Dell EMC SmartFabric OS10

Glossary

09 2020
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

About this guide

The glossary provides a quick definition of the terms used in the OS10 user guide. This guide is intended for system administrators who are responsible for configuring and maintaining networks.

Documentation Feedback

Dell Technologies strives to provide accurate and comprehensive documentation and welcomes your suggestions and comments. You can provide feedback in the following ways:

- Online feedback form—Rate the documentation or provide your feedback on any of our documentation pages at www.dell.com/support.
- Email—Send your feedback to networkingpub.feedback@dell.com. Include the document title, release number, chapter title, and section title of the text corresponding to the feedback.

To get answers to your questions related to Dell EMC SmartFabric OS10 through email, chat, or call, please visit our Technical Support page.

2

Glossary of Terms

A

Access Control List (ACL)	A filter that controls network traffic by dropping or forwarding packets based on a set of configured rules.
Access Port	A port on a VTEP switch that connects to an end host and is a part of the overlay network.
Address Resolution Protocol (ARP)	A protocol that runs over Ethernet and enables end stations to learn the MAC addresses of neighbors on an IP network.
Alerting	A process that triggers problem reporting.
Analyzing and reporting	A process that captures metrics and packets.
Ansible	A simple agentless automation framework. It can configure systems, deploy software, and orchestrate advanced IT tasks such as continuous deployments and zero downtime rolling updates. Ansible supports network automation as part of its core framework.
Anycast address	A unicast address configured on more than one Rendezvous Point (RP). A packet sent to the anycast address is sent to the nearest RP with anycast address, as determined by the routing protocol.
Anycast RP	An implementation strategy that provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM-SM) networks.
Authentication, Authorization, and Accounting (AAA)	A standard framework that controls user access to the switch (authentication), user operations authorized on the switch (authorization), and history of user actions performed during a session (accounting).
Auto	An unauthorized state in 802.1x, in which a device connected to a port is subject to the authorization process. If the process is successful, the port is authorized and the connected device communicates on the network.
Automated switch provisioning	An automated process that enables configuration and monitoring using RESTCONF APIs, Linux DevOps ecosystem, and Ansible.

B

Batch Mode	A mode the enables you to run a batch file with multiple commands.
BFD three-way handshake	A process that exchanges synchronization and acknowledgment messages before the real data communication process begins. BFD session requires a three-way handshake between neighboring routers.
BGP communities	A set of routes with one or more common attributes that are used in dynamic routing policies.
Bidirectional Forwarding Detection (BFD)	A protocol that provides rapid failure detection in links with adjacent routers.
Border Gateway Protocol (BGP)	An external gateway protocol that transmits inter-domain routing information within and between autonomous systems.

C

Command Alias	A shortcut for commonly-used commands.
Configuration mode	A mode that enables you to change the current running configuration.
Control-plane policing	A Quality of Service (QoS) mechanism that increases system security by protecting the route processor from unnecessary traffic and prioritizing important control plane and management traffic.
Converged Enhanced Ethernet (CEE)	A technology that uses DCBX specification v1.01 to enable interoperation with a larger set of switches when using Data Center Bridging (DCB).
Curl command	A Linux shell command that generates HTTPS requests executed on an external server.

D

Data Center Bridging Exchange (DCBX)	A protocol that allows a switch to automatically discover and set up DCBX-enabled peers that are configured with compatible settings. In a converged data center network, DCBX provides plug-and-play capability for server, storage, and networking devices in an end-to-end solution.
Default VLAN	A VLAN instance to which ports are assigned when they are not being used. Ports that are administratively up in the L2 mode are automatically placed in the default VLAN as untagged interfaces. On SmartFabric OS10 switches, VLAN 1 is the default VLAN.
Dell Digital Locker	A service associated with your Dell Technologies user account that enables you to download purchased software, access licensed software products, download updates and patches, manage user and product groups, view software license entitlements, and manage warranty subscriptions.
Dell EMC SmartFabric OS10	A network operating system that supports multiple architectures and environments.
Destination group	An arrangement that identifies the IP address and transport port on a destination server to which telemetry data is streamed.
DHCP relay agent	A process that relays DHCP messages to and from a remote DHCP server, even if the client and server are on different IP networks.
DHCP server	A server that provides network configuration parameters to DHCP clients on request. A DHCP server dynamically allocates four required IP parameters to each computer on the virtual local area network (VLAN) — the IP address, network mask, default gateway, and name server address. DHCP IP address allocation works on a client/server model where the server assigns the client reusable IP information from an address pool.
DHCP snooping	A Layer 2 (L2) security feature that helps networking devices to monitor DHCP messages and block untrusted or rogue DHCP servers.
Dial-out mode	A mode where the switch initiates a session with one or more devices according to the sensor paths and destinations in a subscription.
Differentiated Services Code Point (DSCP)	A network layer service that classifies and manages network traffic and provides Quality of Service (QoS) to modern IP networks.
DNS	A protocol that is responsible for name server registration and management of Nx_Ports that are attached to the switch.
Docker-CE	A free containerization platform that allows you to download and install external packages and run them within OS10.
Duplicate Address Discovery (DAD)	A protocol that verifies the uniqueness of IPv6 home address on the LAN before the address is assigned to a physical interface.

Dynamic Host Configuration Protocol	A protocol that provides information to dynamically assign IP addresses and other configuration parameters to network hosts based on policies.

E

Encapsulated Remote Port Monitoring (ERPM)	A protocol that encapsulates traffic from the source port and forwards it to the destination port in another switch.
Enhanced Transmission Selection (ETS)	A transmission selection algorithm that increases preferred traffic class throughput during network congestion.
Equal Cost Multi-Path (ECMP)	A network routing strategy that provides next-hop packet forwarding to a single destination over multiple best paths.
EXEC mode	A mode that provides access to monitoring and troubleshooting commands.
Expansion port (E_Port)	A port that connects two fibre channel switches to form a multiswitch SAN fabric.
Explicit Congestion Notification (ECN)	An extension to the Internet Protocol and Transmission Control Protocol that allows notification of congestion without any drop in packets.
Extensible Authentication Protocol (EAP)	A protocol that provides device credentials to an authentication server, typically a remote authentication dial-in service (RADIUS), using an intermediary network access device.

F

Fabric Shortest Path First (FSPF)	A standard path selection protocol used by Fibre Channel fabrics.
Far-End Failure Detection (FEFD)	A protocol that detects remote data link errors in a network.
FCoE Initialization Protocol (FIP)	A protocol that establishes Fibre Channel connectivity with Ethernet ports.
Fiber Channel over Ethernet (FCoE)	A storage protocol that enables Fiber Channel communications to run over Ethernet.
Fibre Channel Fabric Port (F_Port)	A switch port that connects the Fibre Channel fabric to a host.
Fibre Channel Zoning (FC zoning)	A process that partitions a Fibre Channel fabric into subsets to restrict unnecessary interactions, improve security, and manage the fabric more effectively.
FIP Snooping Bridge (FSB)	A mode that implements security characteristics to admit valid FCoE traffic in the Ethernet networks.
First Hop Router (FHR)	A router that is directly connected to the multicast source. The FHR is responsible for the Protocol Independent Multicast (PIM) register process.
Force-unauthorized	An unauthorized state in which a device connected to a port is not allowed to communicate on the network without using the authentication process.

Force-authorized	An authorized state in which a device connected to the port can communicate on the network without using the authentication process.
Full-duplex	A transmission mode where a device, such as a switch, can transmit and receive data simultaneously.

G

gRPC Network Management Interface agent (gNMI)	A protocol that enables the telemetry agent to transmit pre-configured sensor groups data to the SmartFabric Director.

H

Half-Duplex	A transmission mode where a device, such as a switch, can transmit and receive data, but not at the same time.
Hello-time	The time interval within which the bridge sends BPDUs.
Hop-by-hop options	An extension header in an IPv6 packet with options that are processed by all IPv6 routers in the packet's path.

I

IGMP	A communication protocol that is used on IPv4 networks to establish multicast group memberships.
IGMP messages	Protocol messages that are used in the host-router communication.
IGMP snooping	A switch protocol that listens to the IGMP messages exchanged between the host and router. It generates a forwarding table that associates ports with multicast groups.
Incoming Interface (IIF)	An interface on which a multicast packet is received. It can be a source interface or the rendezvous point (RP).
Internet Small System Unit System Interface (iSCSI)	A TCP/IP-based protocol that establishes and manages connections between servers and storage devices in a data center network.
Inter-Switch Link (ISL)	A link that joins two fiber channel switches through E Ports.
IPv4 Routing	A routing mechanism that forwards network packets to a destination IP address based on a routing table.
IPv6 Routing	A routing mechanism similar to IPv4 that uses 128-bit IPv6 addresses. IPv6 provides additional routing capabilities such as stateless auto-configuration, header format simplifications, and improved support for options and extensions.

J

Jumbo frames	Ethernet frames with a payload greater than the standard MTU of 1500 bytes (up to a maximum of 9000 bytes).
Jump host	A designated port on a leaf switch in a SmartFabric mode to which an external device such as a laptop can be connected.

L

Last Hop Router (LHR)	The last router in the multicast path that is directly connected to the multicast receiver.
Link Aggregation (LA)	A method of grouping multiple physical interfaces into a single logical interface.
Link Aggregation Control Protocol (LACP)	A protocol that exchanges information between two systems and automatically establishes a link aggregation group (LAG) between them.
Link Layer Discovery Protocol — Media Endpoint Discovery (LLDP-MED)	A protocol that enables endpoint devices and network connected devices to advertise their characteristics and configuration information.
Link Layer Discovery Protocol (LLDP)	A protocol that enables a local area network (LAN) device to advertise its configuration and receive configuration information from adjacent LLDP-enabled infrastructure devices.
Link-State Advertisements (LSA)	The fundamental building blocks of OSPF that communicate the routing topology of the router to all other routers in the network.
LLDP Data Unit (LLDPDU)	A sequence of type-length-value (TLV) structures. LLDP information is sent from each of the configured interfaces at a fixed interval in the form of an Ethernet frame that contains one LLDPDU.

M

Mac-flush-timer	A MAC flush parameter that defines the time used to flush the MAC address entries.
Martian addresses	Special IPv4 and IPv6 addresses that are not routed by routing devices on the Internet.
Max-age	A global parameter that defines the length of time a switch maintains configuration information before it refreshes that information by recomputing the MST topology.
Max-hops	A parameter that defines the maximum number of hops a BPDU travels before a receiving device discards it.
Media Access Control (MAC)	A L2 protocol that determines how data is transmitted between devices within a broadcast domain.
MLD snooping	An IPv6 L2 multicast protocol that enables switches to use the information in MLD packets and generate a forwarding table that associates ports with multicast groups. When switches receive multicast frames, they forward them to their intended receivers.
Multicast	A communication method that allows networking devices to send data to a group of interested receivers in a single transmission, in contrast to unicast and broadcast.
Multicast Listener Discovery (MLD)	A protocol that the IPv6 router uses to discover listeners for a specific multicast group, and to set up and maintain multicast group memberships.
Multicast Listener Discovery Protocol	A protocol that helps to manage the multicast groups. OS10 supports MLDv1and MLDv2 to manage the multicast group memberships on IPv6 networks.
Multicast router	A Layer 3 (L3) router or switch that has multicast features enabled.
Multiple Spanning-Tree (MST)	A protocol that allows mapping of MST instances and multiple VLAN networks to a single spanning-tree instance.

Multiprotocol BGP (MBGP)	An extension to BGP that supports multiple address families—IPv4 and IPv6. MBGP carries multiple sets of unicast and multicast routes depending on the address family.

N

N_Port ID Virtualization (NPIV)	A process that allows multiple N_Port IDs to share a single physical N_Port.
Neighbor Discovery Protocol (NDP)	A protocol that determines if neighboring IPv6 devices are reachable and receives the IPv6 addresses of IPv6 devices on local links.
Network fabric	A fabric that consists of leaf and spine switches that are connected in a SmartFabric cluster.
Network Management System (NMS)	A set of one or more application that allows network administrators manage independent components of a network inside a bigger network management framework.
Network port (VxLAN)	A port on a VTEP switch that connects to the underlay network.
Network Time Protocol (NTP)	A networking protocol for time synchronization between time servers and clients.
Network Virtualization Overlay (NVO)	An overlay network that extends L2 connectivity between server virtual machines (VMs) in a tenant segment over an underlay L3 IP network.
NewServiceTag	Service tag of a new IOM.
Node Port (N_Port)	A port on a network node that acts as a host or storage device.
NPIV Proxy Gateway (NPG)	A gateway that bridges FCoE and FC.

O

Object Tracking Manager (OTM)	A mechanism that tracks the link status of L2 interfaces, and the reachability of IPv4 and IPv6 hosts.
OldServiceTag	Service tag of the faulty IOM.
Open Network Install Environment (ONIE)	A Linux-based operating system that boots on a switch and discovers the network operating system installer images that are available on the network. ONIE provides the environment for the selected network operating system to load on the switch.
Open Shortest Path First (OSPF)	A link-state routing protocol that communicates with all other devices in the same autonomous system area using link-state advertisements (LSAs). OS10 supports up to 10,000 OSPF routes for OSPFv2 to designate up to 8,000 routes as external, and up to 2,000 as inter/intra area routes.
OpenFlow	A communication protocol in a software defined networking (SDN) environment that allows the SDN Controller to interact with the forwarding plane of network devices such as switches and routers.
Orphan ports	Ports that are not part of the VLT port channel but members of the spanned VLANs.
OSPF Autonomous systems	A collection of networks under a common administration that share a common routing strategy. OSPF is an intra-AS, Interior Gateway Routing Protocol (IGRP) that receives routes from and sends routes to other autonomous systems.
Outgoing Interface (OIF)	The interface through which a multicast packet is sent out towards a multicast receiver.

P

Performance monitoring	A process that establishes baselines and defines triggers for detecting performance problems.
PIM Shared Tree (RP Tree)	A unidirectional multicast tree whose root node is the RP. When receivers want to join a multicast group, they send join messages along the shared tree towards the RP.
PIM Shortest Path Tree (SPT)	A shortest path that a multicast packet can take from source to receiver.
PIM Source Specific Multicast (PIM-SSM)	A subset of PIM sparse mode and IGMP version 3 (IGMPv3). PIM-SSM allows receivers to specify the source from which to receive data and the multicast group they want to join.
PIM Sparse Mode (PIM-SM)	A multicast routing protocol that is applicable to large-scale multicast networks with scattered members.
Policy-based route-maps	An ordered set of rules that control the redistribution of IP routes into a protocol domain.
Policy-based routing	A mechanism to redirect IPv4 and IPv6 data packets based on the policies defined to override the forwarding decision of the switch. The forwarding decisions are based on the routing table.
Port Monitoring (Local or Remote)	A process that monitors the ingress and egress traffic on specified ports. Monitoring methods include port-mirroring, remote port monitoring, and encapsulated remote-port monitoring.
Port security	The MAC addresses of the workstations that are allowed to access a port.
Port-scoped VLAN	A Port-VLAN pair that maps to a virtual network ID (VNID). Assign an individual member interface to a virtual network as a tagged or an untagged member.
Precision Time Protocol (PTP)	A protocol that synchronizes clocks on network devices.
Principal switch	A switch that assigns and maintains a unique domain ID across the fabric.
Priority Flow Control (PFC)	A mechanism that prevents frame loss due to congestion. The process uses priority-based flow control to ensure lossless transmission of storage traffic, while transmitting other traffic classes that perform better without flow control.
Privilege levels	A mechanism that limits user access. OS10 supports 16 privilege levels.
Protocol Independent Multicast (PIM)	A standard multicast routing protocol for IP networks that provide one-to-many and many-to-many distribution of data. It is used to dynamically establish and maintain multicast distribution trees and is independent of the mechanisms that any specific unicast routing protocol provides.
Public Key Infrastructure (PKI)	A cybersecurity framework that secures communication and data exchange.

Q

Quality of Service (QoS)	A networking process that reserves network resources for highly critical application traffic with precedence over less critical application traffic. QoS prioritizes different types of traffic and ensures quality of service.

R

Random Early Detection (RED)	A queuing mechanism for congestion avoidance.

Rapid Per-VLAN Spanning-Tree (Rapid-PVST)	A protocol that is a combination of rapid spanning-tree (RSTP) and per-VLAN spanning-tree plus (PVST+) for faster convergence and interoperability.
Rapid Spanning-Tree Protocol (RSTP)	A protocol that provides faster convergence and interoperability with devices that are configured with the Spanning-Tree Protocol (STP) and Multiple Spanning-Tree Protocol (MSTP).
RDMA over Converged Ethernet (RoCE)	A protocol that allows remote direct memory access over an Ethernet network.
Real-Time Clock (RTA)	A system clock that keeps track of the current time.
Remote Direct Memory Access (RDMA)	A technology that enables memory transfers between two systems in a network without involving the CPU of either of the systems.
Remote Port Monitoring (RPM)	A process where port monitoring is done on traffic running across a remote device in the same network.
Rendezvous Point (RP)	A single root node of a shared multicast distribution tree.
Reverse Path Forwarding (RPF)	The path that the router uses to reach the RP or the multicast source.
Role-Based Access Control (RBAC)	A method of restricting system access to authorized users based on the roles of individual users.
Route leaking	A process that enables routes that are configured in a default or nondefault VRF instance to be made available to another VRF instance.
Route reflectors	A device that reorganizes the Internal Border Gateway Protocol iBGP core into a hierarchy and allow route advertisement rules. Route reflection divides iBGP peers into two groups: client peers and nonclient peers.
Routing table	A routing information base or database-type object that is stored in a switch with routes to particular network destinations.
RTAG7	A hash algorithm that load-balances traffic within a trunk group in a controlled manner.

S

SDN controller	An application that communicates with the business logic applications and network devices such as switches.
Secure boot	A feature that verifies the authenticity and integrity of the OS10 image. This feature protects a system from malicious code being loaded and started during the boot process.
Sensor group	A reusable group of multiple sensor paths and exclude filters.
Sensor path	The path used to collect data for streaming telemetry.
sFlow	A standard-based sampling technology that is embedded within switches and routers to monitor network traffic.
Simple Network Management Protocol (SNMP)	A protocol that provides a messaging format for communication between SNMP managers and agents. SNMP provides a standardized framework and common language for network monitoring and device management.
SmartFabric Director (SFD)	A network orchestration solution that manages the switches in a data center with or without any virtual infrastructure.
SmartFabric Services (SFS)	An application suite that provides network fabric automation and API-based programmability.

SNMP agent	The software component that is responsible for the launcher object and responds to queries, carries out requests and issues traps.
SNMP manager	A system that controls and monitors the activities of network hosts using SNMP.
SNMP trap	A message sent by an SNMP Agent to the SNMP manager indicating that an event has occurred on the host running the network resource.
Software Defined Networking (SDN)	An architecture that decouples the software (control plane) from the hardware (data plane). A centralized SDN controller handles the control plane traffic and hardware configuration for data plane flows.
Spanned VLAN	A VLAN that is configured on all the VLT peer nodes.
SSH	A protocol for securely exchanging data between two devices over an untrusted network. In OS10, the secure shell server allows an SSH client to access an OS10 switch through a secure, encrypted connection. The SSH server authenticates remote clients using RADIUS challenge or response, a trusted host file, locally stored passwords, and public keys.
Stateless autoconfiguration	A method for assigning an IPv6 address to an interface. Stateless auto-configuration generates a unique link-local IPv6 address with a FE80::/64 prefix and an interface ID generated from the MAC address.
Static routing	A process where the router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.
Subscription profile	Data collector destinations and stream attributes that are associated with sensor paths. A subscription ties sensor paths and a destination group with a transport protocol, encoding format, and streaming interval. The telemetry agent in the switch attempts to establish a session with each collector in the subscription profile, and streams data to the collector. If a collector is not reachable, the telemetry agent continuously tries to establish the connection at one-minute intervals.
Switch-scoped VLAN	A VLAN that is mapped to a virtual network ID (VNID) in OS10. All member ports of the VLAN are automatically added to the virtual network.
System banners	A messaging mechanism that provides information to configure a system login and message of the day (MOTD) text banners.
System clock	A clock in a system that helps to maintain the correct time.

T

Telnet	A protocol that provides information to set up Telnet TCP/IP connections on the switch.
Transmission Control Protocol (TCP)	A communication protocol that helps exchange messages between computing devices in a network.

U

Unified Forwarding Table (UFT)	A table that consolidates the resources of several search tables (L2, L3 Hosts, and L3 Route [Longest Prefix Match - LPM]) into a single flexible resource.
Uplink Failure Detection (UFD)	A network path that indicates the loss of upstream connectivity to servers connected to the switch.
User Datagram Protocol (UDP)	A communications protocol that helps exchange messages between computing devices in a network. It is a core member of the Internet Protocol suite and is a "stateless" protocol.
User Session Management	A protocol that provides information to manage the active user sessions.

V

Virtual extensible LAN (VXLAN)	A type of network virtualization overlay that encapsulates a tenant payload into IP UDP packets for transport across the IP underlay network.
Virtual fabric (vfabric)	A fabric that divides a physical fabric into logical fabrics.
Virtual LANs (VLANs)	A group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.
Virtual Link Trunking (VLT)	A L2 aggregation protocol used between an end device such as a server and two or more connected network devices. VLT helps to aggregate ports terminating on multiple switches.
Virtual network	An overlay network in the L2 flooding domain.
Virtual network identifier (VNID)	A 16-bit ID number that identifies a virtual network in OS10.
Virtual Router Redundancy Protocol (VRRP)	A protocol that eliminates a single point of failure in a statically routed network.
Virtual Routing and Forwarding (VRF)	A mechanism to partition a physical router into multiple virtual routers.
Virtual Teletype (VTY)	A command line interface (CLI) created on a switch to facilitate a connection through Telnet.
Virtual-network interface	A router interface that connects a virtual network bridge to a tenant VRF routing instance.
VLT domain	A domain that includes VLT peer devices, VLT interconnects, and all port channels in the VLT connected to the attached devices. You must use this configuration mode to assign VLT global parameters.
VLT interconnect (VLTi)	The link between VLT peer switches that synchronizes operating states.
VLT MAC address	A unique MAC address that you assign to the VLT domain. A VLT MAC address is a common address in both VLT peers. If you do not configure a VLT MAC address, the MAC address of the primary peer is used as the VLT MAC address across both peers.
VLT peer device	A pair of devices connected using a dedicated port channel—the VLTi. You must configure VLT peers separately.
VLT port channel	A link aggregation technology that combines two or more physical interfaces into a single logical interface.
VRRP authentication	A process that allows trusted routers to participate in VRRP processes.
VXLAN Network Identifier (VNI)	A 24-bit ID number that defines the broadcast domain.
VXLAN Tunnel Endpoint (VTEP)	A switch with connected end hosts that are assigned to virtual networks. The virtual networks map to VXLAN segments. Local and remote VTEPs perform encapsulation and de-capsulation of VXLAN headers for the traffic between end hosts. A VTEP is also known as a network virtualization edge.

W

Weighted Random Early Detection (WRED)	A queuing discipline for a network scheduler suited for congestion avoidance. It is an extension to RED, where a single queue may have several different sets of queue thresholds.

X

X.509v3 certificates

Certificates that secure communications between the switch and a host, such as a RADIUS server.

Z

Zero Touch Deployment (ZTD)

A process that automates switch deployment and upgrades an existing OS10 image. It executes a CLI batch file to configure the switch, and executes a post-ZTD script to perform additional functions.