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

	§	
WINTERSPRING DIGITAL LLC,	§	
	§	Case No. 2:23-cv-00259-JRG-RSP
Plaintiff,	§	
	§	**JURY TRIAL DEMANDED**
v.	§	
	§	
HEWLETT PACKARD ENTERPRISE COMPANY,	§	
	§	
	§	
Defendant.	§	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Winterspring Digital LLC ("Winterspring" or "Plaintiff") for its Complaint against Hewlett Packard Enterprise Company ("HPE" or "Defendant") alleges as follows:

THE PARTIES

1. Winterspring is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 104 East Houston Street, Marshall, Texas 75670.

2. Upon information and belief, Defendant HPE is a Delaware corporation that maintains regular and established places of business throughout Texas, for example, at its facilities in this District at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. HPE is registered to conduct business in the State of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process. HPE is a leading manufacturer and seller of computer equipment in the world and in the United States. Upon information and belief, HPE does business in Texas and in the Eastern District of Texas, directly or through intermediaries

JURISDICTION

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

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1400(b) and 1391(b) and (c) because, among other things, Defendant is subject to personal jurisdiction in this Judicial District, has a regular and established place of business in this Judicial District, has purposely transacted business involving the accused products in this Judicial District, including sale to one or more customers in Texas, and certain of the acts complained herein, including acts of patent infringement, occurred in this Judicial District.

6. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

7. On January 16, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,164,692 (the "'692 Patent") entitled "Apparatus and Method for

Transmitting 10 Gigabit Ethernet LAN Signals Over a Transport System." A true and correct copy of the '692 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=7164692.

8. On October 4, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,032,646 (the "'646 Patent") entitled "Administering a Communication Network." A true and correct copy of the '646 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=8032646.

9. On September 2, 2008, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,420,975 (the "'975 Patent") entitled "Method and Apparatus For High-Speed Frame Tagger." A true and correct copy of the '975 Patent is available at http://pdfpiw.uspto.gov/.piw?docid=7420975.

10. Winterspring is the sole and exclusive owner of all right, title, and interest in the '692, '646, and '975 Patents (the "Patents-in-Suit") and holds the exclusive right to take all actions necessary to enforce its rights to the Patent-in-Suit, including the filing of this patent infringement lawsuit. Winterspring also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

11. The Patents-in-Suit generally cover systems and methods for routing data over a network.

12. The '692 Patent generally discloses an apparatus and method for transmitting LAN signals over a transport system. A system sends or receives a signal to or from a transport system, converts the signal to an intermediate form, re-clocks the intermediate signal, reconverts and then transmits the signal. The technology described in the '692 Patent was developed by Jeffrey Lloyd Cox and Samir Satish Seth. By way of example, this technology is implemented today in servers,

computers, network switches, modules, and transceivers that receive, convert, monitor, and send 10-Gigabit LAN signals. By way of further example, infringing products include, but are not limited to, the HPE BladeSystem c-Class 10gb SFP+ SR Transceiver and the HPE Aruba SFP+ transceiver module.

13. The ’646 Patent discloses systems and methods for routing traffic through a network with the use of a GUI. The technology described in the ’646 Patent was developed by Siddhartha Nag, Alfred D’Souza, Naveed Alam, and Rakesh Patel of Prom KS Limited Liability Company. By way of example, this technology is implemented today in hardware and software which allow a user with a GUI to optimize routing decisions. By way of further example, infringing products include, but are not limited to, HPE’s SD-Wan Orchestrator.

14. The ’975 Patent discloses an apparatus and methods for examining a packet, determining a protocol type and tagging the packet. The technology described in the ’975 Patent was developed by Velamur Krishnamachari and Dinesh Annayya from Cypress Semiconductor Corporation. By way of example, this technology is implemented today in servers, computers, network switches, modules and software which implement packet tagging.

15. HPE has infringed and is continuing to infringe the Patents-in-Suit by making, using, offering to sell, selling, and/or importing products which implement the technology disclosed in the above Patents-in-Suit.

COUNT I
(Infringement of the ’692 Patent)

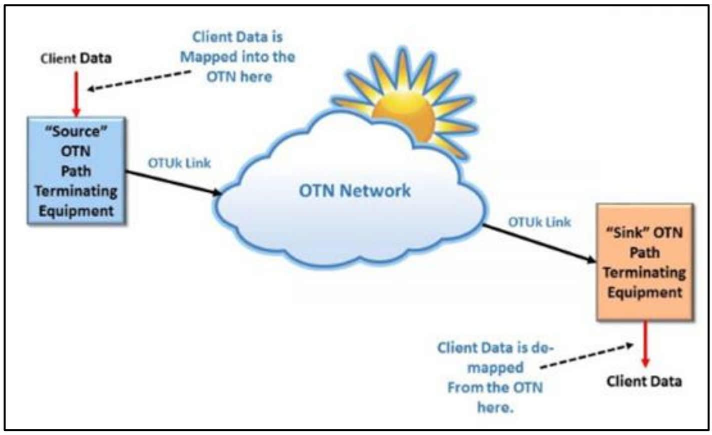
16. Paragraphs 1 through 15 are incorporated by reference as if fully set forth herein.

17. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’692 Patent.

18. Defendant has and continues to directly infringe the ’692 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’692 Patent. Such products include, but are not limited to servers, computers, network switches, modules, and transceivers that receive, convert, monitor, and send 10-Gigabit LAN signals.

19. For example, Defendant has and continues to directly infringe at least claim 10 of the ’692 Patent by making, using, offering to sell, selling, and/or importing into the United States products that receive, convert, and monitor 10GE LAN signals.

20. For example, the HPE SFP+ transceiver module performs a method for transferring a 10GE LAN client signal from a transport system to a client system. The SFP+ 10GE optical transceiver modules can transfer 10GE LAN signal from a transport network to a client system as depicted in the exemplary figure below:


Client Data
Client Data is Mapped into the OTN here
"Source" OTN Path Terminating Equipment
OTUk Link
OTN Network
OTUk Link
"Sink" OTN Path Terminating Equipment
Client Data is de-mapped From the OTN here.
Client Data
[1]

[1] http://sierrahardwaredesign.com/optical-networking/glossary-item-oduoduk-optical-data-unit/.

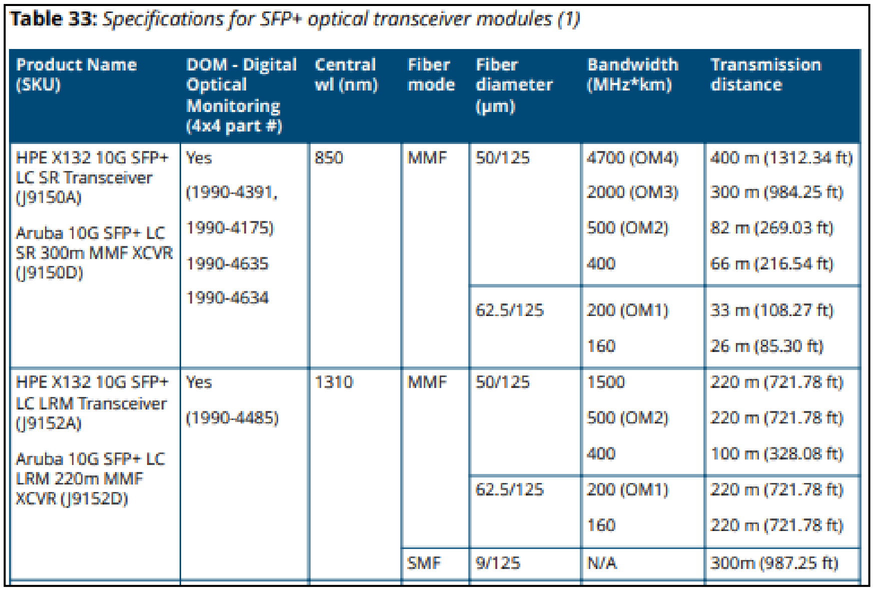
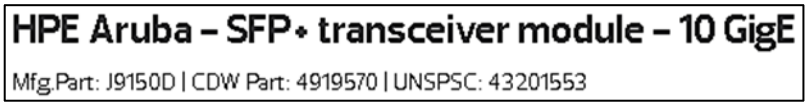


Table 33: *Specifications for SFP+ optical transceiver modules (1)*

Product Name (SKU)	DOM - Digital Optical Monitoring (4x4 part #)	Central wl (nm)	Fiber mode	Fiber diameter (µm)	Bandwidth (MHz*km)	Transmission distance
HPE X132 10G SFP+ LC SR Transceiver (J9150A) Aruba 10G SFP+ LC SR 300m MMF XCVR (J9150D)	Yes (1990-4391, 1990-4175) 1990-4635 1990-4634	850	MMF	50/125	4700 (OM4)	400 m (1312.34 ft)
					2000 (OM3)	300 m (984.25 ft)
					500 (OM2)	82 m (269.03 ft)
					400	66 m (216.54 ft)
				62.5/125	200 (OM1)	33 m (108.27 ft)
					160	26 m (85.30 ft)
HPE X132 10G SFP+ LC LRM Transceiver (J9152A) Aruba 10G SFP+ LC LRM 220m MMF XCVR (J9152D)	Yes (1990-4485)	1310	MMF	50/125	1500	220 m (721.78 ft)
					500 (OM2)	220 m (721.78 ft)
					400	100 m (328.08 ft)
				62.5/125	200 (OM1)	220 m (721.78 ft)
					160	220 m (721.78 ft)
			SMF	9/125	N/A	300m (987.25 ft)

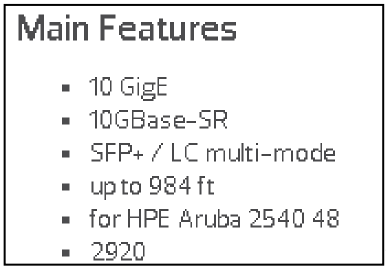
[2]



HPE Aruba – SFP+ transceiver module – 10 GigE

Mfg.Part: J9150D | CDW Part: 4919570 | UNSPSC: 43201553

[3]



Main Features

- 10 GigE
- 10GBase-SR
- SFP+ / LC multi-mode
- up to 984 ft
- for HPE Aruba 2540 48
- 2920

[4]

21. For example, the HPE SFP+ transceiver module performs the step of receiving the 10GE LAN client signal transmitting over the transport system. The SFP+ optical transceiver receives the OTU2e signal, which encapsulates the 10GbE LAN client signal as it travels over the

[2] https://www.solutionbox.com.uy/images/articulos/J4858D_1.pdf.

[3] https://www.cdw.com/product/hpe-aruba-sfp-transceiver-module-10-gige/4919570.

[4] *Id.*

OTN network ("the transport system").[5] The OTU2e encapsulates the ODU, which encapsulates the OPU that contains the 10GE LAN signal as its payload.

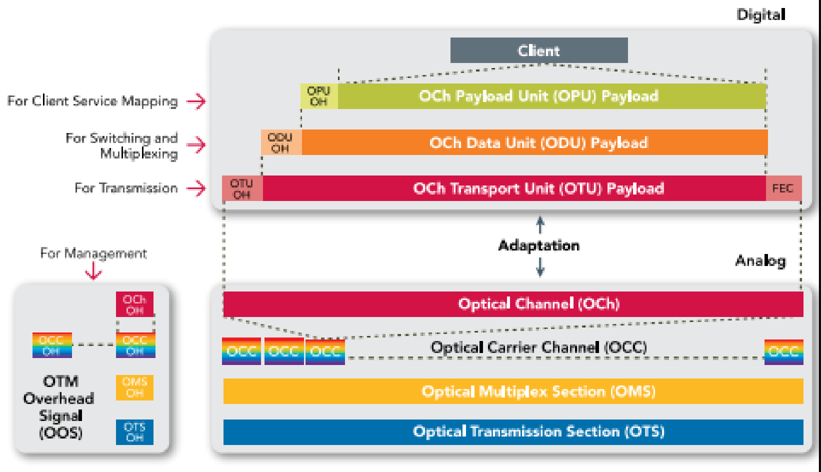
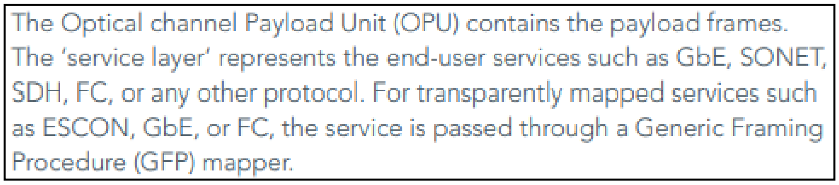
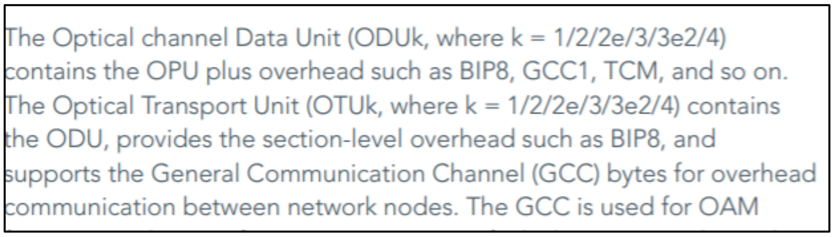

Digital
Client
For Client Service Mapping
OPU OH
OCh Payload Unit (OPU) Payload
For Switching and Multiplexing
ODU OH
OCh Data Unit (ODU) Payload
For Transmission
OTU OH
OCh Transport Unit (OTU) Payload
FEC
Adaptation
Analog
For Management
OCh OH
OCC OH
OCC OH
OMS OH
OTS OH
OTM Overhead Signal (OOS)
Optical Channel (OCh)
OCC
OCC
OCC
Optical Carrier Channel (OCC)
OCC
Optical Multiplex Section (OMS)
Optical Transmission Section (OTS)

Figure 1: Optical Transport Module (OTM) [6]


The Optical channel Payload Unit (OPU) contains the payload frames. The 'service layer' represents the end-user services such as GbE, SONET, SDH, FC, or any other protocol. For transparently mapped services such as ESCON, GbE, or FC, the service is passed through a Generic Framing Procedure (GFP) mapper. [7]

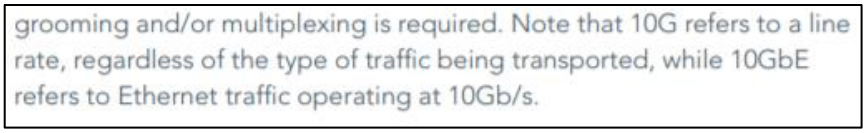

The Optical channel Data Unit (ODUk, where k = 1/2/2e/3/3e2/4) contains the OPU plus overhead such as BIP8, GCC1, TCM, and so on. The Optical Transport Unit (OTUk, where k = 1/2/2e/3/3e2/4) contains the ODU, provides the section-level overhead such as BIP8, and supports the General Communication Channel (GCC) bytes for overhead communication between network nodes. The GCC is used for OAM [8]

[5] *See* footnotes 1-4.

[6] https://media.ciena.com/documents/Experts_Guide_to_OTN_ebook-Utilities-Edition.pdf.

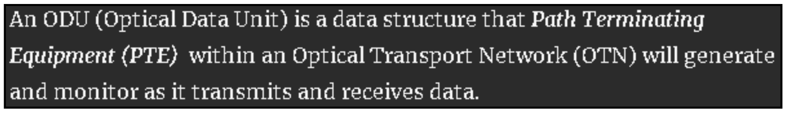
[7] https://media.ciena.com/documents/Experts_Guide_to_OTN_ebook-Utilities-Edition.pdf, pp. 23 and 25.

[8] *Id.*

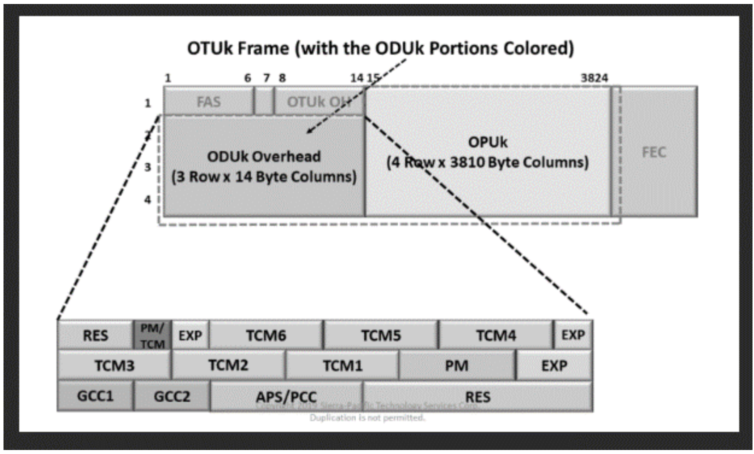


grooming and/or multiplexing is required. Note that 10G refers to a line rate, regardless of the type of traffic being transported, while 10GbE refers to Ethernet traffic operating at 10Gb/s. [9]

22. For example, the HPE SFP+ transceiver module performs the step of converting the 10GE LAN client to an intermediate signal. The received OTU2e signal is unpacked at the receiving end so that the ODU2e ("an intermediate signal") is made accessible.[10]



An ODU (Optical Data Unit) is a data structure that *Path Terminating Equipment (PTE)* within an Optical Transport Network (OTN) will generate and monitor as it transmits and receives data. [11]



[12]

23. For example, the HPE SFP+ transceiver module performs the step of recovering clock data stream from the intermediate signal. As Per the G.709 standard, ODU2e signal is generated using the timing of its client. More generally, OTU2e is considered an overclocked OTN technology because it compensates for the rate mismatch between 10 GE LAN and the OPU2 payload by raising the overall OTU2 data rate from the standard 10.709Gbit/s to fit the 10GE LAN

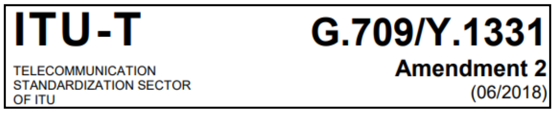
[9] *Id.*

[10] *See* footnote 6.

[11] http://sierrahardwaredesign.com/optical-networking/glossary-item-oduoduk-optical-data-unit/.

[12] *Id.*

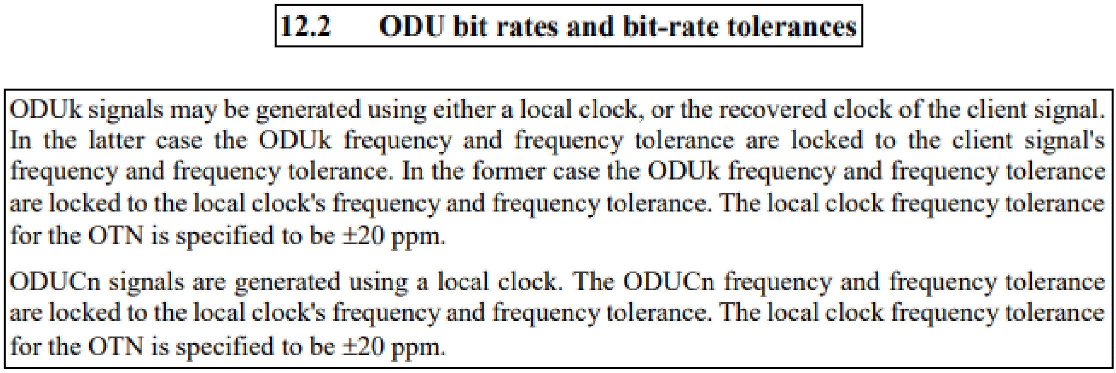
client signal. On the receiving end, the original clock data is recovered as part of the unpacking process so that the data stream can be effectively recovered from the ODU2e intermediate signal.



ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.709/Y.1331
Amendment 2
(06/2018) [13]



12.2 ODU bit rates and bit-rate tolerances

ODUk signals may be generated using either a local clock, or the recovered clock of the client signal. In the latter case the ODUk frequency and frequency tolerance are locked to the client signal's frequency and frequency tolerance. In the former case the ODUk frequency and frequency tolerance are locked to the local clock's frequency and frequency tolerance. The local clock frequency tolerance for the OTN is specified to be ±20 ppm.

ODUCn signals are generated using a local clock. The ODUCn frequency and frequency tolerance are locked to the local clock's frequency and frequency tolerance. The local clock frequency tolerance for the OTN is specified to be ±20 ppm. [14]

24. For example, the HPE SFP+ transceiver module performs the step of recovering a data stream from the intermediate signal. This includes recovering the OPU payload ("a data stream") from the ODU ("the intermediate signal").

[13] Source: ITU-T G.709/Y.1331, pp. 37 and 38.

[14] *Id.*

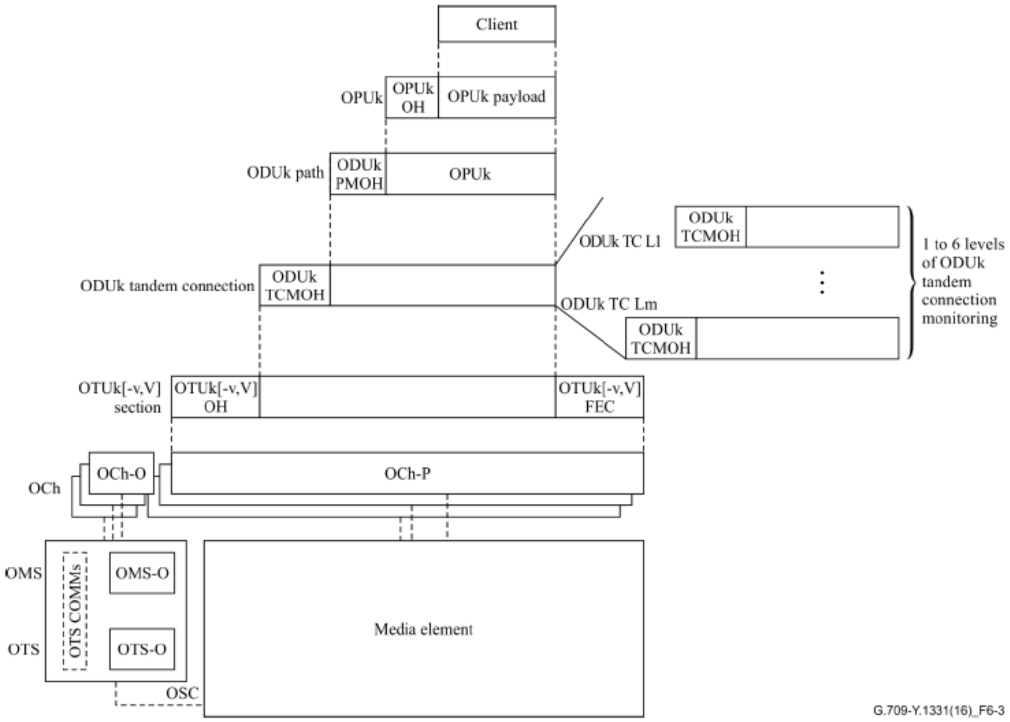
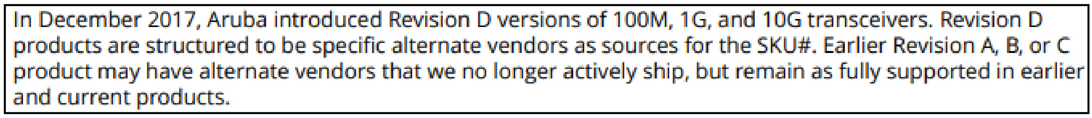


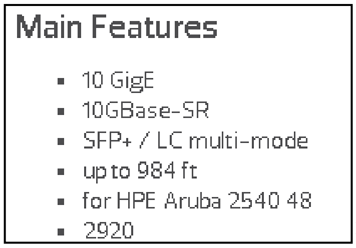
Figure 6-3 – MOTUm interface principal information containment relationships[15]

25. For example, the HPE SFP+ transceiver module performs the step of reconverting the intermediate signal to the 10GE LAN client signal. This includes reconverting the ODU2e ("the intermediate signal") to the 10GE LAN client signal (e.g., based on the recovered clock data and payload).


In December 2017, Aruba introduced Revision D versions of 100M, 1G, and 10G transceivers. Revision D products are structured to be specific alternate vendors as sources for the SKU#. Earlier Revision A, B, or C product may have alternate vendors that we no longer actively ship, but remain as fully supported in earlier and current products.[16]

[15] Source: ITU-T G.709/Y.1331, p. 14.

[16] https://www.solutionbox.com.uy/images/articulos/J4858D_1.pdf, p. 32.



Main Features

- 10 GigE
- 10GBase-SR
- SFP+ / LC multi-mode
- up to 984 ft
- for HPE Aruba 2540 48
- 2920

[17]

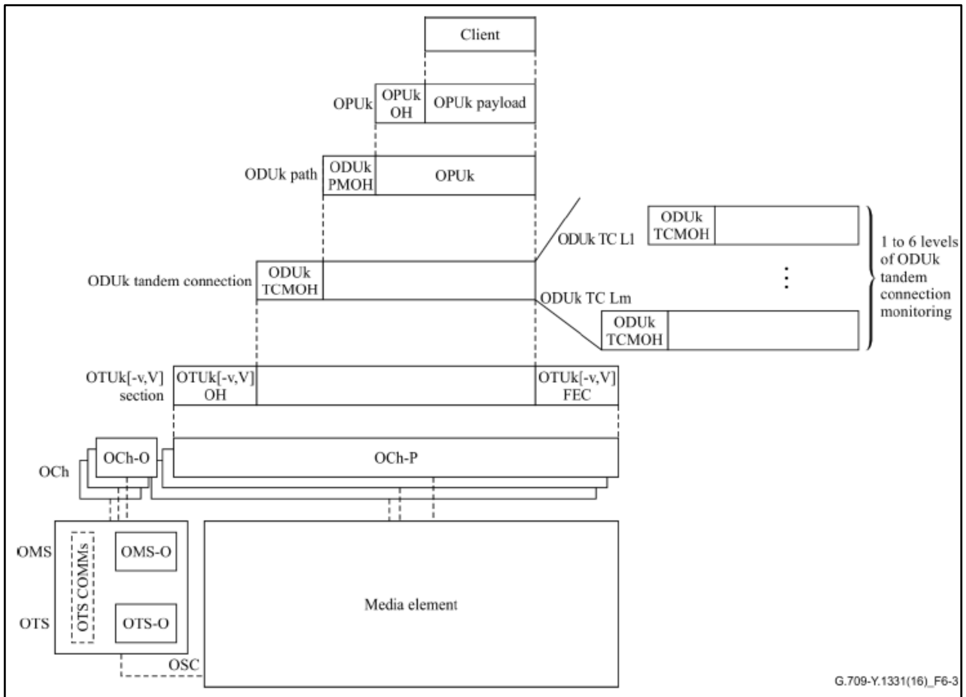


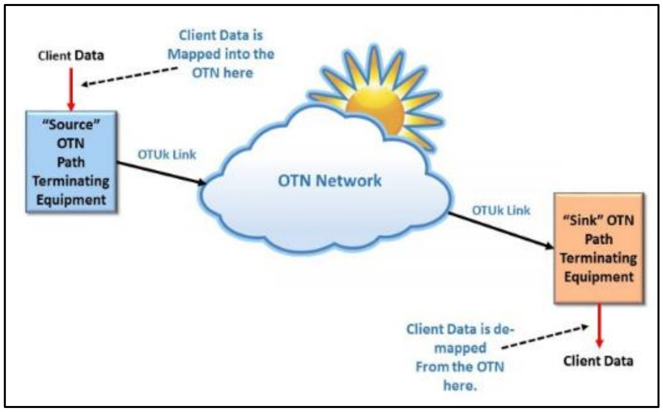
Figure 6-3 – MOTUm interface principal information containment relationships

[18]

26. For example, the HPE SFP+ transceiver module performs the step of transferring the 10GE LAN client to a client system.

[17] https://www.cdw.com/product/hpe-aruba-sfp-transceiver-module-10-gige/4919570.

[18] *See* footnote 15.


Client Data
Client Data is Mapped into the OTN here
"Source" OTN Path Terminating Equipment
OTUk Link
OTN Network
OTUk Link
"Sink" OTN Path Terminating Equipment
Client Data is de-mapped From the OTN here.
Client Data

[19]

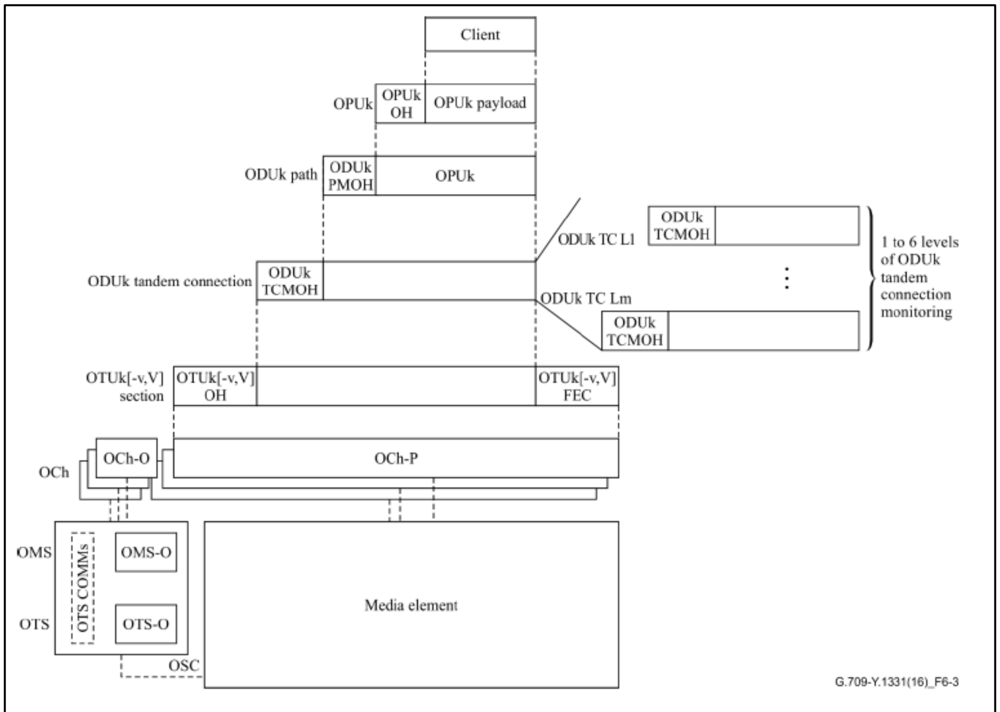


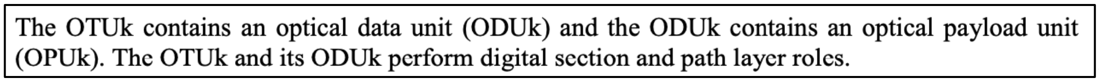
Figure 6-3 – MOTUm interface principal information containment relationships

[20]

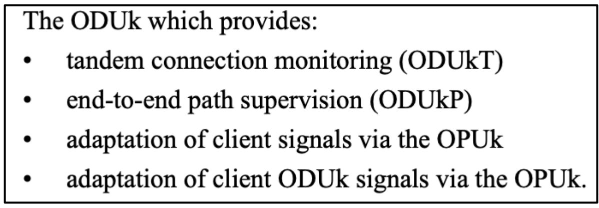
27. For example, the HPE SFP+ transceiver module performs the step of monitoring the intermediate form with a monitoring device, wherein the monitoring device is a 10GE LAN media access controller. Aruba SFP+ optical transceiver modules supports digital optical monitoring (DOM) that allows detailed monitoring and end-to-end path supervision.

[19] *See* footnote 1.

[20] *See* footnote 15.

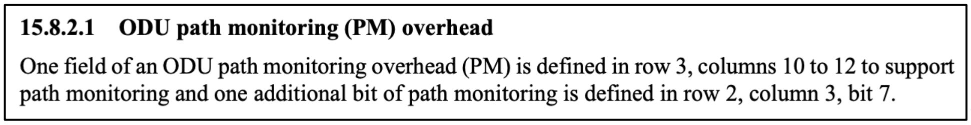


The OTUk contains an optical data unit (ODUk) and the ODUk contains an optical payload unit (OPUk). The OTUk and its ODUk perform digital section and path layer roles.[21]



The ODUk which provides:

- tandem connection monitoring (ODUkT)
- end-to-end path supervision (ODUkP)
- adaptation of client signals via the OPUk
- adaptation of client ODUk signals via the OPUk.[22]



15.8.2.1 ODU path monitoring (PM) overhead

One field of an ODU path monitoring overhead (PM) is defined in row 3, columns 10 to 12 to support path monitoring and one additional bit of path monitoring is defined in row 2, column 3, bit 7.[23]

28. Defendant has and continues to indirectly infringe one or more claims of the ’692 Patent by knowingly and intentionally inducing others, including HPE customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that receive, convert, monitor, and send 10GE LAN signals.

29. Defendant, with knowledge that these products, or the use thereof, infringe the ’692 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’692 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

[21] Source: ITU-T G.709/Y.1331, pp. 11 and 60.

[22] *Id.*

[23] *Id.*

30. Defendant induced infringement by others, including customers and end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’692 Patent, but while remaining willfully blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant’s website and other publications.[24] Upon information and belief, Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.[25]

31. Winterspring has suffered damages as a result of Defendant’s direct and indirect infringement of the ’692 Patent in an amount to be proved at trial.

32. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’692 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT II
(Infringement of ’646 Patent)

31**.** Paragraphs 1 through 15 are incorporated by reference as if fully set forth herein.

32. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’646 Patent.

33. Defendant has and continues to directly infringe the ’646 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making,

[24] *See, e.g.*, https://www.hpe.com/psnow/product-documentation?oid=7263510&cc=us&lc=en&jumpid=in_pdp-psnow-docs.

[25] *See, e.g.*, https://support.hpe.com/connect/s/?language=en_US.

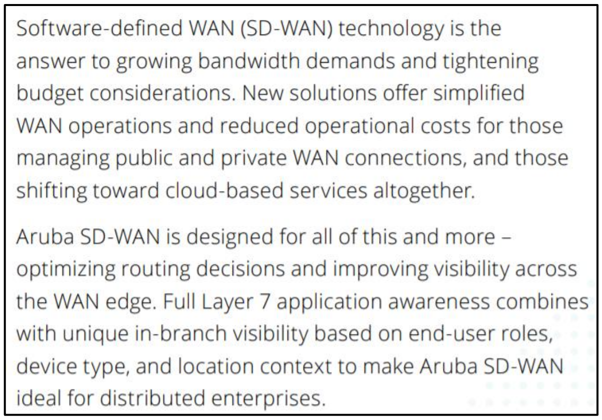
using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’646 Patent. Such products include hardware and software which allow a user with a GUI to optimize routing decisions, including, but not limited to, the Aruba Networks SD-Wan Orchestrator.

34. For example, Defendant has and continues to directly infringe at least claim 1 of the ’646 Patent by making, using, offering to sell, selling, and/or importing into the United States products that include hardware and software which allow a user with a GUI to optimize routing decisions.

35. For example, the HPE SD-Wan Orchestrator performs a method comprising the step of displaying, via a graphical user interface (GUI) on a display, a graphical representation of a plurality of nodes available in a network, wherein the plurality of nodes comprises a first edge node and a second edge node, wherein the plurality of nodes further comprises a plurality of router nodes located between the first edge node and the second edge node.

ARUBA SD-WAN

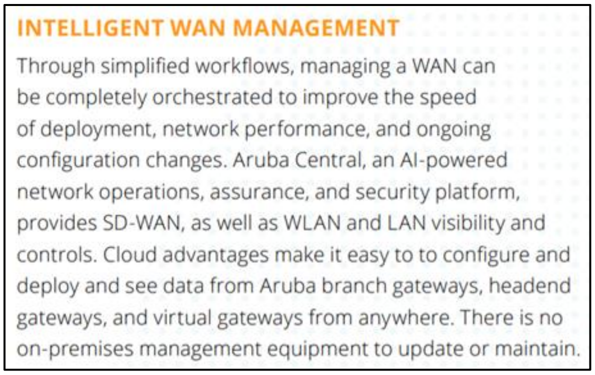
Improved visibility and control at the WAN edge



Software-defined WAN (SD-WAN) technology is the answer to growing bandwidth demands and tightening budget considerations. New solutions offer simplified WAN operations and reduced operational costs for those managing public and private WAN connections, and those shifting toward cloud-based services altogether.

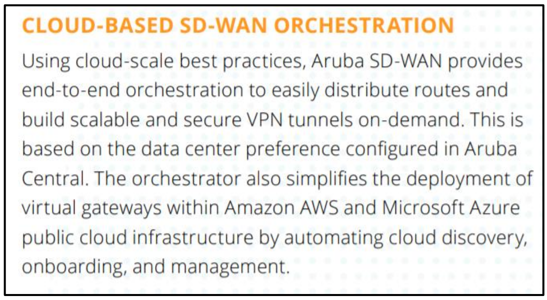
Aruba SD-WAN is designed for all of this and more – optimizing routing decisions and improving visibility across the WAN edge. Full Layer 7 application awareness combines with unique in-branch visibility based on end-user roles, device type, and location context to make Aruba SD-WAN ideal for distributed enterprises.[26]

[26] https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf, Page 1 of 6.



INTELLIGENT WAN MANAGEMENT

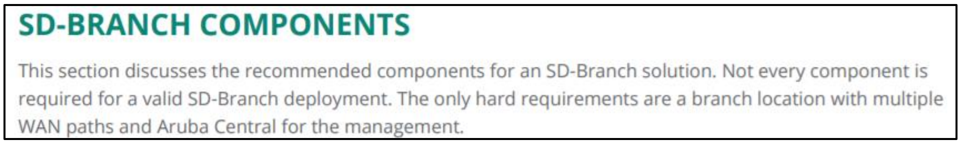
Through simplified workflows, managing a WAN can be completely orchestrated to improve the speed of deployment, network performance, and ongoing configuration changes. Aruba Central, an AI-powered network operations, assurance, and security platform, provides SD-WAN, as well as WLAN and LAN visibility and controls. Cloud advantages make it easy to to configure and deploy and see data from Aruba branch gateways, headend gateways, and virtual gateways from anywhere. There is no on-premises management equipment to update or maintain.



CLOUD-BASED SD-WAN ORCHESTRATION

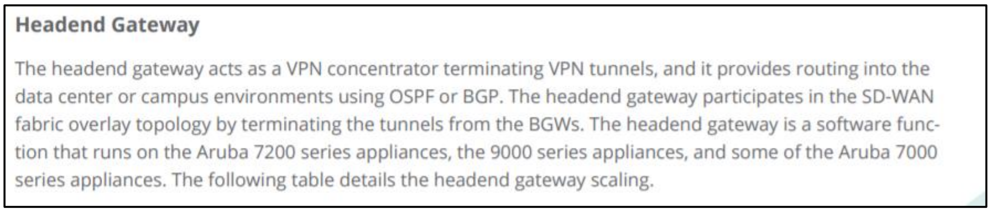
Using cloud-scale best practices, Aruba SD-WAN provides end-to-end orchestration to easily distribute routes and build scalable and secure VPN tunnels on-demand. This is based on the data center preference configured in Aruba Central. The orchestrator also simplifies the deployment of virtual gateways within Amazon AWS and Microsoft Azure public cloud infrastructure by automating cloud discovery, onboarding, and management.

[27]



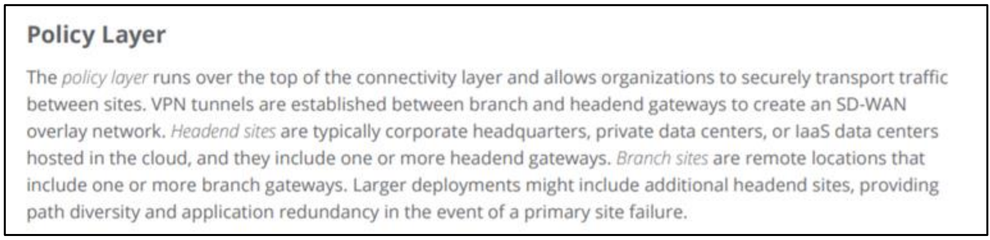
SD-BRANCH COMPONENTS

This section discusses the recommended components for an SD-Branch solution. Not every component is required for a valid SD-Branch deployment. The only hard requirements are a branch location with multiple WAN paths and Aruba Central for the management.



Headend Gateway

The headend gateway acts as a VPN concentrator terminating VPN tunnels, and it provides routing into the data center or campus environments using OSPF or BGP. The headend gateway participates in the SD-WAN fabric overlay topology by terminating the tunnels from the BGWs. The headend gateway is a software function that runs on the Aruba 7200 series appliances, the 9000 series appliances, and some of the Aruba 7000 series appliances. The following table details the headend gateway scaling.



Policy Layer

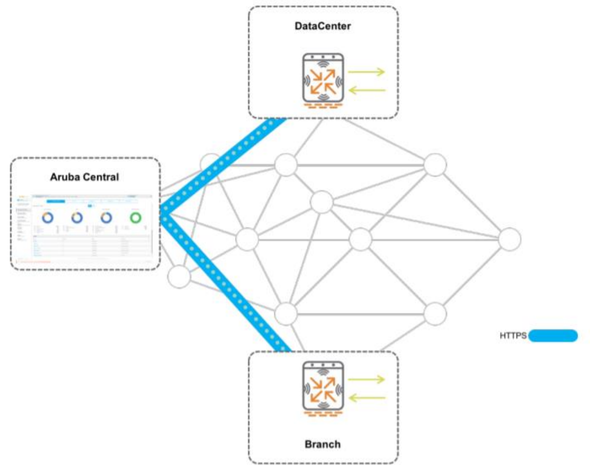
The *policy layer* runs over the top of the connectivity layer and allows organizations to securely transport traffic between sites. VPN tunnels are established between branch and headend gateways to create an SD-WAN overlay network. *Headend sites* are typically corporate headquarters, private data centers, or IaaS data centers hosted in the cloud, and they include one or more headend gateways. *Branch sites* are remote locations that include one or more branch gateways. Larger deployments might include additional headend sites, providing path diversity and application redundancy in the event of a primary site failure.

[28]

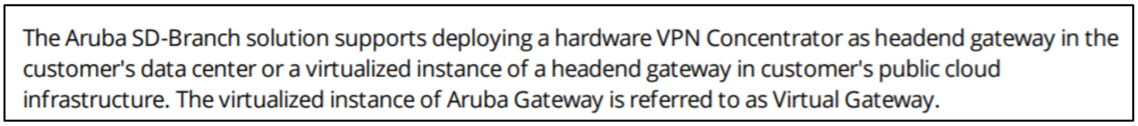
[27] https://www.arubanetworks.com/assets/ds/DS_SD-WAN.pdf, Page 1 of 6.

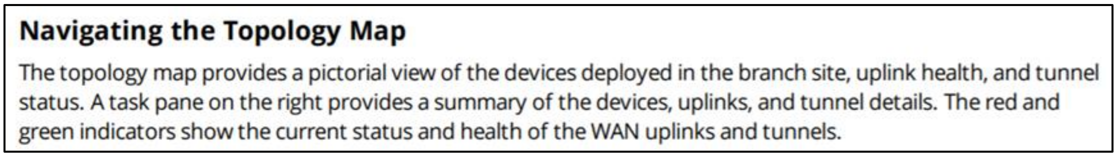
[28] https://www.arubanetworks.com/assets/tg/AVD_SD-Branch-Design.pdf Page 12, 40 of 190.

Figure 2 *Aruba Central and Cloud Communication*



[29]


The Aruba SD-Branch solution supports deploying a hardware VPN Concentrator as headend gateway in the customer's data center or a virtualized instance of a headend gateway in customer's public cloud infrastructure. The virtualized instance of Aruba Gateway is referred to as Virtual Gateway.


Navigating the Topology Map

The topology map provides a pictorial view of the devices deployed in the branch site, uplink health, and tunnel status. A task pane on the right provides a summary of the devices, uplinks, and tunnel details. The red and green indicators show the current status and health of the WAN uplinks and tunnels.

[29] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf Page 18 of 316.

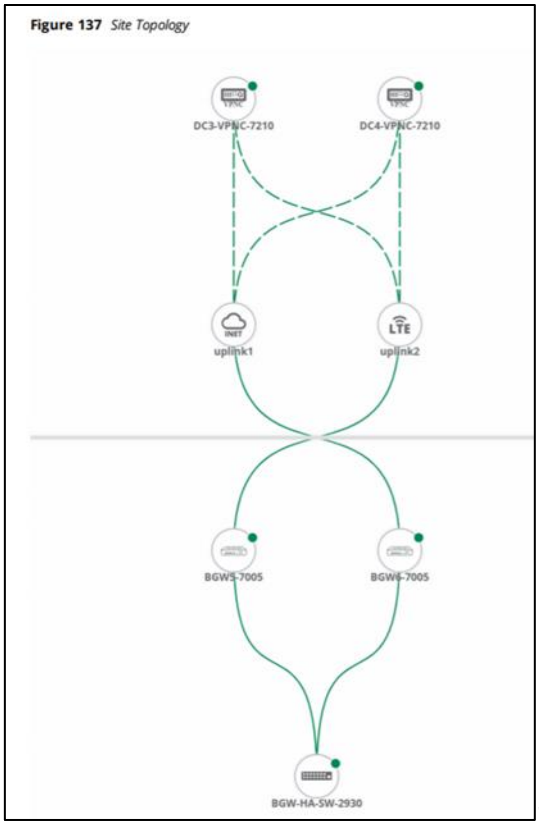
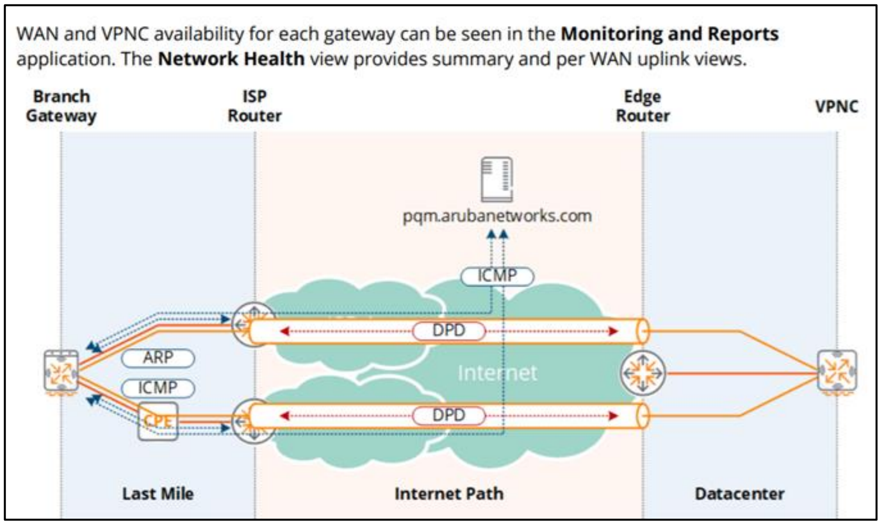


Figure 137 *Site Topology*

[30]



WAN and VPNC availability for each gateway can be seen in the **Monitoring and Reports** application. The **Network Health** view provides summary and per WAN uplink views.

[31]

[30] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf, Page 32, 299, 300 and 316.

[31] https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/14/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Fulldoc.pdf, page 79/229.

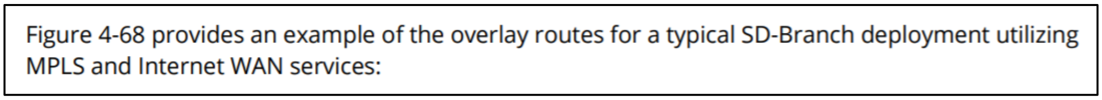
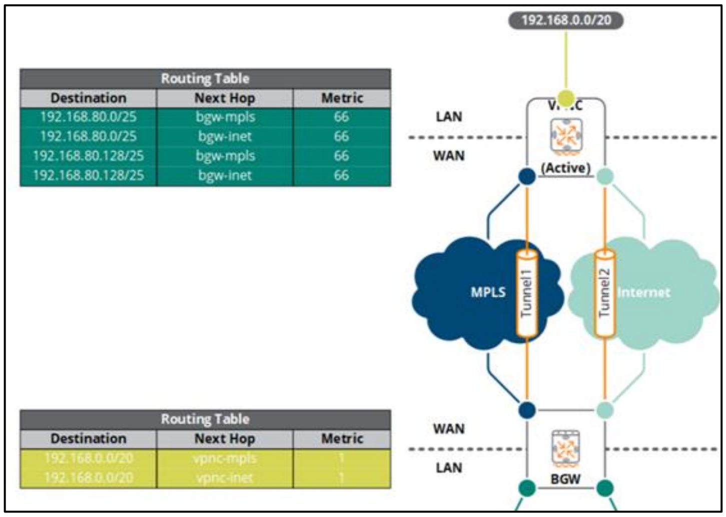


Figure 4-68 provides an example of the overlay routes for a typical SD-Branch deployment utilizing MPLS and Internet WAN services:



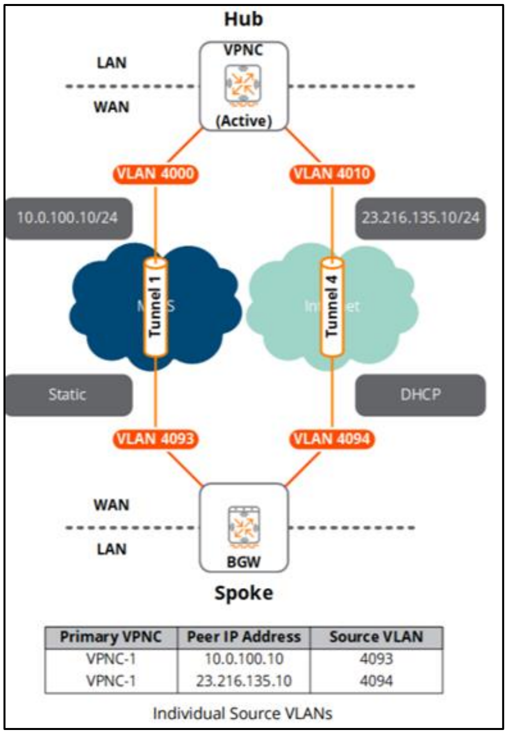
Routing Table		
Destination	Next Hop	Metric
192.168.80.0/25	bgw-mpls	66
192.168.80.0/25	bgw-inet	66
192.168.80.128/25	bgw-mpls	66
192.168.80.128/25	bgw-inet	66

Routing Table		
Destination	Next Hop	Metric
192.168.0.0/20	vpnc-mpls	1
192.168.0.0/20	vpnc-inet	1

[32]

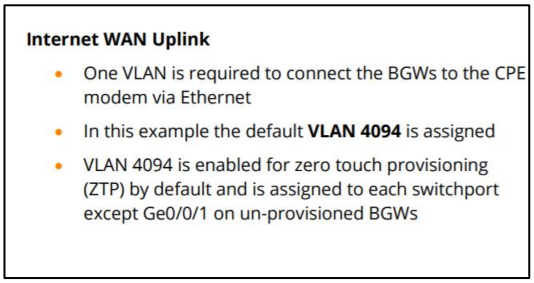
36. For example, the HPE Networks SD-Wan Orchestrator performs the step of displaying, via the GUI, a graphical representation of a plurality of paths available on the network between the first edge node and the second edge node on the network, wherein each of the plurality of paths passes through at least a subset of the plurality of router nodes, wherein the plurality of paths are displayed in a prioritized fashion in accordance with a difference in a number of nodes in each path of the plurality of paths through which traffic between the first edge node and the second edge node will pass if selected.

[32] https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/14/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Fulldoc.pdf, Page 114, 115/229.



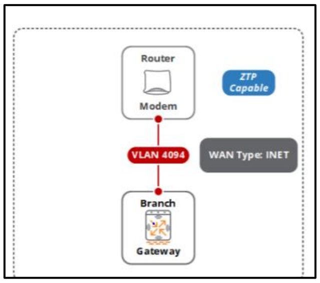
Primary VPNC	Peer IP Address	Source VLAN
VPNC-1	10.0.100.10	4093
VPNC-1	23.216.135.10	4094

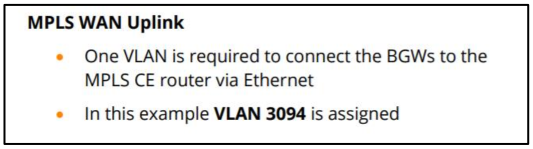
Individual Source VLANs



Internet WAN Uplink

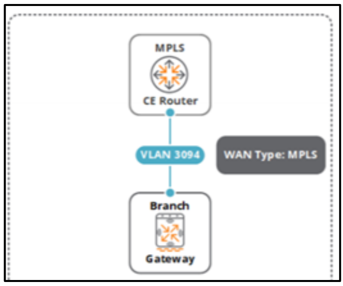
- One VLAN is required to connect the BGWs to the CPE modem via Ethernet
- In this example the default **VLAN 4094** is assigned
- VLAN 4094 is enabled for zero touch provisioning (ZTP) by default and is assigned to each switchport except Ge0/0/1 on un-provisioned BGWs



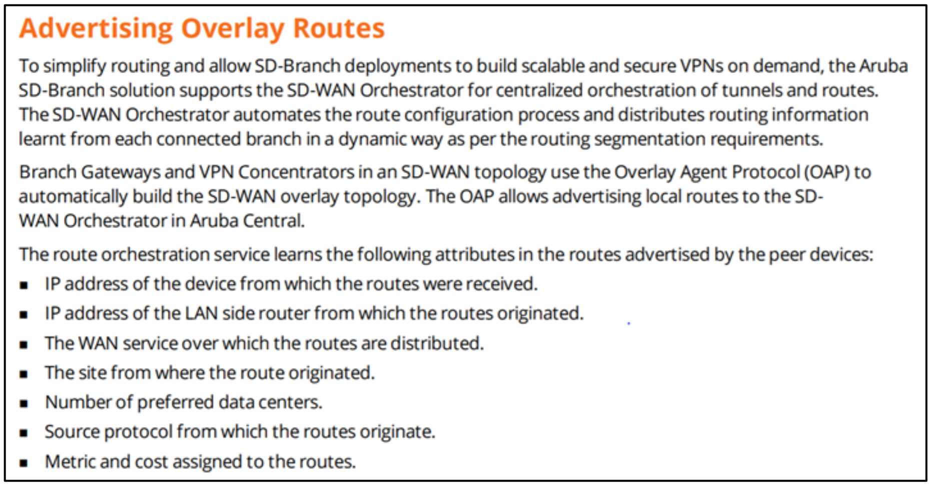


MPLS WAN Uplink

- One VLAN is required to connect the BGWs to the MPLS CE router via Ethernet
- In this example **VLAN 3094** is assigned



[33]



Advertising Overlay Routes

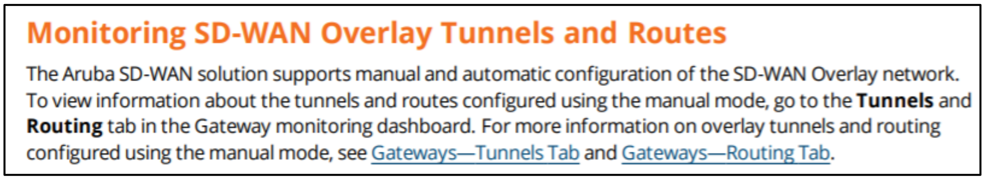
To simplify routing and allow SD-Branch deployments to build scalable and secure VPNs on demand, the Aruba SD-Branch solution supports the SD-WAN Orchestrator for centralized orchestration of tunnels and routes. The SD-WAN Orchestrator automates the route configuration process and distributes routing information learnt from each connected branch in a dynamic way as per the routing segmentation requirements.

Branch Gateways and VPN Concentrators in an SD-WAN topology use the Overlay Agent Protocol (OAP) to automatically build the SD-WAN overlay topology. The OAP allows advertising local routes to the SD-WAN Orchestrator in Aruba Central.

The route orchestration service learns the following attributes in the routes advertised by the peer devices:

- IP address of the device from which the routes were received.
- IP address of the LAN side router from which the routes originated.
- The WAN service over which the routes are distributed.
- The site from where the route originated.
- Number of preferred data centers.
- Source protocol from which the routes originate.
- Metric and cost assigned to the routes.

[34]

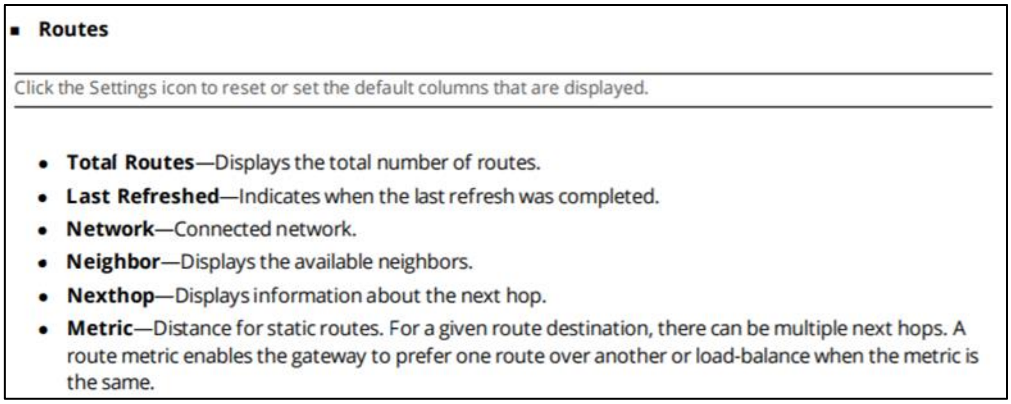


Monitoring SD-WAN Overlay Tunnels and Routes

The Aruba SD-WAN solution supports manual and automatic configuration of the SD-WAN Overlay network. To view information about the tunnels and routes configured using the manual mode, go to the **Tunnels** and **Routing** tab in the Gateway monitoring dashboard. For more information on overlay tunnels and routing configured using the manual mode, see Gateways—Tunnels Tab and Gateways—Routing Tab.

[33] https://community.arubanetworks.com/aruba/attachments/aruba/Aruba-VRDs/128/14/SD-Branch%20Fundamentals%20Guide%20-%20Final%20-%20Fulldoc.pdf, Page 104/229; *see also* https://community.arubanetworks.com/aruba/, Page 207/229.

[34] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf, Page 198 and 199/316.



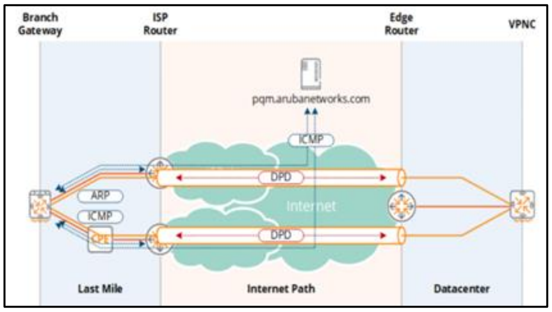
- **Routes**

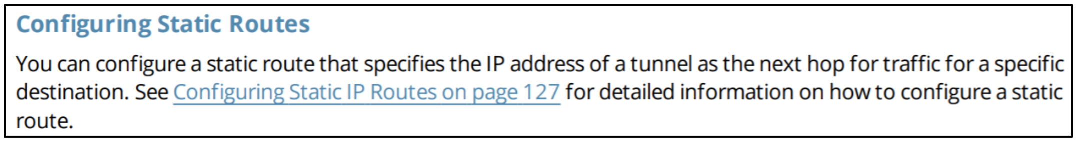
Click the Settings icon to reset or set the default columns that are displayed.

- **Total Routes**—Displays the total number of routes.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Network**—Connected network.
- **Neighbor**—Displays the available neighbors.
- **Nexthop**—Displays information about the next hop.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.

[35]

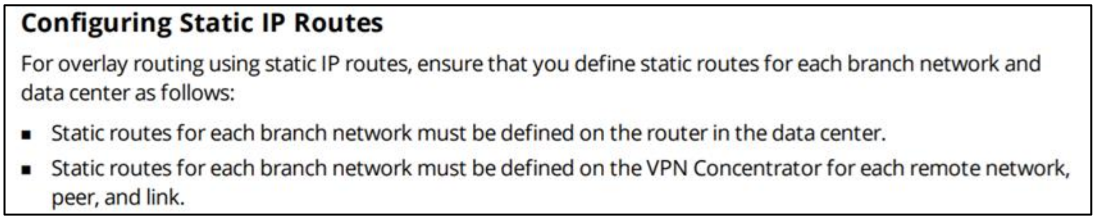
37. For example, the HPE Networks SD-Wan Orchestrator performs the step of selecting a path from the plurality of paths in response to a first user input received via the GUI, wherein the selected path passes through two or more router nodes of the plurality of router nodes. When configuring a static route, the user can select the uplink to use. The corresponding uplink shall contain the corresponding routers.





Configuring Static Routes

You can configure a static route that specifies the IP address of a tunnel as the next hop for traffic for a specific destination. See Configuring Static IP Routes on page 127 for detailed information on how to configure a static route.

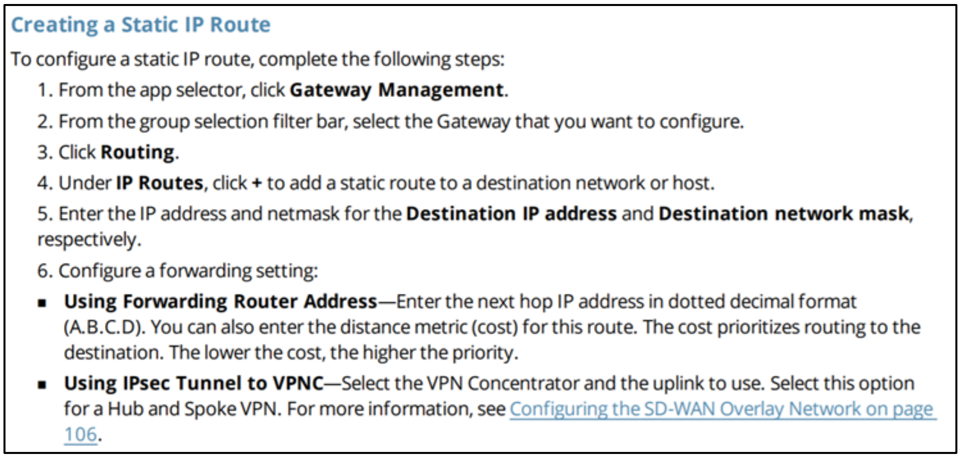


Configuring Static IP Routes

For overlay routing using static IP routes, ensure that you define static routes for each branch network and data center as follows:

- Static routes for each branch network must be defined on the router in the data center.
- Static routes for each branch network must be defined on the VPN Concentrator for each remote network, peer, and link.

[35] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf, Page 280/316.

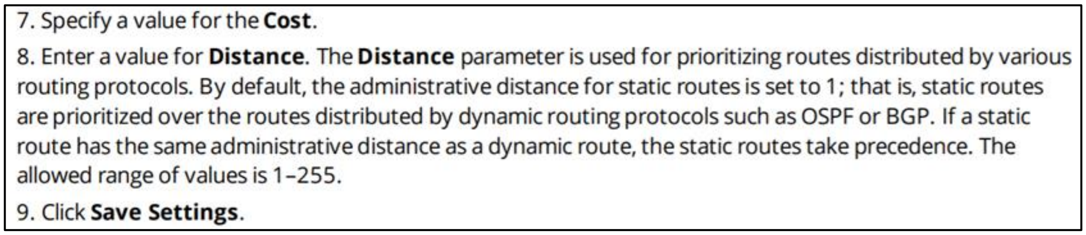


Creating a Static IP Route

To configure a static IP route, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the Gateway that you want to configure.
3. Click **Routing**.
4. Under **IP Routes**, click **+** to add a static route to a destination network or host.
5. Enter the IP address and netmask for the **Destination IP address** and **Destination network mask**, respectively.
6. Configure a forwarding setting:

- **Using Forwarding Router Address**—Enter the next hop IP address in dotted decimal format (A.B.C.D). You can also enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.
- **Using IPsec Tunnel to VPNC**—Select the VPN Concentrator and the uplink to use. Select this option for a Hub and Spoke VPN. For more information, see Configuring the SD-WAN Overlay Network on page 106.



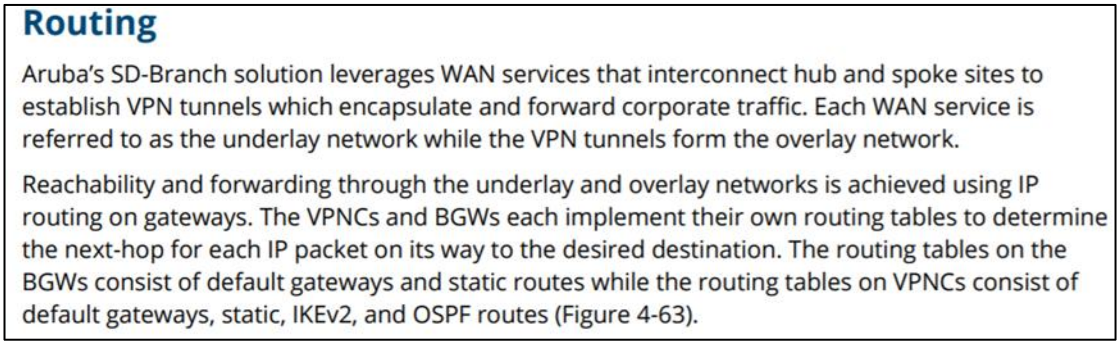
7. Specify a value for the **Cost**.

8. Enter a value for **Distance**. The **Distance** parameter is used for prioritizing routes distributed by various routing protocols. By default, the administrative distance for static routes is set to 1; that is, static routes are prioritized over the routes distributed by dynamic routing protocols such as OSPF or BGP. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. The allowed range of values is 1–255.

9. Click **Save Settings**.

[36]

38. For example, the HPE SD-Wan Orchestrator performs the step of initiating configuration of the two or more router nodes for communication between the first edge node and the second edge node in response to selecting the path. Based on the selection, the routing table of the gateway and the peers are updated in order to implement the static route.

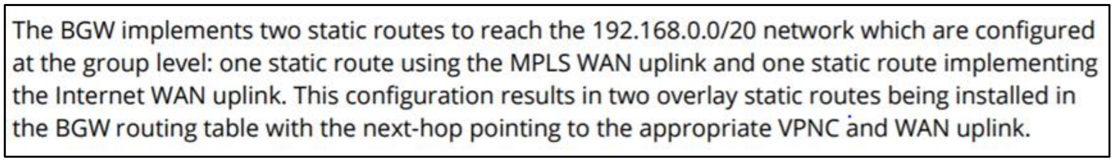


Routing

Aruba's SD-Branch solution leverages WAN services that interconnect hub and spoke sites to establish VPN tunnels which encapsulate and forward corporate traffic. Each WAN service is referred to as the underlay network while the VPN tunnels form the overlay network.

Reachability and forwarding through the underlay and overlay networks is achieved using IP routing on gateways. The VPNCs and BGWs each implement their own routing tables to determine the next-hop for each IP packet on its way to the desired destination. The routing tables on the BGWs consist of default gateways and static routes while the routing tables on VPNCs consist of default gateways, static, IKEv2, and OSPF routes (Figure 4-63).

[36] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf, Page 120 and 127/316.



The BGW implements two static routes to reach the 192.168.0.0/20 network which are configured at the group level: one static route using the MPLS WAN uplink and one static route implementing the Internet WAN uplink. This configuration results in two overlay static routes being installed in the BGW routing table with the next-hop pointing to the appropriate VPNC and WAN uplink.[37]

39. Defendant has and continues to indirectly infringe one or more claims of the ’646 Patent by knowingly and intentionally inducing others, including HPE customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States infringing products.

40. Defendant, with knowledge that these products, or the use thereof, infringed the ’646 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’646 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

41. Defendant induced infringement by others, including customers end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’646 Patent, but while remaining willfully blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant’s website and other publications. Upon information and belief,

[37] https://help.central.arubanetworks.com/2.4.9/documentation/online_help/content/pdfs/aruba_central_sd_wan_solution.pdf, Page 300/316.

Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.

42. Winterspring has suffered damages as a result of Defendant's direct and indirect infringement of the '646 Patent in an amount to be proved at trial.

43. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '646 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT III
(Infringement of the '975 Patent)

44. Paragraphs 1 through 15 are incorporated by reference as if fully set forth herein.

45. Winterspring has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '975 Patent.

46. Defendant has and continues to directly infringe the '975 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '975 Patent. Such products include, but are not limited to, computers, network switches, modules, and software that perform packet tagging.

47. For example, Defendant has and continues to directly infringe at least claim 5 of the '975 Patent by making, using, offering to sell, selling, and/or importing into the United States products that perform packet tagging.

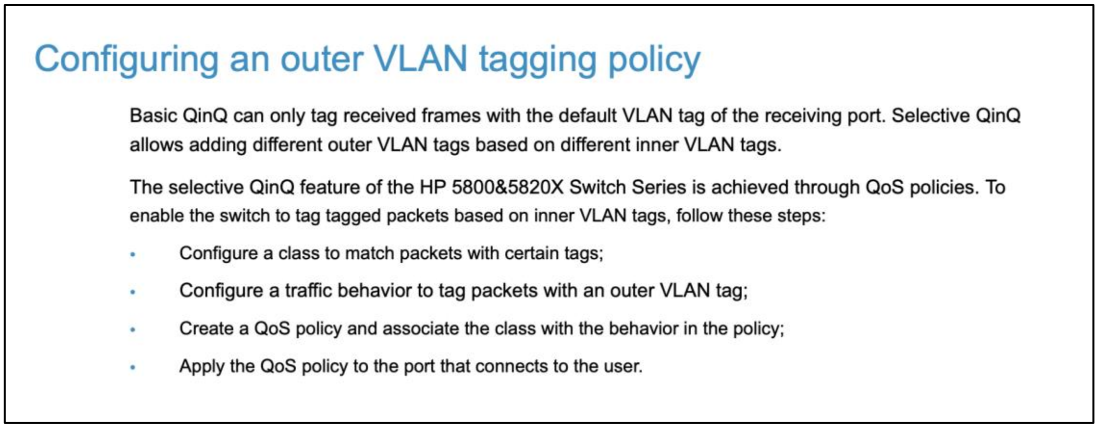
48. For example, the HPE FlexFabric 5820 Switch includes an apparatus comprising a network processor interface suitable for coupling to a network processor and a central processor interface suitable for coupling to a central processor. For example, one or more processing components within the FlexFabric 5820 Switch.

HPE FlexFabric 5820 Switch Series

[38]

49. Upon information and belief, the HPE FlexFabric 5820 Switch further includes a protocol determination logic block to determine a protocol type of data in a packet, wherein the protocol determination logic compares the protocol information in a first pass to predetermined values to procedure a first result and, if the first result is positive, compares the protocol information in a second pass to predetermined values to produce a second result, the first and second results forming a set of results (*e.g.*, VLAN tagging). HPE describes this process at least in its user manuals:

[38] https://cc.cnetcontent.com/vcs/hp-ent/inline-content/NT/8/3/832EE8C710C212FA7B7984447FAC44FF458F1FE5_source.PDF



Configuring an outer VLAN tagging policy

Basic QinQ can only tag received frames with the default VLAN tag of the receiving port. Selective QinQ allows adding different outer VLAN tags based on different inner VLAN tags.

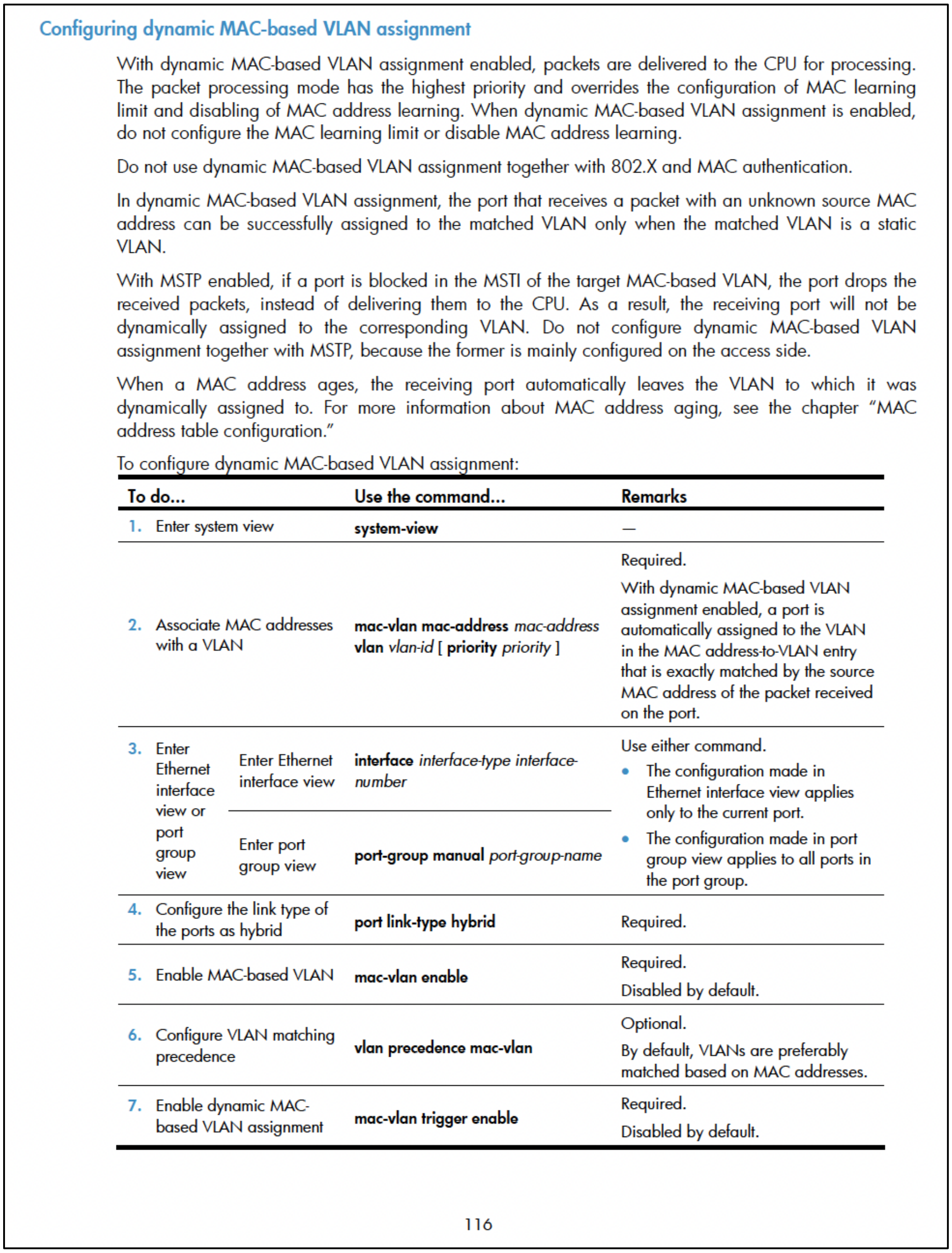
The selective QinQ feature of the HP 5800&5820X Switch Series is achieved through QoS policies. To enable the switch to tag tagged packets based on inner VLAN tags, follow these steps:

- Configure a class to match packets with certain tags;
- Configure a traffic behavior to tag packets with an outer VLAN tag;
- Create a QoS policy and associate the class with the behavior in the policy;
- Apply the QoS policy to the port that connects to the user.

[39]

50. Upon information and belief, the HPE FlexFabric 5820 Switch further comprises a tag select logic block to apply a tag to the packet indicating that the packet has an unknown protocol type if the first result is negative and if the first result is positive, the packet should be sent to either the central processor interface or the network processor interface based on the set of results. For example, such VLAN tagging is additionally described by HPE as follows:

[39] HP 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide.



Configuring dynamic MAC-based VLAN assignment

With dynamic MAC-based VLAN assignment enabled, packets are delivered to the CPU for processing. The packet processing mode has the highest priority and overrides the configuration of MAC learning limit and disabling of MAC address learning. When dynamic MAC-based VLAN assignment is enabled, do not configure the MAC learning limit or disable MAC address learning.

Do not use dynamic MAC-based VLAN assignment together with 802.X and MAC authentication.

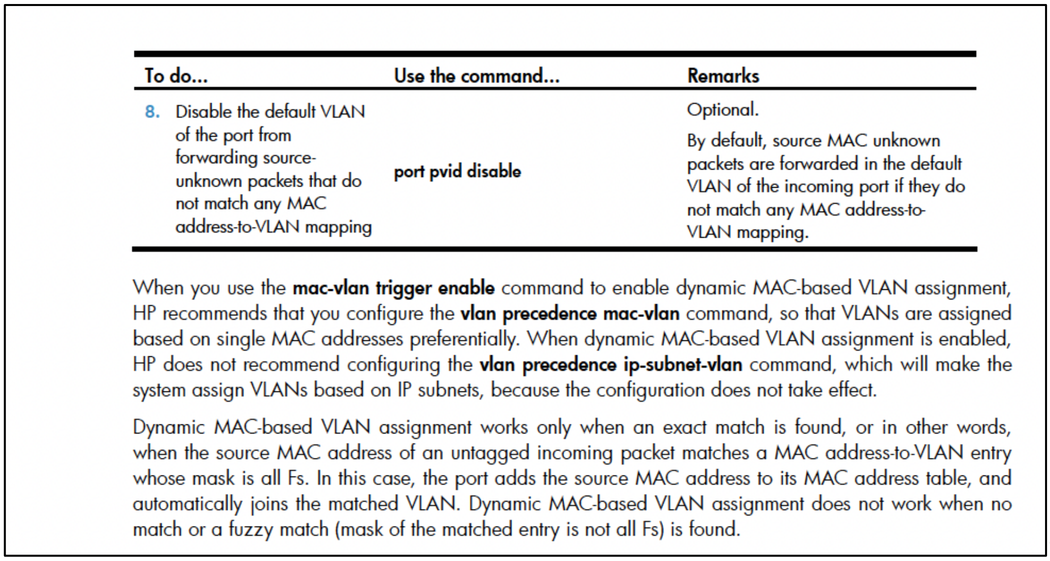
In dynamic MAC-based VLAN assignment, the port that receives a packet with an unknown source MAC address can be successfully assigned to the matched VLAN only when the matched VLAN is a static VLAN.

With MSTP enabled, if a port is blocked in the MSTI of the target MAC-based VLAN, the port drops the received packets, instead of delivering them to the CPU. As a result, the receiving port will not be dynamically assigned to the corresponding VLAN. Do not configure dynamic MAC-based VLAN assignment together with MSTP, because the former is mainly configured on the access side.

When a MAC address ages, the receiving port automatically leaves the VLAN to which it was dynamically assigned to. For more information about MAC address aging, see the chapter "MAC address table configuration."

To configure dynamic MAC-based VLAN assignment:

To do…		Use the command…	Remarks
1. Enter system view		**system-view**	—
2. Associate MAC addresses with a VLAN		**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**priority** *priority*]	Required. With dynamic MAC-based VLAN assignment enabled, a port is automatically assigned to the VLAN in the MAC address-to-VLAN entry that is exactly matched by the source MAC address of the packet received on the port.
3. Enter Ethernet interface view or port group view	Enter Ethernet interface view	**interface** *interface-type interface-number*	Use either command. • The configuration made in Ethernet interface view applies only to the current port. • The configuration made in port group view applies to all ports in the port group.
	Enter port group view	**port-group manual** *port-group-name*	
4. Configure the link type of the ports as hybrid		**port link-type hybrid**	Required.
5. Enable MAC-based VLAN		**mac-vlan enable**	Required. Disabled by default.
6. Configure VLAN matching precedence		**vlan precedence mac-vlan**	Optional. By default, VLANs are preferably matched based on MAC addresses.
7. Enable dynamic MAC-based VLAN assignment		**mac-vlan trigger enable**	Required. Disabled by default.



To do...	Use the command...	Remarks
8. Disable the default VLAN of the port from forwarding source-unknown packets that do not match any MAC address-to-VLAN mapping	**port pvid disable**	Optional. By default, source MAC unknown packets are forwarded in the default VLAN of the incoming port if they do not match any MAC address-to-VLAN mapping.

When you use the **mac-vlan trigger enable** command to enable dynamic MAC-based VLAN assignment, HP recommends that you configure the **vlan precedence mac-vlan** command, so that VLANs are assigned based on single MAC addresses preferentially. When dynamic MAC-based VLAN assignment is enabled, HP does not recommend configuring the **vlan precedence ip-subnet-vlan** command, which will make the system assign VLANs based on IP subnets, because the configuration does not take effect.

Dynamic MAC-based VLAN assignment works only when an exact match is found, or in other words, when the source MAC address of an untagged incoming packet matches a MAC address-to-VLAN entry whose mask is all Fs. In this case, the port adds the source MAC address to its MAC address table, and automatically joins the matched VLAN. Dynamic MAC-based VLAN assignment does not work when no match or a fuzzy match (mask of the matched entry is not all Fs) is found.

[40]

51. Defendant has and continues to indirectly infringe one or more claims of the ’975 Patent by knowingly and intentionally inducing others, including HPE customers and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States infringing products.

52. Defendant, with knowledge that these products, or the use thereof, infringed the ’975 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’975 Patent by providing these products to end users for use in an infringing manner. Alternatively, on information and belief, Defendant has adopted a policy of not reviewing the patents of others, including specifically those related to Defendant’s specific industry, thereby remaining willfully blind to the Patent-in-Suit at least as early as the issuance of the Patents-in-Suit.

53. Defendant induced infringement by others, including customers end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’975 Patent, but while remaining willfully

[40] HP 5820X & 5800 Switch Series Layer 2 - LAN Switching Configuration Guide

blind to the infringement. Defendant has and continues to induce infringement by its customers and end-users by supplying them with instructions on how to operate the Accused Instrumentalities in an infringing manner, while also making publicly available information on the Accused Instrumentalities via Defendant's website and other publications.[41] Upon information and belief, Defendant provides product support to its customers and end-users, where Defendant further instructs them to use the Accused Instrumentalities in an infringing manner.[42]

54. Winterspring has suffered damages as a result of Defendant's direct and indirect infringement of the '975 Patent in an amount to be proved at trial.

55. Winterspring has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '975 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Winterspring prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of one or more of the Patents-in-Suit;

[41] *See, e.g.*, https://www.hpe.com/psnow/doc/c04111589.

[42] *See, e.g.*, https://support.hpe.com/hpesc/public/docDisplay?docId=c02687399&docLocale=en_US&page=GUID-3D1EF05D-E41E-4ADC-AAE5-72F7A5EE2220.html.

c. An order awarding damages sufficient to compensate Winterspring for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Winterspring its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: August 21, 2023

Respectfully submitted,

/s/ *Vincent J. Rubino, III*
Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Road, Suite 206 South
Rye, NY 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

ATTORNEYS FOR PLAINTIFF
WINTERSPRING DIGITAL LLC