Technical Standards Compliance

HPE Aruba Networking EdgeConnect SD-WAN

Contents

Version History

v1.1

March 10, 2023

Technical Standards Compliance: HPE Aruba Networking EdgeConnect SD-WAN

Standards Reference	Specification
IEEE	
IEEE 802.1AB	Local and metropolitan area networks
IEEE 802.1AX-2008	Link Aggregation
IEEE 802.1Q	VLANs
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BASE-X
IEEE 802.3ae	10-Gigabit Ethernet
IEEE 802.3by-2016	802.3cc-2017 25-Gigabit Ethernet
IETF	
RFC 768	User Datagram Protocol
RFC 791	Internet Protocol
RFC 792	ICMP
RFC 793	TCP
RFC 813	Window and Acknowledgement Strategy in TCP
RFC 815	IP datagram reassembly algorithms
RFC 826	ARP
RFC 879	TCP maximum segment size and related topics
RFC 896	Congestion control in IP/TCP internetworks

Standards Reference	Specification
RFC 917	Internet subnets
RFC 919	Broadcasting Internet Datagrams
RFC 922	Broadcasting Internet Datagrams in the Presence of Subnets (IP_BROAD)
RFC 925	Multi-LAN address resolution
RFC 950	Internet Standard Subnetting Procedure
RFC 951	BOOTP
RFC 1027	Proxy ARP
RFC 1035	Domain Names
RFC 1122	Requirements for Internet Hosts - Communications Layers
RFC 1215	Convention for defining traps for use with the SNMP
RFC 1256	ICMP Router Discovery Messages
RFC 1393	Traceroute Using an IP Option
RFC 1403	BGP OSPF Interaction
RFC 1519	CIDR
RFC 1583	OSPF Version 2
RFC 1591	Domain Name System Structure and Delegation
RFC 1661	The Point-to-point Protocol (PPP)
RFC 1757	Remote Network Monitoring Management Information Base
RFC 1772	Application of the Border Gateway Protocol in the Internet
RFC 1812	Requirements for IP Version 4 Router
RFC 1918	Address Allocation for Private Internet
RFC 1930	Guidelines for the creation, selection, and registration of an Autonomous

Standards Reference	Specification
RFC 1997	BGP Communities Attribute
RFC 1998	An Application of the BGP Community Attribute in Multi-home Routing
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DHCP Options and BOOTP Vendor Extensions
RFC 2236	IGMP
RFC 2328	OSPF Version 2
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	IP Authentication Header
RFC 2439	BGP Route Flap Damping
RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2464	Transmission of IPv6 over Ethernet Networks
RFC 2516	A Method for Transmitting PPP over Ethernet (PPoE)
RFC 2544	Network interconnection test
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2548	Microsoft Vendor-specific RADIUS Attributes
RFC 2576	Coexistence between SNMP V1, V2, V3
RFC 2637	Point-to-point tunneling protocol (PPTP)
RFC 2663	IP Network Address Translator (NAT)
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol

Standards Reference	Specification
RFC 2866	RADIUS Accounting
RFC 2918	Route Refresh Capability for BGP-4
RFC 2925	Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 3046	DHCP Relay Agent Information Option
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 3065	Autonomous System Confederation for BGP
RFC 3101	OSPF Not-so-stubby-area option
RFC 3268	Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3376	Internet Group Management Protocol (IGMP), Version 3
RFC 3416	(SNMP Protocol Operations v2)
RFC 3417	(SNMP Transport Mappings)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
RFC 3509	Alternative Implementations of OSPF Area Border Routers
RFC 3575	IANA Considerations for RADIUS
RFC 3623	Graceful OSPF Restart
RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3768	Virtual Router Redundancy Protocol (VRRP)

Standards Reference	Specification
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC 4251	The Secure Shell (SSH) Protocol
RFC 4271	A Border Gateway Protocol 4 (BGP-4)
RFC 4291	IP Version 6 Addressing Architecture
RFC 4301	Security Architecture for IP
RFC 4360	BGP Extended Communities Attribute
RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 4419	Key Exchange for SSH
RFC 4443	Internet Control Message Protocol (ICMPv6)
RFC 4456	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC 4486	Subcodes for BGP Cease Notification Message
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
RFC 4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
RFC 4552	Authentication/Confidentiality for OSPFv3
RFC 4601	PIM Sparse Mode
RFC 4607	Source-Specific Multicast for IP
RFC 4724	Graceful Restart Mechanism for BGP
RFC 4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
RFC 4760	Multiprotocol Extensions for BGP-4

Standards Reference	Specification
RFC 4861	IPv6 Neighbor Discovery
RFC 4868	Using HMAC-SHA-256, SHA-384, SHA-512 with IPsec
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
RFC 4869	Suite B cryptography applied to IPsec.
RFC 4940	IANA Considerations for OSPF
RFC 5065	Autonomous System Confederation for BGP
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial-in User Service (RADIUS)
RFC 5246	TLS Protocol Version 1.2
RFC 5280	X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS
RFC 5289	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
RFC 5424	Syslog Protocol
RFC 5480	Elliptic Curve Cryptography
RFC 5492	Capabilities Advertisement with BGP-4
RFC 5701	IPv6 Address Specific BGP Extended Community Attribute
RFC 5722	Handling of Overlapping IPv6 Fragments
RFC 5759	Suite B Certificate and Certificate Revocation List (CRL) Profile
RFC 5798	VRRP (exclude Accept Mode and sub-sec timer)
RFC 5880	Bidirectional Forwarding Detection

Standards Reference	Specification
RFC 5903	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
RFC 6379	Suite B Cryptographic Suites for IPsec
RFC 6380	Suite B Profile for Internet Protocol Security (IPsec)
RFC 6460	Suite B Profile for Transport Layer Security (TLS)
RFC 6587	Transmission of Syslog Messages over TCP
RFC 6987	OSPF Stub Router Advertisement
RFC 7230	Hypertext Transfer Protocol (HTTP/1.1)
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 7313	Enhanced Route Refresh Capability for BGP-4
RFC 7348	VXLAN: A Framework for Overlaying Virtualized layer 2 Networks over Layer 3 Networks
RFC 7456	Loss and Delay measurement
RFC 7540	HTTP/2 (flow mode, proxy mode)
RFC 7717	IKEv2-Derived Shared Secret Key for OWAMP
RFC 7911	Advertisement of Multiple Paths in BGP
RFC 8201	Path MTU Discovery for IP version 6
RFC 8247	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 8290	Flow Queue CoDel Packet Scheduler and Active Queue Management Algorithm
RFC 8365	Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)

Standards Reference	Specification
NIST	
FIPS 140-2	Security Requirements for Cryptographic modules
FIPS 140-3	Security Requirements for Cryptographic modules
FIPS 180-4	Secure Hash Standard (SHS)
FIPS 186-4	Digital Signature Standard
FIPS 197	Advanced Encryption Standard (AES)
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
SP 800-38C	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
SP-800-52 Rev 2	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
SP 800-56A	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-56B	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
SP 800-56C	Recommendation for Key-Derivation Methods in Key-Establishment Schemes

Standards Reference	Specification
SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation
SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
SP 800-132	Recommendation for Password-Based Key Derivation
SP 800-133 Rev 2	Recommendation for Cryptographic Key Generation

Regulatory	
EMC	FCC Part 15 Class A, EN 55024/55032/55035 Class A, VCCI Class A, EN 61000-3-2/3-3
Safety	UL/CB 60950-1 / 62368-1, EN 60950 / 62368

Learn more at

www.arubanetworks.com