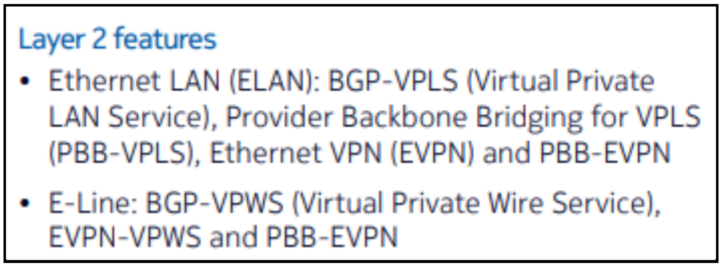
Table 4. Nokia 7450 ESS MDA summary

MDA type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
Ethernet MDA-XP				
10/100/1000BASE-TX	48	8 x mini RJ-21	960	480
1000BASE	10, 12, 20	SFP	200, 240, 400	100, 120, 200
10GBASE/1000BASE (LAN/WAN PHY) (combination)	2/12	XFP/SFP	40/240	20/120
10GBASE (LAN/WAN/PHY)	1, 2, 4	XFP	20, 40, 80	10, 20, 40

Table 5. Nokia 7750 SR MDA summary of support on the 7450 ESS family*

MDA type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
Ethernet MDA-XP				
10/100/1000BASE-TX	48	8 x mini RJ-21	960	480
1000BASE	10, 12, 20	SFP	200, 240, 400	100, 120, 200
10GBASE/1000BASE (LAN/WAN/PHY) (combination)	2/12	XFP/SFP	40/240	20/120
10GBASE (LAN/WAN PHY)	1, 2, 4	XFP	20, 40, 80	10, 20, 40

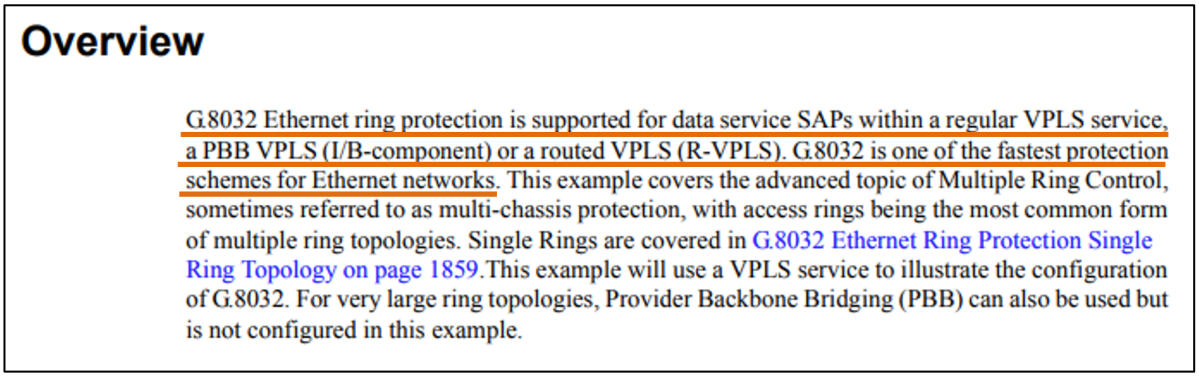
https://onestore.nokia.com/asset/164727 **(pages 4-5)**



Layer 2 features

- Ethernet LAN (ELAN): BGP-VPLS (Virtual Private LAN Service), Provider Backbone Bridging for VPLS (PBB-VPLS), Ethernet VPN (EVPN) and PBB-EVPN
- E-Line: BGP-VPWS (Virtual Private Wire Service), EVPN-VPWS and PBB-EVPN

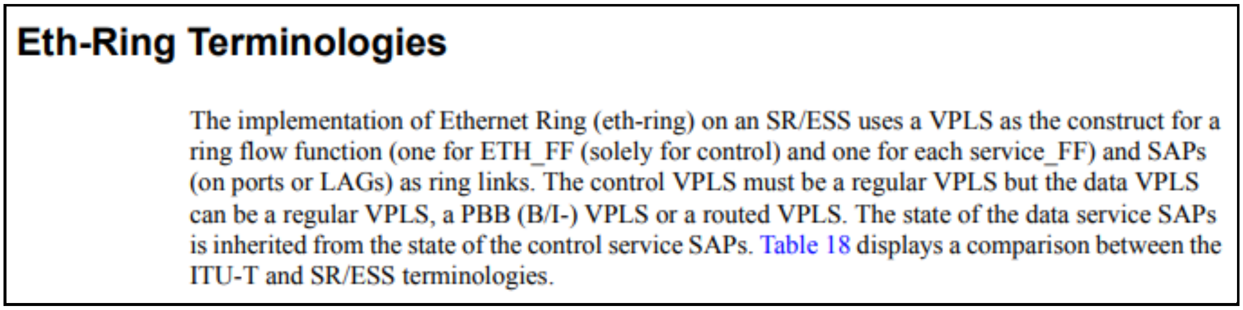
https://onestore.nokia.com/asset/164727 **(page 6)**



Overview

G.8032 Ethernet ring protection is supported for data service SAPs within a regular VPLS service, a PBB VPLS (I/B-component) or a routed VPLS (R-VPLS). G.8032 is one of the fastest protection schemes for Ethernet networks. This example covers the advanced topic of Multiple Ring Control, sometimes referred to as multi-chassis protection, with access rings being the most common form of multiple ring topologies. Single Rings are covered in G.8032 Ethernet Ring Protection Single Ring Topology on page 1859.This example will use a VPLS service to illustrate the configuration of G.8032. For very large ring topologies, Provider Backbone Bridging (PBB) can also be used but is not configured in this example.

https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/G8032-MultiRing.pdf **(page 5)**

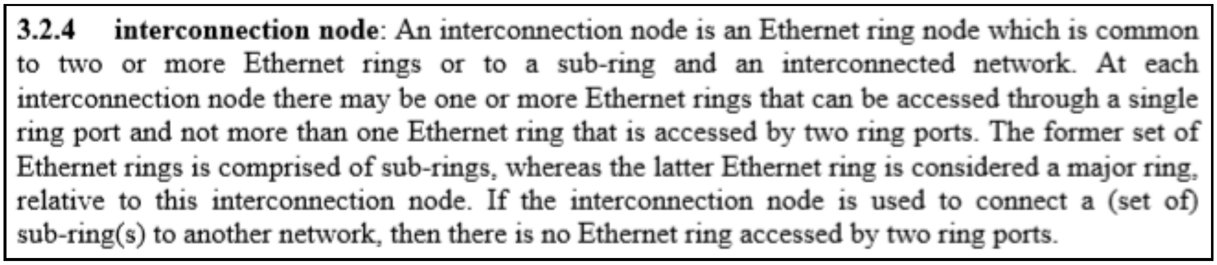


Eth-Ring Terminologies

The implementation of Ethernet Ring (eth-ring) on an SR/ESS uses a VPLS as the construct for a ring flow function (one for ETH_FF (solely for control) and one for each service_FF) and SAPs (on ports or LAGs) as ring links. The control VPLS must be a regular VPLS but the data VPLS can be a regular VPLS, a PBB (B/I-) VPLS or a routed VPLS. The state of the data service SAPs is inherited from the state of the control service SAPs. Table 18 displays a comparison between the ITU-T and SR/ESS terminologies.

https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/G8032-MultiRing.pdf **(page 5)**

161. Defendants' 7450 Ethernet Service Switch is a communication system with a connection established between the bi-directional ring network and the second network via a selected connection terminal point in an active state:



3.2.4 interconnection node: An interconnection node is an Ethernet ring node which is common to two or more Ethernet rings or to a sub-ring and an interconnected network. At each interconnection node there may be one or more Ethernet rings that can be accessed through a single ring port and not more than one Ethernet ring that is accessed by two ring ports. The former set of Ethernet rings is comprised of sub-rings, whereas the latter Ethernet ring is considered a major ring, relative to this interconnection node. If the interconnection node is used to connect a (set of) sub-ring(s) to another network, then there is no Ethernet ring accessed by two ring ports.

https://www.itu.int/rec/T-REC-G.8032/en **(page 9)**

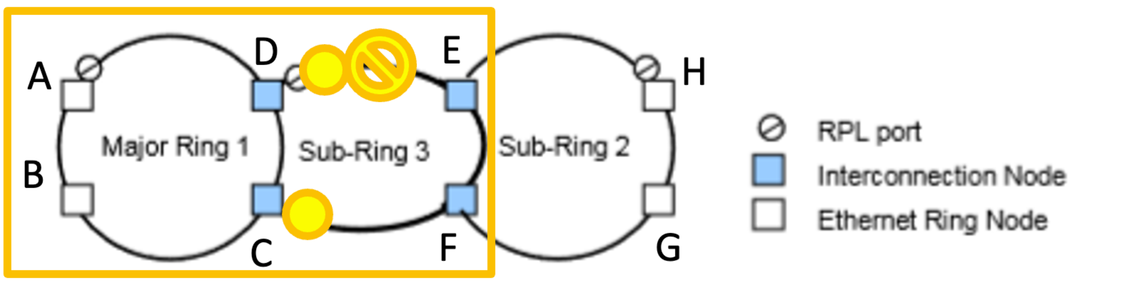
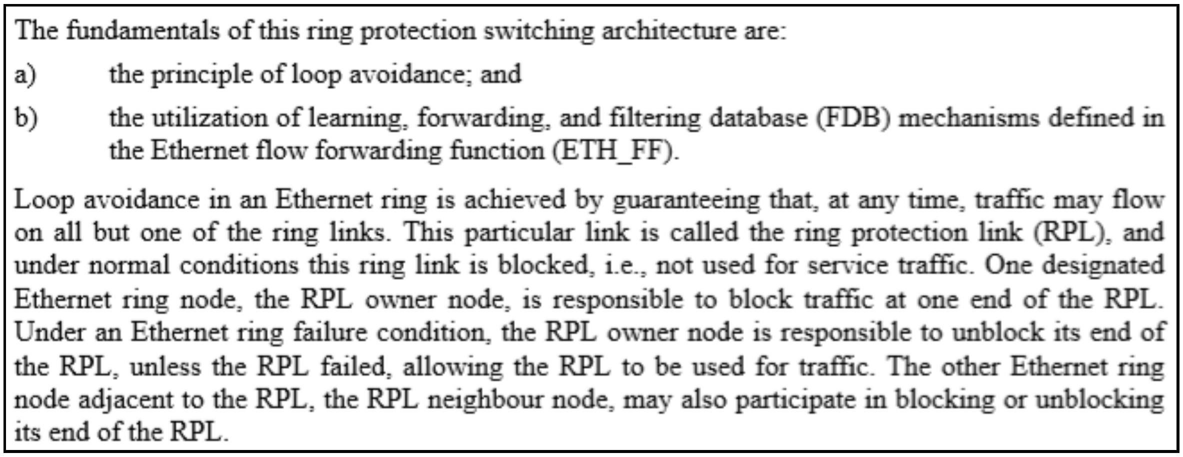


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

162. Defendants' 7450 Ethernet Service Switch is a communication system wherein as long as the nodes and spans are fully operational, all of the connection terminal points except the selected connection termination point are maintained in a deactivated state, so that only the selected connection termination point to the second network is active:



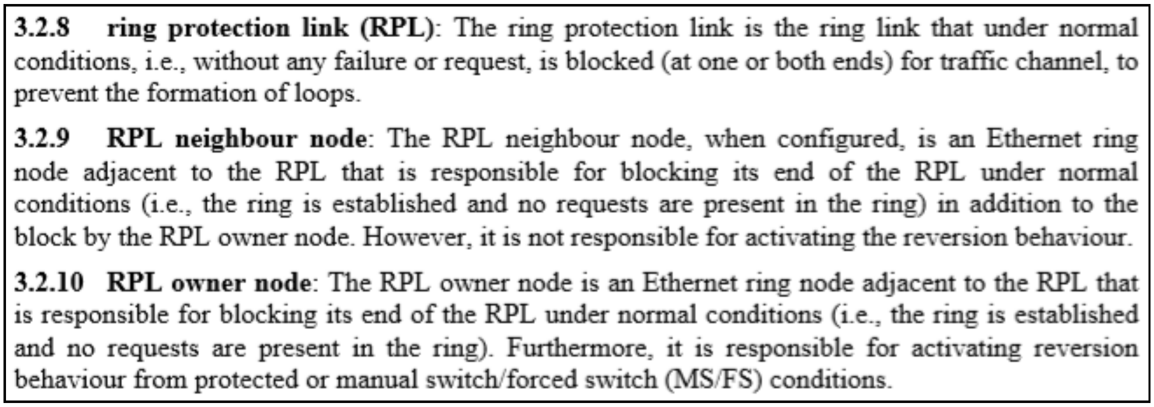
The fundamentals of this ring protection switching architecture are:

a) the principle of loop avoidance; and

b) the utilization of learning, forwarding, and filtering database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible to unblock its end of the RPL, unless the RPL failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbour node, may also participate in blocking or unblocking its end of the RPL.

https://www.itu.int/rec/T-REC-G.8032/en **(page 12)**

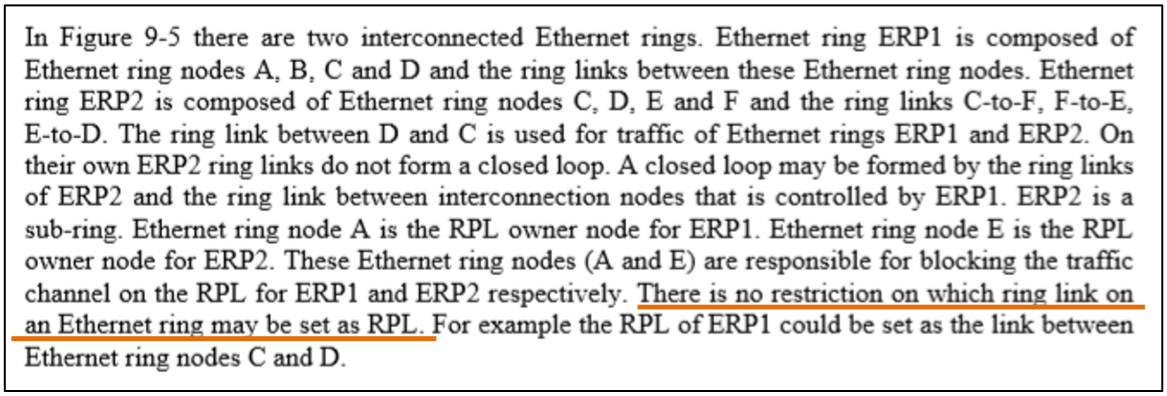


3.2.8 ring protection link (RPL): The ring protection link is the ring link that under normal conditions, i.e., without any failure or request, is blocked (at one or both ends) for traffic channel, to prevent the formation of loops.

3.2.9 RPL neighbour node: The RPL neighbour node, when configured, is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block by the RPL owner node. However, it is not responsible for activating the reversion behaviour.

3.2.10 RPL owner node: The RPL owner node is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring). Furthermore, it is responsible for activating reversion behaviour from protected or manual switch/forced switch (MS/FS) conditions.

https://www.itu.int/rec/T-REC-G.8032/en (page 10)



In Figure 9-5 there are two interconnected Ethernet rings. Ethernet ring ERP1 is composed of Ethernet ring nodes A, B, C and D and the ring links between these Ethernet ring nodes. Ethernet ring ERP2 is composed of Ethernet ring nodes C, D, E and F and the ring links C-to-F, F-to-E, E-to-D. The ring link between D and C is used for traffic of Ethernet rings ERP1 and ERP2. On their own ERP2 ring links do not form a closed loop. A closed loop may be formed by the ring links of ERP2 and the ring link between interconnection nodes that is controlled by ERP1. ERP2 is a sub-ring. Ethernet ring node A is the RPL owner node for ERP1. Ethernet ring node E is the RPL owner node for ERP2. These Ethernet ring nodes (A and E) are responsible for blocking the traffic channel on the RPL for ERP1 and ERP2 respectively. There is no restriction on which ring link on an Ethernet ring may be set as RPL. For example the RPL of ERP1 could be set as the link between Ethernet ring nodes C and D.

https://www.itu.int/rec/T-REC-G.8032/en (page 19)

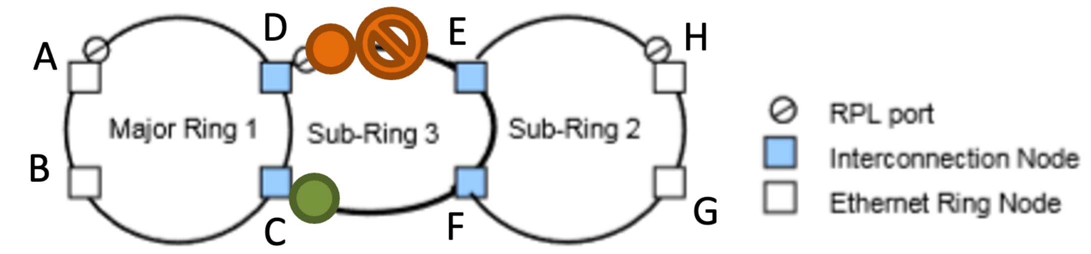
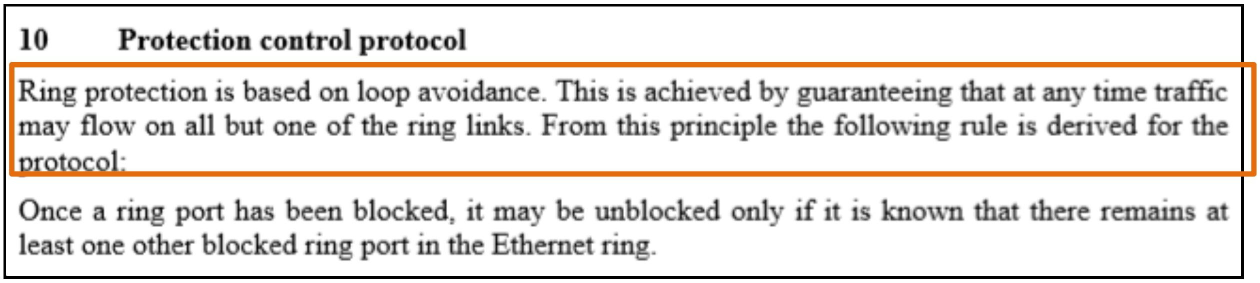


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en (page 27)



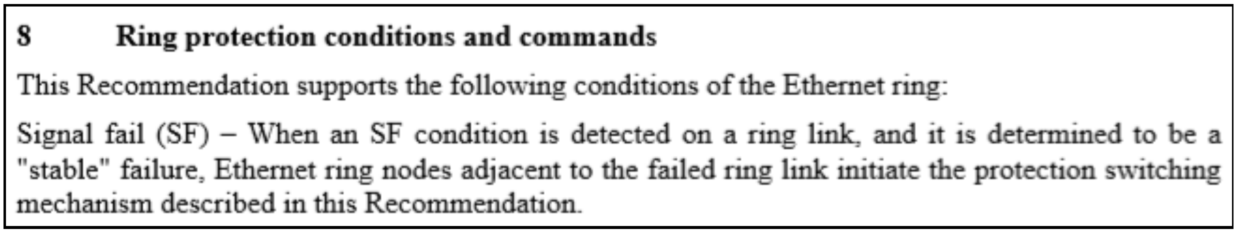
10 Protection control protocol

Ring protection is based on loop avoidance. This is achieved by guaranteeing that at any time traffic may flow on all but one of the ring links. From this principle the following rule is derived for the protocol:

Once a ring port has been blocked, it may be unblocked only if it is known that there remains at least one other blocked ring port in the Ethernet ring.

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

163. Defendants' 7450 Ethernet Service Switch is a communication system wherein the nodes are arranged to exchange messages indicative of a failure in at least two spans of the ring network causing a segmentation of the ring network and leading to an isolation of a first node of the ring network from at least one second node of the ring network:

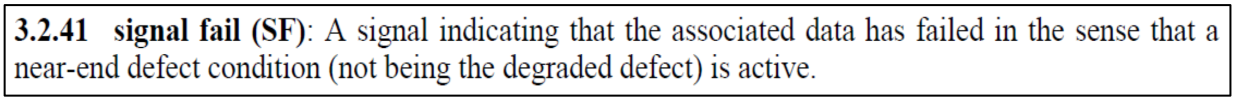


8 Ring protection conditions and commands

This Recommendation supports the following conditions of the Ethernet ring:

Signal fail (SF) – When an SF condition is detected on a ring link, and it is determined to be a "stable" failure, Ethernet ring nodes adjacent to the failed ring link initiate the protection switching mechanism described in this Recommendation.

https://www.itu.int/rec/T-REC-G.8032/en **(page 13)**



3.2.41 signal fail (SF): A signal indicating that the associated data has failed in the sense that a near-end defect condition (not being the degraded defect) is active.

ITU recommendation ITU-T G.806

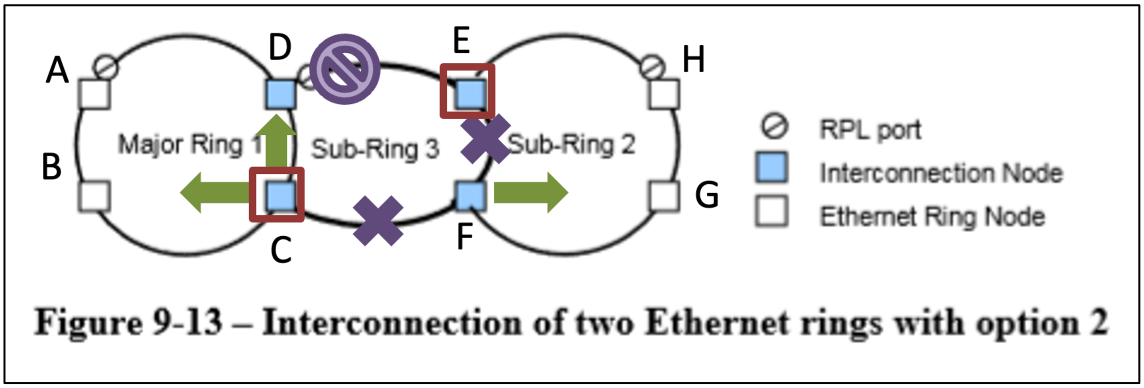
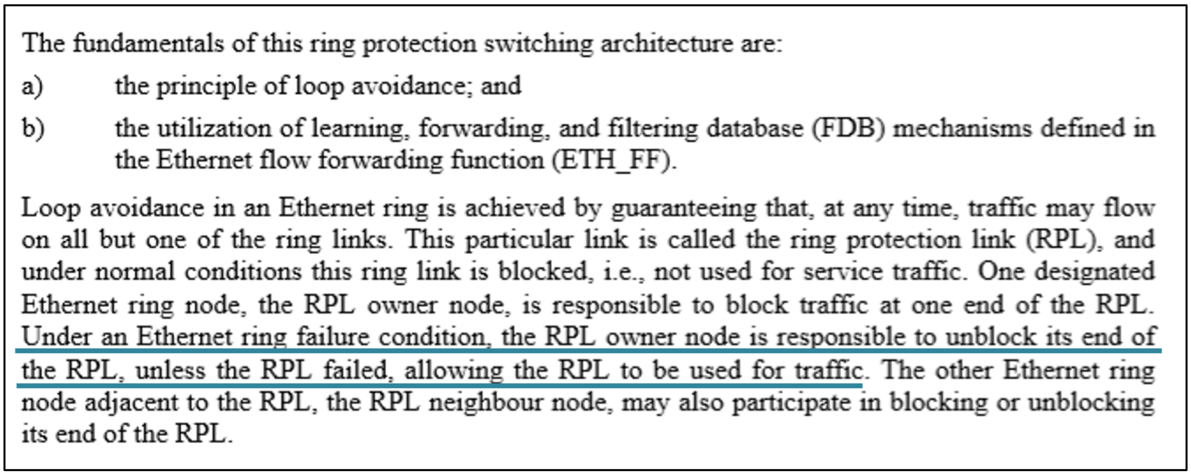


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

164. Defendants' 7450 Ethernet Service Switch is a communication system that responsively to the messages, to activate at least one of the deactivated connection termination points so as to overcome the segmentation and maintain connectivity of the first node with the at least one second node of the ring network, without creating a loop in the VPLS via the second network:



The fundamentals of this ring protection switching architecture are:

a) the principle of loop avoidance; and

b) the utilization of learning, forwarding, and filtering database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible to unblock its end of the RPL, unless the RPL failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbour node, may also participate in blocking or unblocking its end of the RPL.

https://www.itu.int/rec/T-REC-G.8032/en **(page 12)**

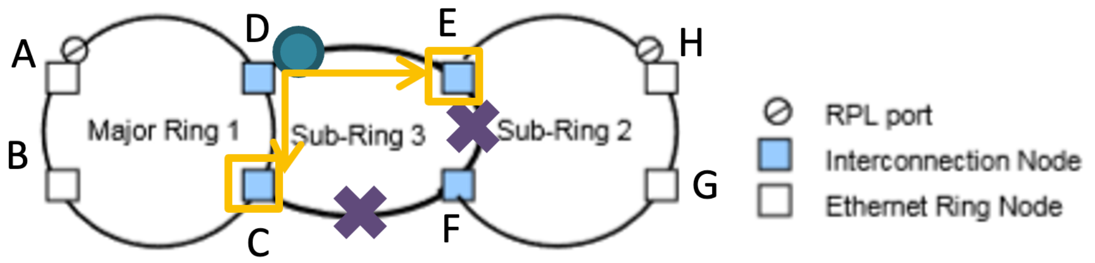
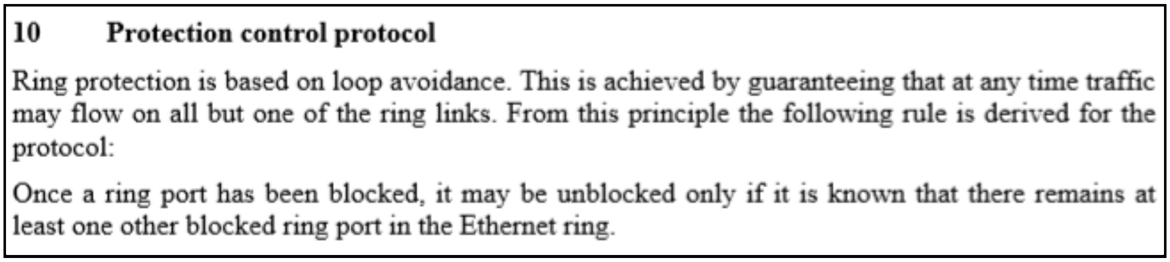


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**



10 Protection control protocol

Ring protection is based on loop avoidance. This is achieved by guaranteeing that at any time traffic may flow on all but one of the ring links. From this principle the following rule is derived for the protocol:

Once a ring port has been blocked, it may be unblocked only if it is known that there remains at least one other blocked ring port in the Ethernet ring.

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

Willful Infringement

165. Defendants have had actual knowledge of the '150 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated February 27, 2017.

166. Defendants have had actual knowledge of the '150 Patent and its infringement thereof at least as of service of Plaintiff's Complaint.

167. Defendants' risk of infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendants.

168. Notwithstanding this knowledge, Defendants have knowingly or with reckless disregard willfully infringed the '150 Patent. Defendants have thus had actual notice of the infringement of the '150 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff's valid patent rights, either literally or equivalently.

169. This objective risk was either known or so obvious that it should have been known to Defendants. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

170. Defendants have induced and is knowingly inducing its customers and/or end users to directly infringe the '150 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

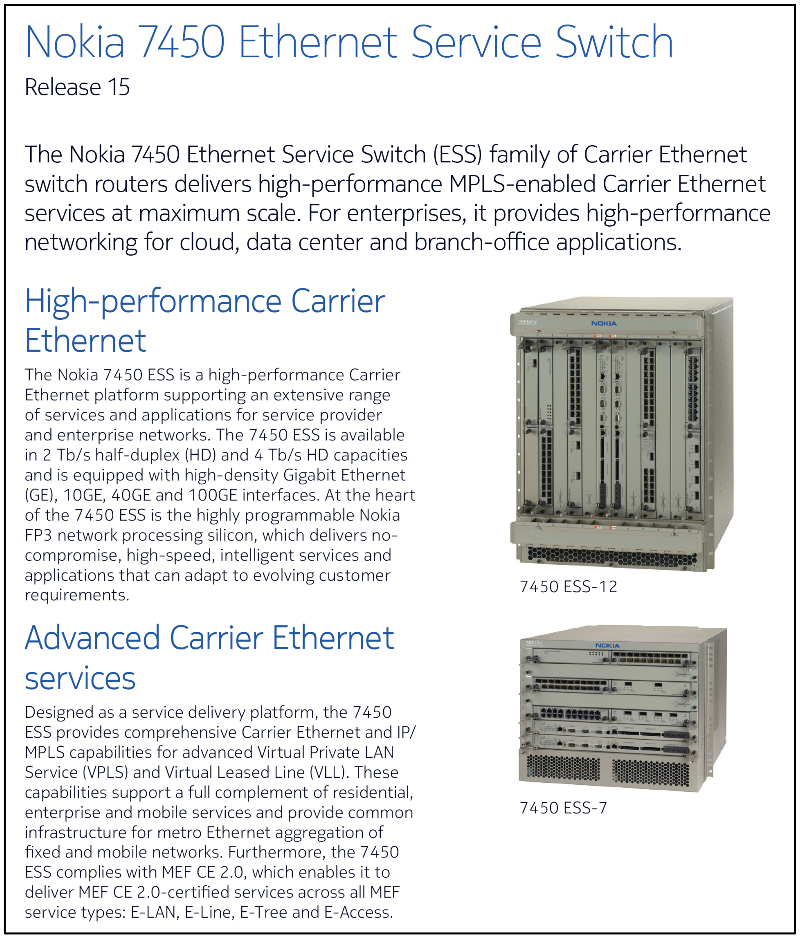
171. Defendants have knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the accused products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

172. Defendants' indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support, that induce its customers and/or end users to directly infringe '150 Patent. Defendants' indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendants' indirect infringement further includes providing application notes instructing its customers on infringing uses of the '150 Accused Products. The '150 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '150 Patent, either literally or equivalently. Defendants know and intend that customers who purchase the '150 Accused Products will use those products for their intended purpose. For example, Defendants' United States website: https://www.nokia.com, instructs customers to use the '150 Accused Products in numerous infringing applications. Furthermore, Defendants provide instructions and other resources via its "Doc Center" (https://documentation.nokia.com), "Nokia Service Routing Certification" and training courses from its "NokiaEDU Training Centers" (https://www.nokia.com/networks/training/src/courses/#open-enrollment), and elsewhere on using the '150 Accused Products. Defendants' customers directly infringe the '150 patent when they follow Defendants' provided instructions on website, videos, and elsewhere. Defendants' customers who follow Defendants' provided instructions directly infringe claims of the '150 Patent.

173. In addition, Defendants specifically intend that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendants' infringing products. Defendants know following its instructions directly infringes claims of the '150 Patent, including claim 1.

174. Defendants' customers who follow Defendants' provided instructions directly infringe the method of claim 1 of the '150 Patent.

175. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method for communication over a bi-directional ring network that includes nodes connected by spans of the ring network:



Nokia 7450 Ethernet Service Switch

Release 15

The Nokia 7450 Ethernet Service Switch (ESS) family of Carrier Ethernet switch routers delivers high-performance MPLS-enabled Carrier Ethernet services at maximum scale. For enterprises, it provides high-performance networking for cloud, data center and branch-office applications.

High-performance Carrier Ethernet

The Nokia 7450 ESS is a high-performance Carrier Ethernet platform supporting an extensive range of services and applications for service provider and enterprise networks. The 7450 ESS is available in 2 Tb/s half-duplex (HD) and 4 Tb/s HD capacities and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces. At the heart of the 7450 ESS is the highly programmable Nokia FP3 network processing silicon, which delivers no-compromise, high-speed, intelligent services and applications that can adapt to evolving customer requirements.

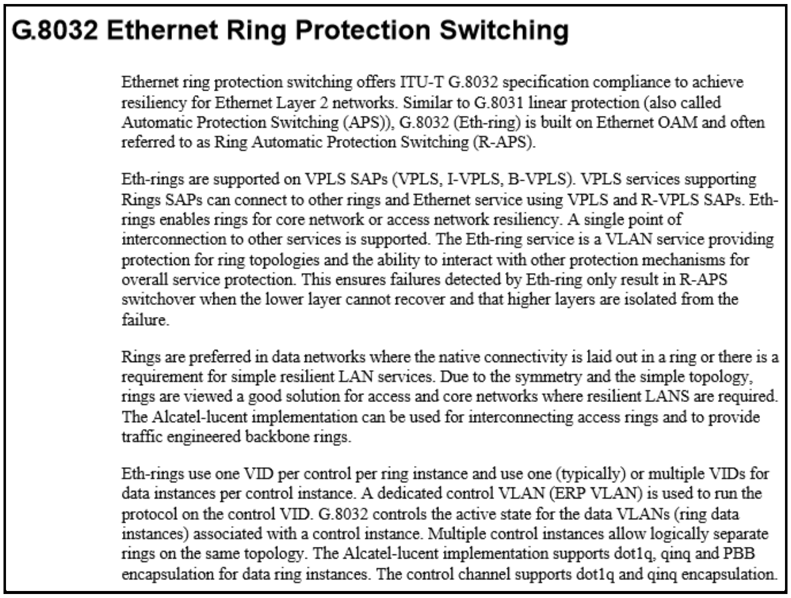
7450 ESS-12

Advanced Carrier Ethernet services

Designed as a service delivery platform, the 7450 ESS provides comprehensive Carrier Ethernet and IP/MPLS capabilities for advanced Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL). These capabilities support a full complement of residential, enterprise and mobile services and provide common infrastructure for metro Ethernet aggregation of fixed and mobile networks. Furthermore, the 7450 ESS complies with MEF CE 2.0, which enables it to deliver MEF CE 2.0-certified services across all MEF service types: E-LAN, E-Line, E-Tree and E-Access.

7450 ESS-7

https://onestore.nokia.com/asset/164727 **(page 1)**



G.8032 Ethernet Ring Protection Switching

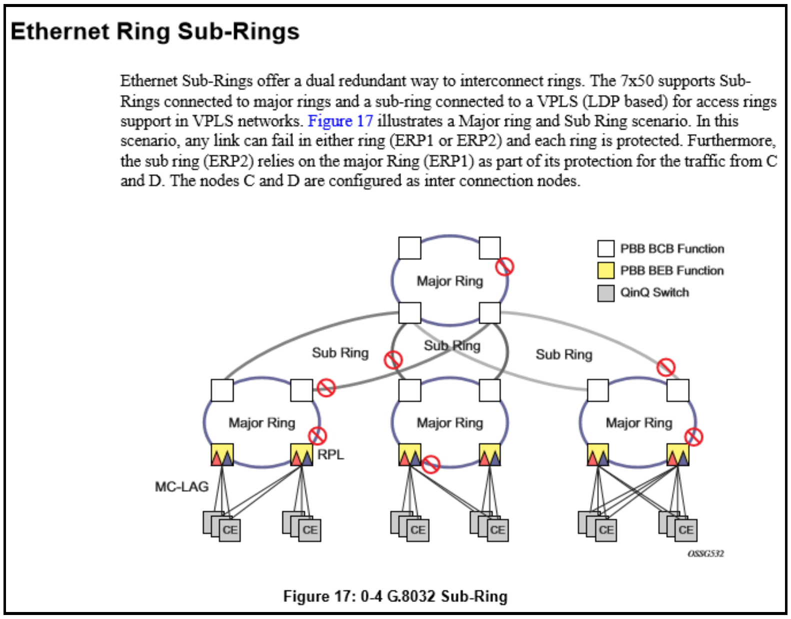
Ethernet ring protection switching offers ITU-T G.8032 specification compliance to achieve resiliency for Ethernet Layer 2 networks. Similar to G.8031 linear protection (also called Automatic Protection Switching (APS)), G.8032 (Eth-ring) is built on Ethernet OAM and often referred to as Ring Automatic Protection Switching (R-APS).

Eth-rings are supported on VPLS SAPs (VPLS, I-VPLS, B-VPLS). VPLS services supporting Rings SAPs can connect to other rings and Ethernet service using VPLS and R-VPLS SAPs. Eth-rings enables rings for core network or access network resiliency. A single point of interconnection to other services is supported. The Eth-ring service is a VLAN service providing protection for ring topologies and the ability to interact with other protection mechanisms for overall service protection. This ensures failures detected by Eth-ring only result in R-APS switchover when the lower layer cannot recover and that higher layers are isolated from the failure.

Rings are preferred in data networks where the native connectivity is laid out in a ring or there is a requirement for simple resilient LAN services. Due to the symmetry and the simple topology, rings are viewed a good solution for access and core networks where resilient LANS are required. The Alcatel-lucent implementation can be used for interconnecting access rings and to provide traffic engineered backbone rings.

Eth-rings use one VID per control per ring instance and use one (typically) or multiple VIDs for data instances per control instance. A dedicated control VLAN (ERP VLAN) is used to run the protocol on the control VID. G.8032 controls the active state for the data VLANs (ring data instances) associated with a control instance. Multiple control instances allow logically separate rings on the same topology. The Alcatel-lucent implementation supports dot1q, qinq and PBB encapsulation for data ring instances. The control channel supports dot1q and qinq encapsulation.

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301070804_V1_7450%20ESS%20OS%20Services%20Guide%209.0R4.pdf **(page 57)**



Ethernet Ring Sub-Rings

Ethernet Sub-Rings offer a dual redundant way to interconnect rings. The 7x50 supports Sub-Rings connected to major rings and a sub-ring connected to a VPLS (LDP based) for access rings support in VPLS networks. Figure 17 illustrates a Major ring and Sub Ring scenario. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Furthermore, the sub ring (ERP2) relies on the major Ring (ERP1) as part of its protection for the traffic from C and D. The nodes C and D are configured as inter connection nodes.

Figure 17: 0-4 G.8032 Sub-Ring

https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/9301070804_V1_7450%20ESS%20OS%20Services%20Guide%209.0R4.pdf **(page 63)**

176. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method that provisions a virtual private local area network service (VPLS) to serve users over the bi-directional ring network, the VPLS comprising connection termination points provisioned respectively on a plurality of nodes so as to connect each of the nodes to a second network external to the ring network:

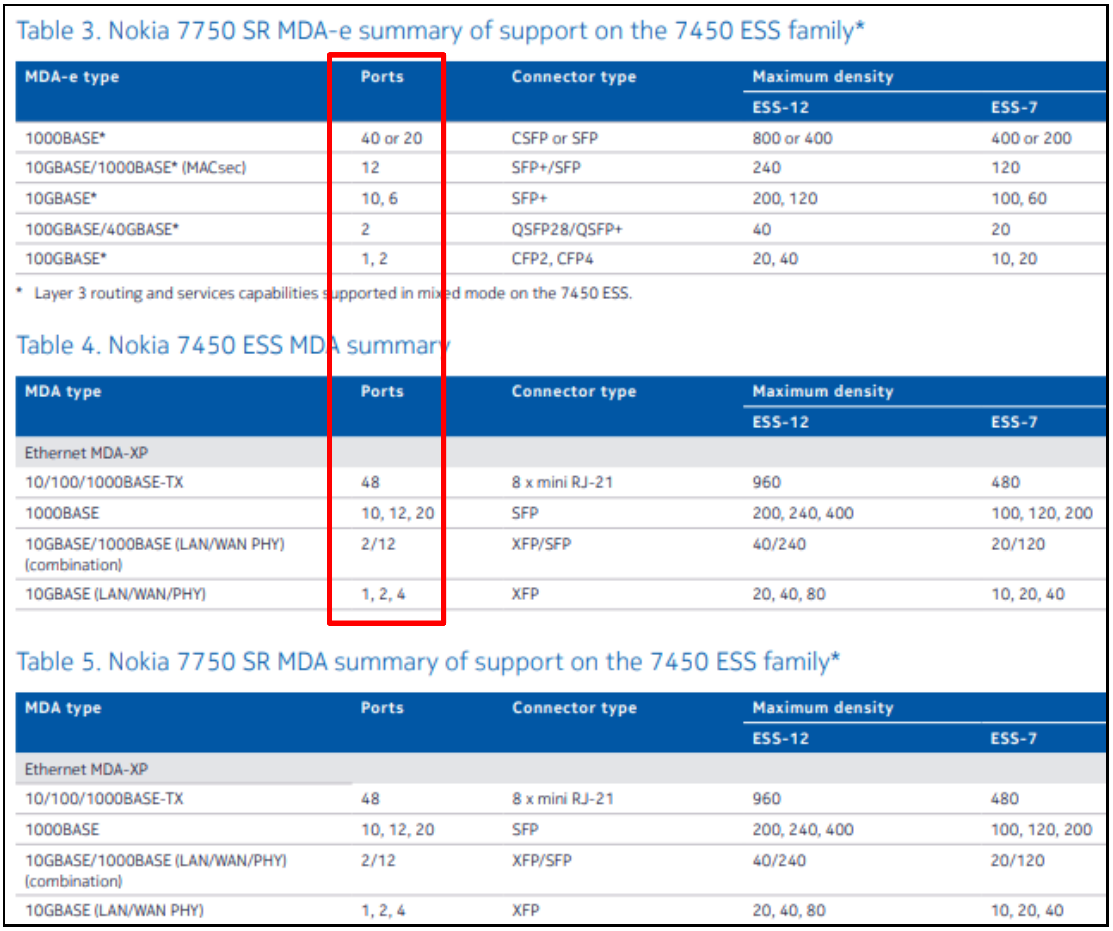


Table 3. Nokia 7750 SR MDA-e summary of support on the 7450 ESS family*

MDA-e type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
1000BASE*	40 or 20	CSFP or SFP	800 or 400	400 or 200
10GBASE/1000BASE* (MACsec)	12	SFP+/SFP	240	120
10GBASE*	10, 6	SFP+	200, 120	100, 60
100GBASE/40GBASE*	2	QSFP28/QSFP+	40	20
100GBASE*	1, 2	CFP2, CFP4	20, 40	10, 20

* Layer 3 routing and services capabilities supported in mixed mode on the 7450 ESS.

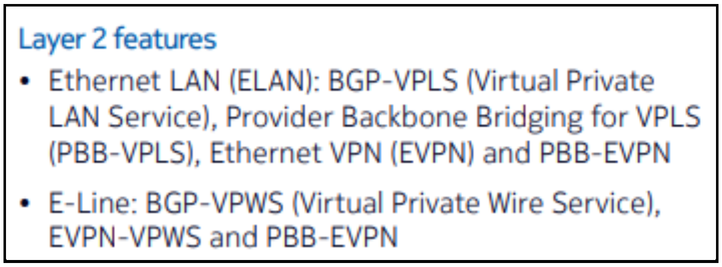
Table 4. Nokia 7450 ESS MDA summary

MDA type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
Ethernet MDA-XP				
10/100/1000BASE-TX	48	8 x mini RJ-21	960	480
1000BASE	10, 12, 20	SFP	200, 240, 400	100, 120, 200
10GBASE/1000BASE (LAN/WAN PHY) (combination)	2/12	XFP/SFP	40/240	20/120
10GBASE (LAN/WAN/PHY)	1, 2, 4	XFP	20, 40, 80	10, 20, 40

Table 5. Nokia 7750 SR MDA summary of support on the 7450 ESS family*

MDA type	Ports	Connector type	Maximum density	
			ESS-12	ESS-7
Ethernet MDA-XP				
10/100/1000BASE-TX	48	8 x mini RJ-21	960	480
1000BASE	10, 12, 20	SFP	200, 240, 400	100, 120, 200
10GBASE/1000BASE (LAN/WAN/PHY) (combination)	2/12	XFP/SFP	40/240	20/120
10GBASE (LAN/WAN PHY)	1, 2, 4	XFP	20, 40, 80	10, 20, 40

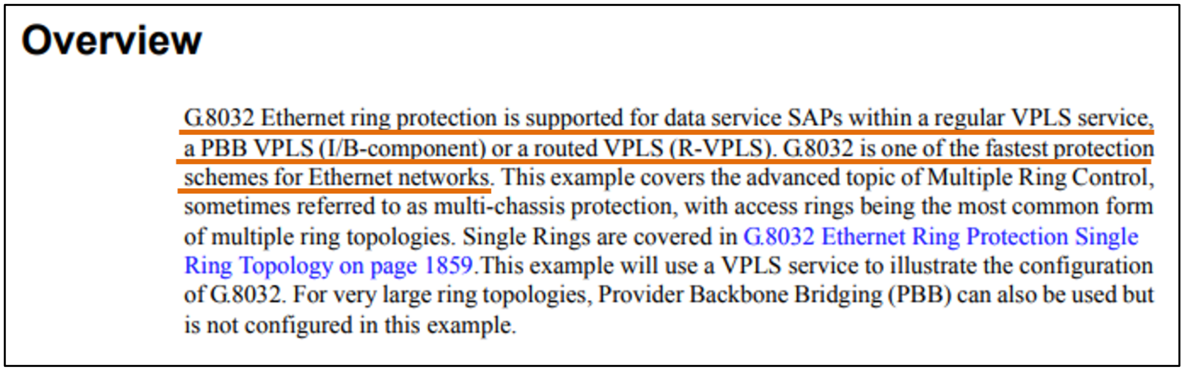
https://onestore.nokia.com/asset/164727 **(pages 4-5)**



Layer 2 features

- Ethernet LAN (ELAN): BGP-VPLS (Virtual Private LAN Service), Provider Backbone Bridging for VPLS (PBB-VPLS), Ethernet VPN (EVPN) and PBB-EVPN
- E-Line: BGP-VPWS (Virtual Private Wire Service), EVPN-VPWS and PBB-EVPN

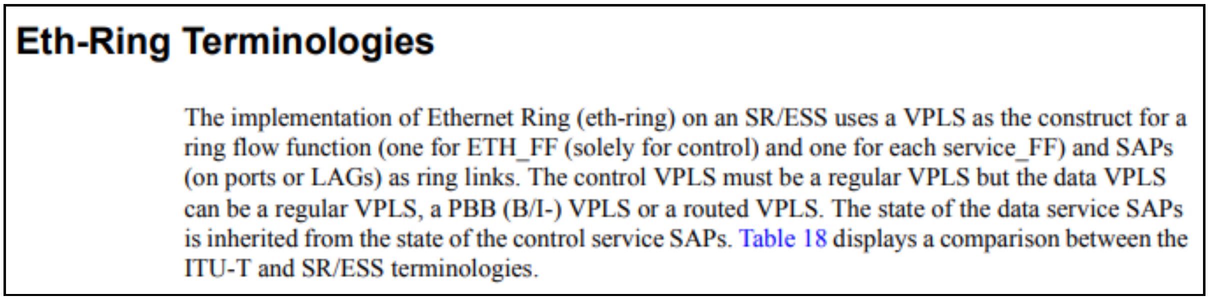
https://onestore.nokia.com/asset/164727 **(page 6)**



Overview

G.8032 Ethernet ring protection is supported for data service SAPs within a regular VPLS service, a PBB VPLS (I/B-component) or a routed VPLS (R-VPLS). G.8032 is one of the fastest protection schemes for Ethernet networks. This example covers the advanced topic of Multiple Ring Control, sometimes referred to as multi-chassis protection, with access rings being the most common form of multiple ring topologies. Single Rings are covered in G.8032 Ethernet Ring Protection Single Ring Topology on page 1859.This example will use a VPLS service to illustrate the configuration of G.8032. For very large ring topologies, Provider Backbone Bridging (PBB) can also be used but is not configured in this example.

https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/G8032-MultiRing.pdf **(page 5)**

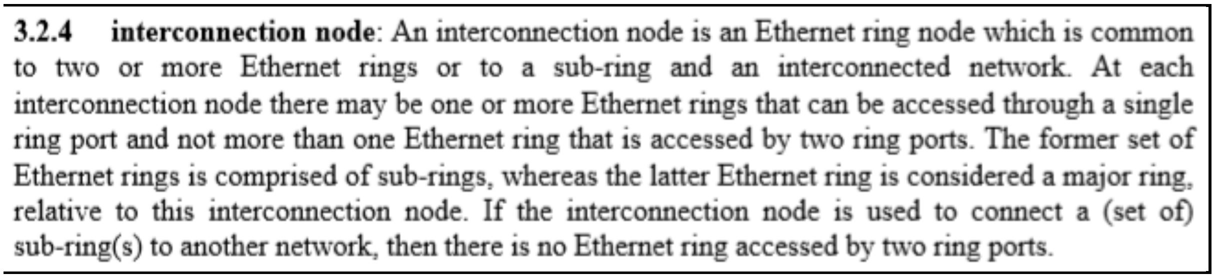


Eth-Ring Terminologies

The implementation of Ethernet Ring (eth-ring) on an SR/ESS uses a VPLS as the construct for a ring flow function (one for ETH_FF (solely for control) and one for each service_FF) and SAPs (on ports or LAGs) as ring links. The control VPLS must be a regular VPLS but the data VPLS can be a regular VPLS, a PBB (B/I-) VPLS or a routed VPLS. The state of the data service SAPs is inherited from the state of the control service SAPs. Table 18 displays a comparison between the ITU-T and SR/ESS terminologies.

https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/G8032-MultiRing.pdf **(page 5)**

177. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method that activates a selected connection termination point, to establish a connection between the bi-directional ring network and the second network:



3.2.4 interconnection node: An interconnection node is an Ethernet ring node which is common to two or more Ethernet rings or to a sub-ring and an interconnected network. At each interconnection node there may be one or more Ethernet rings that can be accessed through a single ring port and not more than one Ethernet ring that is accessed by two ring ports. The former set of Ethernet rings is comprised of sub-rings, whereas the latter Ethernet ring is considered a major ring, relative to this interconnection node. If the interconnection node is used to connect a (set of) sub-ring(s) to another network, then there is no Ethernet ring accessed by two ring ports.

https://www.itu.int/rec/T-REC-G.8032/en **(page 9)**

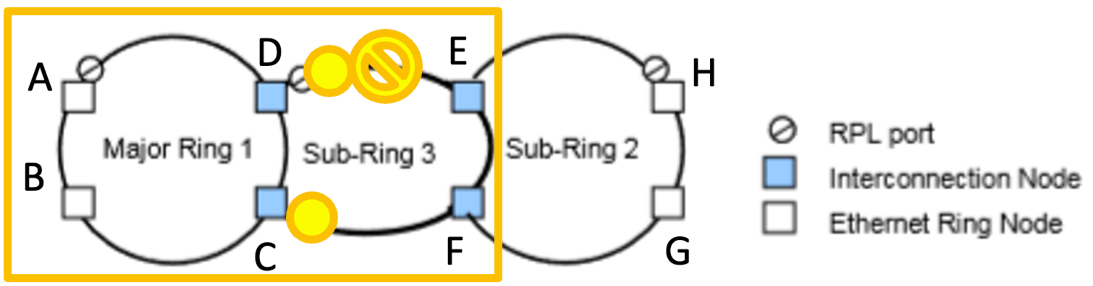
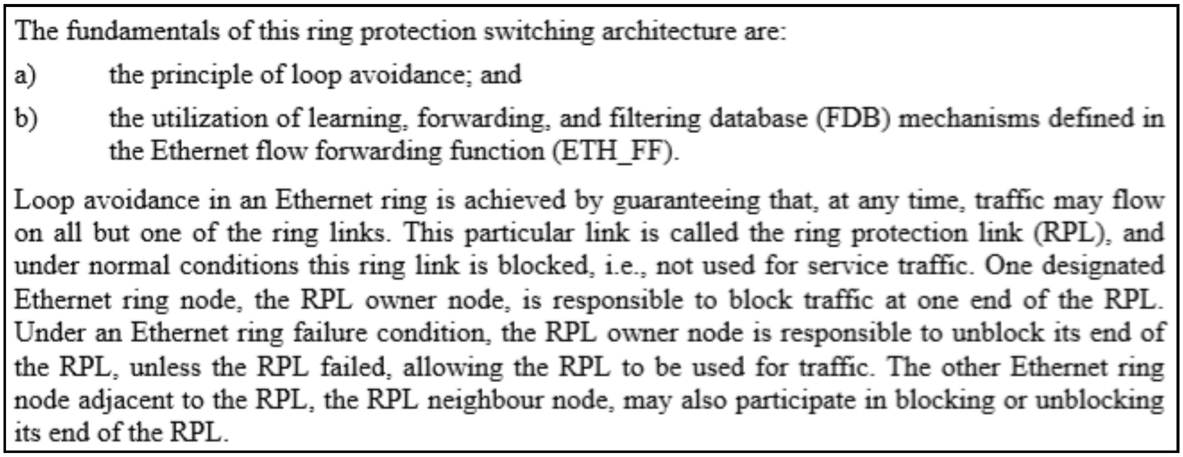


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

178. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method that, as long as the nodes and spans are fully operational, maintains all of the connection termination points except the selected connection termination point in a deactivated state, so that only the selected connection termination point to the second network is active:



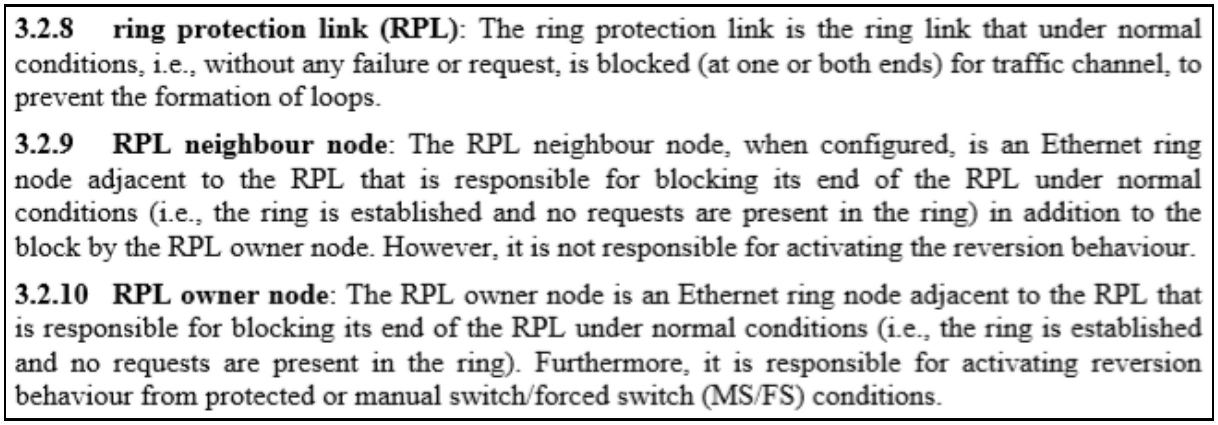
The fundamentals of this ring protection switching architecture are:

a) the principle of loop avoidance; and

b) the utilization of learning, forwarding, and filtering database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible to unblock its end of the RPL, unless the RPL failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbour node, may also participate in blocking or unblocking its end of the RPL.

https://www.itu.int/rec/T-REC-G.8032/en (**Page 12 of PDF**)

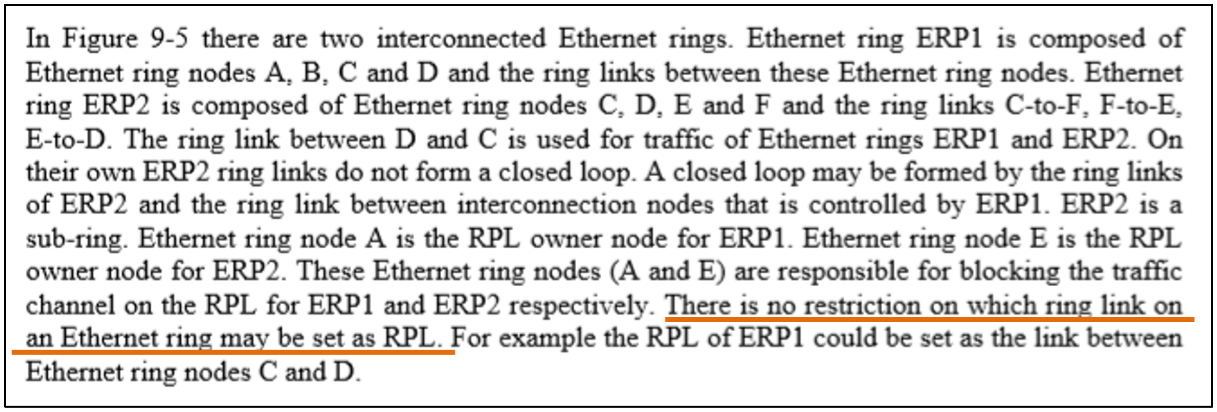


3.2.8 ring protection link (RPL): The ring protection link is the ring link that under normal conditions, i.e., without any failure or request, is blocked (at one or both ends) for traffic channel, to prevent the formation of loops.

3.2.9 RPL neighbour node: The RPL neighbour node, when configured, is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block by the RPL owner node. However, it is not responsible for activating the reversion behaviour.

3.2.10 RPL owner node: The RPL owner node is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring). Furthermore, it is responsible for activating reversion behaviour from protected or manual switch/forced switch (MS/FS) conditions.

https://www.itu.int/rec/T-REC-G.8032/en **(Page 10 of PDF)**



In Figure 9-5 there are two interconnected Ethernet rings. Ethernet ring ERP1 is composed of Ethernet ring nodes A, B, C and D and the ring links between these Ethernet ring nodes. Ethernet ring ERP2 is composed of Ethernet ring nodes C, D, E and F and the ring links C-to-F, F-to-E, E-to-D. The ring link between D and C is used for traffic of Ethernet rings ERP1 and ERP2. On their own ERP2 ring links do not form a closed loop. A closed loop may be formed by the ring links of ERP2 and the ring link between interconnection nodes that is controlled by ERP1. ERP2 is a sub-ring. Ethernet ring node A is the RPL owner node for ERP1. Ethernet ring node E is the RPL owner node for ERP2. These Ethernet ring nodes (A and E) are responsible for blocking the traffic channel on the RPL for ERP1 and ERP2 respectively. There is no restriction on which ring link on an Ethernet ring may be set as RPL. For example the RPL of ERP1 could be set as the link between Ethernet ring nodes C and D.

https://www.itu.int/rec/T-REC-G.8032/en **(page 19)**

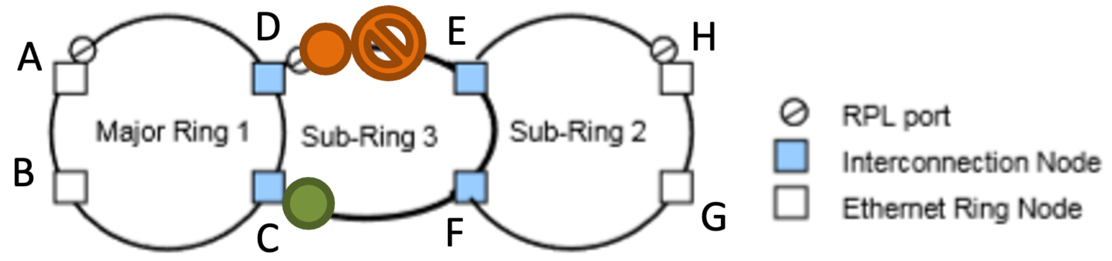
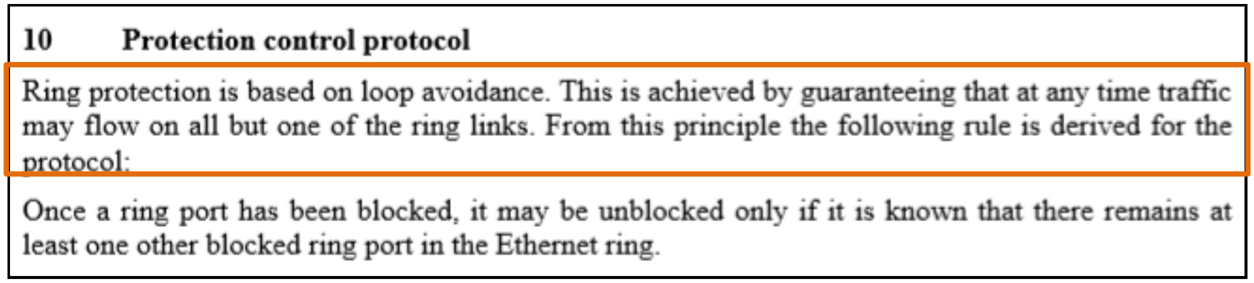


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**



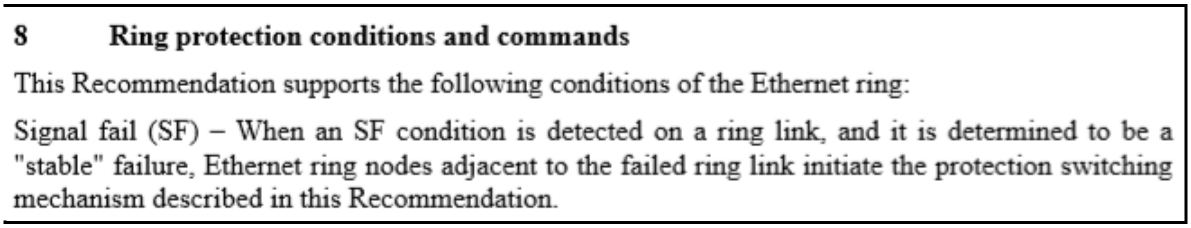
10 Protection control protocol

Ring protection is based on loop avoidance. This is achieved by guaranteeing that at any time traffic may flow on all but one of the ring links. From this principle the following rule is derived for the protocol:

Once a ring port has been blocked, it may be unblocked only if it is known that there remains at least one other blocked ring port in the Ethernet ring.

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

179. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method that exchanges messages among the nodes indicative of a failure in at least two spans of the ring network causing a segmentation of the ring network and leading to an isolation of a first node of the ring network from at least one second node of the ring network:

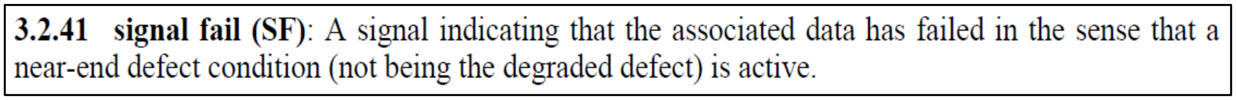


8 Ring protection conditions and commands

This Recommendation supports the following conditions of the Ethernet ring:

Signal fail (SF) – When an SF condition is detected on a ring link, and it is determined to be a "stable" failure, Ethernet ring nodes adjacent to the failed ring link initiate the protection switching mechanism described in this Recommendation.

https://www.itu.int/rec/T-REC-G.8032/en **(page 13)**



3.2.41 signal fail (SF): A signal indicating that the associated data has failed in the sense that a near-end defect condition (not being the degraded defect) is active.

ITU recommendation ITU-T G.806

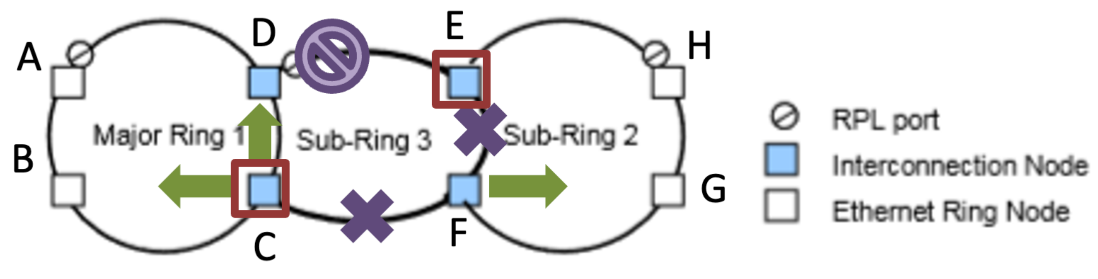
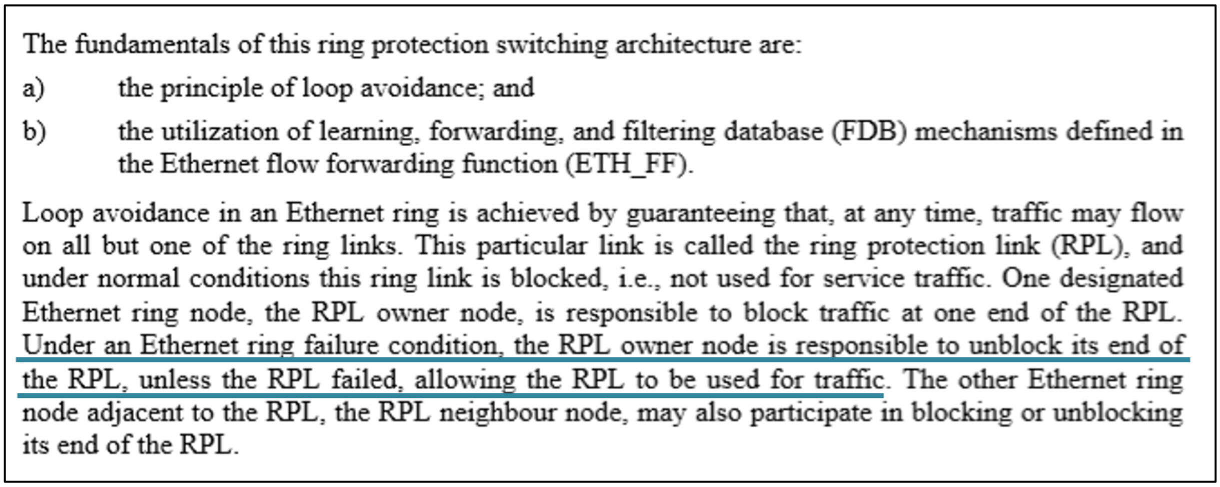


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

180. Defendants instruct its customers use the 7450 Ethernet Service Switch in a method that, responsively to the messages, activates at least one of the deactivated connection termination points so as to overcome the segmentation and maintain connectivity of the first node with the at least one second node of the ring network without creating a loop in the VPLS via the second network:



The fundamentals of this ring protection switching architecture are:

a) the principle of loop avoidance; and

b) the utilization of learning, forwarding, and filtering database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated Ethernet ring node, the RPL owner node, is responsible to block traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL owner node is responsible to unblock its end of the RPL, unless the RPL failed, allowing the RPL to be used for traffic. The other Ethernet ring node adjacent to the RPL, the RPL neighbour node, may also participate in blocking or unblocking its end of the RPL.

https://www.itu.int/rec/T-REC-G.8032/en **(page 12)**

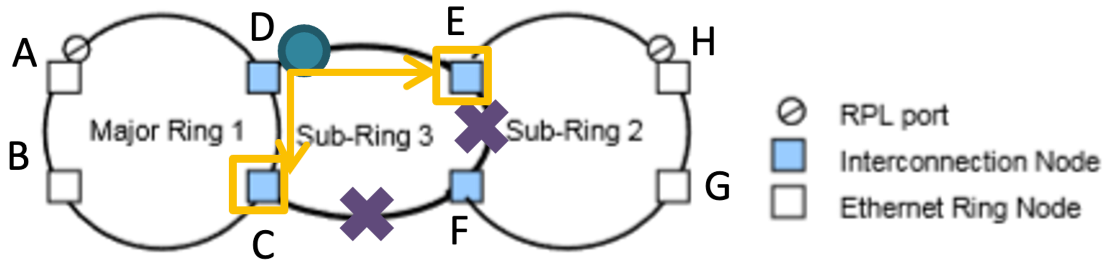
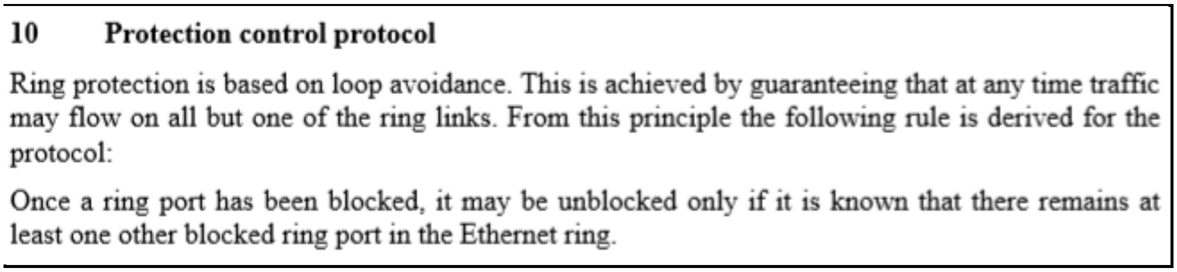


Figure 9-13 – Interconnection of two Ethernet rings with option 2

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**



10 Protection control protocol

Ring protection is based on loop avoidance. This is achieved by guaranteeing that at any time traffic may flow on all but one of the ring links. From this principle the following rule is derived for the protocol:

Once a ring port has been blocked, it may be unblocked only if it is known that there remains at least one other blocked ring port in the Ethernet ring.

https://www.itu.int/rec/T-REC-G.8032/en **(page 27)**

181. As a result of Defendants' infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement, which by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

V. NOTICE

182. Correct Transmission has complied with the notice requirement of 35 U.S.C. § 287 and does not currently distribute, sell, offer for sale, or make products embodying the Asserted Patents. This notice requirement has been complied with by all relevant persons at all relevant times.

VI. JURY DEMAND

183. Plaintiff demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to FED. R. CIV. P. 38.

VII. PRAYER FOR RELIEF

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

A. That the Court determine that one or more claims of the Asserted Patents is infringed by Defendants, both literally and under the doctrine of equivalents;

B. That the Court determine that one or more claims of the Asserted Patents is indirectly infringed by Defendants;

C. That the Court award damages adequate to compensate Plaintiff for the patent infringement that has occurred, together with prejudgment and post-judgment interest and costs, and an ongoing royalty for continued infringement;

D. That the Court permanently enjoin Defendants pursuant to 35 U.S.C. § 283;

E. That the Court find this case to be exception pursuant to 35 U.S.C. § 285;

F. That the Court determine that Defendants' infringements were willful;

G. That the Court award enhanced damages against Defendants pursuant to 35 U.S.C. § 284;

H. That the Court award reasonable attorneys' fees; and

I. That the Court award such other relief to Plaintiff as the Court deems just and proper.

Dated: September 2, 2022

Respectfully Submitted,

/s/ Bradley D. Liddle
E. Leon Carter
lcarter@carterarnett.com
Texas Bar No. 03914300
Bradley D. Liddle
bliddle@carterarnett.com
Texas Bar No. 24074599
Theresa M. Dawson
Texas State Bar No. 24565128
Michael Pomeroy
Texas State Bar No. 24098952
Monica Litle
mlitle@carterarnett.com
Texas Bar No. 24102101
Scott W. Breedlove
sbreedlove@carterarnett.com
State Bar No. 00790361
Joshua J. Bennett
jbennett@carterarnett.com
Texas Bar No. 24059444
CARTER ARNETT PLLC
8150 N. Central Expy, 5th Floor
Dallas, Texas 75206
Telephone No. (214) 550-8188
Facsimile No. (214) 550-8185

ATTORNEYS FOR PLAINTIFF