IN THE UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

OPTIMORPHIX, INC.,

Plaintiff,

v.

VMWARE, INC.,

Defendant.

Civil Action No._________

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

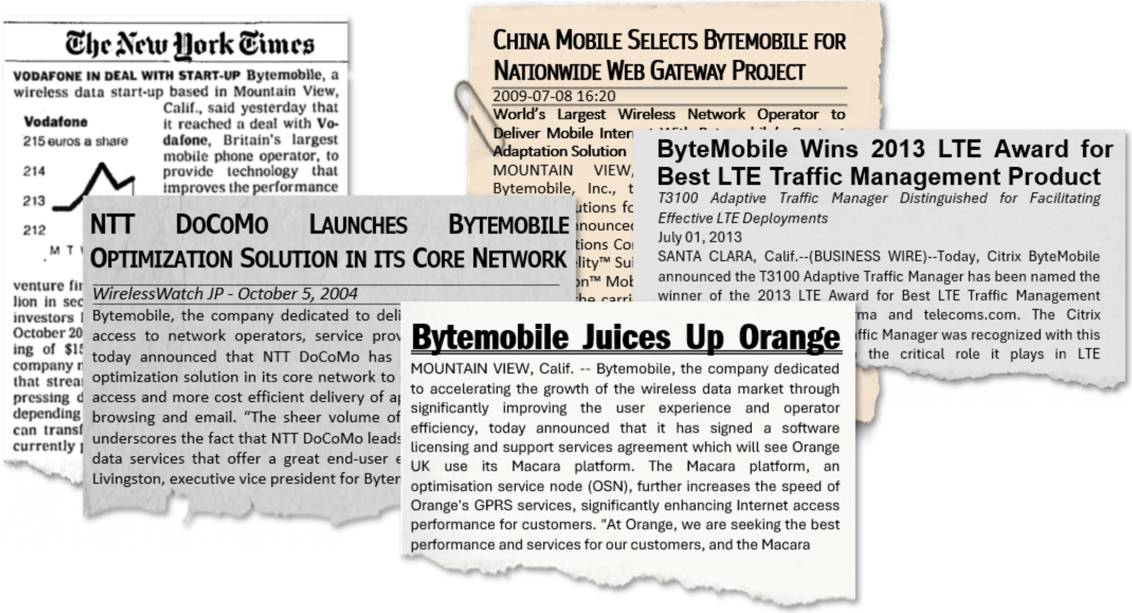
OptiMorphix, Inc. ("OptiMorphix" or "Plaintiff") brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,031,314 (the "'314 patent"); 7,586,871 (the "'871 patent"); 7,616,559 (the "'559 patent"); 7,136,353 (the "'353 patent"); and 8,521,901 (the "'901 patent") (collectively, the "patents-in-suit"). Defendant VMware, Inc. ("VMware" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

THE PARTIES

1. Plaintiff OptiMorphix, Inc. ("Plaintiff" or "OptiMorphix") is a Delaware corporation that holds a portfolio of over 250 patent assets that were developed at Citrix Systems, Inc. ("Citrix") and Bytemobile, Inc.

2. Bytemobile, Inc. ("Bytemobile") was a global leader in mobile internet solutions for network operators. The company was founded in 2000. Bytemobile's mission was to optimize video and web content services for mobile network operators to improve users' experiences while maximizing the efficiency of network infrastructure.

3. Bytemobile was established during a time when the mobile landscape was evolving rapidly. The advent of 3G technology, coupled with increasingly sophisticated smartphones, led to a surge in demand for data services. However, mobile networks at the time were not optimized to handle this influx, particularly for data-rich services like video streaming. Recognizing this opportunity, Bytemobile sought to create solutions that would enable network operators to deliver high-quality, consistent mobile data services. By 2011, Bytemobile was a "market leader in video and web optimization, with more than 125 cumulative operator deployments in 60 countries.[1]



The New York Times

VODAFONE IN DEAL WITH START-UP Bytemobile, a wireless data start-up based in Mountain View, Calif., said yesterday that it reached a deal with Vodafone, Britain's largest mobile phone operator, to provide technology that improves the performance

Vodafone
215 euros a share
214
213
212
M T

venture fi
lion in sec
investors
October 20
ing of $15
company r
that strea
pressing d
depending
can transf
currently

CHINA MOBILE SELECTS BYTEMOBILE FOR NATIONWIDE WEB GATEWAY PROJECT

2009-07-08 16:20

World's Largest Wireless Network Operator to Deliver Mobile Inter
Adaptation Solution

MOUNTAIN VIEW,
Bytemobile, Inc., t
utions fc
nounced
tions Co
lity™ Su
n™ Mob
he carri

ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product

T3100 Adaptive Traffic Manager Distinguished for Facilitating Effective LTE Deployments

July 01, 2013

SANTA CLARA, Calif.--(BUSINESS WIRE)--Today, Citrix ByteMobile announced the T3100 Adaptive Traffic Manager has been named the winner of the 2013 LTE Award for Best LTE Traffic Management
ma and telecoms.com. The Citrix
ffic Manager was recognized with this
the critical role it plays in LTE

NTT DOCOMO LAUNCHES BYTEMOBILE OPTIMIZATION SOLUTION IN ITS CORE NETWORK

WirelessWatch JP - October 5, 2004

Bytemobile, the company dedicated to deli
access to network operators, service prov
today announced that NTT DoCoMo has
optimization solution in its core network to
access and more cost efficient delivery of ap
browsing and email. "The sheer volume of
underscores the fact that NTT DoCoMo leads
data services that offer a great end-user e
Livingston, executive vice president for Byten

Bytemobile Juices Up Orange

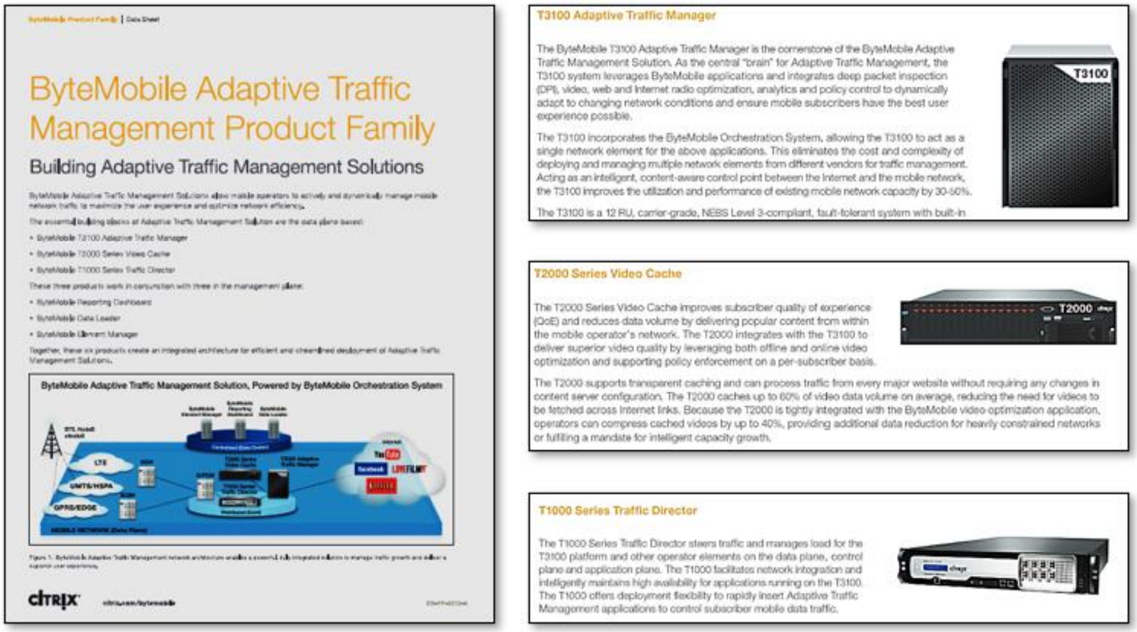
MOUNTAIN VIEW, Calif. -- Bytemobile, the company dedicated to accelerating the growth of the wireless data market through significantly improving the user experience and operator efficiency, today announced that it has signed a software licensing and support services agreement which will see Orange UK use its Macara platform. The Macara platform, an optimisation service node (OSN), further increases the speed of Orange's GPRS services, significantly enhancing Internet access performance for customers. "At Orange, we are seeking the best performance and services for our customers, and the Macara

Andrew Zipern, *Vodafone in Deal with Start-Up Bytemobile,* NYTimes at C4 (January 29, 2002) ("Bytemobile, a wireless data start-up . . . reached a deal with Vodafone, Britain's largest mobile phone operator"); *NTT DoCoMo Launches Bytemobile Optimization Solution in its Core Network,* WIRELESSWATCH IP (October 5, 2004) ("NTT DoCoMo has deployed Bytemobile's optimization solution in its core network"); *China Mobile Selects Bytemobile for Nationwide Web Gateway Project*, BUSINESS WIRE (July 8, 2009) ("A Bytemobile customer since 2004, CMCC has deployed its web optimization solutions"); *Bytemobile Juices Up Orange*, ESPICOM TELECOMMUNICATION NEWS (October 10, 2002) ("Orange customers will experience faster application performance and Web page downloads"); *ByteMobile Wins 2013 LTE Award for Best LTE Traffic Management Product*, MARKETSCREENER (July 1, 2013) ("ByteMobile technology has been deployed . . . in networks serving nearly two billion subscribers.").

[1] *Bytemobile: Importance of Video and Web Optimizations*, TELECOM REVIEW at 58 (2011); *see also Bytemobile Secures Its 36th Video Optimisation Win for MNO Deployment*, TOTAL TELECOM & TOTAL TELECOM MAGAZINE (March 21, 2011).

4. Bytemobile products, such as the Unison platform and the T3100 Adaptive Traffic Manager, were designed to optimize mobile data traffic in real-time, ensuring a high-quality mobile internet experience for end-users. This approach was groundbreaking at the time and set the stage for many of the mobile data optimization techniques used today.

5. Bytemobile's innovative technologies and customer-centric approach led to rapid growth and success. Bytemobile's innovative product portfolio included: the T3100 Adaptive Traffic Manager which was designed to handle high volumes of traffic efficiently and provide real-time optimization, compression, and management of mobile data; Bytemobile's T2000 Series Video Cache, which supported transparent caching of content; and Bytemobile's T1000 Series Traffic Director, which enabled traffic steering and load balancing for high availability of applications.



ByteMobile Product Family | Data Sheet

ByteMobile Adaptive Traffic Management Product Family

Building Adaptive Traffic Management Solutions

ByteMobile Adaptive Traffic Management Solutions allow mobile operators to actively and dynamically manage mobile network traffic to maximize the user experience and optimize network efficiency.

The essential building blocks of Adaptive Traffic Management Solution are the data plane based:

- ByteMobile T3100 Adaptive Traffic Manager
- ByteMobile T2000 Series Video Cache
- ByteMobile T1000 Series Traffic Director

These three products work in conjunction with three in the management plane:

- ByteMobile Reporting Dashboard
- ByteMobile Data Loader
- ByteMobile Element Manager

Together, these six products create an integrated architecture for efficient and streamlined deployment of Adaptive Traffic Management Solutions.

ByteMobile Adaptive Traffic Management Solution, Powered by ByteMobile Orchestration System

ByteMobile Element Manager
ByteMobile Reporting Dashboard
ByteMobile Data Loader
LTE
UMTS/HSPA
GPRS/EDGE
T2000 Series Video Cache
T3100 Adaptive Traffic Manager
T1000 Series Traffic Director
Internet
MOBILE NETWORK (Data Plane)

Figure 1. ByteMobile Adaptive Traffic Management network architecture enables a powerful, fully integrated solution to manage traffic growth and deliver a superior user experience.

citrix citrix.com/bytemobile

T3100 Adaptive Traffic Manager

The ByteMobile T3100 Adaptive Traffic Manager is the cornerstone of the ByteMobile Adaptive Traffic Management Solution. As the central "brain" for Adaptive Traffic Management, the T3100 system leverages ByteMobile applications and integrates deep packet inspection (DPI), video, web and Internet radio optimization, analytics and policy control to dynamically adapt to changing network conditions and ensure mobile subscribers have the best user experience possible.

The T3100 incorporates the ByteMobile Orchestration System, allowing the T3100 to act as a single network element for the above applications. This eliminates the cost and complexity of deploying and managing multiple network elements from different vendors for traffic management. Acting as an intelligent, content-aware control point between the Internet and the mobile network, the T3100 improves the utilization and performance of existing mobile network capacity by 30-50%.

The T3100 is a 12 RU, carrier-grade, NEBS Level 3-compliant, fault-tolerant system with built-in

T2000 Series Video Cache

The T2000 Series Video Cache improves subscriber quality of experience (QoE) and reduces data volume by delivering popular content from within the mobile operator's network. The T2000 integrates with the T3100 to deliver superior video quality by leveraging both offline and online video optimization and supporting policy enforcement on a per-subscriber basis.

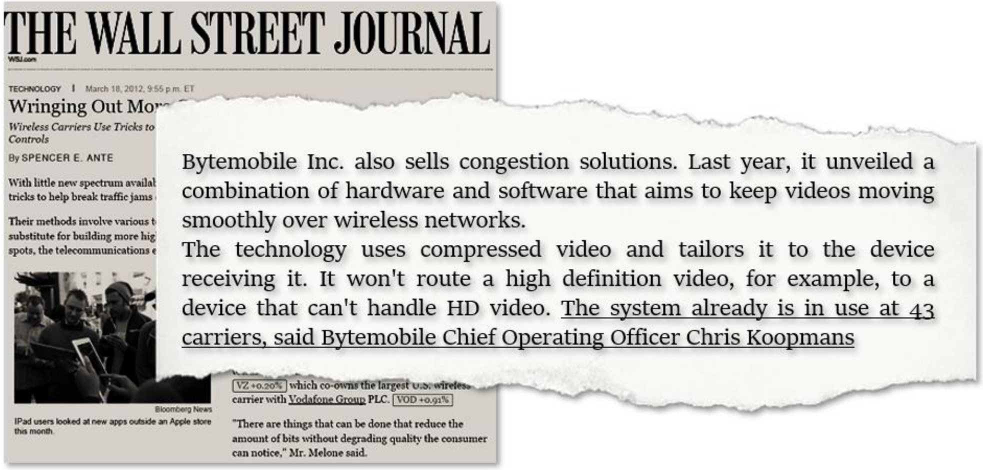
The T2000 supports transparent caching and can process traffic from every major website without requiring any changes in content server configuration. The T2000 caches up to 60% of video data volume on average, reducing the need for videos to be fetched across Internet links. Because the T2000 is tightly integrated with the ByteMobile video optimization application, operators can compress cached videos by up to 40%, providing additional data reduction for heavily constrained networks or fulfilling a mandate for intelligent capacity growth.

T1000 Series Traffic Director

The T1000 Series Traffic Director steers traffic and manages load for the T3100 platform and other operator elements on the data plane, control plane and application plane. The T1000 facilitates network integration and intelligently maintains high availability for applications running on the T3100. The T1000 offers deployment flexibility to rapidly insert Adaptive Traffic Management applications to control subscriber mobile data traffic.

Bytemobile Adaptive Traffic Management Product Family, BYTEMOBILE DATA SHEET at 1-2 (2014).

6. Bytemobile's groundbreaking technologies also included products for data optimization. Bytemobile's data optimization solutions were designed to compress and accelerate data transfer. By reducing the size of data packets without compromising quality, these technologies allowed faster data transmission and minimized network congestion. Bytemobile also offered solutions to analyze and manage network traffic, allowing network operators to identify patterns, allocate bandwidth intelligently, and prioritize different types of content.



THE WALL STREET JOURNAL

WSJ.com

TECHNOLOGY | March 18, 2012, 9:55 p.m. ET

Wringing Out Mor

Wireless Carriers Use Tricks to
Controls

By SPENCER E. ANTE

With little new spectrum availal
tricks to help break traffic jams

Their methods involve various t
substitute for building more hig
spots, the telecommunications e

Bytemobile Inc. also sells congestion solutions. Last year, it unveiled a combination of hardware and software that aims to keep videos moving smoothly over wireless networks.

The technology uses compressed video and tailors it to the device receiving it. It won't route a high definition video, for example, to a device that can't handle HD video. The system already is in use at 43 carriers, said Bytemobile Chief Operating Officer Chris Koopmans

Bloomberg News

IPad users looked at new apps outside an Apple store this month.

VZ +0.20% which co-owns the largest U.S. wireless carrier with Vodafone Group PLC. VOD +0.91%

"There are things that can be done that reduce the amount of bits without degrading quality the consumer can notice," Mr. Melone said.

Spencer E. Ante, *Wringing Out More Capacity*, WALL STREET JOURNAL at B3 (March 19, 2012) (emphasis added).

7. In July 2012, Bytemobile was acquired by Citrix Systems, Inc. ("Citrix") for $435 million. Bytemobile "became part of [Citrix's] Enterprise division and extend[ed] [Citrix's] industry reach into the mobile and cloud markets."[2]

8. OptiMorphix owns a portfolio of patents developed at Bytemobile and later Citrix. Highlighting the importance of the patents-in-suit is the fact that the OptiMorphix's patent portfolio has been cited by over 4,800 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the networking, content delivery, and cloud computing fields. OptiMorphix's patents have been cited by companies such as:

[2] CITRIX SYSTEMS, INC. 2012 ANNUAL REPORT at 33 (2013).

- Amazon.com, Inc. (263 citing patents and applications)[3]
- Oracle (59 citing patents and applications)[4]
- Alphabet, Inc. (103 citing patents and applications)[5]
- Broadcom Ltd. (93 citing patents and applications)[6]
- Cisco Systems, Inc. (277 citing patents and applications)[7]
- Lumen Technologies, Inc. (77 citing patents and applications)[8]
- Intel Corporation (45 citing patents and applications)[9]
- Microsoft Corporation (150 citing patents and applications)[10]
- AT&T, Inc. (93 citing patents and applications)[11]
- Verizon Communications, Inc. (31 citing patents and applications)[12]
- Juniper Networks, Inc. (29 citing patents and applications)[13]

9. Defendant VMware, Inc. ("VMware"), is a corporation organized and existing under the laws of the State of Delaware. On information and belief, VMware is involved in the design, manufacture, use, offering for sale, sale, and/or importation to the United States of the Accused Products defined below. VMware has a registered agent to accept service of process within the State of Delaware located at 251 Little Falls Drive, Wilmington, Delaware 19808.

10. On information and belief, Defendant has used, sold, or offered to sell products and services, including the Accused Products defined herein, in the State of Delaware.

Jurisdiction And Venue

11. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

[3] *See e.g.*, U.S. Patent Nos. 7,817,563; 9,384,204; 9,462,019; 11,343,551; and 11,394,620.
[4] *See e.g.*, U.S. Patent Nos. 7,475,402; 7,574,710; 8,589,610; 8,635,185; and 11,200,240.
[5] *See e.g.*, U.S. Patent Nos. 7,743,003; 8,458,327; 9,166,864; 9,665,617; and 10,733,376.
[6] *See e.g.*, U.S. Patent Nos. 7,636,323; 8,448,214; 9,083,986; 9,357,269; and 10,091,528.
[7] *See e.g.*, U.S. Patent Nos. 7,656,800; 7,930,734; 8,339,954; 9,350,822; and 10,284,484.
[8] *See e.g.*, U.S. Patent Nos. 7,519,353; 8,315,179; 8,989,002; 10,511,533; and 11,233,740.
[9] *See e.g.*, U.S. Patent Nos. 7,394,809; 7,408,932; 9,515,942; 9,923,821; and 10,644,961.
[10] *See e.g.*, U.S. Patent Nos. 8,248,944; 9,071,841; 9,852,118; 10,452,748; and 11,055,47.
[11] *See e.g.*, U.S. Patent Nos. 8,065,374; 8,429,302; 9,558,293; 9,800,638; and 10,491,645.
[12] *See e.g.*, U.S. Patent Nos. 8,149,706; 8,930,559; 9,253,231; 10,003,697; and 10,193,942.
[13] *See e.g.*, U.S. Patent Nos. 8,112,800; 8,509,071; 8,948,174; 9,407,726; and 11,228,631.

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

13. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). VMware is organized under the laws of the State of Delaware.

14. This Court has personal jurisdiction over VMware because it is organized under the laws of the State of Delaware and maintains a registered agent in Delaware.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,031,314

15. U.S. Patent No. 7,031,314 (the "'314 patent") entitled, *Systems and Methods for Providing Differentiated Services Within a Network Communication System*, was filed on April 19, 2002. The '314 patent claims priority to U.S. Provisional Patent Application No. 60/291,918, which was filed on May 16, 2001, and U.S. Provisional Patent Application No. 60/309,213 filed on July 31, 2001. The '314 patent is subject to a 35 U.S.C. § 154(b) term extension of 625 days. A true and correct copy of the '314 patent is attached hereto as Exhibit 1.

16. The '314 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '314 patent.

17. The ‘314 patent is directed to solving the problem of deploying differentiated services within existing network infrastructure. The patent identifies that existing network infrastructure was generally not designed to support a wide variety of application-specific and subscriber-specific services as the corresponding data flowed through a network. “Consequently, the different and potentially incompatible requirements of the increasingly diverse applications, Subscribers and networking environments has placed demands on the existing network infrastructure for which the network infrastructure was not originally designed to handle.” ‘314 patent, col. 1:37-42.

18. The ‘314 patent addresses the issue of identifying the data streams on which to perform the differentiated services, which may involve a significant processing penalty. “The problem with deploying these differentiated services within the existing network infrastructure is that the network infrastructure was not designed to support a wide variety application-specific and subscriber specific services as the corresponding data flows through the network.” ‘314 patent, col. 1:47-52.

19. The inventions disclosed in the ‘314 patent provide significant benefits and improvements to the function of the hardware in a computer network by enabling differentiated services within the network infrastructure. By incorporating a service module within the network infrastructure that can intercept packets, determine whether the connection corresponds to a service application, and then break and reestablish the connection for application-specific processing, the invention allows for a more efficient and flexible network communication system.

20. The inventions taught by the ‘314 patent solves discrete, technological problems associated with computer systems, specifically those related to network communication systems. The patent addresses the limitations of existing network infrastructures that were not designed to

support a wide variety of application-specific and subscriber-specific services as data flows through the network. It also solves the problem of the significant processing penalty associated with identifying the data streams on which to perform the differentiated services.

21. The '314 patent family has been cited by 1,469 United States and international patents and patent applications as relevant prior art. Specifically, 141 United States and international patents and patent applications have cited the '314 patent itself as relevant prior art. The following companies and research institutions have cited the '314 patent as relevant prior art:

- Cisco Technology, Inc.
- Alphabet Inc.
- Oracle Corporation
- International Business Machines Corp.
- Microsoft Corporation
- Qualcomm, Inc.
- Telefonaktiebolaget Lm Ericsson
- Intel Corporation
- Check Point Software Technologies Ltd.
- Hitachi, Ltd.
- Open Text Corporation
- Fujitsu Limited
- Broadcom Limited
- Samsung Electronics Co., Ltd.

U.S. PATENT NO. 7,586,871

22. U.S. Patent No. 7,586,871 (the "'871 patent") entitled, *Platform and Method for Providing Data Services in a Communication Network*, was filed on January 11, 2006. The '871 patent claims priority to U.S. Application Ser. No. 10/061,953, which was filed on February 2, 2002, which claims the benefit of U.S. Provisional Applications No. 60/292,564, which was filed on May 22, 2001, and No. 60/293,756, which was filed on May 25, 2001. The '871 patent also claims the benefit of U.S. Provisional Application No. 60/654,730, which was filed on February

18, 2005. The ‘871 patent is subject to a 35 U.S.C. § 154(b) term extension of 748 days. A true and correct copy of the ‘871 patent is attached hereto as Exhibit 2.

23. The ‘871 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘871 patent.

24. The ‘871 patent generally relates to a communication node and corresponding method for processing data communications passing through the node between a first data network and a second data network. The method includes detecting an event associated with data communication arriving at the node from the first data network, determining whether the data communication is to be suspended for service at the node based on the detected event, and processing suspended data communication based on information in the data communication. The patent also covers the detection of return data communication arriving at the node from the second data network in response to the processed data communication from the first data network. The detected return data communication is allowed to pass through the node without processing the detected return data communication.

25. The ‘871 patent is directed to solving the problem of efficiently providing data services, such as content filtering, in a communication network. This includes the ability to determine whether a packet flow should be suspended for filtering a content request based on packet flow characteristics detected at the layers implemented in hardware, without the need for assistance from higher layers in the architecture implemented in software.

26. The ‘871 patent teaches the use of a communication node that processes data communication between two networks. This node detects an event associated with data communication from the first network, determines whether the data communication should be suspended for service at the node based on the detected event, and processes suspended data

communication based on information in the data communication. The ‘871 patent also teaches the detection of return data communication from the second network in response to the processed data communication from the first network, allowing this return data communication to pass through the node without further processing. This approach allows for more efficient processing of data communication, reducing the need to inspect every packet in a flow and avoiding the need to terminate or establish a communication session associated with the data communication.

27. The inventions disclosed in the ‘871 patent provide significant benefits and improvements to the function of the hardware in a computer network. Specifically, the inventions taught by the ‘871 patent can determine whether a packet flow should be suspended for filtering a content request based on packet flow characteristics detected at the layers implemented in hardware. This improves the efficiency and scalability of content filtering and other services, particularly for mobile data networks that carry delay-sensitive traffic such as voice or video streaming traffic.

28. The ‘871 patent family has been cited by 962 United States and international patents and patent applications as relevant prior art. 166 United States and international patents and patent applications have cited the ‘871 patent itself as relevant prior art. The following companies and research institutions have cited the ‘871 patent as relevant prior art:

- A10 Networks, Inc.
- Thoma Bravo, LLC
- AT&T, Inc.
- NEC Corporation
- Nokia Corporation
- Cisco Systems, Inc.
- Juniper Networks, Inc.
- Fujitsu Limited

U.S. PATENT NO. 7,616,559

29. U.S. Patent No. 7,616,559 (the "'559 patent") entitled, *Multi-Link Network Architecture, Including Security, In Seamless Roaming Communications Systems And Methods*, was filed on September 2, 2004. The '559 patent claims priority to Provisional Application No. 60/499,648, which was filed on September 3, 2003. The '559 patent is subject to a 35 U.S.C. § 154(b) term extension of 638 days. A true and correct copy of the '559 patent is attached hereto as Exhibit 3.

30. The '559 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '559 patent.

31. The '559 patent generally relates to a communications system that provides secure communications of information over multiple communication links. This system includes a client device, a server device, and at least one communication channels, elements, modes, and links for connecting the devices for communication of information between them. The system includes a link detector for determining the existence and usability of the communication links for communication of the information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

32. The '559 patent is directed to solving the problem of ensuring secure and reliable communication over multiple communication links, especially in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics.

33. The ‘559 patent identifies the shortcomings of the prior art. Specifically, the specification describes that when multiple links, both physical elements and the bands or channels within each such element, are employed for communications in data networks, substantial coordination of communicated information, as well as security of the information, is exponentially complicated. In wireless communications, concurrent or sequential operations can occur over cellular or wireless LAN technologies. Each of these wireless communications methods experiences substantially greater complexity in timing, security, packet sequencing, data loss, and connectivity, over wired communications conditions.

34. The ‘559 patent teaches the use of a system that includes a link detector for determining the existence and usability of the communication links for communication of the information, a pathfinder for selecting one or more of the communication links for communication of at least some of the information, a link handover for switching to the selected one or more communication links for communication of the information or portion thereof, and an auto reconnector for re-connecting to detected and selected one or more communication links for communication of the information or portions of it in the event that any communication is hindered, terminated, or upset.

35. The inventions disclosed in the ‘559 patent provide significant benefits and improvements to the function of the hardware in a computer network by ensuring secure and reliable communication over multiple communication links. This is particularly beneficial in environments that include mobile or other roaming devices capable of communicating over multiple channels and with channel switching characteristics. The system’s ability to detect usable communication links, select the most suitable ones, switch between them as needed, and reconnect

in the event of communication disruption greatly enhances the reliability and efficiency of data transmission in a computer network.

36. The ‘559 patent family has been cited by 17 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies and research institutions have cited the ‘559 patent family as relevant prior art:

- International Business Machines Corporation
- Samsung Electronics Co., Ltd
- Alphabet Inc.
- Research In Motion Limited
- BT Group plc

U.S. PATENT NO. 7,136,353

37. U.S. Patent No. 7,136,353 (the "‘353 patent") entitled, *Quality of Service Management for Multiple Connections Within a Network Communication System*, was filed on May 17, 2002. The ‘353 patent claims priority to Provisional Application No. 60/309,212, filed on July 31, 2001 and Provisional Application No. 60/291,825, filed on May 18, 2001. The ‘353 patent is subject to a 35 U.S.C. § 154(b) term extension of 945 days. A true and correct copy of the ‘353 patent is attached hereto as Exhibit 4.

38. The ‘353 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the ‘353 patent.

39. The ‘353 patent primarily relates to managing the quality of service (QoS) in a network communication system, especially focusing on multiple connections between a sender and a receiver. It introduces a methodology where a host-level transmission rate is allocated among multiple connections based on a ratio of a weight associated with each connection and the sum of the weights associated with the connections. This approach aims to optimize the transmission of data packets, particularly in environments where multiple connections to the same

host might compete for bandwidth, ensuring efficient utilization and prioritization of data transmission.

40. The ‘353 patent is directed to solving the problem of efficiently managing multiple connections in a network communication system to optimize data packet transmission and improve the quality of service. It addresses issues related to the allocation of transmission rates among multiple connections, selective transmission of data packets, and ensuring that higher priority connections are allocated a more significant portion of the available transmission rate than lower priority connections.

41. The ‘353 patent identifies shortcomings in the prior art. Specifically, the specification describes that conventional Transport Control Protocol (TCP) architectures, which were primarily designed for reliable, sequenced transmission of non-real-time data streams over high-bandwidth wireline channels, tend to exhibit sub-optimal performance when employed in environments with different or incompatible characteristics, such as wireless networks. Traditional TCP architectures face issues related to flow control, congestion control, and error recovery mechanisms, especially in scenarios involving multiple connections between a sender and a receiver, leading to inefficient use of resources and decreased overall throughput.

42. The inventions disclosed in the ‘353 patent provide significant benefits and improvements to the function of the hardware in a computer network by ensuring that data transmission across multiple connections is managed efficiently and prioritized according to the significance of each connection. The methodology ensures that higher priority connections are allocated more bandwidth, reducing bursty data transmissions and ensuring that data is transmitted at a rate that the communication channel can support, thereby optimizing the utilization of network resources and enhancing the overall quality of service.

43. The invention taught by the ‘353 patent solves discrete, technological problems associated with computer systems; specifically, it addresses the technical challenges related to managing and optimizing data packet transmission across multiple connections in a network communication system. It provides a systematic approach to allocate transmission rates, manage data packet transmission, and prioritize connections, ensuring efficient utilization of network resources and improved quality of service.

44. The technologies taught in the ‘353 patent constitute an improvement in computer network technology by introducing a systematic and efficient methodology to manage multiple connections in a network communication system. The teachings in the ‘353 patent provide a mechanism to allocate transmission rates among connections, selectively transmit data packets, and prioritize connections based on associated weights, ensuring that higher priority connections are allocated a more significant portion of the available transmission rate, thereby optimizing data transmission and enhancing the quality of service in network communication systems.

45. The ‘353 patent family has been cited by 1,469 United States and international patents and patent applications as relevant prior art. Specifically, 77 United States and international patents and patent applications have cited the ‘353 patent itself as relevant prior art. The following companies and research institutions have cited the ‘353 patent as relevant prior art:

- Broadcom Limited
- Cisco Systems, Inc.
- Commscope, Inc.
- Intel Corporation
- Interdigital, Inc.
- Lumen Technologies, Inc
- Microsoft Corporation
- NEC Corporation
- Netapp Inc.
- Nokia Corporation
- Oracle Corporation
- Panasonic Corporation

- Rensselaer Polytechnic Institute
- Samsung Electronics Co., Ltd.
- Telefonaktiebolaget Lm

U.S. PATENT NO. 8,521,901

46. U.S. Patent No. 8,521,901 (the "'901 patent") entitled, *TCP Burst Avoidance*, was filed on December 22, 2008. The '901 patent claims priority to Provisional Patent Application No. 61/017,275, filed on December 28, 2007. The '901 patent is subject to a 35 U.S.C. § 154(b) term extension of 525 days. A true and correct copy of the '901 patent is attached hereto as Exhibit 5.

47. The '901 patent has been in full force and effect since its issuance. OptiMorphix, Inc. owns by assignment the entire right, title, and interest in and to the '901 patent.

48. The '901 patent generally relates to methods and systems for minimizing packet bursts. The '901 patent teaches implementing a packet scheduler layer between the network layer and the transport layer of a device, which smooths the delivery of TCP packets by delaying their delivery, thus addressing the challenges posed by the rapid and bursty transmission of data packets in network communications.

49. The '901 patent is directed to solving the problem of TCP packet bursts in high-speed data networks, which can result from the buffering of TCP acknowledgment packets. These bursts can cause packet loss and inefficient use network bandwidth.

50. The '901 patent identifies the shortcomings of the prior art. Specifically, the specification describes that the prior art does not adequately address the issues of packet loss and inefficient bandwidth utilization resulting from the bursty nature of TCP packet transmission in data networks. The prior technologies do not effectively manage the sudden bursts of TCP

acknowledgment packets, which can be caused by buffering, leading to suboptimal utilization of available bandwidth and undesirable packet loss.

51. The ‘901 patent teaches the use of a packet scheduler layer, which is positioned between the network and transport layers of a device. This layer receives, smoothens (by delaying), and sends TCP packets to ensure that the delivery of these packets is managed in a manner that mitigates the issues of packet bursts. The packet scheduler layer manages both incoming and outgoing packets, ensuring that the transmission of these packets is smoothed out, thereby minimizing packet loss and ensuring more efficient use of available bandwidth. This approach provides benefits that differ from conventional methods by ensuring that TCP packet transmission is managed in a way that minimizes packet loss and ensures efficient bandwidth utilization, thereby addressing the specific challenges posed by TCP packet bursts in high-speed data networks.

52. The invention taught by the ’901 patent solves discrete, technological problems associated with computer systems; specifically, it addresses the issues of packet loss and inefficient bandwidth utilization in high-speed data networks by managing the transmission of TCP packets in a manner that smoothens their delivery, thereby ensuring that the available bandwidth is utilized efficiently and that packet loss is minimized.

53. The ‘901 patent family has been cited by 21 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘901 patent family as relevant prior art:

- Lenovo Group Limited
- Telefonaktiebolaget Lm Ericsson
- Qualcomm, Inc.
- Nippon Telegraph & Telephone Corp.
- Hitachi, Ltd.

- Cisco Systems, Inc.
- Akamai Technologies, Inc.
- Huawei Technologies Co., Ltd.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,031,314

54. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

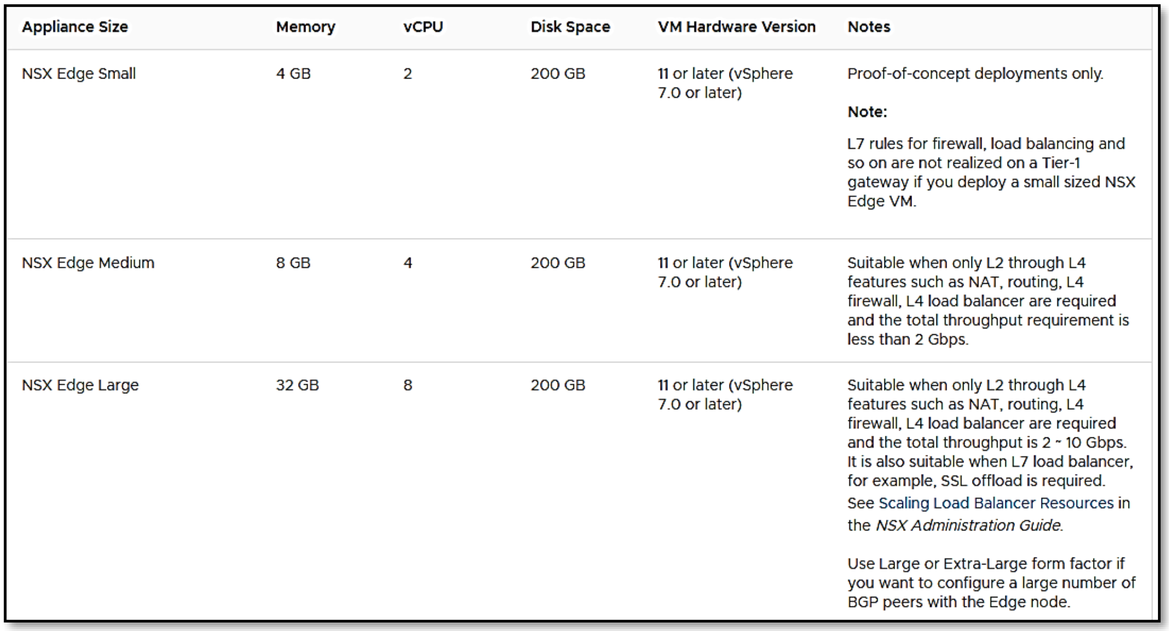
55. VMware designs, makes, uses, sells, and/or offers for sale in the United States products for providing differentiated services within a network communication system.

56. VMware designs, makes, sells, offers to sell, imports, and/or uses the following products: VMware NSX Data Center for vSphere Versions 6.1 and later; VMware NSX Versions 4.0.0.1 and later; VMware NSX-T Data Center Versions 2.0 and later; VMware NSX Advanced Load Balancer Versions 20.1.4 and later; and VMware NSX+ (collectively, the "VMware '314 Product(s)").

57. One or more VMware subsidiaries and/or affiliates use the VMware '314 Products in regular business operations.

58. The VMware '314 Products comprise a processing unit.

59. The VMware '314 Products comprise a storage component, functionally connected to the processor, responsible for retaining data and instructions that, upon execution by the processor, direct the processor's operations.



Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version	Notes
NSX Edge Small	4 GB	2	200 GB	11 or later (vSphere 7.0 or later)	Proof-of-concept deployments only. **Note:** L7 rules for firewall, load balancing and so on are not realized on a Tier-1 gateway if you deploy a small sized NSX Edge VM.
NSX Edge Medium	8 GB	4	200 GB	11 or later (vSphere 7.0 or later)	Suitable when only L2 through L4 features such as NAT, routing, L4 firewall, L4 load balancer are required and the total throughput requirement is less than 2 Gbps.
NSX Edge Large	32 GB	8	200 GB	11 or later (vSphere 7.0 or later)	Suitable when only L2 through L4 features such as NAT, routing, L4 firewall, L4 load balancer are required and the total throughput is 2 ~ 10 Gbps. It is also suitable when L7 load balancer, for example, SSL offload is required. See Scaling Load Balancer Resources in the *NSX Administration Guide*. Use Large or Extra-Large form factor if you want to configure a large number of BGP peers with the Edge node.

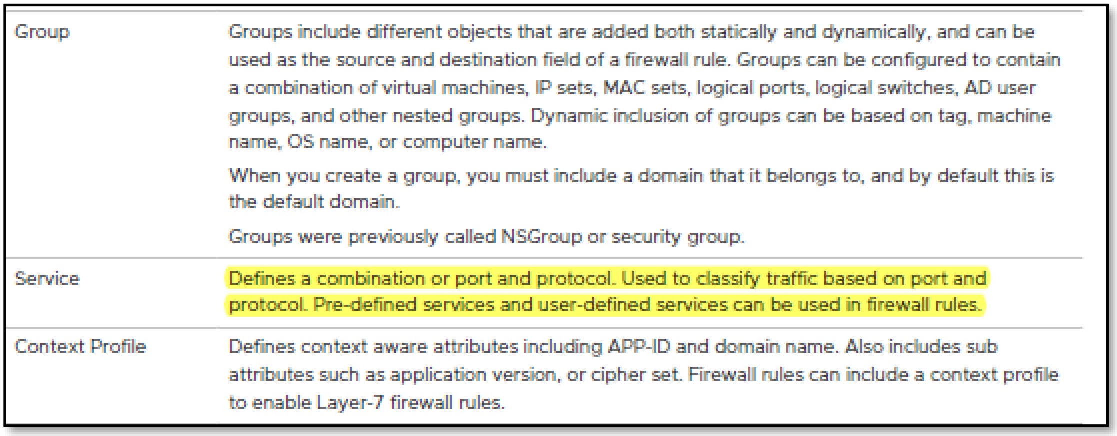
VMware 4.1 NSX Installation Guide, VMWARE DOCUMENTATION at 29-30 (August 22, 2023).

60. The memory unit in the VMware '314 Products stores data related to connections, service applications, and other system elements. In addition, the VMware '314 Products store in memory instructions that guide the processor in classifying connections, forming connections, and redirecting data.

61. The VMware '314 Products contain functionality for requesting a connection between the client and server to ascertain if it aligns with predefined service criteria, where the predetermined service criteria are linked to at least one of the multiple service applications.

62. The VMware '314 Products perform differentiated services within a network communication system. Specifically, The VMware '314 Products contain functionality for classifying a connection that has been requested between the client and the server to determine whether the connection matches predetermined service criteria. When a connection is requested, various attributes of the request are analyzed by the VMware '314 Products. These attributes could include the source, destination, requested service type, priority, or other data associated with the connection.

63. The VMware '314 Products compare attributes associated with a connection against predetermined service criteria. Specifically, the predetermined service criteria can include a set of rules or conditions associated with various service applications.



Group	Groups include different objects that are added both statically and dynamically, and can be used as the source and destination field of a firewall rule. Groups can be configured to contain a combination of virtual machines, IP sets, MAC sets, logical ports, logical switches, AD user groups, and other nested groups. Dynamic inclusion of groups can be based on tag, machine name, OS name, or computer name. When you create a group, you must include a domain that it belongs to, and by default this is the default domain. Groups were previously called NSGroup or security group.
Service	Defines a combination or port and protocol. Used to classify traffic based on port and protocol. Pre-defined services and user-defined services can be used in firewall rules.
Context Profile	Defines context aware attributes including APP-ID and domain name. Also includes sub attributes such as application version, or cipher set. Firewall rules can include a context profile to enable Layer-7 firewall rules.

VMware NSX-T 3.0 Data Center Administration Guide, VMWARE DOCUMENTATION at 228 (September 13, 2023) (emphasis added).

64. The VMware '314 Products contain functionality for establishing an initial connection between the client and the service module, and a subsequent connection between the service module and the server when the connection aligns with the predefined service requirements.

65. The VMware '314 Products include functionality that enables forming two connections: a first connection between the client and the service module, and a second connection between the service module and a server. The forming of a first and second connection is done by the VMware '314 Products in response to a connection matching the predetermined service criteria.

66. The VMware '314 Products orchestrate the formation of a connection between the client and the service module, following the protocols and parameters that relate to the classified service criteria.

67. The VMware ‘314 Products establish a connection between the service module and a server.

68. The VMware ‘314 Products comprise functionality that utilizes the initial and secondary connections to redirect a portion or more of the data communication between the client and a server towards the service application related to the pre-established service parameters.

69. The VMware ‘314 Products comprise a service module that manages the flow of data between the client and the server, directing a portion or all of the data to specific service applications based on the matched criteria.

70. VMware has directly infringed and continues to directly infringe the ‘314 patent by, among other things, making, using, offering for sale, and/or selling technology comprising a system for performing differentiated services within a network communication system, including but not limited to the VMware ‘314 Products.

71. The VMware ‘314 Products are available to businesses and individuals throughout the United States.

72. The VMware ‘314 Products are provided to businesses and individuals located in this District.

73. By making, using, testing, offering for sale, and/or selling products and services comprising a system for performing differentiated services within a network communication system, including but not limited to the VMware ‘314 Products, VMware has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘314 patent, including at least claim 27 pursuant to 35 U.S.C. § 271(a).

74. VMware also indirectly infringes the ‘314 patent by actively inducing infringement under 35 U.S.C. § 271(b).

75. VMware has had knowledge of the ‘314 patent since at least service of this Complaint or shortly thereafter, and VMware knew of the ‘314 patent and knew of its infringement, including by way of this lawsuit.

76. VMware intended to induce patent infringement by third-party customers and users of the VMware ‘314 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. VMware specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘314 patent. VMware performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘314 patent and with the knowledge that the induced acts would constitute infringement. For example, VMware provides the VMware ‘314 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘314 patent, including at least claim 27, and VMware further provides documentation and training materials that cause customers and end users of the VMware ‘314 Products to utilize the products in a manner that directly infringe one or more claims of the ‘314 patent.[14] By providing instruction and training to customers and end-users on how to use the VMware ‘314 Products in a manner that directly infringes one or more claims of the ‘314 patent, including at

[14] *See e.g.*, *VMware NSX 20.1.4 Advanced Load Balancer Configuration Guide*, VMWARE DOCUMENTATION (2021); *VMware NSX Networking! Edges, Routers, Segments and more*, VMWARE NSX YOUTUBE CHANNEL (July 21, 2023), available at: https://www.youtube.com/watch?v=dc-VKzb4NcA; *VMware NSX-T Data Center 3.0 Installation Guide*, VMWARE DOCUMENTATION (August 12, 2021); *VMware NSX-T Data Center 3.0 Administration Guide*, VMWARE DOCUMENTATION (September 13, 2023); *VMware NSX-T Reference Design Guide Software Version 3.0*, VMWARE DOCUMENTATION (December 2020); *VMware NSX Data Center for vSphere 6.4 Administration Guide*, VMWARE DOCUMENTATION (August 25, 2022); and *vSphere Networking For VMware vSphere 7.0*, VMWARE DOCUMENTATION (2023).

least claim 27, VMware specifically intended to induce infringement of the '314 patent. VMware engaged in such inducement to promote the sales of the VMware '314 Products, e.g., through VMware user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '314 patent. Accordingly, VMware has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '314 patent, knowing that such use constitutes infringement of the '314 patent.

77. The '314 patent is well-known within the industry as demonstrated by multiple citations to the '314 patent in published patents and patent applications assigned to technology companies and academic institutions. VMware is utilizing the technology claimed in the '314 patent without paying a reasonable royalty. VMware is infringing the '314 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

78. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '314 patent.

79. As a result of VMware's infringement of the '314 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for VMware's infringement, but in no event less than a reasonable royalty for the use made of the invention by VMware together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,586,871

80. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

81. VMware designs, makes, uses, sells, and/or offers for sale in the United States products that process data communications passing through a node between a first data network and a second data network.

82. VMware designs, makes, sells, offers to sell, imports, and/or uses the following products: VMware NSX-T Data Center Versions 2.0 and later and VMWare NSX Cloud (collectively, the “VMware ‘871 Product(s)”).

83. One or more VMware subsidiaries and/or affiliates use the VMware ‘871 Products in regular business operations.

84. The VMware ‘871 Products detect an event associated with a data communication arriving at the node from a first data network.

85. The VMware '871 Products monitor incoming data packets at the node from a first data network.

86. The VMware ‘871 Products determine whether the data communication is to be suspended for service at the node based on the detected event. Specifically, once an event associated with the data communication is detected by the VMware ‘871 Products, the system evaluates the nature and severity of the event. The decision to suspend or allow the communication is based on rules and policies configured by the VMware ‘871 Products.

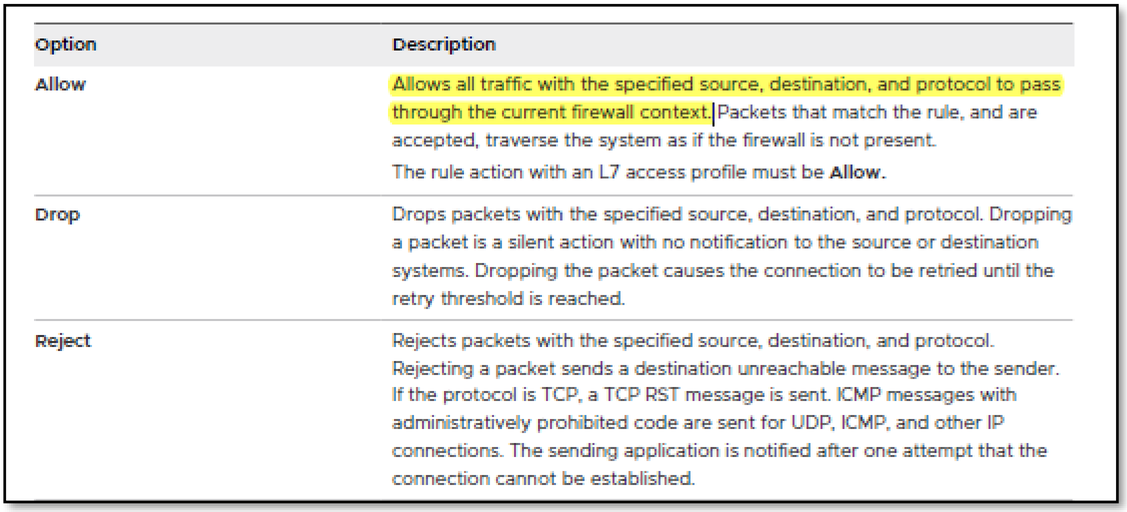
87. The VMware ‘871 Products determine (based on a detected event) whether the data communication should be suspended at the node.

88. The VMware ‘871 Products process one or more suspended data communications using information in the suspended data communication. Specifically, the VMware ‘871 Products isolate the suspended data communication for (at least in part) the purpose of processing the

suspended data communication. Based on the analysis and processing, the VMware '871 Products determine how to handle the suspended data communication.

89. The VMware '871 Products detect a return data communication arriving at the node from the second data network in response to the processed data communication from the first data network. Further, the VMware '871 Products allow the detected return data communication to pass through the node without processing.

90. The VMware '871 Products monitor the incoming data communication from the second data network. If the detected return data communication is associated with prior processed data communication from the first network the VMware '871 Products determine that the return data communication does not need further processing at the node.

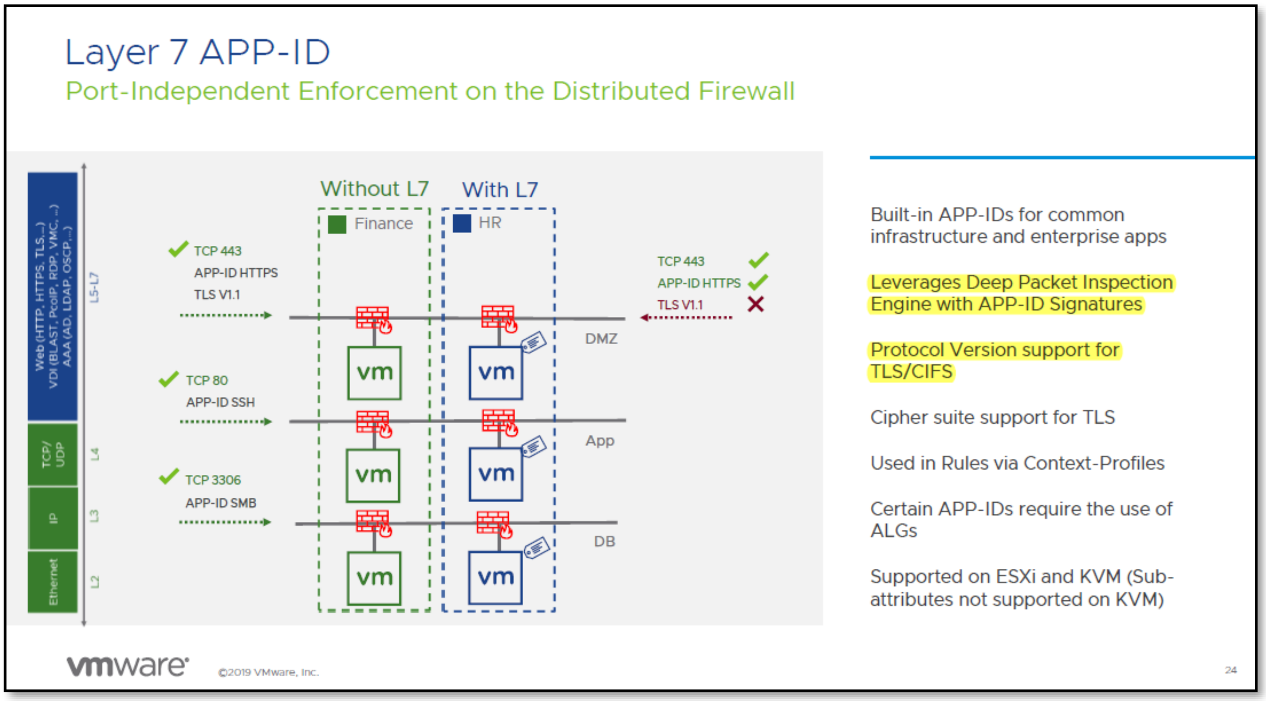


Option	Description
Allow	Allows all traffic with the specified source, destination, and protocol to pass through the current firewall context. Packets that match the rule, and are accepted, traverse the system as if the firewall is not present. The rule action with an L7 access profile must be **Allow**.
Drop	Drops packets with the specified source, destination, and protocol. Dropping a packet is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached.
Reject	Rejects packets with the specified source, destination, and protocol. Rejecting a packet sends a destination unreachable message to the sender. If the protocol is TCP, a TCP RST message is sent. ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections. The sending application is notified after one attempt that the connection cannot be established.

VMware NSX-T Data Center 3.2 Security Quick Start Guide, VMWARE DOCUMENTATION AT 353 (May 17, 2022) (emphasis added).

91. The VMware '871 Products process a suspended data communication based on information in the data communication.

92. The VMWare '871 Products enable Deep Packet Inspection that can be enabled via rules based on a packet stream matching a predefined criteria.



Layer 7 APP-ID

Port-Independent Enforcement on the Distributed Firewall

Built-in APP-IDs for common infrastructure and enterprise apps

Leverages Deep Packet Inspection Engine with APP-ID Signatures

Protocol Version support for TLS/CIFS

Cipher suite support for TLS

Used in Rules via Context-Profiles

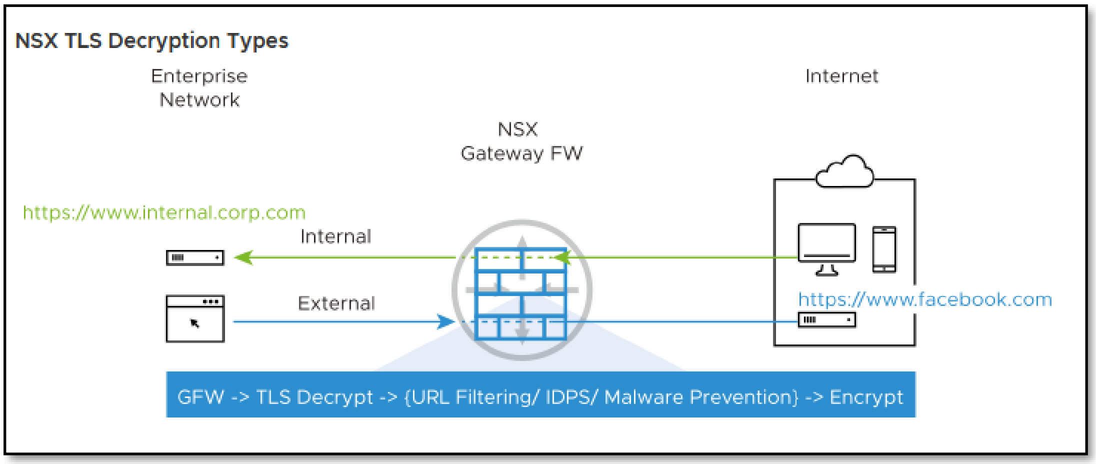
Certain APP-IDs require the use of ALGs

Supported on ESXi and KVM (Sub-attributes not supported on KVM)

vmware® ©2019 VMware, Inc. 24

What's New With NSX-T Micro-Segmentation – SAI2565BU, VMWORLD 2019 PRESENTATION at 24 (2019) (emphasis added).

93. The VMware '871 Products support TLS inspection wherein the '871 Products decrypts encrypted traffic and makes it available for advanced security features such as IDS/IPS, Malware Prevention, and URL Filtering. TLS inspection can be configured to suspend data packets that match certain patterns or rules. The following diagram depicts how the traffic is handled by the TLS internal and external decryption types.



VMware NSX-T Data Center 3.2 Security Quick Start Guide, VMWARE DOCUMENTATION AT 357 (May 17, 2022).

94. VMware has directly infringed and continues to directly infringe the ‘871 patent by, among other things, making, using, offering for sale, and/or selling technology that process data communications passing through a node between a first data network and a second data network, including but not limited to the VMware ‘871 Products.

95. The VMware ‘871 Products are available to businesses and individuals throughout the United States.

96. The VMware ‘871 Products are provided to businesses and individuals located in this District.

97. By making, using, testing, offering for sale, and/or selling products and services that process data communications passing through a node between a first data network and a second data network, including but not limited to the VMware ‘871 Products, VMware has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘871 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

98. VMware also indirectly infringes the ‘871 patent by actively inducing infringement under 35 U.S.C. § 271(b).

99. VMware has had knowledge of the ‘871 patent since at least service of this Complaint or shortly thereafter, and VMware knew of the ‘871 patent and knew of its infringement, including by way of this lawsuit.

100. VMware intended to induce patent infringement by third-party customers and users of the VMware ‘871 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. VMware specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘871 patent. VMware performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘871 patent and with the knowledge that the induced acts would constitute infringement. For example, VMware provides the VMware ‘871 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘871 patent, including at least claim 1, and VMware further provides documentation and training materials that cause customers and end users of the VMware ‘871 Products to utilize the products in a manner that directly infringe one or more claims of the ‘871 patent.[15] By providing instruction and training to customers and end-users on how to use the VMware ‘871 Products in a manner that directly infringes one or more claims of the ‘871 patent, including at least claim 1, VMware specifically intended to induce infringement of the ‘871 patent. VMware

[15] *See e.g.*, *VMware NSX-T Data Center 3.0 Installation Guide*, VMWARE DOCUMENTATION (August 12, 2021); *VMware NSX-T Networking Fundamentals*, VMWARE, INC. HANDS-ON LABS YOUTUBE CHANNEL (November 2, 2021), available at: https://www.youtube.com/watch?v=f37sgw_apHM; *VMware NSX-T Data Center 3.0 Administration Guide*, VMWARE DOCUMENTATION (September 13, 2023); *VMware NSX-T Data Center 3.2 Security Quick Start Guide*, VMWARE DOCUMENTATION (May 17, 2022); *VMware NSX-T – A Complete Internal Firewall*, VMWARE NSX YOUTUBE CHANNEL (December 7, 2021), available at: https://www.youtube.com/watch?v=euKlUxug6N4; and *What’s New With NSX-T Micro-Segmentation – SAI2565BU*, VMWORLD 2019 PRESENTATION (2019).

engaged in such inducement to promote the sales of the VMware ‘871 Products, e.g., through VMware user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘871 patent. Accordingly, VMware has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘871 patent, knowing that such use constitutes infringement of the ‘871 patent.

101. The ‘871 patent is well-known within the industry as demonstrated by multiple citations to the ‘871 patent in published patents and patent applications assigned to technology companies and academic institutions. VMware is utilizing the technology claimed in the ‘871 patent without paying a reasonable royalty. VMware is infringing the ‘871 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

102. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘871 patent.

103. As a result of VMware’s infringement of the ‘871 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for VMware’s infringement, but in no event less than a reasonable royalty for the use made of the invention by VMware together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,616,559

104. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

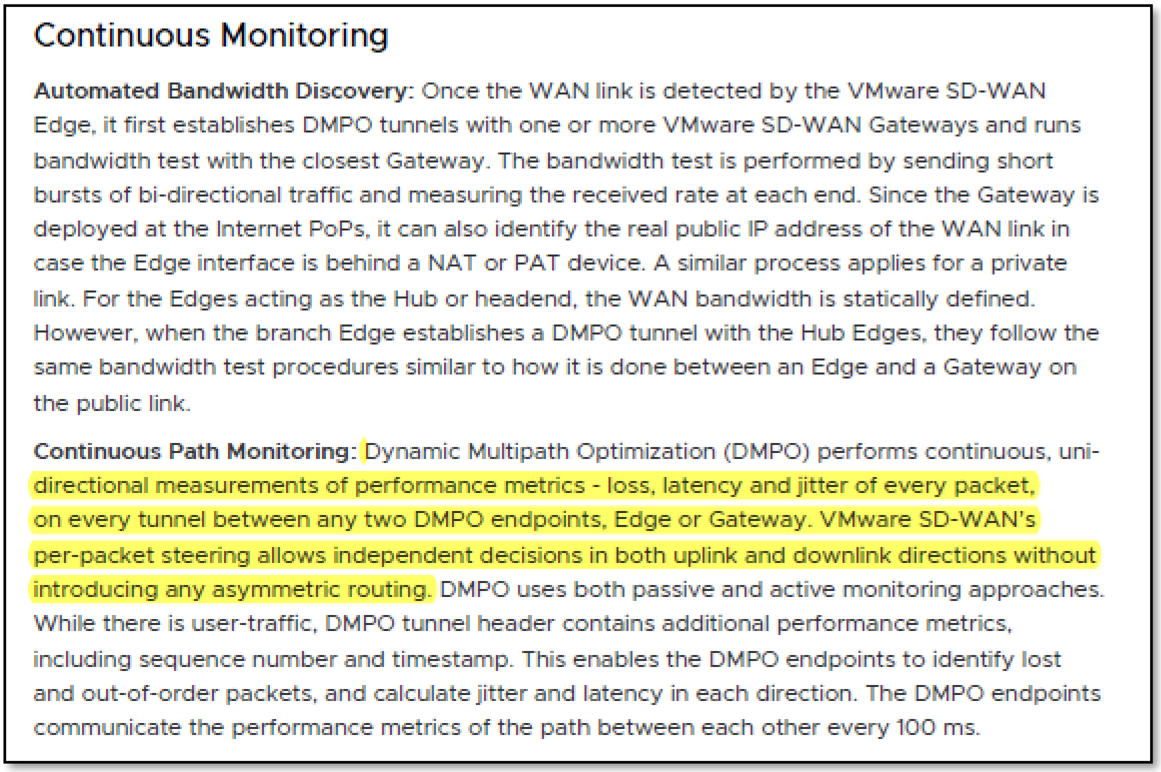
105. VMware designs, makes, uses, sells, and/or offers for sale in the United States products that communicate information over multiple communications links.

106. VMware designs, makes, sells, offers to sell, imports, and/or uses the following products: VMware SD-WAN Versions 3.4.0 and later (the "VMware '559 Product(s)").

107. One or more VMware subsidiaries and/or affiliates use the VMware '559 Products in regular business operations.

108. The VMware '559 Products identify an initial communication path with a specific security protocol for the transmission of data between a client system and a server system.

109. The VMware '559 Products detect a first communications link having a first security feature for communicating data between a client device and a server device. The VMware '559 Products utilize algorithms to ensure the first security level's parameters, such as encryption and authentication protocols are met. By identifying the presence of this first communications link, the VMware '559 Products can prioritize a communications link for use based on predefined security requirements or other criteria.



Continuous Monitoring

Automated Bandwidth Discovery: Once the WAN link is detected by the VMware SD-WAN Edge, it first establishes DMPO tunnels with one or more VMware SD-WAN Gateways and runs bandwidth test with the closest Gateway. The bandwidth test is performed by sending short bursts of bi-directional traffic and measuring the received rate at each end. Since the Gateway is deployed at the Internet PoPs, it can also identify the real public IP address of the WAN link in case the Edge interface is behind a NAT or PAT device. A similar process applies for a private link. For the Edges acting as the Hub or headend, the WAN bandwidth is statically defined. However, when the branch Edge establishes a DMPO tunnel with the Hub Edges, they follow the same bandwidth test procedures similar to how it is done between an Edge and a Gateway on the public link.

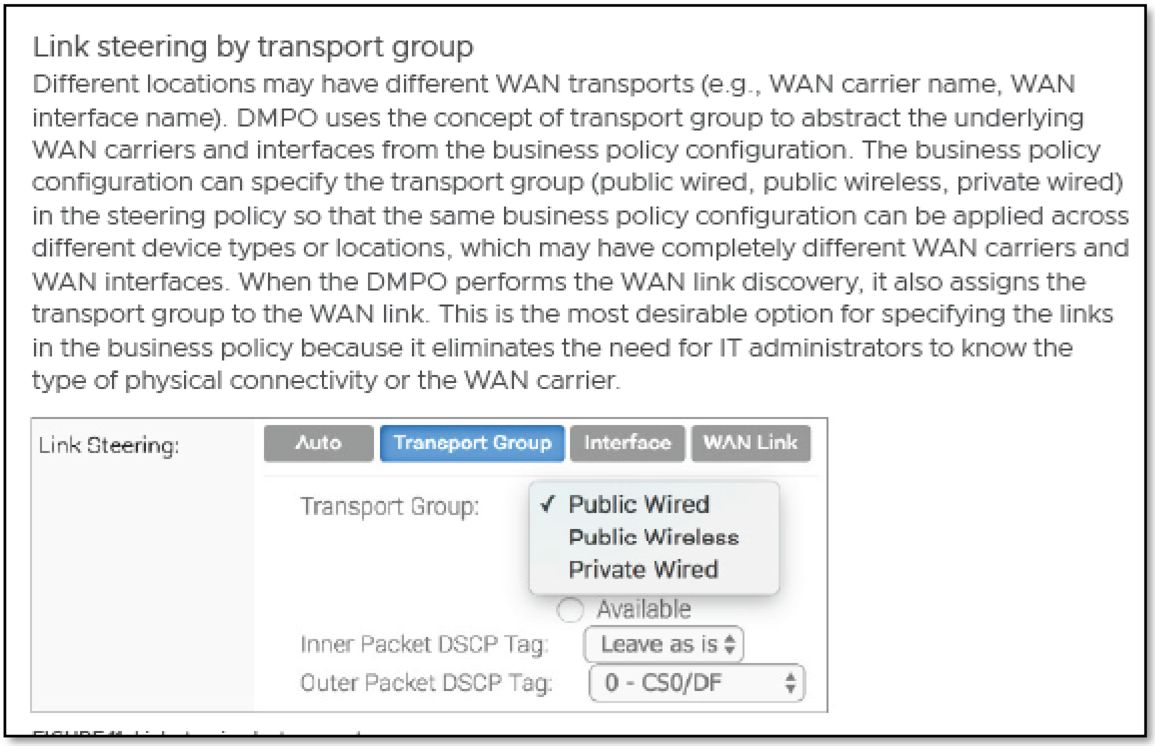
Continuous Path Monitoring: Dynamic Multipath Optimization (DMPO) performs continuous, uni-directional measurements of performance metrics - loss, latency and jitter of every packet, on every tunnel between any two DMPO endpoints, Edge or Gateway. VMware SD-WAN's per-packet steering allows independent decisions in both uplink and downlink directions without introducing any asymmetric routing. DMPO uses both passive and active monitoring approaches. While there is user-traffic, DMPO tunnel header contains additional performance metrics, including sequence number and timestamp. This enables the DMPO endpoints to identify lost and out-of-order packets, and calculate jitter and latency in each direction. The DMPO endpoints communicate the performance metrics of the path between each other every 100 ms.

VMware SD-WAN 5.3 Administration Guide, VMWARE DOCUMENTATION at 65 (2023) (emphasis added).

110. The VMware '559 Products contain functionality for identifying an alternate communication pathway that possesses a different level of security for exchanging data between a client and a server.

111. The VMware '559 Products detect a second communications link having a second security feature. The second communications link enables data to be sent between a client and server. Further, the VMware '559 Products monitor network channels and enable security protocols to evaluate the parameters of the second communications link. The security features used by the VMware '559 Products include encryption standards and/or authentication technology. The second communications link serves to ensure continuous data transfer by the VMware '559 Products if the first communications link is unavailable.

112. The VMware '559 Products determine if the initial communication path is inaccessible, opting for the alternate communication pathway with its distinct security level, to facilitate data transmission between a client and server.



Link steering by transport group

Different locations may have different WAN transports (e.g., WAN carrier name, WAN interface name). DMPO uses the concept of transport group to abstract the underlying WAN carriers and interfaces from the business policy configuration. The business policy configuration can specify the transport group (public wired, public wireless, private wired) in the steering policy so that the same business policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces. When the DMPO performs the WAN link discovery, it also assigns the transport group to the WAN link. This is the most desirable option for specifying the links in the business policy because it eliminates the need for IT administrators to know the type of physical connectivity or the WAN carrier.

Link Steering: Transport Group

Transport Group: ✓ Public Wired

Inner Packet DSCP Tag: Leave as is

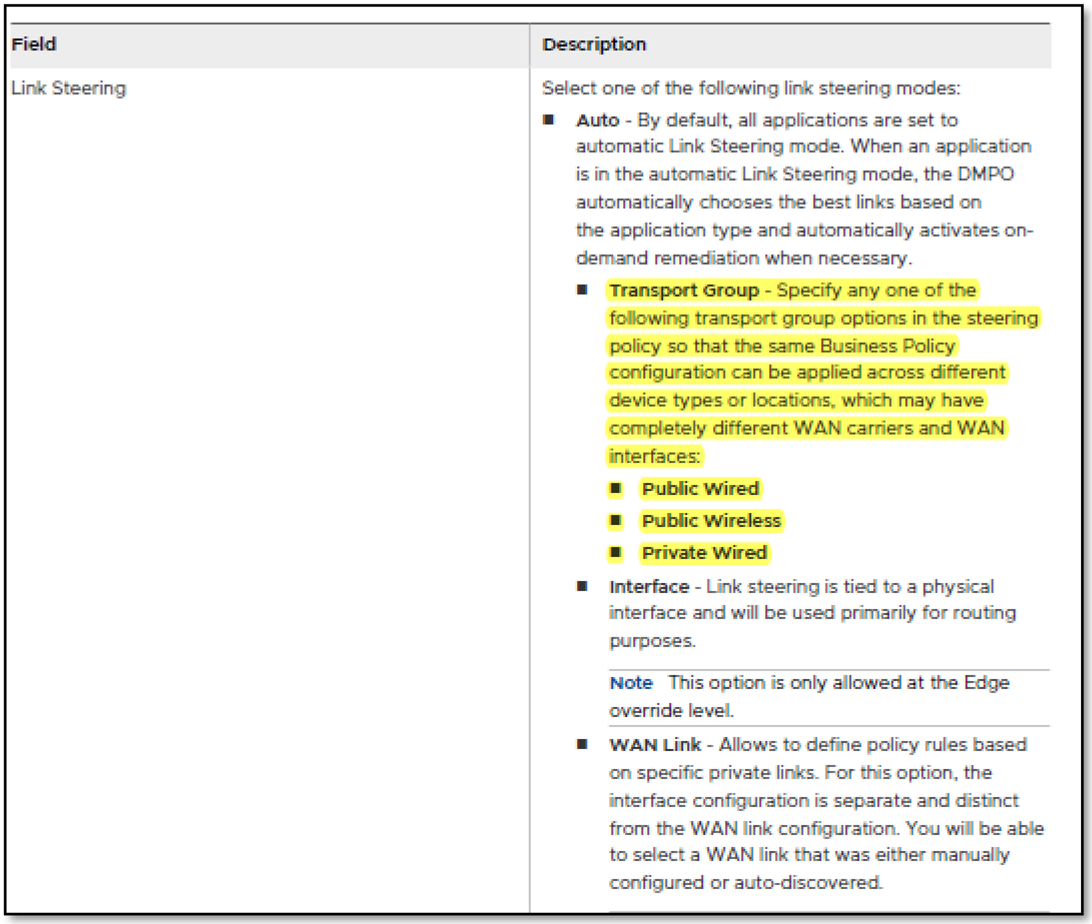
Outer Packet DSCP Tag: 0 - CS0/DF

VMware Dynamic Multipath Optimization – White Paper, VMWARE DOCUMENTATION AT 13 (December 2020).

113. The VMware '559 Products select the first communications link, having first security, for communicating between a client device and a server. After the detection of both the first and second communications links, the VMware '559 Products prioritize the link with the higher security features (e.g., first link) for data transmission. This prioritization by the VMware '559 Products is based on pre-established security criteria and network conditions. If the first link meets the requirements, it is selected by the VMware '559 Products to provide enhanced security and reliability.

114. The VMware '559 Products maintain a connection with one of either the initial or alternate communication pathways, to ensure uninterrupted data exchange between the client system and the server system.

115. The VMware '559 Products enable Link Steering wherein traffic can be steered over different links with different security profiles.



Field	Description
Link Steering	Select one of the following link steering modes: ■ **Auto** - By default, all applications are set to automatic Link Steering mode. When an application is in the automatic Link Steering mode, the DMPO automatically chooses the best links based on the application type and automatically activates on-demand remediation when necessary. ■ **Transport Group** - Specify any one of the following transport group options in the steering policy so that the same Business Policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces: ■ **Public Wired** ■ **Public Wireless** ■ **Private Wired** ■ **Interface** - Link steering is tied to a physical interface and will be used primarily for routing purposes. **Note** This option is only allowed at the Edge override level. ■ **WAN Link** - Allows to define policy rules based on specific private links. For this option, the interface configuration is separate and distinct from the WAN link configuration. You will be able to select a WAN link that was either manually configured or auto-discovered.

VMware SD-WAN 5.3 Administration Guide, VMWARE DOCUMENTATION at 572 (2023) (emphasis added).

116. If the first communications link is not available, the VMware '559 Products select the second communications link having second security, for communicating between the client device and the server device. This action is prompted when the preferred first link, typically with higher security, is unavailable or fails to meet a criteria. The VMware '559 Products switch to the

second link, ensuring continuous communication. While generally considered less secure, the second link serves as a contingency, allowing uninterrupted information flow between a client and server.

117. If the data transmission is interrupted over the alternate communication pathway, the VMware '559 Products contain functionality for restoring the connection to the initial communication link to continue exchanging information between the client and the server.

118. The VMware '559 Products enable linking to one of either the first communications link and the second communications link, to maintain communicative connectivity during communications between the client and server. The VMware '559 Products establish a dynamic link management process, maintaining an active connection by continuously evaluating both communication links.

119. The VMware '559 Products contain functionality where if communication disruption occurs over the primary communication link, the alternate communication link is reestablished to facilitate the exchange of information between the client and server.

120. The VMware '559 Products enable reconnecting to the first communications link for communicating information between the client and server if communications are hindered over the second communications link. This step is a part of a resilient communication strategy that actively monitors both links and switches back to the first link when issues are detected with the second communications link.

121. The VMware '559 Products enable reconnecting to the second communications link for communicating information between the client device and the server device, if communications are hindered over the first communications link. If issues are detected on the

primary link, the VMware ‘559 Products automatically switch to the secondary link, maintaining the communication while also adhering to the security protocols.

122. VMware has directly infringed and continues to directly infringe the ‘559 patent by, among other things, making, using, offering for sale, and/or selling technology comprising a method of communicating information over multiple communications links, including but not limited to the VMware ‘559 Products.

123. The VMware ‘559 Products are available to businesses and individuals throughout the United States.

124. The VMware ‘559 Products are provided to businesses and individuals located in this District.

125. By making, using, testing, offering for sale, and/or selling products and services comprising a method of communicating information over multiple communications links, including but not limited to the VMware ‘559 Products, VMware has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the ‘559 patent, including at least claim 5 pursuant to 35 U.S.C. § 271(a).

126. VMware also indirectly infringes the ‘559 patent by actively inducing infringement under 35 U.S.C. § 271(b).

127. VMware has had knowledge of the ‘559 patent since at least service of this Complaint or shortly thereafter, and VMware knew of the ‘559 patent and knew of its infringement, including by way of this lawsuit.

128. VMware intended to induce patent infringement by third-party customers and users of the VMware ‘559 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. VMware

specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘559 patent. VMware performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘559 patent and with the knowledge that the induced acts would constitute infringement. For example, VMware provides the VMware ‘559 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘559 patent, including at least claim 5, and VMware further provides documentation and training materials that cause customers and end users of the VMware ‘559 Products to utilize the products in a manner that directly infringe one or more claims of the ‘559 patent.[16] By providing instruction and training to customers and end-users on how to use the VMware ‘559 Products in a manner that directly infringes one or more claims of the ‘559 patent, including at least claim 5, VMware specifically intended to induce infringement of the ‘559 patent. VMware engaged in such inducement to promote the sales of the VMware ‘559 Products, e.g., through VMware user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘559 patent. Accordingly, VMware has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘559 patent, knowing that such use constitutes infringement of the ‘559 patent.

129. The ‘559 patent is well-known within the industry as demonstrated by multiple citations to the ‘559 patent in published patents and patent applications assigned to technology companies and academic institutions. VMware is utilizing the technology claimed in the ‘559

[16] *See e.g.*, *Dynamic Multipath Optimization*, VMWARE KNOWLEDGE BASE ARTICLE (September 2, 2021), available at: https://kb.vmware.com/s/article/2733094; *VMware SD-WAN 5.3 Administration Guide*, VMWARE DOCUMENTATION (2023); *VMware Dynamic Multipath Optimization – White Paper*, VMWARE DOCUMENTATION (December 2020); *VMware SD-Wan 4.2 Administration Guide*, VMWARE DOCUMENTATION (2020); and *VMware SD-WAN Client 1.0 Administrator Guide, VMware Documentation* (2022).

patent without paying a reasonable royalty. VMware is infringing the ‘559 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

130. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘559 patent.

131. As a result of VMware’s infringement of the ‘559 patent, Plaintiff has suffered monetary damages, and seeks recovery in an amount adequate to compensate for VMware’s infringement, but in no event less than a reasonable royalty for the use made of the invention by VMware together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,136,353

132. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

133. VMware designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network.

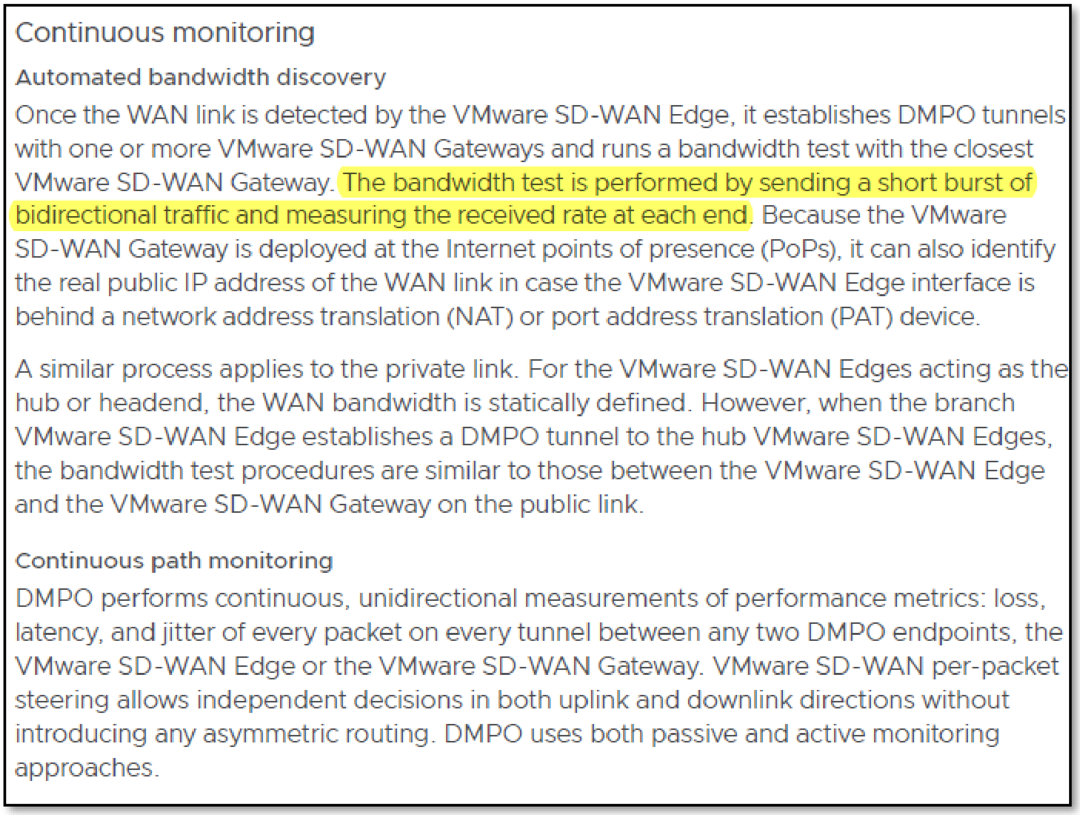
134. VMware designs, makes, sells, offers to sell, imports, and/or uses the following products: VMware SD-WAN Versions 3.4.0 and later (the “VMware ‘353 Product(s)”).

135. One or more VMware subsidiaries and/or affiliates use the VMware ‘353 Products in regular business operations.

136. The VMware ‘353 Products determine a host-level transmission rate between the sender and receiver by summing a current transmission rate associated with each of a plurality of connections.

137. The VMware '353 Products identify a present transmission rate for individual connections between a host and client device.

138. The VMware '353 Products conduct automated bandwidth discovery in which a bandwidth test is performed by sending a short burst of bidirectional traffic and measuring the received rate at each end.



Continuous monitoring

Automated bandwidth discovery

Once the WAN link is detected by the VMware SD-WAN Edge, it establishes DMPO tunnels with one or more VMware SD-WAN Gateways and runs a bandwidth test with the closest VMware SD-WAN Gateway. The bandwidth test is performed by sending a short burst of bidirectional traffic and measuring the received rate at each end. Because the VMware SD-WAN Gateway is deployed at the Internet points of presence (PoPs), it can also identify the real public IP address of the WAN link in case the VMware SD-WAN Edge interface is behind a network address translation (NAT) or port address translation (PAT) device.

A similar process applies to the private link. For the VMware SD-WAN Edges acting as the hub or headend, the WAN bandwidth is statically defined. However, when the branch VMware SD-WAN Edge establishes a DMPO tunnel to the hub VMware SD-WAN Edges, the bandwidth test procedures are similar to those between the VMware SD-WAN Edge and the VMware SD-WAN Gateway on the public link.

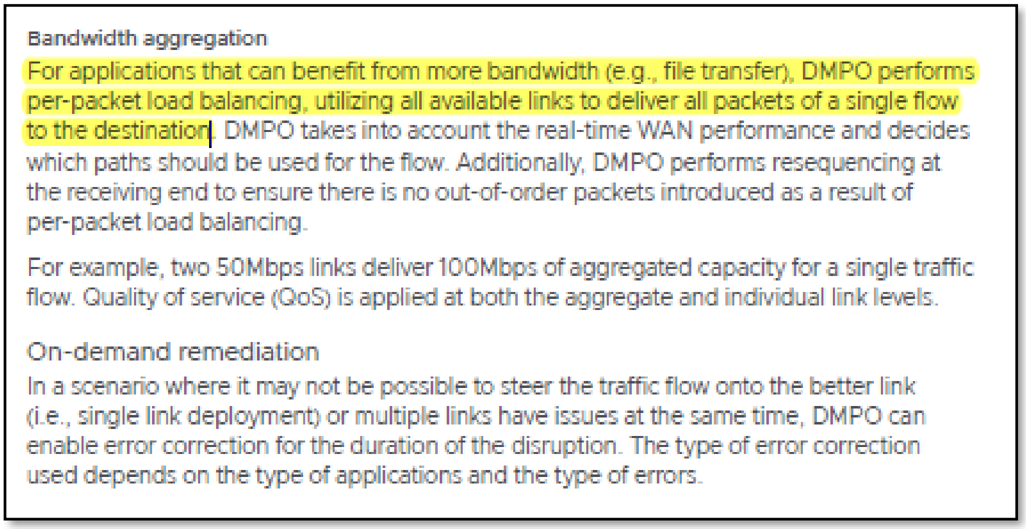
Continuous path monitoring

DMPO performs continuous, unidirectional measurements of performance metrics: loss, latency, and jitter of every packet on every tunnel between any two DMPO endpoints, the VMware SD-WAN Edge or the VMware SD-WAN Gateway. VMware SD-WAN per-packet steering allows independent decisions in both uplink and downlink directions without introducing any asymmetric routing. DMPO uses both passive and active monitoring approaches.

VMware Dynamic Multipath Optimization – White Paper, VMWARE DOCUMENTATION AT 4 (December 2020) (emphasis added).

139. The VMware '353 Products compute a host-level transmission rate by totaling the current transmission rates over several connections.

140. The VMware '353 Products perform bandwidth aggregation across connections that utilizes all available links to deliver packets across different connections.



Bandwidth aggregation

For applications that can benefit from more bandwidth (e.g., file transfer), DMPO performs per-packet load balancing, utilizing all available links to deliver all packets of a single flow to the destination. DMPO takes into account the real-time WAN performance and decides which paths should be used for the flow. Additionally, DMPO performs resequencing at the receiving end to ensure there is no out-of-order packets introduced as a result of per-packet load balancing.

For example, two 50Mbps links deliver 100Mbps of aggregated capacity for a single traffic flow. Quality of service (QoS) is applied at both the aggregate and individual link levels.

On-demand remediation

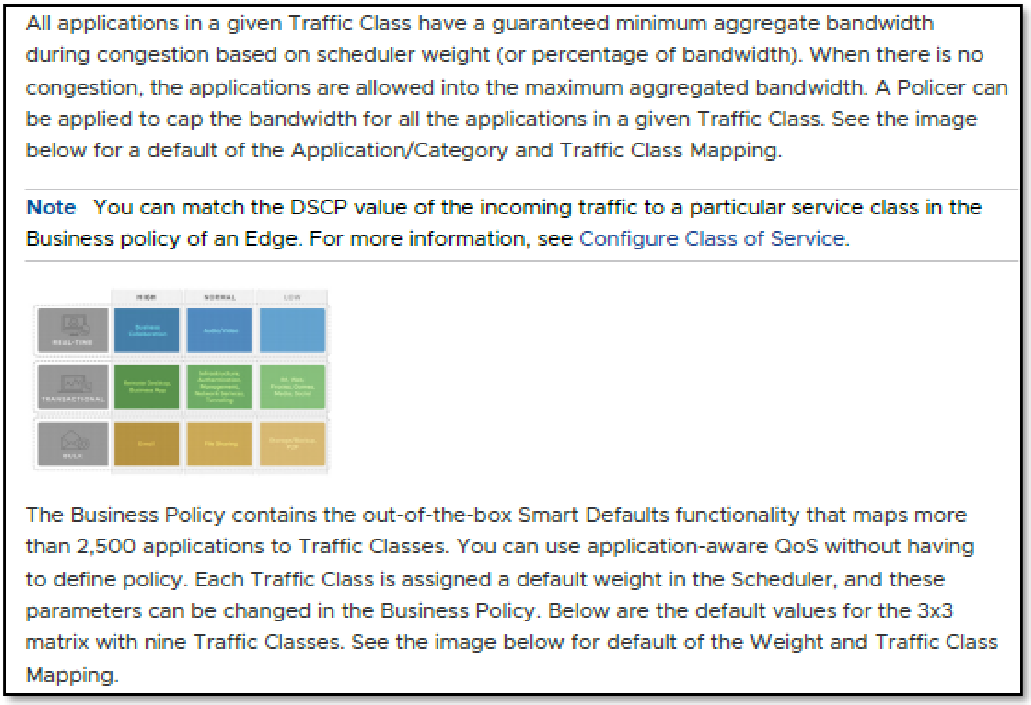
In a scenario where it may not be possible to steer the traffic flow onto the better link (i.e., single link deployment) or multiple links have issues at the same time, DMPO can enable error correction for the duration of the disruption. The type of error correction used depends on the type of applications and the type of errors.

VMware Dynamic Multipath Optimization – White Paper, VMWARE DOCUMENTATION AT 6 (December 2020) (emphasis added).

141. The VMware '353 Products allocate the host-level transmission rate across multiple connections based on a ratio of a weight related to each connection and the total of the weights for set of multiple connections.

142. The VMware '353 Products choose data packets for transmission in a way that each chosen data packet is linked with the connection exhibiting the greatest discrepancy between the allocated transmission rate and the actual transmission rate for the connection.

143. The VMware '353 Products perform packet scheduling including through the use of a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth.



All applications in a given Traffic Class have a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth). When there is no congestion, the applications are allowed into the maximum aggregated bandwidth. A Policer can be applied to cap the bandwidth for all the applications in a given Traffic Class. See the image below for a default of the Application/Category and Traffic Class Mapping.

Note You can match the DSCP value of the incoming traffic to a particular service class in the Business policy of an Edge. For more information, see Configure Class of Service.

HIGH
NORMAL
LOW
REAL-TIME
Business Collaboration
Audio/Video
TRANSACTIONAL
Remote Desktop, Business App
Infrastructure, Authentication, Management, Network Services, Tunneling
IM, Web, Proxies, Games, Media, Social
BULK
Email
File Sharing
Storage/Backup, P2P

The Business Policy contains the out-of-the-box Smart Defaults functionality that maps more than 2,500 applications to Traffic Classes. You can use application-aware QoS without having to define policy. Each Traffic Class is assigned a default weight in the Scheduler, and these parameters can be changed in the Business Policy. Below are the default values for the 3x3 matrix with nine Traffic Classes. See the image below for default of the Weight and Traffic Class Mapping.

VMware SD-WAN 5.3 Administration Guide, VMWARE DOCUMENTATION at 587 (2023).

144. The VMware '353 Products allocate the host-level transmission rate among the plurality of connections based on a ratio of a weight associated with each connection and a sum of the weights for the plurality of connections.

145. The VMware '353 Products transmit data packets from the host across the related connections based on data packets associated with connections having a highest difference between the allocated transmission rate and an actual transmission rate are transmitted first. Further, each data packet being transmitted from the sender is transmitted in response to each expiration of a transmission timer having a period corresponding to the host-level transmission rate.

146. VMware has directly infringed and continues to directly infringe the '353 patent by, among other things, making, using, offering for sale, and/or selling technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network, including but not limited to the VMware '353 Products.

147. The VMware '353 Products are available to businesses and individuals throughout the United States.

148. The VMware '353 Products are provided to businesses and individuals located in this District.

149. By making, using, testing, offering for sale, and/or selling products and services comprising technology for managing multiple connections for sending data packets between a sender and a receiver in a computer network, including but not limited to the VMware '353 Products, VMware has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the '353 patent, including at least claim 13 pursuant to 35 U.S.C. § 271(a).

150. VMware also indirectly infringes the '353 patent by actively inducing infringement under 35 U.S.C. § 271(b).

151. VMware has had knowledge of the '353 patent since at least service of this Complaint or shortly thereafter, and VMware knew of the '353 patent and knew of its infringement, including by way of this lawsuit.

152. VMware intended to induce patent infringement by third-party customers and users of the VMware '353 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. VMware specifically intended and was aware that the normal and customary use of the accused products would infringe the '353 patent. VMware performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '353 patent and with the knowledge that the induced acts would constitute infringement. For example, VMware provides the VMware '353 Products that have the capability of operating in a manner that infringe one or more of the claims of the '353 patent, including at least claim 13, and VMware further provides documentation

and training materials that cause customers and end users of the VMware ‘353 Products to utilize the products in a manner that directly infringe one or more claims of the ‘353 patent.[17] By providing instruction and training to customers and end-users on how to use the VMware ‘353 Products in a manner that directly infringes one or more claims of the ‘353 patent, including at least claim 13, VMware specifically intended to induce infringement of the ‘353 patent. VMware engaged in such inducement to promote the sales of the VMware ‘353 Products, e.g., through VMware user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘353 patent. Accordingly, VMware has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘353 patent, knowing that such use constitutes infringement of the ‘353 patent.

153. The ‘353 patent is well-known within the industry as demonstrated by multiple citations to the ‘353 patent in published patents and patent applications assigned to technology companies and academic institutions. VMware is utilizing the technology claimed in the ‘353 patent without paying a reasonable royalty. VMware is infringing the ‘353 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

154. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘353 patent.

[17] *See e.g.*, *Dynamic Multipath Optimization*, VMWARE KNOWLEDGE BASE ARTICLE (September 2, 2021), available at: https://kb.vmware.com/s/article/2733094; *VMware SD-WAN 5.3 Administration Guide*, VMWARE DOCUMENTATION (2023); *VMware Dynamic Multipath Optimization – White Paper*, VMWARE DOCUMENTATION (December 2020); *VMware SD-Wan 4.2 Administration Guide*, VMWARE DOCUMENTATION (2020); and *VMware SD-WAN Client 1.0 Administrator Guide, VMware Documentation* (2022).

155. As a result of VMware's infringement of the '353 patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for VMware's infringement, but in no event less than a reasonable royalty for the use made of the invention by VMware together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,521,901

156. Plaintiff references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

157. VMware designs, makes, uses, sells, and/or offers for sale in the United States products comprising technology for a data packet scheduler that reduces packet bursts.

158. VMware designs, makes, sells, offers to sell, imports, and/or uses the following products: VMware SD-WAN Versions 3.4.0 and later (the "VMware '901 Product(s)").

159. One or more VMware subsidiaries and/or affiliates use the VMware '901 Products in regular business operations.

160. The VMware '901 Products receive a transmission control protocol (TCP) packet from a sending layer on the first device. The sending layer is one of the network interface layer or the transport layer and the TCP packet is sent over a connection between the first device and a second device.

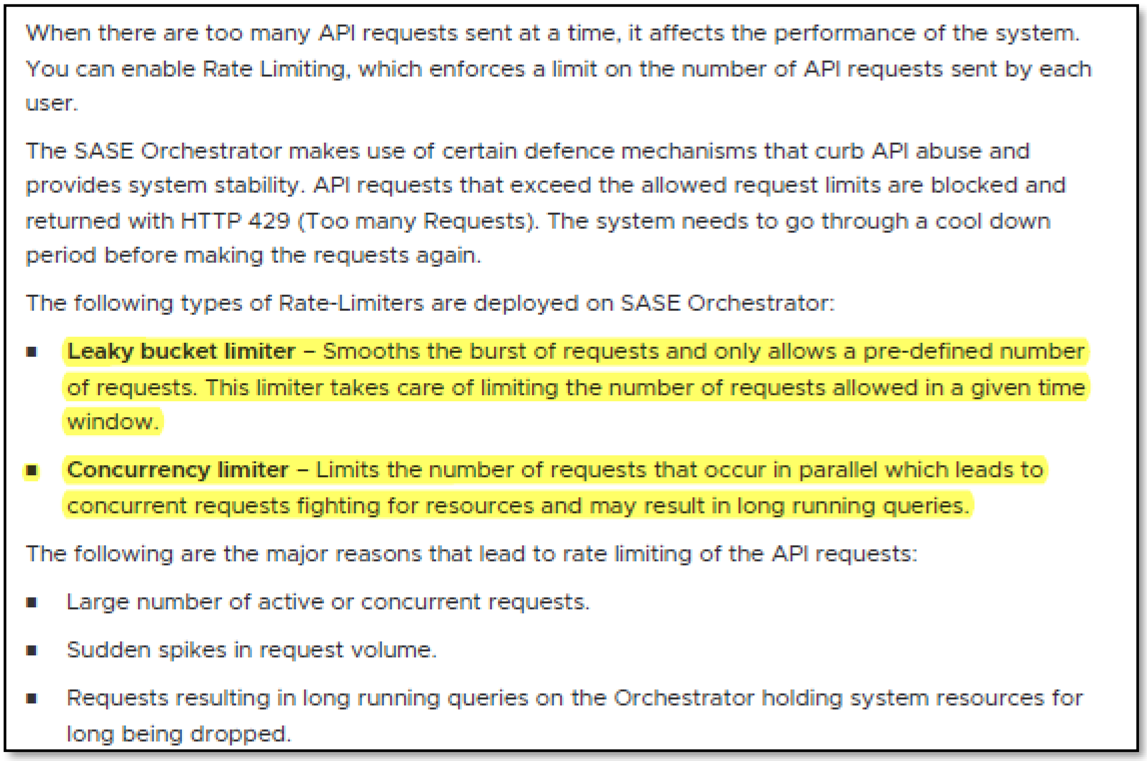
161. VMware '901 Products contain functionality for receiving and sending TCP packets and comprise functionality for optimizing the flow of data between devices over various network paths.

162. VMware '901 Products store information about the connection between a first device and the second device. The information stored by the VMware '901 products include a last packet delivery time for a specific connection/link. Specifically, the VMware '901 products store

information about the network connection, such as metrics regarding packet delivery, latency, and jitter, to optimize the path selection and improve performance.

163. VMware '901 Products determine if a TCP packet is part of a bursty transmission on the connection by looking at whether a burst count for the connection is greater than a burst-count threshold.

164. The VMware '901 Products make use of a leaky bucket limiter and concurrency limiter to monitor packet burstiness.



When there are too many API requests sent at a time, it affects the performance of the system. You can enable Rate Limiting, which enforces a limit on the number of API requests sent by each user.

The SASE Orchestrator makes use of certain defence mechanisms that curb API abuse and provides system stability. API requests that exceed the allowed request limits are blocked and returned with HTTP 429 (Too many Requests). The system needs to go through a cool down period before making the requests again.

The following types of Rate-Limiters are deployed on SASE Orchestrator:

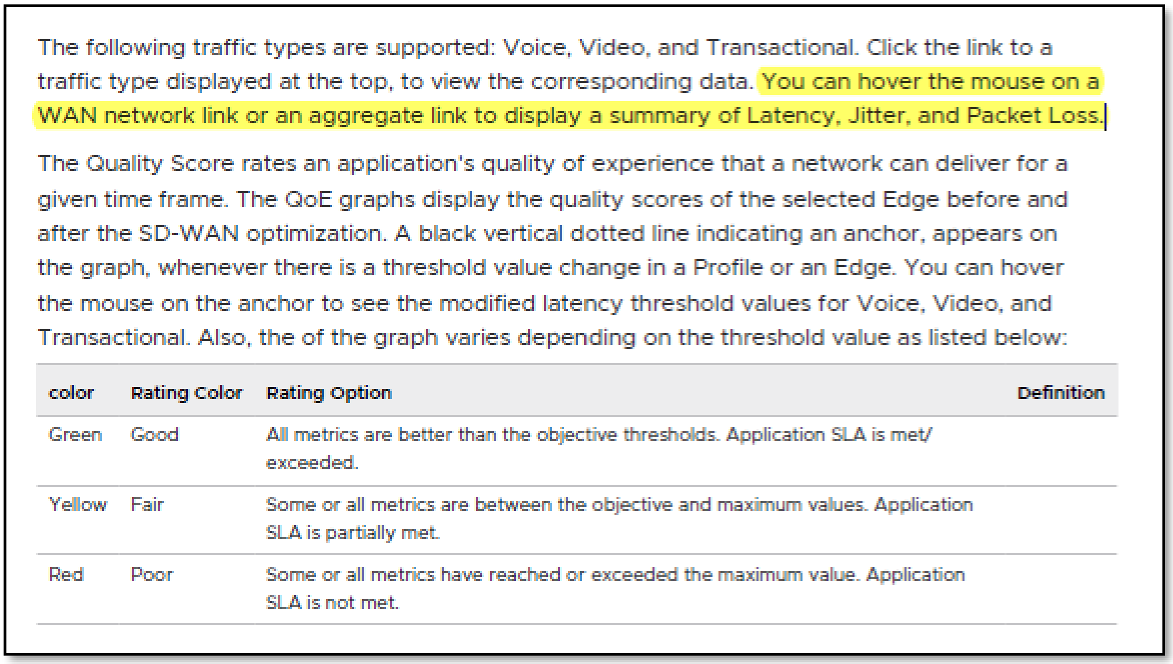
- **Leaky bucket limiter** – Smooths the burst of requests and only allows a pre-defined number of requests. This limiter takes care of limiting the number of requests allowed in a given time window.
- **Concurrency limiter** – Limits the number of requests that occur in parallel which leads to concurrent requests fighting for resources and may result in long running queries.

The following are the major reasons that lead to rate limiting of the API requests:

- Large number of active or concurrent requests.
- Sudden spikes in request volume.
- Requests resulting in long running queries on the Orchestrator holding system resources for long being dropped.

VMware SASE Orchestrator SD-WAN 5.3 Deployment and Monitoring Guide, VMWARE DOCUMENTATION at 73 (2023) (emphasis added).

165. VMware '901 Products calculate a delay time for a connection using the last packet delivery time after determining that the TCP packet is part of a bursty transmission. Specifically, the VMware '901 Products measure latency and jitter for each connection/link. This measurement is then used to determine the burstiness of a TCP packet transmission.



The following traffic types are supported: Voice, Video, and Transactional. Click the link to a traffic type displayed at the top, to view the corresponding data. You can hover the mouse on a WAN network link or an aggregate link to display a summary of Latency, Jitter, and Packet Loss.

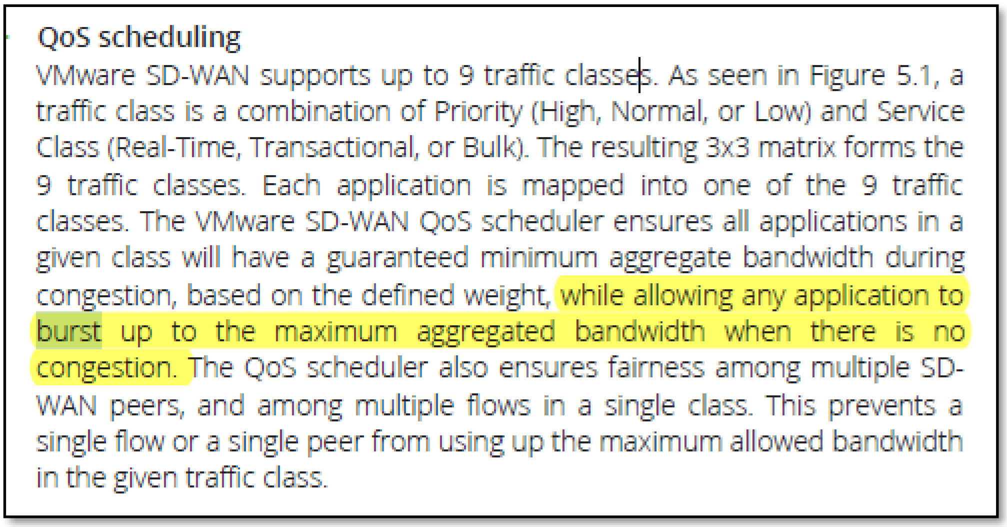
The Quality Score rates an application's quality of experience that a network can deliver for a given time frame. The QoE graphs display the quality scores of the selected Edge before and after the SD-WAN optimization. A black vertical dotted line indicating an anchor, appears on the graph, whenever there is a threshold value change in a Profile or an Edge. You can hover the mouse on the anchor to see the modified latency threshold values for Voice, Video, and Transactional. Also, the of the graph varies depending on the threshold value as listed below:

color	Rating Color	Rating Option	Definition
Green	Good	All metrics are better than the objective thresholds. Application SLA is met/ exceeded.	
Yellow	Fair	Some or all metrics are between the objective and maximum values. Application SLA is partially met.	
Red	Poor	Some or all metrics have reached or exceeded the maximum value. Application SLA is not met.	

VMware SD-WAN 5.3 Administration Guide, VMWARE DOCUMENTATION at 125 (2023) (emphasis added).

166. The VMware '901 Products contain functionality for delivering the TCP packet to a receiving layer based on the calculated delay time, wherein the receiving layer is either the network interface layer or the transport layer that is not the sending layer. Specifically, the VMware '901 Products manage packet transmission times and delays as part of the VMware '901 Product's traffic optimization and prioritization functionality.

167. The VMware '901 Products enable sending the TCP packet to the receiving layer.



QoS scheduling

VMware SD-WAN supports up to 9 traffic classes. As seen in Figure 5.1, a traffic class is a combination of Priority (High, Normal, or Low) and Service Class (Real-Time, Transactional, or Bulk). The resulting 3x3 matrix forms the 9 traffic classes. Each application is mapped into one of the 9 traffic classes. The VMware SD-WAN QoS scheduler ensures all applications in a given class will have a guaranteed minimum aggregate bandwidth during congestion, based on the defined weight, while allowing any application to burst up to the maximum aggregated bandwidth when there is no congestion. The QoS scheduler also ensures fairness among multiple SD-WAN peers, and among multiple flows in a single class. This prevents a single flow or a single peer from using up the maximum allowed bandwidth in the given traffic class.

Application Performance with Dynamic Multipath Optimization – White Paper, VMWARE DOCUMENTATION at 5 (2019) (emphasis added).

168. VMware has directly infringed and continues to directly infringe the '901 patent by, among other things, making, using, offering for sale, and/or selling technology for a data packet scheduler that reduces packet bursts, including but not limited to the VMware '901 Products.

169. The VMware '901 Products are available to businesses and individuals throughout the United States.

170. The VMware '901 Products are provided to businesses and individuals located in this District.

171. By making, using, testing, offering for sale, and/or selling products and services comprising technology for a data packet scheduler that reduced packet bursts, including but not limited to the VMware '901 Products, VMware has injured Plaintiff and is liable to Plaintiff for directly infringing one or more claims of the '901 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

172. VMware also indirectly infringes the '901 patent by actively inducing infringement under 35 U.S.C. § 271(b).

173. VMware has had knowledge of the ‘901 patent since at least service of this Complaint or shortly thereafter, and VMware knew of the ‘901 patent and knew of its infringement, including by way of this lawsuit.

174. VMware intended to induce patent infringement by third-party customers and users of the VMware ‘901 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. VMware specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘901 patent. VMware performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘901 patent and with the knowledge that the induced acts would constitute infringement. For example, VMware provides the VMware ‘901 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘901 patent, including at least claim 1, and VMware further provides documentation and training materials that cause customers and end users of the VMware ‘901 Products to utilize the products in a manner that directly infringe one or more claims of the ‘901 patent.[18] By providing instruction and training to customers and end-users on how to use the VMware ‘901 Products in a manner that directly infringes one or more claims of the ‘901 patent, including at least claim 1, VMware specifically intended to induce infringement of the ‘901 patent. VMware engaged in such inducement to promote the sales of the VMware ‘901 Products, e.g., through VMware user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘901 patent. Accordingly, VMware has

[18] *See e.g., Dynamic Multipath Optimization,* VMWARE KNOWLEDGE BASE ARTICLE (September 2, 2021), available at: https://kb.vmware.com/s/article/2733094; *VMware SD-WAN 5.3 Administration Guide*, VMWARE DOCUMENTATION (2023); *VMware Dynamic Multipath Optimization – White Paper*, VMWARE DOCUMENTATION (December 2020); *VMware SD-Wan 4.2 Administration Guide*, VMWARE DOCUMENTATION (2020); and *VMware SD-WAN Client 1.0 Administrator Guide, VMware Documentation* (2022).

induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘901 patent, knowing that such use constitutes infringement of the ‘901 patent.

175. The ‘901 patent is well-known within the industry as demonstrated by multiple citations to the ‘901 patent in published patents and patent applications assigned to technology companies and academic institutions. VMware is utilizing the technology claimed in the ‘901 patent without paying a reasonable royalty. VMware is infringing the ‘901 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

176. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘901 patent.

177. As a result of VMware’s infringement of the ‘901 patent, Plaintiff has suffered monetary damages, and seek recovery in an amount adequate to compensate for VMware’s infringement, but in no event less than a reasonable royalty for the use made of the invention by VMware together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff OptiMorphix, Inc. respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff that VMware has infringed, either literally and/or under the doctrine of equivalents, the ‘314, ‘871, ‘559, ‘353, and ‘901 patents;

B. An award of damages resulting from VMware’s acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that VMware's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff reasonable attorneys' fees against VMware.

E. Any and all other relief to which Plaintiff may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff OptiMorphix, Inc. requests a trial by jury of any issues so triable by right.

Dated: October 12, 2023

OF COUNSEL:

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
Erin E. McCracken (CA SB No. 244523)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com
E-Mail: eem@bergerhipskind.com

BAYARD, P.A.

/s/ Stephen B. Brauerman
Stephen B. Brauerman (#4952)
Ronald P. Golden III (#6254)
600 N. King Street, Suite 400
P.O. Box 25130
Wilmington, DE 19801
(302) 655-5000
sbrauerman@bayardlaw.com
rgolden@bayardlaw.com

Attorneys for Plaintiff
OptiMorphix, Inc.