UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
NORTHEASTERN DIVISION

CORRECT TRANSMISSION, LLC	§	
	§	
Plaintiff,	§	
	§	
	§	
v.	§	Case No. 5:21-CV-690-LCB
	§	
ADTRAN, INC.	§	**JURY TRIAL DEMANDED**
	§	
Defendant.	§	
	§	

THIRD AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Correct Transmission, LLC ("Correct Transmission" or "Plaintiff"), by and through its attorneys, for its Second Amended Complaint for patent infringement against ADTRAN, Inc. ("ADTRAN" or "Defendant"), and demanding trial by jury, hereby alleges, on information and belief with regard to the actions of Defendant 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 Defendant's 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.   Defendant manufactures, provides, uses, sells, offers for sale, imports, and/or distributes 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 Defendant's 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 16192 Coastal Highway, Lewes, DE 19958.

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

6.   ADTRAN, Inc. ("ADTRAN") is a Delaware corporation with its principal place of business at 901 Explorer Boulevard, Huntsville, Alabama 35806. ADTRAN may be served through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

III.   JURISDICTION AND VENUE

7.   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.

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

9.   This Court has personal jurisdiction over ADTRAN in this action because ADTRAN has committed acts within this Judicial District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over ADTRAN would not offend traditional notions of fair play and substantial justice. Defendant ADTRAN, 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, making, using, offering to sell and selling products and/or services that infringe the Asserted Patents. Moreover, ADTRAN is registered to do business in the State of Alabama, has offices and facilities in the State of Alabama, and actively directs its activities to customers located in the State of Alabama.

10.   Venue is proper in this district under 28 U.S.C. §§ 1391(b)–(d) and 1400(b). Defendant ADTRAN is registered to do business in the State of Alabama, has offices in the State of Alabama, and upon information and belief, has transacted business in this Judicial District and has committed acts of direct and indirect infringement in this Judicial District. ADTRAN maintains a regular and established place of business in the Northern District of Alabama, including its Corporate Headquarters located at 901 Explorer Boulevard, Huntsville, Alabama 35806.

IV.   COUNTS OF PATENT INFRINGEMENT

11.   Plaintiff alleges that Defendant has 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

12.   Plaintiff incorporates by reference the allegations in paragraphs 1

through 11 as if fully set forth herein.

13.   The '669 Patent, entitled "PACKET FRAGMENTATION WITH

NESTED INTERRUPTIONS," was filed on January 8, 2001 and issued on April 5,

2005.

14.   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.

Technical Description

15.   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).

16.   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

17.   Defendant, without authorization or license from Plaintiff, has been and is 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. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '669 Patent. Defendant additionally provides services that practice methods that infringe one or more claims of the '669 Patent. Defendant

further tests and uses, at its own US facilities, its telecommunications equipment that infringes one or more claims of the '669 Patent. Defendant further directly infringes one or more method claims of the '669 Patent by providing the '669 Accused Products which initiate and perform those methods without any user modification. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include ADTRAN NetVanta 3448 Multiservice Access Router, and all other substantially similar products (collectively the "'669 Accused Products").

18.   Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendant's 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.

19.   Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the manufacture, use, sale, offer for sale, importation, or distribution of Defendant's NetVanta 3448 Multiservice Access Router.

20.   Defendant's NetVanta 3448 Multiservice Access Router is a non-limiting example of a router that meets all limitations of claim 1 of the '669 Patent, either literally or equivalently.

21.   Correct Transmission, in conjunction with the information contained herein, provides an exemplary, non-limiting basis for Defendant's infringement of the '669 Patent attached hereto as Exhibit F.

22.   The NetVanta 3448 Multiservice Access Router performs a method for transmitting data over a channel.

Standards Protocols

Complementing the versatile hardware, the AOS allows for the support of standards-based switching, Virtual LAN (VLAN) tagging, static and default routes, and demand routing. This enables fast, accurate network convergence using routing protocols such as BGP, OSPF, and RIP. In addition, the AOS terminates MPLS, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, and HDLC Wide Area Network (WAN) protocols. Multihoming is also available to provide redundant or backup WAN links to multiple ISPs, guaranteeing a wide-area connection.

Protocols

- eBGP/iBGP
- OSPF
- RIP (v1 and v2)
- PIM Sparse Mode
- Demand Routing
- Policy-based Routing
- GRE
- ATM (ADSL)
- Frame Relay
- Multilink Frame Relay
- Layer 3 Backup
- Multi-VRF CE
- PPP
- Multilink PPP
- PPPoE
- PPPoA
- IGMP v2
- RFC 1483
- HDLC
- PPP Dial Backup
- PAP and CHAP
- Multihoming
- VRRP

https://portal.ADTRAN.com/pub/Library/Data_Sheets/International_/I61200821E1-8_NV3448_english.pdf

Multilink PPP (MLPPP) Overview

Link Aggregation

PPP and other data link layer protocols establish point-to-point connections over a single carrier line. However, a single line may not provide sufficient bandwidth to meet a business' requirements. This lack of bandwidth can lead to congestion and dropped packets.
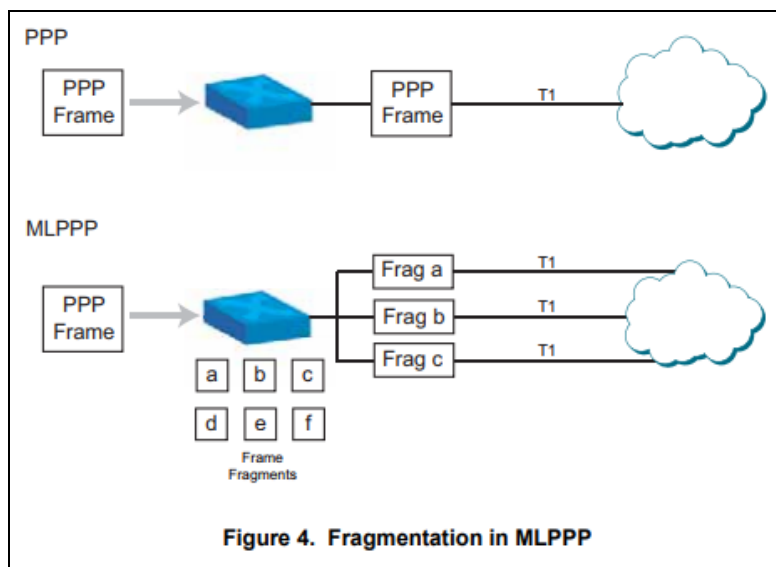
Purchasing a high-bandwidth T3 line to sidestep these limitations is not always feasible because some environments do not support them. In addition, a T3 line can be quite expensive. Often, an organization only wants to double or triple its bandwidth, rather than increase it twenty-eight fold. The purchase of a high-cost T3 line is difficult to justify when much of the bandwidth will not be used.

AOS products support link aggregation protocols, such as MLPPP, to address these problems. Such protocols treat multiple carrier lines as a single bundle, providing two advantages:

• Faster connections - Traffic can access the combined bandwidth of the bundle.

• More stable connections - If one line goes down, the other(s) can still carry traffic.

https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/502/1/Configuring%20PPP%20in%20AOS.pdf (page 6)

23.   The NetVanta 3448 Multiservice Access Router receives a first datagram for transmission at a first priority.

Figure 4. Fragmentation in MLPPP

https://supportforums.adtran.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

> High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.
>
> https://supportforums.adtran.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf **(Page 22)**

> **Functional Notes**
>
> QoS policies are configured in the ADTRAN Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the match command) and one or more action items (using the priority, bandwidth, shape average, or set commands).
>
> https://supportforums.adtran.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf **(Page 4387)**

24.   The NetVanta 3448 Multiservice Access 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.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high

priority packets are encapsulated as PPP and sent to the next available link. Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.
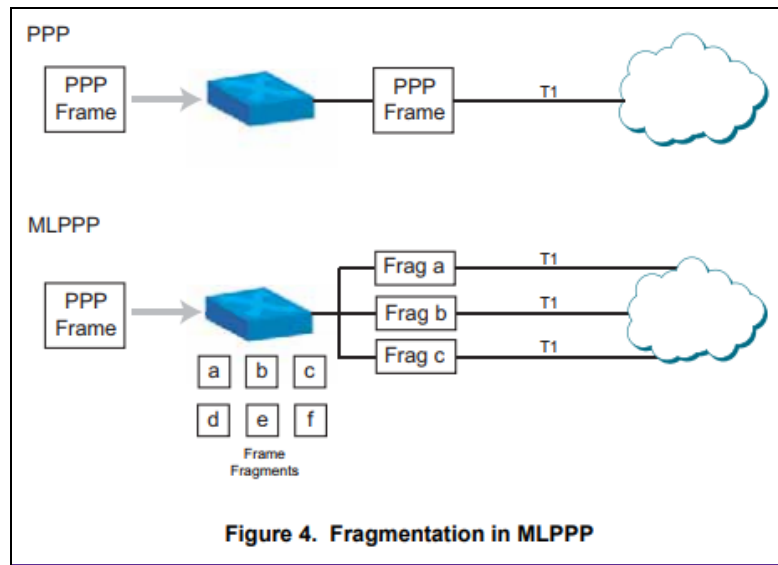
https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

25.   The NetVanta 3448 Multiservice Access Router responds to receiving the second datagram, and decides to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.

MLPPP takes advantage of multiple physical links by fragmenting frames into smaller pieces called frame fragments. These fragments are passed simultaneously over separate cables and then reassembled by the receiving peer (see Figure 4).

11

Figure 4. Fragmentation in MLPPP

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.
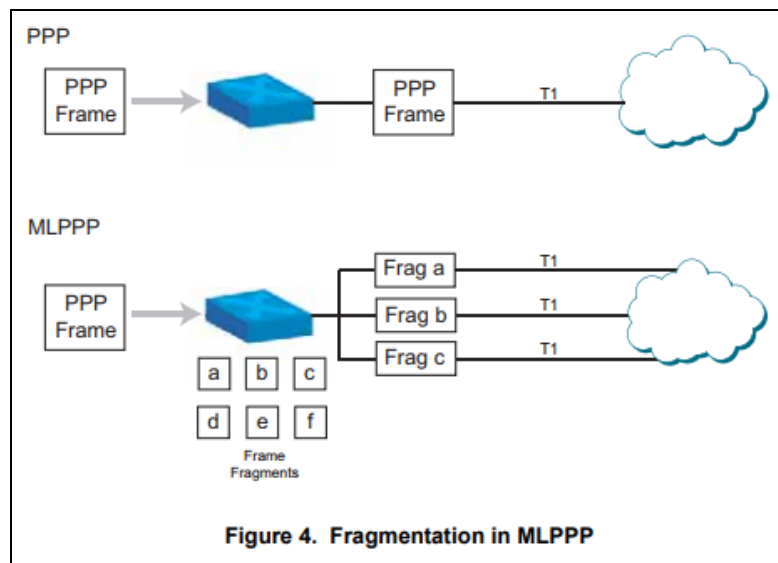
ADTRAN Operating System, Command Reference Guide, https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/428/7/AOS%20R13.12.0%20Command%20Reference%20Guide.pdf

12

(page 2702)

26.   The NetVanta 3448 Multiservice Access Router is configured to transmit the fragments of the first datagram over the channel, beginning with the first fragment.

> MLPPP takes advantage of multiple physical links by fragmenting frames into smaller pieces called frame fragments. These fragments are passed simultaneously over separate cables and then reassembled by the receiving peer (see Figure 4).

Figure 4. Fragmentation in MLPPP

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

27.   The NetVanta 3448 Multiservice Access Router is configured to transmit at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. <u>Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link.</u> Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

<u>High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.</u>

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. <u>The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority.</u> In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

28.   The NetVanta 3448 Multiservice Access Router transmits 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.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link. Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

29.   The NetVanta 3448 Multiservice Access Router adds a field to the fragment indicating the number of datagrams whose transmission has been interrupted.

30.   The NetVanta 3448 Multiservice Access Router includes a variety of headers, including a fragmentation header, PPP header, etc. that include fields indicating the number of fragments whose transmission is interrupted.

Extension Headers in IPv6

An additional difference in IPv4 and IPv6 headers is that the IPv6 packets include extension headers as a method of presenting additional packet and protocol information and options. This additional information is contained between the IPv6 header and the upper-layer header in a packet and allows you to chain extension headers together using the Next Header field. The Next Header field in IPv6 indicates to the router which extension header should be expected next. If there are no additional extension headers, the Next Header field in the IPv6 packet indicates the upper-layer header instead. These upper-layer headers include Transmission Control Protocol (TCP) headers, User Datagram Protocol (UDP) headers, ICMPv6 headers, encapsulated IP packets, etc.

Extension header options are examined at the destination only, except for hop-by-hop options. Extension headers include the following options (in this order):

1. Hop-by-Hop Options Header: Reviewed by all nodes in the packet path.

2. Destination Options Header: Reviewed by intermediate destinations along the packet path when the Routing Header is present.

3. Routing Header: Used to determine the packet path along intermediate nodes before the final packet destination.

4. Fragment Header: Used to break the packet into fragments and put the fragments back together at the final destination. These fragments allow packets larger than the path maximum transmission unit (MTU) to pass.

5. Authentication Header: Part of IPsec. This header functions exactly as in IPv4.

6. Encapsulating Security Payload Header: Part of IPsec. This header functions exactly as in IPv4.

7. Destination Options Header: Reviewed by the final packet destination.

Configuring IPv6 in AOS,
https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/234/1/Configuring%20IPv6%20in%20AOS.pdf   (page 5)

MLPPP Header

The MLPPP header helps the receiving peer reconstruct frame fragments in the correct order. When a peer sends a PPP frame across an MLPPP connection, it first fragments the PPP frame. It then encapsulates fragments in new PPP frames and simultaneously sends them over each aggregated line. The new PPP frame includes the following:

• A new PPP header

• A four-field MLPPP header

• A fragment of the original PPP frame

The MLPPP header includes a flag and a sequence number. The sequence number indicates the fragment's place in the reconstructed PPP frame.

16

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 7)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

31.   ADTRAN's Operating System (AOS) allows tracking of several packet fragmentation statistics, including, but not limited to the number of fragmented packets, number of interrupted packets, dropped packets, and out of sequence packets.

```
Enable Mode Command Set                                    Command Reference Guide

>enable
#show frame-relay fragment frame-relay 1.1
DLCI =  17 FRAGMENT SIZE = 100
rx frag. pkts                46      tx frag. pkts               48
rx frag. bytes             4598      tx frag. bytes            4724
rx non-frag. pkts            18      tx non-frag. pkts           28
rx non-frag. bytes         1228      tx non-frag. bytes        1960
rx assembled pkts            23      tx pre-fragment pkts        34
rx assembled bytes         5478      tx pre-fragment bytes     6324
dropped reassembling pkts     0      dropped fragmenting pkts     0
rx out-of-sequence fragments  0
rx unexpected beginning fragment 0
```

ADTRAN Operating System, Command Reference Guide, https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/428/7/AOS%20R13.12.0%20Command%20Reference%20Guide.pdf (page 654)

32.   The exact implementation of ADTRAN's packet header fields is not publicly available and a review of ADTRAN's source code is necessary to Plaintiff's theories of Defendant's past and/or continued infringement.

Willful Infringement

33.   Defendant has had actual knowledge of the '669 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated October 2, 2017.

34.   Defendant has had actual knowledge of the '669 Patent and its infringement thereof at least as of service of Plaintiff's Original Complaint.

35.   Defendant's infringement of the Asserted Patents was either known or was so obvious that it should have been known to Defendant.

36.   Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard infringed the '669 Patent. Defendant continued to commit acts of infringement despite being on notice of an objectively high likelihood that its actions constituted infringement of Plaintiff's valid patent rights, either literally or equivalently.

37.   Defendant is therefore liable for willful infringement. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

38.   Defendant has induced and is knowingly inducing its distributors, testers, trainers, customers and/or end users to directly infringe the '669 Patent, with the specific intent to induce acts constituting infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

39.   Defendant has knowingly contributed to direct infringement by its customers and end users 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.

40.   Defendant's 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, including: ADTRAN NetVanta 3448 Multiservice Access Router Datasheet; Configuring PPP in AOS; and ADTRAN Operating System (AOS) Command Reference Guide AOS Version R12.3.0.

41.   Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers

19

on infringing uses of the '669 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. Defendant knows and intends that customers who purchase the '669 Accused Products will use those products for their intended purpose. For example, Defendant's United States website, https://www.ADTRAN.com, instructs customers to use the '669 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/channel/UCwNcc0XO_f9Xl17A_MQ1r5w) and elsewhere providing instructions on using the '669 Accused Products. Defendant's customers directly infringe the '669 patent when they follow Defendant's provided instructions on website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '669 Patent.

42.   In addition, Defendant specifically intends 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 Defendant's infringing products. Defendant knows following its instructions directly infringes claims of the '669 Patent, including for example Claim 1.

43.   NetVanta 3448 Multiservice Access Routers implement a method for transmitting data over a channel.

Standards Protocols

Complementing the versatile hardware, the AOS allows for the support of standards-based switching, Virtual LAN (VLAN) tagging, static and default routes, and demand routing. This enables fast, accurate network convergence using routing protocols such as BGP, OSPF, and RIP. In addition, the AOS terminates MPLS, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, and HDLC Wide Area Network (WAN) protocols. Multihoming is also available to provide redundant or backup WAN links to multiple ISPs, guaranteeing a wide-area connection.

Protocols
- eBGP/iBGP
- OSPF
- RIP (v1 and v2)
- PIM Sparse Mode
- Demand Routing
- Policy-based Routing
- GRE
- ATM (ADSL)
- Frame Relay
- Multilink Frame Relay
- Layer 3 Backup
- Multi-VRF CE

- PPP
- Multilink PPP
- PPPoE
- PPPoA
- IGMP v2
- RFC 1483
- HDLC
- PPP Dial Backup
- PAP and CHAP
- Multihoming
- VRRP

https://portal.ADTRAN.com/pub/Library/Data_Sheets/International_/I61200821E1-8_NV3448_english.pdf

Multilink PPP (MLPPP) Overview

Link Aggregation

PPP and other data link layer protocols establish point-to-point connections over a single carrier line. However, a single line may not provide sufficient bandwidth to meet a business' requirements. This lack of bandwidth can lead to congestion and dropped packets.
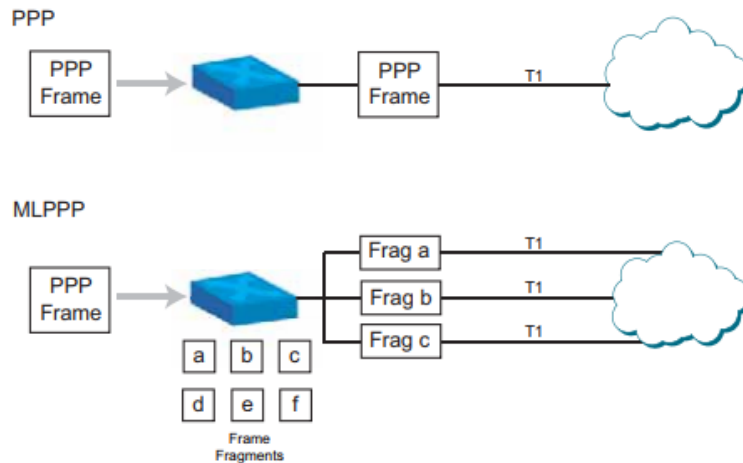
Purchasing a high-bandwidth T3 line to sidestep these limitations is not always feasible because some environments do not support them. In addition, a T3 line can be quite expensive. Often, an organization only wants to double or triple its bandwidth, rather than increase it twenty-eight fold. The purchase of a high-cost T3 line is difficult to justify when much of the bandwidth will not be used.

AOS products support link aggregation protocols, such as MLPPP, to address these problems. Such protocols treat multiple carrier lines as a single bundle, providing two advantages:

• Faster connections - Traffic can access the combined bandwidth of the bundle.

• More stable connections - If one line goes down, the other(s) can still carry traffic.

https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/502/1/Configuring%20PPP%20in%20AOS.pdf (page 6)

22

44.   NetVanta 3448 Multiservice Access Routers receive a first datagram for transmission at a first priority.

Figure 4. Fragmentation in MLPPP

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.

https://supportforums.adtran.com/servlet/JiveServlet/download Body/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf **(Page 22)**

Functional Notes

QoS policies are configured in the ADTRAN Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the match command) and one or more action items (using the priority, bandwidth, shape average, or set commands).

https://supportforums.adtran.com/servlet/JiveServlet/download Body/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (**Page 4387**)

45.   NetVanta 3448 Multiservice Access Routers receive a second datagram for transmission at a second priority, higher than the first priority, before the transmission of the first datagram is completed.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link. Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

46.   NetVanta 3448 Multiservice Access Routers, responsive to receiving the second datagram, decide to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.

MLPPP takes advantage of multiple physical links by fragmenting frames into smaller pieces called frame fragments. These fragments are passed simultaneously over separate cables and then reassembled by the receiving peer (see Figure 4).

Figure 4. Fragmentation in MLPPP

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

47.   NetVanta 3448 Multiservice Access Routers transmit the fragments of

the first datagram over the channel, beginning with the first fragment.

MLPPP takes advantage of multiple physical links by fragmenting frames into smaller pieces called frame fragments. These fragments are passed simultaneously over separate cables and then reassembled by the receiving peer (see Figure 4).
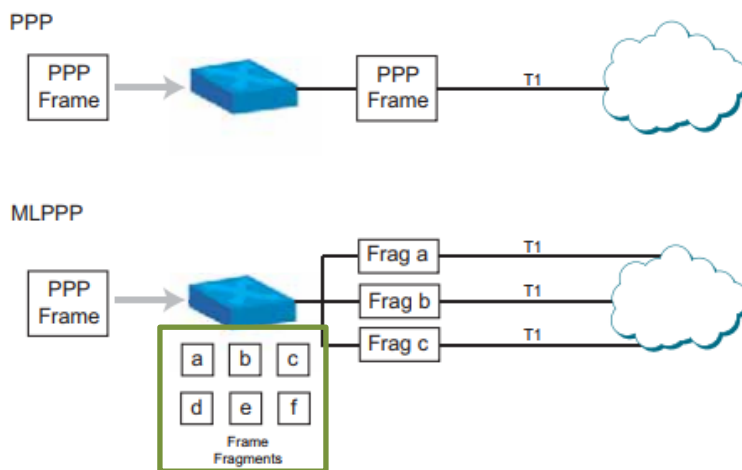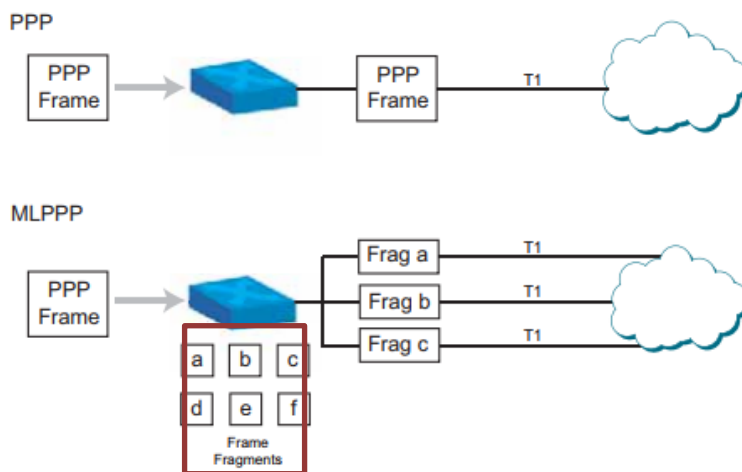

Figure 4. Fragmentation in MLPPP

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 6)

26

48.   NetVanta 3448 Multiservice Access Routers transmit at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. <u>Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link.</u> Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

<u>High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.</u>

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. <u>The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority.</u> In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

49.   In NetVanta 3448 Multiservice Access Routers, 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.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link. Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a "Priority" flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 22)

MLPPP Header

The MLPPP header helps the receiving peer reconstruct frame fragments in the correct order. When a peer sends a PPP frame across an MLPPP connection, it first fragments the PPP frame. It then encapsulates fragments

in new PPP frames and simultaneously sends them over each aggregated line. The new PPP frame includes the following:

• A new PPP header

• A four-field MLPPP header

• A fragment of the original PPP frame

The MLPPP header includes a flag and a sequence number. The sequence number indicates the fragment's place in the reconstructed PPP frame.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 7)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

50.   The NetVanta 3448 Multiservice Access Router adds a field to the fragment indicating the number of datagrams whose transmission has been interrupted.

51.   The NetVanta 3448 Multiservice Access Router includes a variety of headers, including a fragmentation header, PPP header, etc. that include fields indicating the number of fragments whose transmission is interrupted.

Extension Headers in IPv6

An additional difference in IPv4 and IPv6 headers is that the IPv6 packets include extension headers as a method of presenting additional packet and protocol information and options. This additional information is contained between the IPv6 header and the upper-layer header in a packet and allows you to chain extension headers together using the Next Header field. The Next Header field in IPv6 indicates to the router which extension header should be expected next. If there are no additional extension headers, the Next Header field in the IPv6 packet indicates the upper-layer header instead. These upper-layer headers include Transmission Control Protocol (TCP) headers, User Datagram Protocol (UDP) headers, ICMPv6 headers, encapsulated IP packets, etc.

Extension header options are examined at the destination only, except for hop-by-hop options. Extension headers include the following options (in this order):

1. Hop-by-Hop Options Header: Reviewed by all nodes in the packet path.

2. Destination Options Header: Reviewed by intermediate destinations along the packet path when the Routing Header is present.

3. Routing Header: Used to determine the packet path along intermediate nodes before the final packet destination.

4. Fragment Header: Used to break the packet into fragments and put the fragments back together at the final destination. These fragments allow packets larger than the path maximum transmission unit (MTU) to pass.

5. Authentication Header: Part of IPsec. This header functions exactly as in IPv4.

6. Encapsulating Security Payload Header: Part of IPsec. This header functions exactly as in IPv4.

7. Destination Options Header: Reviewed by the final packet destination.

Configuring IPv6 in AOS,
https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/234/1/Configuring%20IPv6%20in%20AOS.pdf   (page 5)

MLPPP Header

The MLPPP header helps the receiving peer reconstruct frame fragments in the correct order. When a peer sends a PPP frame across an MLPPP connection, it first fragments the PPP frame. It then encapsulates fragments in new PPP frames and simultaneously sends them over each aggregated line. The new PPP frame includes the following:

• A new PPP header

• A four-field MLPPP header

• A fragment of the original PPP frame

The MLPPP header includes a flag and a sequence number. The sequence number indicates the fragment's place in the reconstructed PPP frame.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/1654-102-2-1705/Configuring%20PPP%20in%20AOS.pdf (Page 7)

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

https://supportforums.ADTRAN.com/servlet/JiveServlet/downloadBody/2011-102-35-11873/AOS%20R12.3.0%20CRG.pdf (Page 3128)

52.   ADTRAN's Operating System (AOS) allows tracking of several packet fragmentation statistics, including, but not limited to the number of fragmented packets, number of interrupted packets, dropped packets, and out of sequence packets.

```
Enable Mode Command Set                                    Command Reference Guide

>enable
#show frame-relay fragment frame-relay 1.1
DLCI =  17 FRAGMENT SIZE = 100
rx frag. pkts                46      tx frag. pkts               48
rx frag. bytes             4598      tx frag. bytes            4724
rx non-frag. pkts            18      tx non-frag. pkts           28
rx non-frag. bytes         1228      tx non-frag. bytes        1960
rx assembled pkts            23      tx pre-fragment pkts        34
rx assembled bytes         5478      tx pre-fragment bytes     6324
dropped reassembling pkts     0      dropped fragmenting pkts     0
rx out-of-sequence fragments  0
rx unexpected beginning fragment 0
```

ADTRAN Operating System, Command Reference Guide, https://supportcommunity.adtran.com/jmaxz83287/attachments/jmaxz83287/nv-aos/428/7/AOS%20R13.12.0%20Command%20Reference%20Guide.pdf (page 654)

53.   The exact implementation of ADTRAN's packet header fields is not publicly available and a review of ADTRAN's source code is necessary to Plaintiff's theories of Defendant's past and/or continued infringement.

54.   As a result of Defendant's 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 U.S.C. § 284.

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

55.   Plaintiff incorporates by reference the allegations in paragraphs 1 through 11 as if fully set forth herein.

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

57.   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.

Technical Description

58.   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)

59.   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 may add when they connect their own equipment to the network." (col. 6, ll. 2-9).

Direct Infringement

60.   Defendant, without authorization or license from Plaintiff, has 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. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '523 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '523 Patent. Defendant further tests and uses, at its own US facilities, its telecommunications equipment that infringes one or more claims of the '523 Patent. Defendant further directly infringes one or more method claims of the '523 Patent by providing the '523 Accused Products which initiate and perform those methods without any user modification. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include ADTRAN NetVanta 4305, and all other substantially similar products (collectively the "'523 Accused Products").

61.   Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendant's 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.

62.   Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendant's NetVanta 4305.

63.   Correct Transmission, in conjunction with the information contained herein, provides an exemplary, non-limiting basis for Defendant's infringement of the '523 Patent attached hereto as Exhibit G.

64.   Defendant's NetVanta 4305 is a non-limiting example of a router that meets all limitations of claim 10 of the '523 Patent, either literally or equivalently.

65.   Defendant's NetVanta 4305 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:

NetVanta 4305

Part Number: 1202890E1

A Modular Access Router that delivers cost-effective Internet access, MPLS, corporate Frame Relay, point-to-point connectivity, ADSL, and VPN for large-bandwidth applications supporting up to

View More Images

eight T1s. The NetVanta 4305 includes a built-in firewall and two Ethernet LAN ports, and can support the optional IPSec Virtual Private Networking (VPN) and Voice Quality Monitoring as well.

- Three-slot, dual-Ethernet IP access router for eight T1s of bandwidth
- Stateful inspection firewall for network security
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering to manage Internet access and enforce Internet usage policies
- Recognizable Command Line Interface (CLI) and intuitive Web-based Graphical User Interface (GUI)

Features and Benefits

- Modular router supporting up to eight T1s
- Dual auto-sensing 10/100Base-T interface for LAN segmentation
- Quality of Service (QoS) for delay-sensitive traffic like Voice over IP (VoIP)
- Inherent URL filtering to manage employee Internet access and enforce Internet usage policies
- Standards-based routing/switching protocols
- Stateful inspection firewall for network security
- Recognizable Command Line Interface (CLI) to reduce learning curve
- Intuitive Web-based Graphical User Interface (GUI) with step-by-step setup wizards
- Wi-Fi Access Controller for centralized management of NetVanta Wireless Access Points (WAPs)

https://portal.adtran.com/web/page/portal/Adtran/product/1202890E1/12

36

Layer 2 Switch Provisioning

As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

○ **Spanning Tree Port Configurations**

Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.

It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.

Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.

More information and detailed configurations options for STP can be found using the document 🄫 **Configuring Spanning Tree in AOS**.

https://supportcommunity.adtran.com/t5/AOS/Switch-Provisioning-Best-Practices/ta-p/23917

Multiservice Routers

Delivering greater throughput, the NetVanta 3448, NetVanta 3458 and NetVanta 1335 Multiservice Access Routers offer a variety of networking functionality wrapped into a single chassis. These VoIP-ready, all-in-one routers include a modular Wide Area Network (WAN) interface, IP router, PoE switch (Layer 2 or Layer 3), firewall, VPN and a built-in Wi-Fi Access Controller. In addition to the convenience and ease-of-use of a single platform, these multi-function routers contribute to a reduced Total Cost of Ownership (TCO).

Modular Routers

ADTRAN's industry-leading series of NetVanta 3000/4000/5000 Modular Routers is designed for cost-effective Internet access, MPLS, Frame Relay, PPP, Ethernet services, point-to-point, ADSL, and VPN connectivity. These full-featured solutions support line rates ranging from 10 Mbps to 750 Mbps, at a cost that is significantly lower than other name-brand routers. The NetVanta 3000 Series is a full-featured, low-cost, access router platform that fits seamlessly into your existing network. For higher-bandwidth applications, the NetVanta 4000 Series offers access routing that supports up to 750 Mbps platform. The NetVanta 5000 Series offers access routing for large-bandwidth applications supporting up to two T3s of performance.

https://portal.ADTRAN.com/web/page/portal/ADTRAN/product/1202890E1/118

66.   Defendant's NetVanta 4305 is a communication device comprising one

or more ports, adapted to send and receive traffic via the label-switched tunnels:

○ **Spanning Tree Port Configurations**

Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.

It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.

Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.

More information and detailed configurations options for STP can be found using the document 🗎 **Configuring Spanning Tree in AOS**.

https://supportforums.ADTRAN.com/docs/DOC-6441

67.   Defendant's NetVanta 4305 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://portal.adtran.com/pub/Library/Product_Brochures/International/NetVanta_Router_Brochure_International.pdf

40

Layer 2 Switch Provisioning

As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

○ Spanning Tree Settings

Though Spanning Tree in AOS does not require configuration to keep a network loop free, all switches must perform spanning tree calculations to keep this protocol working properly. The more efficient the RSTP configurations are, the better the switches will perform.

First off, the root switch of any layer 2 network is very important. The whole spanning "tree" is created from this switch's location in the logical network and it will perform more calculations than the individual switches in the rest of the network. There are two main considerations to this: making sure the root switch can handle the processor load and making sure the root switch is in a central part of the network. The root switch (or switches based on your design) should always reside in the distribution layer and should not be elected so that each switch is taking the least amount of switch links to the network core. Though RSTP will help you do this by default, think about picking a "root" branch of an actual tree assuming that the "core" exists at the very top. You would want to pick the most center branch at the top of the tree below the core. If you pick a lower branch near one side, some switches needlessly have to take a longer path to reach the root switch.

To ensure that a switch is the root switch as long as it is functioning normally, enter the global command **spanning-tree priority 0**. Spanning-tree will always elect this switch the root (make sure there is only one switch in your network set in this manner).

It is also recommended that the network has a alternate root switch as well so that any administrators will know which switch has become the root if the primary root fails. To achieve this, on the desired alternate root switch, enter the global configuration command **spanning-tree priority 4096**. All other switches should have their spanning-tree priorities set to default.

○ Spanning Tree Port Configurations

Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.

It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.

Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.

More information and detailed configurations options for STP can be found using the document **Configuring Spanning Tree in AOS**.

```
BridgeId ::= OCTET STRING (SIZE (8))    -- the
                                        -- Bridge-Identifier
                                        -- as used in the
                                        -- Spanning Tree
-- Protocol to uniquely identify a bridge.  Its first two
-- octets (in network byte order) contain a priority
-- value and its last 6 octets contain the MAC address
-- used to refer to a bridge in a unique fashion
-- (typically, the numerically smallest MAC address
-- of all ports on the bridge).
```

https://supportforums.ADTRAN.com/docs/DOC-6441

Willful Infringement

68.   Defendant has had actual knowledge of the '523 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

69.   Defendant has had actual knowledge of the '523 Patent and its infringement thereof at least as of service of Plaintiff's Original Complaint.

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

71.   Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the '523 Patent. Defendant has 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.

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

Indirect Infringement

73.   Defendant has 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.

74.   Defendant has 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.

75.   Defendant's 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.

76.   Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect

infringement further includes providing application notes instructing its customers on infringing uses of the '523 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. Defendant knows and intends that customers who purchase the '523 Accused Products will use those products for their intended purpose. For example, Defendant's United States website: https://www.ADTRAN.com, instructs customers to use the '523 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/channel/UCwNcc0XO_f9Xl17A_MQ1r5w) and elsewhere providing instructions on using the '523 Accused Products. Defendant's customers directly infringe the '523 patent when they follow Defendant's provided instructions on website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '523 Patent.

77.   In addition, Defendant specifically intends 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 Defendant's infringing products. Defendant knows following its instructions directly infringes claims of the '523 Patent, including for example Claim 1.

78.   Defendant's customers who follow Defendant's provided instructions directly infringe the method of Claim 1 of the '523 Patent.

79.   Defendant instructs its customers use the NetVanta 4305 in a method for communication:

https://portal.adtran.com/web/page/portal/Adtran/product/1202890E1/12

Layer 2 Switch Provisioning

As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

https://supportforums.ADTRAN.com/docs/DOC-6441

80.   Defendant instructs its customers use the NetVanta 4305 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:

Multiservice Routers

Delivering greater throughput, the NetVanta 3448, NetVanta 3458 and NetVanta 1335 Multiservice Access Routers offer a variety of networking functionality wrapped into a single chassis. These VoIP-ready, all-in-one routers include a modular Wide Area Network (WAN) interface, IP router, PoE switch (Layer 2 or Layer 3), firewall, VPN and a built-in Wi-Fi Access Controller. In addition to the convenience and ease-of-use of a single platform, these multi-function routers contribute to a reduced Total Cost of Ownership (TCO).

Modular Routers

ADTRAN's industry-leading series of NetVanta 3000/4000/5000 Modular Routers is designed for cost-effective Internet access, MPLS, Frame Relay, PPP, Ethernet services, point-to-point, ADSL, and VPN connectivity. These full-featured solutions support line rates ranging from 10 Mbps to 750 Mbps, at a cost that is significantly lower than other name-brand routers. The NetVanta 3000 Series is a full-featured, low-cost, access router platform that fits seamlessly into your existing network. For higher-bandwidth applications, the NetVanta 4000 Series offers access routing that supports up to 750 Mbps platform. The NetVanta 5000 Series offers access routing for large-bandwidth applications supporting up to two T3s of performance.

https://portal.ADTRAN.com/web/page/portal/ADTRAN/product/1202890E1/118

Layer 2 Switch Provisioning

As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

○ **Spanning Tree Port Configurations**

Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.

It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.

Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.

More information and detailed configurations options for STP can be found using the document 📄 **Configuring Spanning Tree in AOS**.

https://supportforums.ADTRAN.com/docs/DOC-6441

81.   Defendant instructs its customers use the NetVanta 4305 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:

NetVanta Fixed-port Access Routers

- Affordable routing and switching solutions for business broadband networks

- Innovative ADSL2+ technology provides further reach and higher bandwidth up to 25 Mbps

- Integral stateful inspection firewall protects against DoS attempts

- Optional standards-based IPSec VPN tunneling secures Internet communications

NetVanta 4430

- Three-slot (one Wide Module and two NIM slots), dual-Ethernet

- Terminates up to eight T1s of bandwidth or 200 Mbps Carrier Ethernet (NetVanta 4430)

- Supports optional IPSec VPN tunnels and VQM

- Wi-Fi Access Controller for centralised management of NetVanta APs

- Gigabit Ethernet and SFP interfaces (NetVanta 4430)

Layer 2 Switch Provisioning

As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

> ○ **Spanning Tree Port Configurations**
>
> Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.
>
> It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.
>
> Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.
>
> More information and detailed configurations options for STP can be found using the document 🗎 **Configuring Spanning Tree in AOS**.

```
BridgeId ::= OCTET STRING (SIZE (8))    -- the
                                        -- Bridge-Identifier
                                        -- as used in the
                                        -- Spanning Tree
-- Protocol to uniquely identify a bridge.  Its first two
-- octets (in network byte order) contain a priority
-- value and its last 6 octets contain the MAC address
-- used to refer to a bridge in a unique fashion
-- (typically, the numerically smallest MAC address
-- of all ports on the bridge).
```

https://supportforums.ADTRAN.com/docs/DOC-6441

82.   Defendant instructs its customers use the NetVanta 4305, 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:

> **Layer 2 Switch Provisioning**
>
> As indicated above, a Layer 2 switch in the scope of this document is a switch with no routing capabilities, like a 1st generation NetVanta 1234, or a Layer 3 switch that is in "layer 2 mode" like a NetVanta 1534 with routing disabled and with no units using the switch as their default gateway. This is an important differentiation to make in when deploying switches as Layer 2 only switches (units not in the routing paths). Commonly, a network administrator could assume that having no units pointed at a switch's IP address as a default gateway would mean the switch is not routing. While this is somewhat true, Layer 3 switches can still route multicast traffic in this mode if IP route-cache express is on. If it is, all Layer 3 multicast traffic will be routed between any VLANs configured on the unit. Considering all of this, if intending to deploy a switch as a Layer 2 switch, ADTRAN recommends only enabling one VLAN (the management VLAN) on the switch and disabling routing using the global **no ip routing** command.

○ **Spanning Tree Settings**

Though Spanning Tree in AOS does not require configuration to keep a network loop free, all switches must perform spanning tree calculations to keep this protocol working properly. The more efficient the RSTP configurations are, the better the switches will perform.

First off, the root switch of any layer 2 network is very important. The whole spanning "tree" is created from this switch's location in the logical network and it will perform more calculations than the individual switches in the rest of the network. There are two main considerations to this: making sure the root switch can handle the processor load and making sure the root switch is in a central part of the network. The root switch (or switches based on your design) should always reside in the distribution layer and should not be elected so that each switch is taking the least amount of switch links to the network core. Though RSTP will help you do this by default, think about picking a "root" branch of an actual tree assuming that the "core" exists at the very top. You would want to pick the most center branch at the top of the tree below the core. If you pick a lower branch near one side, some switches needlessly have to take a longer path to reach the root switch.

To ensure that a switch is the root switch as long as it is functioning normally, enter the global command **spanning-tree priority 0**. Spanning-tree will always elect this switch the root (make sure there is only one switch in your network set in this manner).

It is also recommended that the network has a alternate root switch as well so that any administrators will know which switch has become the root if the primary root fails. To achieve this, on the desired alternate root switch, enter the global configuration command **spanning-tree priority 4096**. All other switches should have their spanning-tree priorities set to default.

○ **Spanning Tree Port Configurations**

Individual port configurations are very important to STP processing and calculation as well. STP knows of a network topology change when a link changes state in certain ways. When this happens, the network has to perform calculations to converge to a new "tree". Each time this happens, precious CPU cycles are used to calculate all the different STP equations and processes all of the messages. To help STP out with this, a network administrator can tell STP which ports it needs to pay attention to and which to ignore changes on. This is done through a configuration option called "Edgeport mode". When a port is in Edgeport mode, this means that STP should consider this port as connected to an end user piece of equipment that does not participate in STP nor can cause a loop. When this port changes state, STP will ignore the change and will not re-converge. In a very busy network, this can save 1000s of convergence instances. Furthermore, to protect from a user accidentally plugging a switch into an edgeport and causing a loop, edgeport will still listen for STP messages and convert back to a normal switchport if a BPDU is received.

It is recommended that all ports connected to end user equipment in a network are in Edgeport mode. This can be achieved using the interface level **spanning-tree edgeport** command on each port.

Another concern can be deploying non-AOS switches in the same network with AOS switches. If these switches do not run RSTP/STP, or run their own proprietary protocol to prevent layer 2 loops, it is recommended these are segmented from AOS switches. All links connecting the two "segments" should be configured with the interface level **spanning-tree bpdufilter enable** command. This will segment the two STP domains and they can be managed separately. The only concern is that loops created by redundant links between the two segments must be manually controlled.

More information and detailed configurations options for STP can be found using the document 🗎 **Configuring Spanning Tree in AOS**.

https://supportcommunity.adtran.com/t5/AOS/Switch-Provisioning-Best-Practices/ta-p/23917

83.   As a result of Defendant's 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
INFRINGEMENT OF U.S. PATENT 7,283,465

84.   Plaintiff incorporates by reference the allegations in paragraphs 1 through 11as if fully set forth herein.

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

86.   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.

Technical Description

87.   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*.

88.   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

89.   Defendant, without authorization or license from Plaintiff, has been and is 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. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '465 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '465 Patent. Defendant further tests and uses, at its own US facilities, its telecommunications equipment that infringes one or more claims of the '465 Patent.   Defendant further directly infringes one or more method claims of the '465 Patent by providing the '465 Accused Products which initiate and perform those methods without any user modification. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271.   Exemplary infringing instrumentalities include ADTRAN NetVanta 1500 Series Ethernet Switches, and all other substantially similar products (collectively the "'465 Accused Products").

90.   Correct   Transmission   names   these   exemplary   infringing instrumentalities to serve as notice of Defendant's infringing acts, however 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.

91.   Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271

for the use, manufacture, sale, offer of sale, importation, or distribution of

Defendant's NetVanta 1500 Series Ethernet Switch.

92.   Defendant's NetVanta 1500 Series Ethernet Switch is a non-limiting

example of a an ethernet switch that meets all limitations of claim 1 of the '465

Patent, either literally or equivalently.

93.   Correct Transmission, in conjunction with the information contained

herein, provides an exemplary, non-limiting basis for Defendant's infringement of

the '465 Patent attached hereto as Exhibit H.

94.   Defendant's NetVanta 1500 Series Ethernet Switch comprises a data

communication network:

NetVanta 1550-48

Part Number: 17101548F1

The NetVanta 1550-48 48-port, fully managed Gigabit switch is a part of our portfolio of best switches for Voice over IP (VoIP). Purpose built for enterprises looking to upgrade their networks with high-

View More Images

performance, reliable, scalable and easy to manage switching solutions, the NetVanta 1550-48 switches are ideal for premises or hosted VoIP, Wi-Fi expansion, video streaming, Gigabit to the desktop, and campus networking.

The NetVanta 1550-48 switch offers:

- Advanced multi-layer switching
- "Voice-aware" features
- 10 Gig uplinks
- Built-in surge protection

Features and Benefits

- 48 10/100/1000Base-T ports
- Four SFP+ ports that support up to 10 Gbps each
- Multi-layer switching (Layer 2 and Layer 3)
- Non-blocking switching capacity up to 176 Gbps
- Faster VoIP deployments with VoIP Setup Wizard, Advanced QoS and "zero-touch" phone setup
- Fully managed (Web GUI and CLI)
- Standard RJ-45 console port and Micro-USB port for management
- Limited lifetime warranty
- Included advance hardware replacement

https://portal.ADTRAN.com/web/page/portal/ADTRAN/product/17101548F1/4495

56

95.   Defendant's NetVanta 1500 Series Ethernet Switch comprises a network comprising 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:

ActivChassis Overview

ActivChassis is a feature in which multiple devices, such as Layer 2 or Layer 3 switches, are connected to create a virtual chassis that can be managed as a single virtual switch. In essence, multiple devices are stacked using ActivChassis ports to create a larger logical device comprised of the individual devices. This feature allows multiple devices to share resources and operate as though they are part of a larger chassis-based system, while allowing configuration and control of the logical device from a single member. In ActivChassis, each device adds its set of ports and hardware tables to form a logical device.

ActivChassis in the Network

The following figures illustrate how ActivChassis looks internally (as a connected group of devices sharing resources) and how it looks externally to the rest of the network (as a singular device). *Figure 1* displays an ActivChassis built from four Layer 2/3 switches whose ActivChassis ports are interconnected to form a ring. *Figure 2* displays the external view of the ActivChassis as a single device.
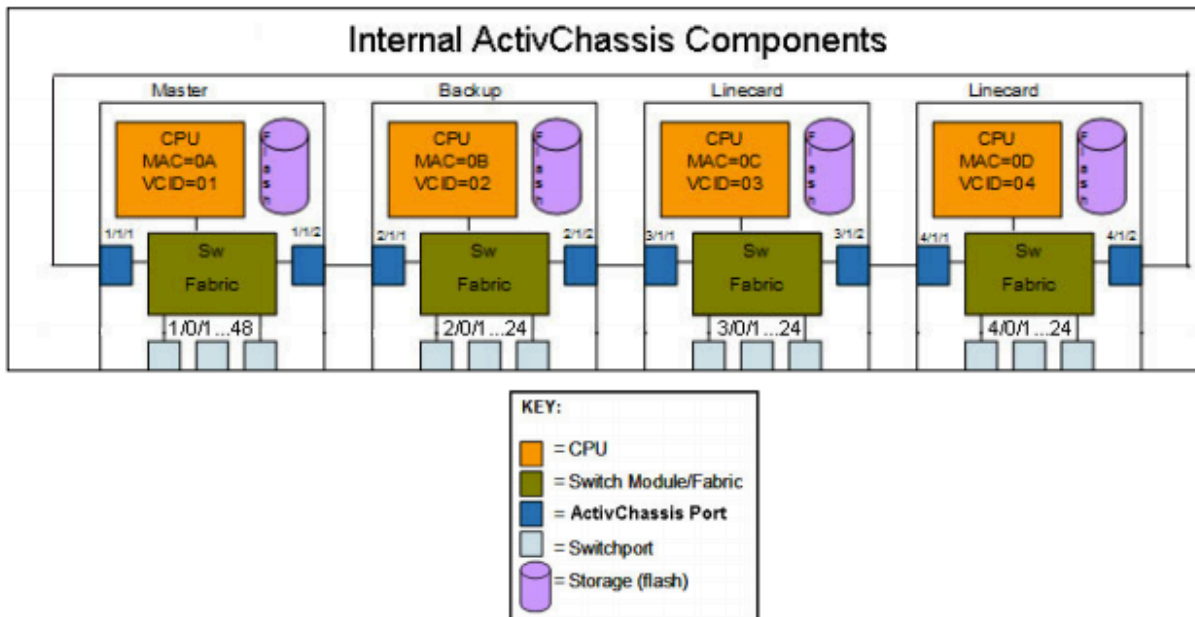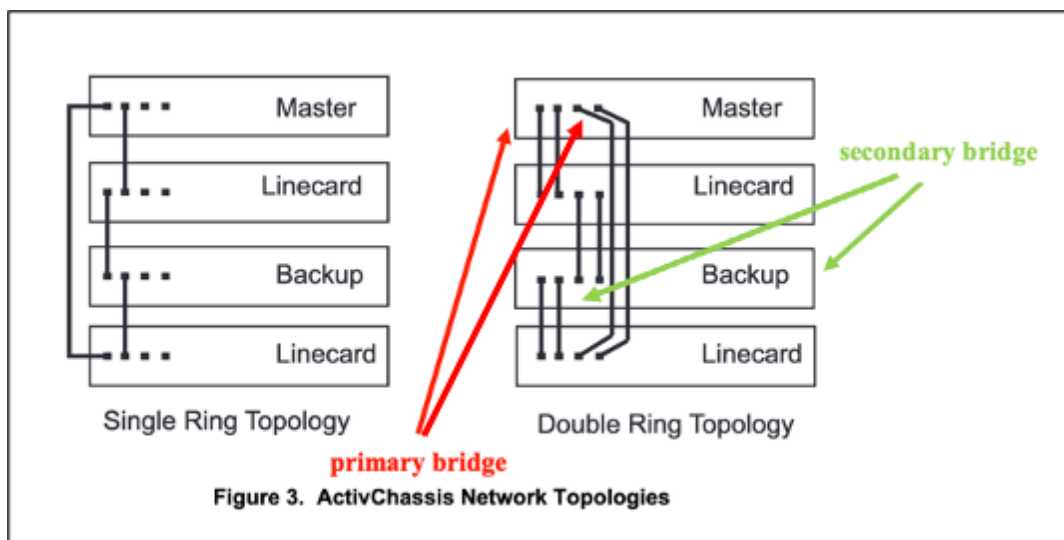

Figure 1. Internal View of ActivChassis

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (pages 2-3)

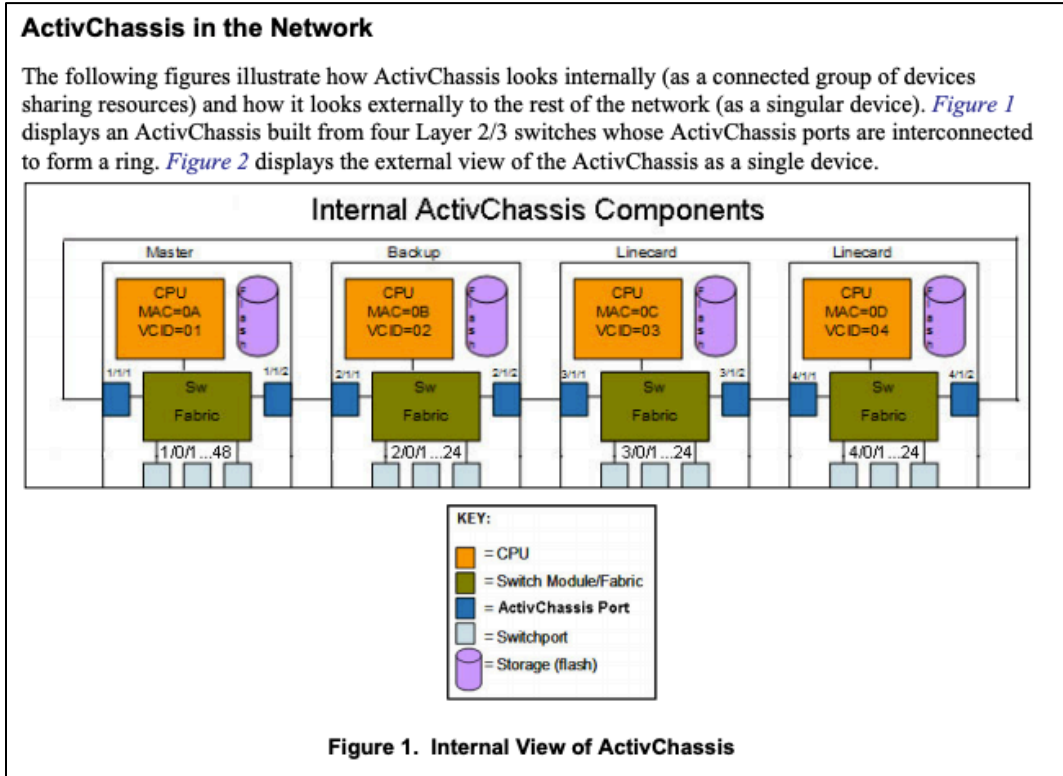96.   For example, the ActivChassis forms a ring network comprising a plurality of primary and secondary bridges.

Figure 3. ActivChassis Network Topologies

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 5)
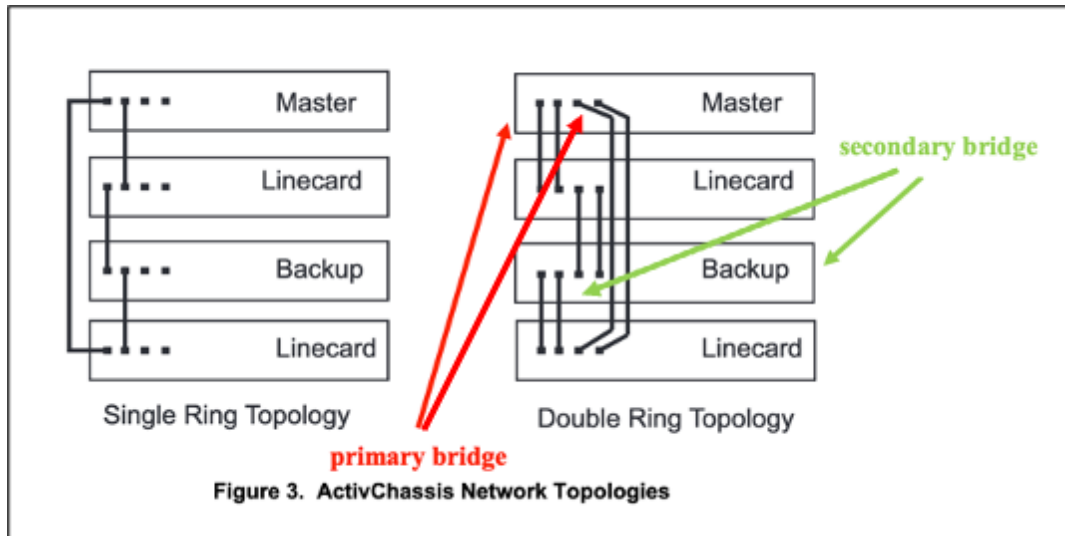
How ActivChassis Functions

ActivChassis functions as a virtual chassis, in which several devices are logically connected to form a larger device. The larger device is a logical construct, a virtual chassis, and is managed by one specific device (the master), which controls and coordinates the operation of the virtual chassis. The many devices connected to create the ActivChassis form a larger routing engine that is composed of the resources of the connected devices. The routing engine begins to operate over ActivChassis once the component devices are connected. ActivChassis component devices include a master device, a backup device, and a linecard device. The master device performs all control functions for the ActivChassis, including coordination of chassis functions, calculation and dissemination of shortest path topology within the chassis backplane, coordination with the backup device, and configuration of the ActivChassis itself. It also provides the management interface for the ActivChassis and the routing engine functions. In the event the master is lost, the backup device takes over as the master device, and shares its configuration and coordination of ActivChassis features with the master device. Linecard devices are neither the master nor the backup devices of the chassis, and supply their physical resources (switchports, Layer 2 and Layer 3 hardware-based forwarding tables, etc.) to the ActivChassis. Linecard devices receive their individual functions from the ActivChassis and are directly controlled by the ActivChassis master device.

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 2)

97. Defendant's NetVanta 1500 Series Ethernet Switch is a network comprising 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:

ActivChassis in the Network

The following figures illustrate how ActivChassis looks internally (as a connected group of devices sharing resources) and how it looks externally to the rest of the network (as a singular device). *Figure 1* displays an ActivChassis built from four Layer 2/3 switches whose ActivChassis ports are interconnected to form a ring. *Figure 2* displays the external view of the ActivChassis as a single device.

Figure 1. Internal View of ActivChassis

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 3)

Figure 3. ActivChassis Network Topologies

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 5)
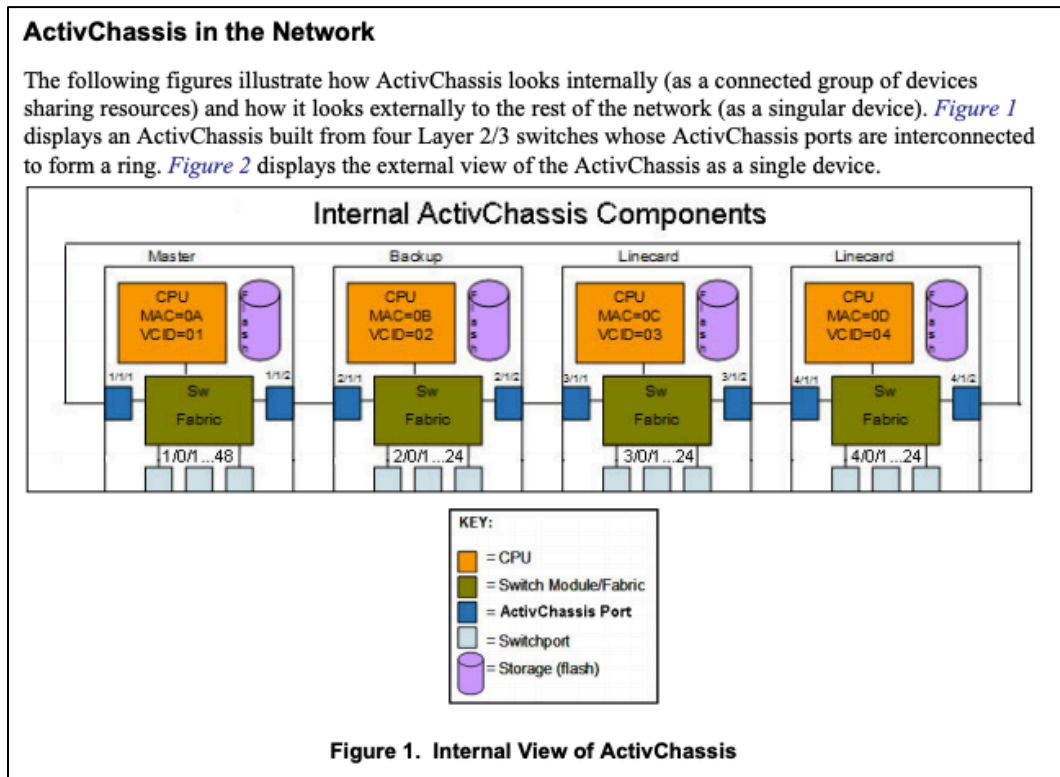
How ActivChassis Functions

ActivChassis functions as a virtual chassis, in which several devices are logically connected to form a larger device. The larger device is a logical construct, a virtual chassis, and is managed by one specific device (the master), which controls and coordinates the operation of the virtual chassis. The many devices connected to create the ActivChassis form a larger routing engine that is composed of the resources of the connected devices. The routing engine begins to operate over ActivChassis once the component devices are connected. ActivChassis component devices include a master device, a backup device, and a linecard device. The master device performs all control functions for the ActivChassis, including coordination of chassis functions, calculation and dissemination of shortest path topology within the chassis backplane, coordination with the backup device, and configuration of the ActivChassis itself. It also provides the management interface for the ActivChassis and the routing engine functions. In the event the master is lost, the backup device takes over as the master device, and shares its configuration and coordination of ActivChassis features with the master device. Linecard devices are neither the master nor the backup devices of the chassis, and supply their physical resources (switchports, Layer 2 and Layer 3 hardware-based forwarding tables, etc.) to the ActivChassis. Linecard devices receive their individual functions from the ActivChassis and are directly controlled by the ActivChassis master device.
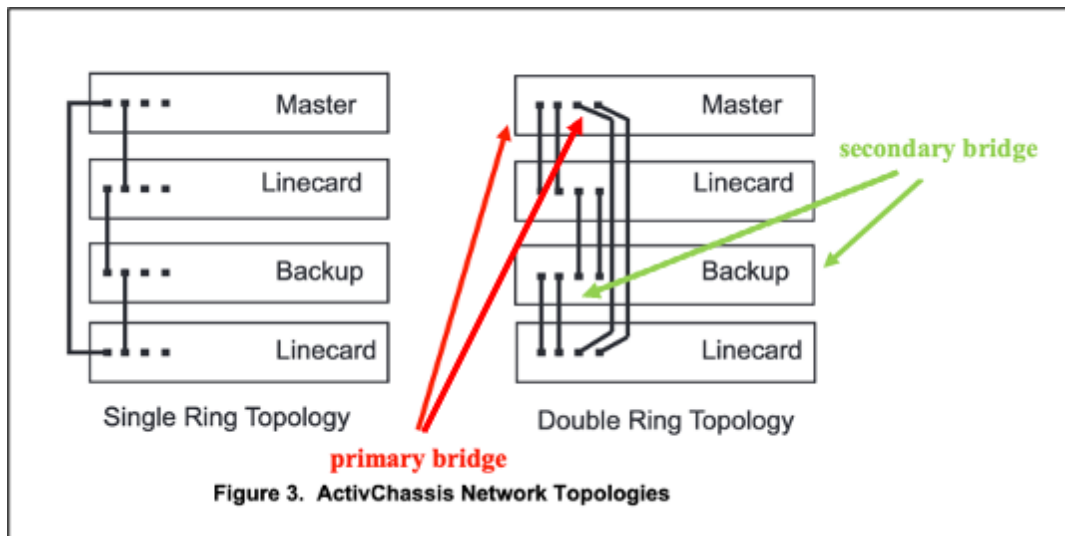
https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 2)

98.   Defendant's NetVanta 1500 Series Ethernet Switch is a network 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:

ActivChassis in the Network

The following figures illustrate how ActivChassis looks internally (as a connected group of devices sharing resources) and how it looks externally to the rest of the network (as a singular device). *Figure 1* displays an ActivChassis built from four Layer 2/3 switches whose ActivChassis ports are interconnected to form a ring. *Figure 2* displays the external view of the ActivChassis as a single device.

Figure 1. Internal View of ActivChassis

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 3)

Figure 3. ActivChassis Network Topologies

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 5)

99.   Defendant's NetVanta 1500 Series Ethernet Switch is a network 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:

How ActivChassis Functions

ActivChassis functions as a virtual chassis, in which several devices are logically connected to form a larger device. The larger device is a logical construct, a virtual chassis, and is managed by one specific device (the master), which controls and coordinates the operation of the virtual chassis. The many devices connected to create the ActivChassis form a larger routing engine that is composed of the resources of the connected devices. The routing engine begins to operate over ActivChassis once the component devices are connected. ActivChassis component devices include a master device, a backup device, and a linecard device. The master device performs all control functions for the ActivChassis, including coordination of chassis functions, calculation and dissemination of shortest path topology within the chassis backplane, coordination with the backup device, and configuration of the ActivChassis itself. It also provides the management interface for the ActivChassis and the routing engine functions. In the event the master is lost, the backup device takes over as the master device, and shares its configuration and coordination of ActivChassis features with the master device. Linecard devices are neither the master nor the backup devices of the chassis, and supply their physical resources (switchports, Layer 2 and Layer 3 hardware-based forwarding tables, etc.) to the ActivChassis. Linecard devices receive their individual functions from the ActivChassis and are directly controlled by the ActivChassis master device.

ActivChassis and Hardware Tables

ActivChassis devices have local hardware-based forwarding tables for Layer 2 and Layer 3 switching. These resources are shared resources by ActivChassis. In most applications, the hardware tables of the device owning the switchport on which a packet is received (ingress port) determine where the packet is delivered within the ActivChassis (egress port, CPU, etc.). The hardware tables of each device are transparent to external operation. Hardware tables are used during packet inspection at ingress to the ActivChassis and switch the packet as quickly as possible towards its final destination within the chassis. If

packet and it is switched across the ActivChassis backplane to the destination port, often without further inspection for basic Layer 2 and Layer 3 switching. In addition to the typical information contained in Layer 2 and Layer 3 hardware tables, the destination port of each table entry (MAC address of IP network) is also mapped to its ActivChassis address. When an ActivChassis header is applied to the packet at ingress, the ActivChassis addresses of the source (ingress) and destination (egress) ports are mapped into the ActivChassis header.

The master device then synchronizes certain content of its file system to each ActivChassis member's file system. Information that is synchronized includes the hardware manifest and the primary and backup software image. Additionally, the master device's startup configuration is synchronized to the active backup device. Not included in the synchronization are the VCID setting of the local device.

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (pages 2, 11-12)
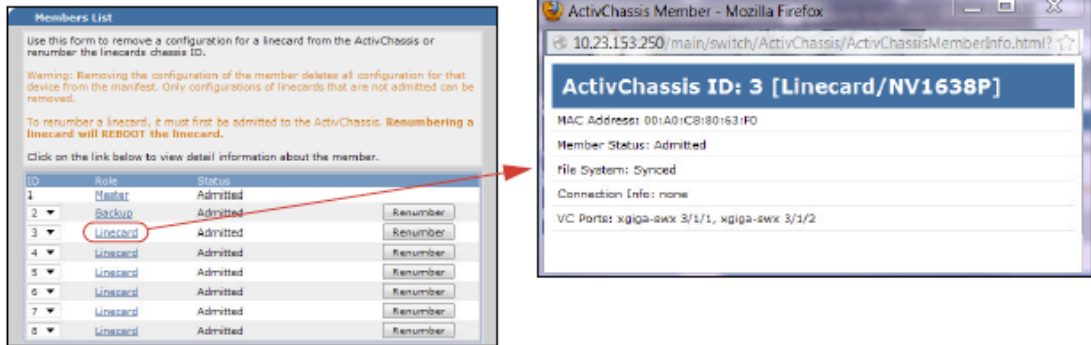
100.   After the initial synchronization between the master device and backup devices, periodic synchronization occurs, i.e., when there is a change in the configuration.

> After the initial synchronization, additional synchronization only takes place when the information on the master device's file system changes, for example, when the running configuration is written to the startup configuration file, or when a new device is admitted to ActivChassis and the manifest is updated. There may be a slight delay before a change in the master device's file system is fully synchronized with the other members.

https://portal.ADTRAN.com/web/page/portal/ADTRAN/product/17101548F1/4495

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 34)

101.   Defendant's NetVanta 1500 Series Ethernet Switch is a network 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:

> **Backup**: In this role, the device performs as a backup to the master device. When the master device is operational, the backup device performs as a linecard device, except that its files are fully synchronized with that of the master device. The backup device becomes the master if the master device fails or is removed from the ActivChassis. In the event a master device fails, the backup device replaces the master device and assumes ActivChassis and routing engine control.

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 6)

> **How ActivChassis Functions**
>
> ActivChassis functions as a virtual chassis, in which several devices are logically connected to form a larger device. The larger device is a logical construct, a virtual chassis, and is managed by one specific device (the master), which controls and coordinates the operation of the virtual chassis. The many devices connected to create the ActivChassis form a larger routing engine that is composed of the resources of the connected devices. The routing engine begins to operate over ActivChassis once the component devices are connected. ActivChassis component devices include a master device, a backup device, and a linecard device. The master device performs all control functions for the ActivChassis, including coordination of chassis functions, calculation and dissemination of shortest path topology within the chassis backplane, coordination with the backup device, and configuration of the ActivChassis itself. It also provides the management interface for the ActivChassis and the routing engine functions. In the event the master is lost, the backup device takes over as the master device, and shares its configuration and coordination of ActivChassis features with the master device. Linecard devices are neither the master nor the backup devices of the chassis, and supply their physical resources (switchports, Layer 2 and Layer 3 hardware-based forwarding tables, etc.) to the ActivChassis. Linecard devices receive their individual functions from the ActivChassis and are directly controlled by the ActivChassis master device.

https://supportcommunity.adtran.com/t5/General/Configuring-ActivChassis-in-AOS/ta-p/24316?attachment-id=2351 (page 2)

Willful Infringement

102.   Defendant has had actual knowledge of the '465 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

103.   Defendant has had actual knowledge of the '465 Patent and its infringement thereof at least as of service of Plaintiff's Original Complaint.

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

105.   Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the '465 Patent. Defendant has 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.

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

Indirect Infringement

107.   Defendant has 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.

108.   Defendant has 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.

109.   Defendant's 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 by configuring a data communication network that meets all of the elements of at least Claims 1 and 16.

110.   Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers on infringing uses of the '46 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. Defendant knows and intends that customers who purchase the '465 Accused Products will use those products for their intended purpose. For example, Defendant's United States website https://www.ADTRAN.com, instructs customers to use the '465 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional   videos   on   YouTube (https://www.youtube.com/channel/UCwNcc0XO_f9Xl17A_MQ1r5w)   and elsewhere providing instructions on using the '465 Accused Products. Defendant's

customers directly infringe the '465 Patent when they follow Defendant's provided instructions on its website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '465 Patent.

111. In addition, Defendant specifically intends 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 Defendant's infringing products.

112. As a result of Defendant's 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

113. Plaintiff incorporates by reference the allegations in paragraphs 1 through 11 as if fully set forth herein.

114. 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.

115. 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.

Technical Description

116.   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*.

117.   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

118.   Defendant, without authorization or license from Plaintiff, has been and is 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. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '928 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '928 Patent. Defendant further tests and uses, at its own US facilities, its telecommunications equipment that infringes one or more claims of the '928 Patent. Defendant further directly infringes one or more method claims of the '928 Patent by providing the '928 Accused Product

which initiate and perform those methods without any user modification. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Total Access 5000, and all other substantially similar products (collectively the "'928 Accused Products").

119.   Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendant's 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.

120.   Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, important, or distribution of Defendant's Total Access 5000.

121.   Defendant's Total Access 5000 is a non-limiting example of an ethernet that meets all limitations of claim 14 of the '928 Patent, either literally or equivalently.

122.   Correct Transmission, in conjunction with the information contained herein, provides an exemplary, non-limiting basis for Defendant's infringement of the '928 Patent attached hereto as Exhibit I.

123.   Defendant's Total Access 5000 is a system for using Connectivity Fault Management (CFM) functions to examine aggregated link connections:

Introduction

The ADTRAN Total Access 5000 is a carrier class Multiservice Access Platform (MSAP) enabling service providers to evolve to an IP/Ethernet network model while preserving legacy investments. The Total Access 5000 is designed around a pure IP/Ethernet core that offers unparalleled bandwidth to each subscriber. The backplane architecture provides a fully redundant, dedicated dual star bus to each individual slot, supporting up to 80 Gbps of non-blocking redundant throughput. This bandwidth scalability, combined with the next generation architecture, ensures a long product lifecycle and long-term investment protection as bandwidth demands continue to increase.

Features and Benefits

- SFP and XFPs for copper and optical connectivity
- 802.ah for Ethernet Operation, Administration and Maintenance (OAM) connectivity fault management
- 802.1p for Class of Service (CoS)
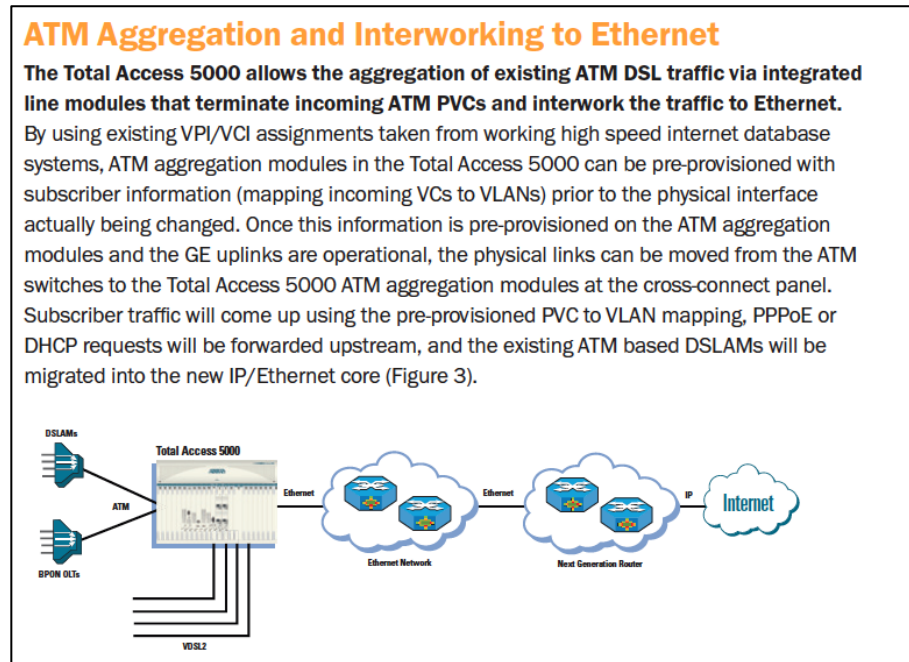
ATM Aggregation and Interworking to Ethernet

The Total Access 5000 allows the aggregation of existing ATM DSL traffic via integrated line modules that terminate incoming ATM PVCs and interwork the traffic to Ethernet.
By using existing VPI/VCI assignments taken from working high speed internet database systems, ATM aggregation modules in the Total Access 5000 can be pre-provisioned with subscriber information (mapping incoming VCs to VLANs) prior to the physical interface actually being changed. Once this information is pre-provisioned on the ATM aggregation modules and the GE uplinks are operational, the physical links can be moved from the ATM switches to the Total Access 5000 ATM aggregation modules at the cross-connect panel. Subscriber traffic will come up using the pre-provisioned PVC to VLAN mapping, PPPoE or DHCP requests will be forwarded upstream, and the existing ATM based DSLAMs will be migrated into the new IP/Ethernet core (Figure 3).
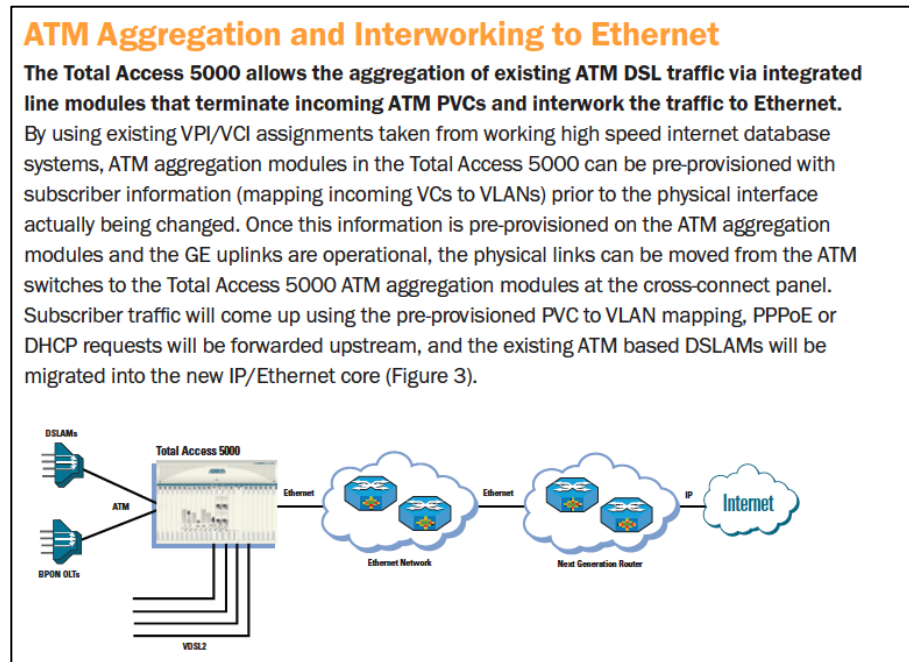
https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

124.   Defendant's Total Access 5000 comprises a plurality of maintenance entities connected to a CFM domain, each one of said maintenance entities comprising a port definer module:

ATM Aggregation and Interworking to Ethernet

The Total Access 5000 allows the aggregation of existing ATM DSL traffic via integrated line modules that terminate incoming ATM PVCs and interwork the traffic to Ethernet. By using existing VPI/VCI assignments taken from working high speed internet database systems, ATM aggregation modules in the Total Access 5000 can be pre-provisioned with subscriber information (mapping incoming VCs to VLANs) prior to the physical interface actually being changed. Once this information is pre-provisioned on the ATM aggregation modules and the GE uplinks are operational, the physical links can be moved from the ATM switches to the Total Access 5000 ATM aggregation modules at the cross-connect panel. Subscriber traffic will come up using the pre-provisioned PVC to VLAN mapping, PPPoE or DHCP requests will be forwarded upstream, and the existing ATM based DSLAMs will be migrated into the new IP/Ethernet core (Figure 3).

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

125.   Defendant's Total Access 5000 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:

ATM Aggregation and Interworking to Ethernet

The Total Access 5000 allows the aggregation of existing ATM DSL traffic via integrated line modules that terminate incoming ATM PVCs and interwork the traffic to Ethernet. By using existing VPI/VCI assignments taken from working high speed internet database systems, ATM aggregation modules in the Total Access 5000 can be pre-provisioned with subscriber information (mapping incoming VCs to VLANs) prior to the physical interface actually being changed. Once this information is pre-provisioned on the ATM aggregation modules and the GE uplinks are operational, the physical links can be moved from the ATM switches to the Total Access 5000 ATM aggregation modules at the cross-connect panel. Subscriber traffic will come up using the pre-provisioned PVC to VLAN mapping, PPPoE or DHCP requests will be forwarded upstream, and the existing ATM based DSLAMs will be migrated into the new IP/Ethernet core (Figure 3).

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

126.   Defendant's Total Access 5000 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:

The Gigabit Ethernet ports can be configured independently to support either network uplinks or downlinks, or they can be "bonded" together via IEEE 802.3ad Link Aggregation to deliver an aggregate two Gigabit Ethernet connection to the network.

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

Willful Infringement

127. Defendant has had actual knowledge the '928 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

128.   Defendant has had actual knowledge of the '928 Patent and its infringement thereof at least as of service of Plaintiff's Original Complaint.

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

130.   Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the '928 Patent. Defendant has 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.

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

Indirect Infringement

132.   Defendant has 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.

133.   Defendant has 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.

134. Defendant's 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.

135. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's 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. Defendant knows and intends that customers who purchase the '928 Accused Products will use those products for their intended purpose. For example, Defendant's United States website: https://www.ADTRAN.com, instructs customers to use the '928 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/channel/UCwNcc0XO_f9Xl17A_MQ1r5w) and elsewhere providing instructions on using the '928 Accused Products. Defendant's

customers directly infringe the '928 patent when they follow Defendant's provided instructions on website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '928 Patent.

136.   In addition, Defendant specifically intends 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 Defendant's infringing products. Defendant knows following its instructions directly infringes claims of the '928 Patent, including for example Claim 22.

137.   Defendant's customers who follow Defendant's provided instructions directly infringe the method of claim 22 of the '928 Patent.

138.   Defendant instructs its customers use the Total Access 5000 to implement connectivity fault management (CFM) functions in a network.
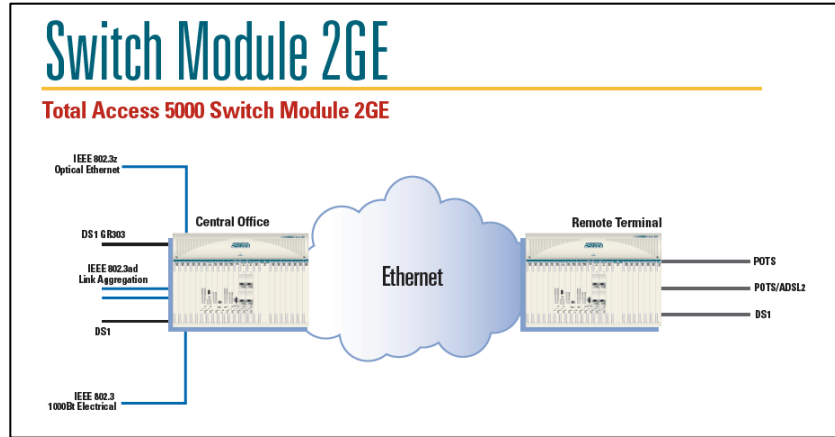
Introduction

The ADTRAN Total Access 5000 is a carrier class Multiservice Access Platform (MSAP) enabling service providers to evolve to an IP/Ethernet network model while preserving legacy investments. The Total Access 5000 is designed around a pure IP/Ethernet core that offers unparalleled bandwidth to each subscriber. The backplane architecture provides a fully redundant, dedicated dual star bus to each individual slot, supporting up to 80 Gbps of non-blocking redundant throughput. This bandwidth scalability, combined with the next generation architecture, ensures a long product lifecycle and long-term investment protection as bandwidth demands continue to increase.

Features and Benefits

- SFP and XFPs for copper and optical connectivity
- 802.ah for Ethernet Operation, Administration and Maintenance (OAM) connectivity fault management
- 802.1p for Class of Service (CoS)

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

139.   Defendant instructs its customers use the Total Access 5000 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:

Introduction

The ADTRAN Total Access 5000 is a carrier class Multiservice Access Platform (MSAP) enabling service providers to evolve to an IP/Ethernet network model while preserving legacy investments. The Total Access 5000 is designed around a pure IP/Ethernet core that offers unparalleled bandwidth to each subscriber. The backplane architecture provides a fully redundant, dedicated dual star bus to each individual slot, supporting up to 80 Gbps of non-blocking redundant throughput. This bandwidth scalability, combined with the next generation architecture, ensures a long product lifecycle and long-term investment protection as bandwidth demands continue to increase.

Features and Benefits

- SFP and XFPs for copper and optical connectivity
- 802.ah for Ethernet Operation, Administration and Maintenance (OAM) connectivity fault management
- 802.1p for Class of Service (CoS)

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5
K_ATM%20to%20Ethernet%20IP.pdf

140.   Defendant instructs its customers use the Total Access 5000 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:

**ATM Aggregation and Interworking to Ethernet**

The Total Access 5000 allows the aggregation of existing ATM DSL traffic via integrated line modules that terminate incoming ATM PVCs and interwork the traffic to Ethernet. By using existing VPI/VCI assignments taken from working high speed internet database systems, ATM aggregation modules in the Total Access 5000 can be pre-provisioned with subscriber information (mapping incoming VCs to VLANs) prior to the physical interface actually being changed. Once this information is pre-provisioned on the ATM aggregation modules and the GE uplinks are operational, the physical links can be moved from the ATM switches to the Total Access 5000 ATM aggregation modules at the cross-connect panel. Subscriber traffic will come up using the pre-provisioned PVC to VLAN mapping, PPPoE or DHCP requests will be forwarded upstream, and the existing ATM based DSLAMs will be migrated into the new IP/Ethernet core (Figure 3).

Switch Module 2GE
Total Access 5000 Switch Module 2GE
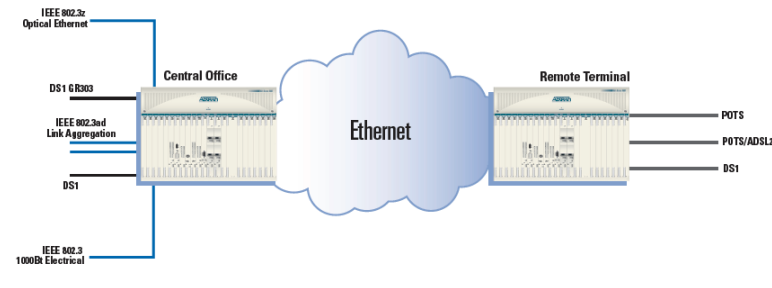
https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

141.   Defendant instructs its customers use the Total Access 5000 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:

> The Gigabit Ethernet ports can be configured independently to support either network uplinks or downlinks, or they can be "bonded" together via IEEE 802.3ad Link Aggregation to deliver an aggregate two Gigabit Ethernet connection to the network.

https://portal.ADTRAN.com/pub/Library/Product_Brochures/Default/CN021_TA5K_ATM%20to%20Ethernet%20IP.pdf

142.   As a result of Defendant's 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

143.   Plaintiff incorporates by reference the allegations in paragraphs 1 through 11 as if fully set forth herein.

144.   The '150 Patent, entitled "VPLS FAILURE PROTECTION IN RING NETWORKS" was filed on January 18, 2006 and issued on July 19, 2011.

145.   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.

Technical Description

146.   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).

147.   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).

148.   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

149.   Defendant, without authorization or license from Plaintiff, has been and is 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. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringe one or more claims of the

'150 Patent. Defendant further provide services that practice methods that infringe one or more claims of the '150 Patent. Defendant further tests and uses, at its own US facilities, its telecommunications equipment that infringes one or more claims of the '150. Patent. Defendant further directly infringes one or more method claims of the '150 Patent by providing the '150 Accused Products which initiate and perform those methods without any user modification. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include ADTRAN NetVanta 8044M Fiber NTE, and all other substantially similar products (collectively the "'150 Accused Products").

150. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendant's 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.

151. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendant's NetVanta 8044M Fiber NTE.

152. Defendant's NetVanta 8044M Fiber NTE is a non-limiting example of switches that operate to meet all limitations of claim 11 of the '150 Patent, either literally or equivalently.

153.   Correct Transmission, in conjunction with the information contained herein, provides an exemplary, non-limiting basis for Defendant's infringement of the '150 Patent and attached hereto as Exhibit J.

154.   Defendant's NetVanta 8044M Fiber NTE 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:

Facilities Protection

- Ethernet Ring Protection Switching (ERPS) ITU-T G.8032
  - ◆ 50 ms failover
  - ◆ 1 or 2.5 Gbps unblocked ring capacity
- Link Protection Group

The NetVanta 8044M supports two variations of fiber access topology: Point-to-Point and Ethernet ring to deliver both legacy ATM/TDM and next-generation IP/Ethernet services.
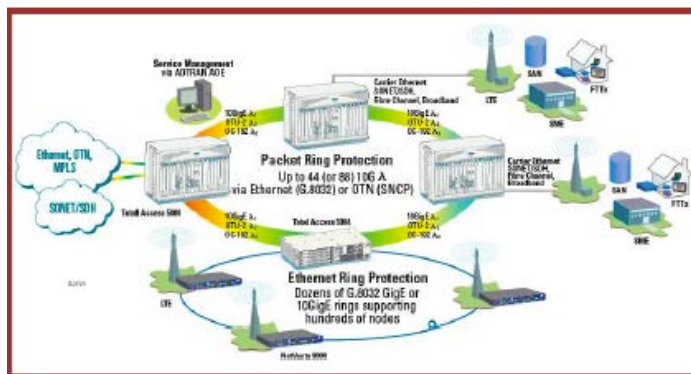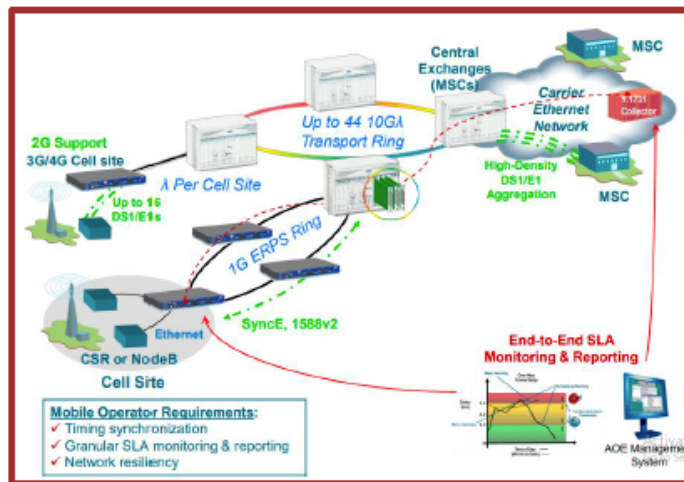
Ethernet Services Support

- Classification of Traffic based on:
  - ◆ Per UNI port, CE VLAN ID (C-Tag) and/or CE VLAN P-bits, Source and/or destination MAC address, DSCP fields
- Single stack VLAN and double stack VLANs (Q-in-Q)
  - ◆ Manipulation based on 802.1p and DSCP fields
  - ◆ STAG TPID provisioning supports 802.1ad and 802.1Q standards
  - ◆ Port based service support
- Services Scale and Flexibility
  - ◆ MEF 9, 14 compliant EPL, EVPL, ELAN, ETREE
  - ◆ 8 Queues, Strict Priority and/or Weighted Fair Schedulers

https://portal.ADTRAN.com/pub/Library/Data_Sheets/Default_Public/6117
4801G1-8_NV8044M.pdf

155.   Defendant's NetVanta 8044M Fiber NTE 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:

https://portal.ADTRAN.com/pub/Library/Data_Sheets/Default_Public/6117
4801G1-8_NV8044M.pdf

**8.2   Topology examples for interconnected Ethernet rings**

Figure 25 represents examples of a topology composed of three or more interconnected Ethernet rings. The R-APS virtual channels are not depicted for simplification. When the sub-ring is operated with an R-APS virtual channel, it is deployed on an Ethernet ring that the sub-ring is connected to, as illustrated in Figure 23 and Figure 24. There is no limit to the number of interconnected Ethernet rings.

a)   Location of the RPL for a sub-ring

The RPL can be placed on any ring link of a sub-ring. The RPL for a sub-ring cannot be placed on a major ring link between the interconnection nodes.

b)   Intermediate Ethernet ring node(s) between interconnection nodes

Ethernet ring node(s) that are part of a major ring can be placed between the interconnection nodes.

c)   Multiple sub-rings connected to a major ring

A major ring can accommodate multiple sub-rings. A pair of two interconnection nodes on a major ring can accommodate multiple sub-rings.

d)   Sub-ring(s) interconnection

A sub-ring can accommodate other sub-ring(s) on its ring link(s). The rules of b) and c) can be applied.

e)   A sub-ring connected to multiple Ethernet rings

A sub-ring can be accommodated in two or more different major rings or sub-rings. For example, sub-ring 2 is attached to a major ring and sub-ring 1, and sub-ring 5 is attached to both sub-ring 3 and sub-ring 4.

f)   A sub-ring attached to multiple major rings

A sub-ring can be attached to multiple major rings that are disjoint relative to each other. Multiple R-APS virtual channels are required (if using the sub-ring with R-APS virtual channel model).

g)   A sub-ring connected to a network that supports any technology network

A sub-ring can be attached to a network that supports any other technology (e.g., xSTP, VPLS, etc.).

https://www.itu.int/rec/T-REC-G.8032/en

156.   Defendant's NetVanta 8044M Fiber NTE 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.

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

https://www.itu.int/rec/T-REC-G.8032/en
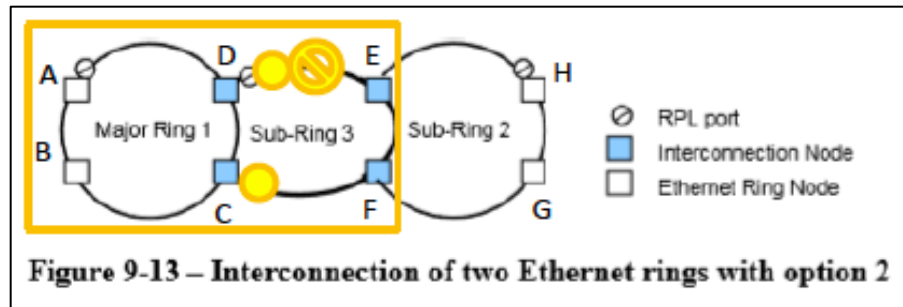
157.   Defendant's NetVanta 8044M Fiber NTE is a communication system wherein as long as the nodes and spans are fully operational, all of the connection terminal points except the selected connection termination point are maintained in a deactivated state, so that only the selected connection termination 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).
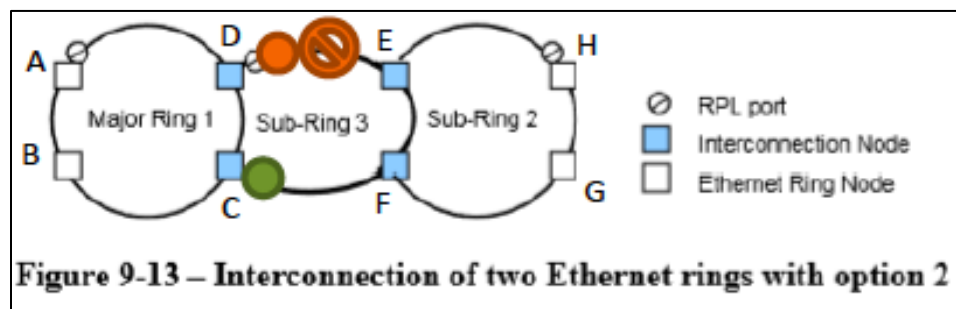>
> Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated 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.

> **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.

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.

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

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

158.   Defendant's NetVanta 8044M Fiber NTE 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 of PDF)**

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.

Source: ITU recommendation ITU-T G.806

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

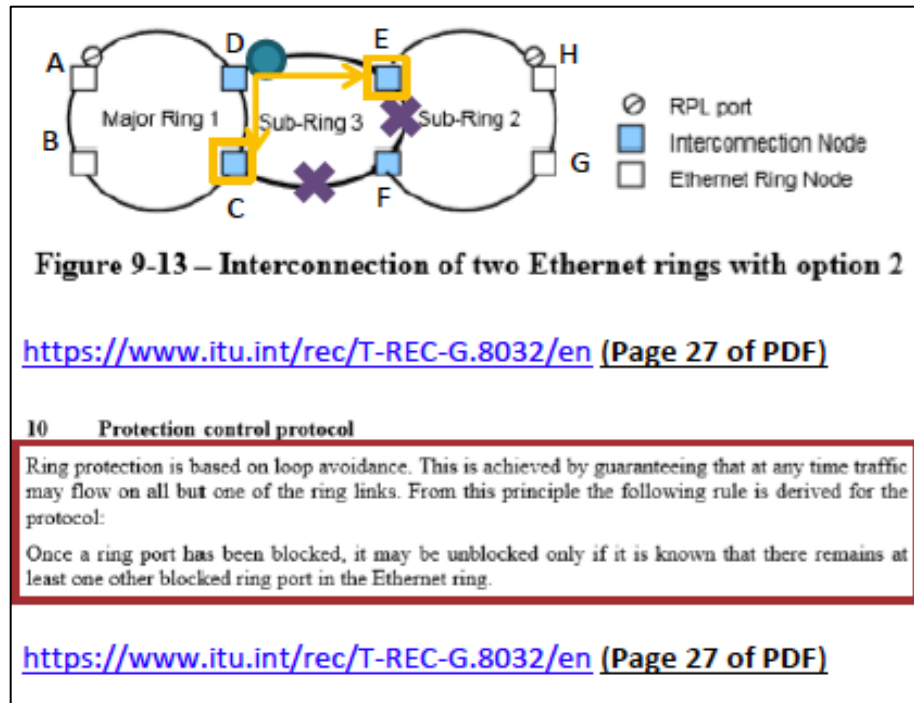https://www.itu.int/rec/T-REC-G.8032/en **(Page 27 of PDF)**

159.   Defendant's NetVanta 8044M Fiber NTE 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 of PDF)**

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

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

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 of PDF)

Willful Infringement

160.   Defendant has had actual knowledge of the '150 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

161.   Defendant has had actual knowledge of the '150 Patent and its infringement thereof at least as of May 2018, when Orckit IP filed an action against Defendant and its German subsidiary in the District Court of Düsseldorf, Germany asserting infringement of EP1974485B1, the European patent corresponding to the '150 Patent, by the NetVanta Product series. The claims of EP1974485B1 are substantially identical in scope to at least some claims in the '150 Patent.

162.   On June 9, 2019, the District Court of Düsseldorf, Germany issued a judgment against ADTRAN, Inc. and ADTRAN GmbH.   The District Court of Düsseldorf found that ADTRAN had infringed EP1974485B1 based on the NetVanta product series.   The German Injunctive relief was awarded in the case.

163.   Defendant has had actual knowledge of the '150 Patent and its infringement thereof at least as of service of Plaintiff's Original Complaint.

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

165.   Notwithstanding this knowledge and notwithstanding the Duesseldorf judgment, Defendant has knowingly or with reckless disregard willfully infringed the '150 Patent.   Defendant has 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.

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

Indirect Infringement

167.   Defendant has 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.

168. Defendant has 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 '150 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.

169. Defendant's 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. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's 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. Defendant knows and intends that customers who purchase the '150 Accused Products will use those products for their intended purpose.   For example, Defendant's United States website https://www.ADTRAN.com, instructs customers

to use the '150 Accused Products in numerous infringing applications. Furthermore,

Defendant   provides   instructional   videos   on   YouTube

(https://www.youtube.com/channel/UCwNcc0XO_f9Xl17A_MQ1r5w)   and

elsewhere providing instructions on using the '150 Accused Products. Defendant's

customers directly infringe the '150 patent when they follow Defendant's provided

instructions on website, videos, and elsewhere. Defendant's customers who follow

Defendant's provided instructions directly infringe claims of the '150 Patent.

170.   In addition, Defendant specifically intends 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 Defendant's infringing products. Defendant knows following its

instructions directly infringes claims of the '150 Patent, including claim 1.

171.   Defendant's customers who follow Defendant's provided instructions

directly infringe the method of claim 1 of the '150 Patent.

172.   Defendant instructs its customers use the NetVanta 8044M Fiber NTE

in a method for communication over a bi-directional ring network that includes

nodes connected by spans of the ring network:

ADTRAN

NetVanta 8044M
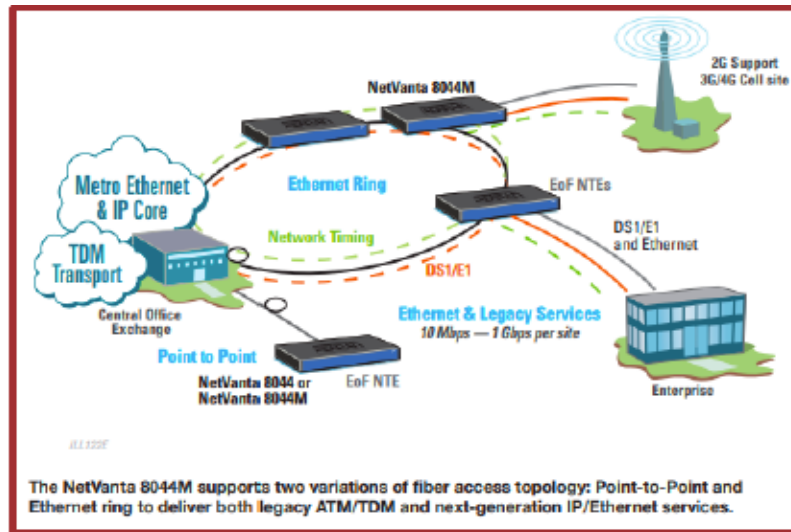Carrier Ethernet Network Termination

Product Specifications

Front Panel Interfaces

- Four 10/100/1000 Base-T Ethernet interfaces via RJ-45
- Four Gigabit Ethernet interfaces via SFP cages, angled to reduce overall product depth and improve cable management
- All Ethernet ports may be used for either network WAN or customer-side LAN connections
- 100BaseX SFP also supported to allow Fast Ethernet fiber lease
- Ethernet faceplate ports support either 1 Gbps or 2.5 Gbps ITU-T G.8032 Ethernet Ring Protection Switching (ERPS)
- DB9 local craft port for support of RS-232 interface for local management
- Two expansion access/service module slots (see next sub-sections for options)
- Field replaceable fan module (may be required to support future expansion modules)
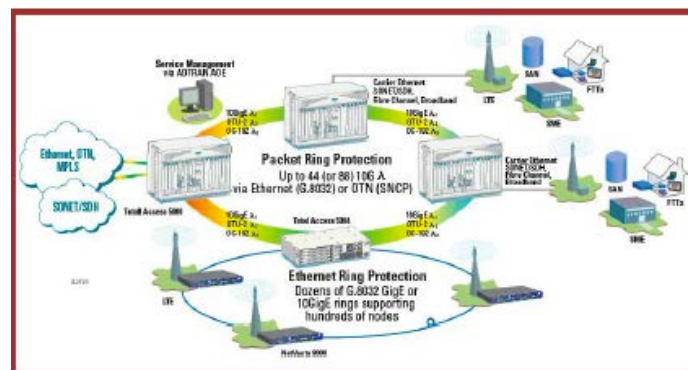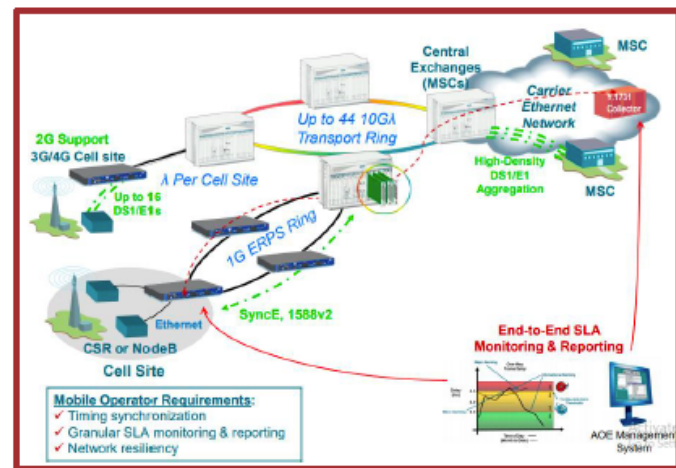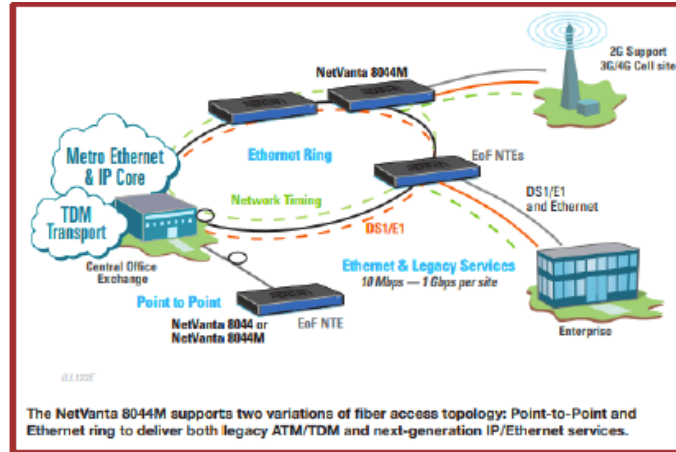
Facilities Protection

- Ethernet Ring Protection Switching (ERPS) ITU-T G.8032
  - 50 ms failover
  - 1 or 2.5 Gbps unblocked ring capacity
- Link Protection Group

97

The NetVanta 8044M supports two variations of fiber access topology: Point-to-Point and Ethernet ring to deliver both legacy ATM/TDM and next-generation IP/Ethernet services.

Ethernet Services Support
- Classification of Traffic based on:
  - Per UNI port, CE VLAN ID (C-Tag) and/or CE VLAN P-bits, Source and/or destination MAC address, DSCP fields
- Single stack VLAN and double stack VLANs (Q-in-Q)
  - Manipulation based on 802.1p and DSCP fields
  - STAG TPID provisioning supports 802.1ad and 802.1Q standards
  - Port based service support
- Services Scale and Flexibility
  - MEF 9, 14 compliant EPL, EVPL, ELAN, ETREE
  - 8 Queues, Strict Priority and/or Weighted Fair Schedulers

https://portal.ADTRAN.com/pub/Library/Data_Sheets/Default_Public/6117480
1G1-8_NV8044M.pdf

173.   Defendant instruct its customers use the NetVanta 8044M Fiber NTE 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:

The NetVanta 8044M supports two variations of fiber access topology: Point-to-Point and Ethernet ring to deliver both legacy ATM/TDM and next-generation IP/Ethernet services.

https://portal.ADTRAN.com/pub/Library/Data_Sheets/Default_Public/61174801G1-8_NV8044M.pdf

**8.2   Topology examples for interconnected Ethernet rings**

Figure 25 represents examples of a topology composed of three or more interconnected Ethernet rings. The R-APS virtual channels are not depicted for simplification. When the sub-ring is operated with an R-APS virtual channel, it is deployed on an Ethernet ring that the sub-ring is connected to, as illustrated in Figure 23 and Figure 24. There is no limit to the number of interconnected Ethernet rings.

a)   Location of the RPL for a sub-ring

The RPL can be placed on any ring link of a sub-ring. The RPL for a sub-ring cannot be placed on a major ring link between the interconnection nodes.

b)   Intermediate Ethernet ring node(s) between interconnection nodes

Ethernet ring node(s) that are part of a major ring can be placed between the interconnection nodes.

c)   Multiple sub-rings connected to a major ring

A major ring can accommodate multiple sub-rings. A pair of two interconnection nodes on a major ring can accommodate multiple sub-rings.

d)   Sub-ring(s) interconnection

A sub-ring can accommodate other sub-ring(s) on its ring link(s). The rules of b) and c) can be applied.

e)   A sub-ring connected to multiple Ethernet rings

A sub-ring can be accommodated in two or more different major rings or sub-rings. For example, sub-ring 2 is attached to a major ring and sub-ring 1, and sub-ring 5 is attached to both sub-ring 3 and sub-ring 4.

f)   A sub-ring attached to multiple major rings

A sub-ring can be attached to multiple major rings that are disjoint relative to each other. Multiple R-APS virtual channels are required (if using the sub-ring with R-APS virtual channel model).

g)   A sub-ring connected to a network that supports any technology network

A sub-ring can be attached to a network that supports any other technology (e.g., xSTP, VPLS, etc.).

https://www.itu.int/rec/T-REC-G.8032/en

174.   Defendant instructs its customers use the NetVanta 8044M Fiber NTE 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.

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

https://www.itu.int/rec/T-REC-G.8032/en
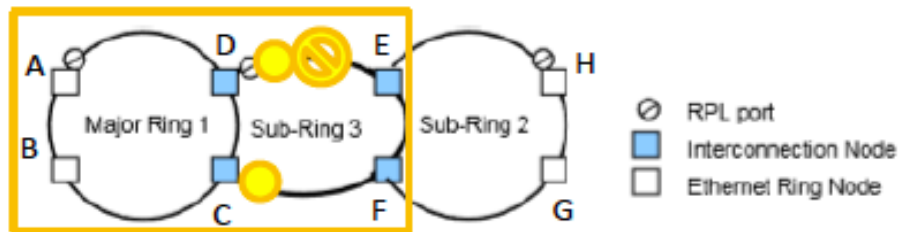
175.   Defendant instructs its customers use the NetVanta 8044M Fiber NTE

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).
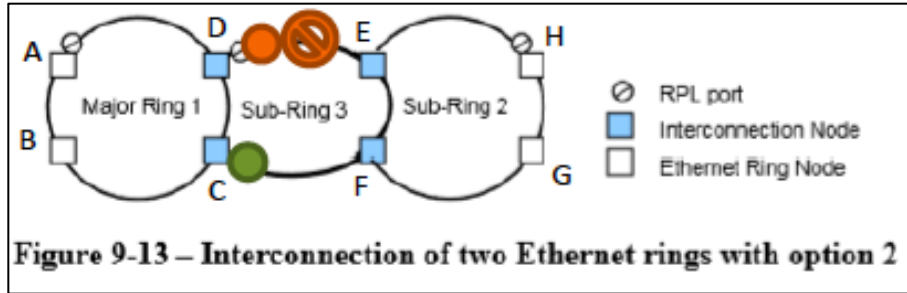>
> Loop avoidance in an Ethernet ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this ring link is blocked, i.e., not used for service traffic. One designated 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.

> 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.

> 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.

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

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

176.   Defendant instructs its customers use the NetVanta 8044M Fiber NTE 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 of PDF)

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.

Source: 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 of PDF)

177.   Defendant instructs its customers use the NetVanta 8044M Fiber NTE 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.
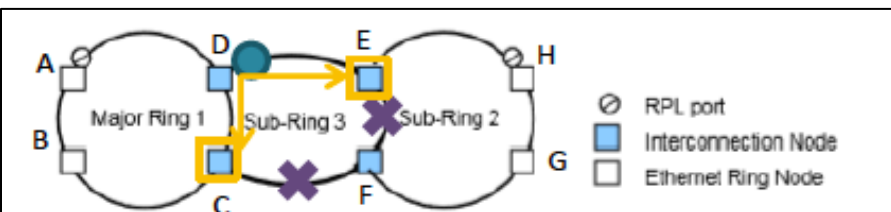
https://www.itu.int/rec/T-REC-G.8032/en **(Page 12 of PDF)**

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

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

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 of PDF)**

178.   As a result of Defendant's 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

179.   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

180.   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 Defendant as follows:

A.   That the Court determine that one or more claims of the Asserted Patents is infringed by Defendant, 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 Defendant;

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 Defendant 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 Defendant's infringements were willful;

G.   That the Court award enhanced damages against Defendant 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: March 21, 2023

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
Scott W. Breedlove
sbreedlove@carterarnett.com
State Bar No. 00790361
Joshua J. Bennett
jbennett@carterarnett.com
Texas Bar No. 24059444
Michael Pomeroy
mpomeroy@carterarnett.com
Texas Bar No. 24098952
Theresa Dawson
Texas Bar No. 24065128
tdawson@carterarnett.com
Monica Litle Goff
mgoff@carterarnett.com
Texas Bar No. 24102101
Nathan Cox
ncox@careterarnett.com
Texas Bar No. 24105751
CARTER ARNETT PLLC
8150 N. Central Expy, 5th Floor
Dallas, Texas 75206
Telephone No. (214) 550-8188
Facsimile No. (214) 550-8185

Rebekah McKinney (ASB-3137-T64J)
mckinney@watsonmckinney.com
WATSON MCKINNEY, LLP
200 Clinton Avenue, W. #110
Huntsville, Alabama 35801
Telephone No.: (256) 536-7453
Facsimile No.: (256) 536-2689

ATTORNEYS FOR PLAINTIFF