ADTRAN Switch Engine (ASE) Device Glossary

The following article outlines common terms, acronyms, protocols, and concepts used with the ASE device command line interface (CLI), web-based graphical user interface (GUI), and any documentation associated with the ASE device product lines. Topics are organized alphabetically in the following sections:

A

ACE

Access Control Entry (ACE). ACEs are entries in an access control list (ACL) that specify the criteria used to permit or deny traffic that matches additional criteria specified in the entry. Each ACE is associated with a unique ID, and can be used to match three types of traffic fames: EtherType, ARP, and IPv4.

ACL

Access Control List (ACL). The ACL lists configured ACEs in a table format, including the specific criteria used to permit or deny users or groups access to specific traffic objects (such as processes or programs). Each accessible traffic object contains an identifier links to it's ACL, and the ACL configuration determines access rights to the traffic object.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

- **ACL** > **Access Control List**
- **ACL** > **Ports**
- **ACL** > **Rate Limiters**

In the **Access Control List** menu, ACEs are displayed with the highest priority entry at the top and the lowest priority entry at the bottom. By default, the ACE display table is empty. Ingress frames will only match on one ACE, even if it could match more than one configured ACE. The first matching ACE takes action on the frame (**permit** or **deny**), and a counter associated with that ACE is incremented. Each ACE can be associated with a policy, a single specified ingress port, or **any** ingress port (the whole switch). If an ACE policy is created, then that policy can be associated with a group of ports (using the **ACL** > **Ports** menu). The maximum number of supported ACE entries is **64**. The help text associated with the **Access Control List** menu describes the parameters that can be configured for each ACE.

In the **Ports** menu, policy IDs are assigned to an ingress port. By assigning ports a policy ID, the same traffic rules can be applied to multiple ports. Traffic policies are created in the **Access Control List** menu. In addition, specific traffic properties (such **Action**, **Rate Limiter**, or **Port copy** settings) can be specified for each ingress port. These properties are only applied if traffic frames do no not match a configured ACE. If ingress traffic does not match an ACE configured on the port, a counter associated with that port is incremented. The help text associated with the **Ports** menu describes each specific property than can be configured on the port.

In the **Rate Limiters** menu, rate limiters are configured. Up to **15** different rate limiters can be specified; each can range from **1** to **1024K** packets per second. Rate limiter IDs can be assigned to ACEs or ingress ports using the **Access Control List** or **Ports** menus.

AES

Advanced Encryption Standard (AES). AES is an encryption key protocol applied in 802.1i standards to improve wireless local area network (WLAN) security. This encryption standard, set by the U.S. government, will replace *DES* and 3DES. AES has a fixed-block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

Auto Media Select (AMS). AMS is a feature used by dual media ports (ports that support both copper (CU) and fiber (SFP) cables) to determine if an SFP or a CU cable has been inserted into the port, and then switch to the appropriate media type for the cable. If both SFP and CU cables are inserted, the port selects the preferred media type.

APS

Automatic Protection Switching (APS). APS is a protocol used to ensure that switching is done bidirectionally in the two ends of a protection group, as defined in G.8031.

Aggregation

Aggregation is when multiple ports are used in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

ARP

Address Resolution Protocol (ARP). ARP i s a protocol used to convert an Internet Protocol (IP) address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP inspection is a security feature used to validate ARP requests and responses within the switch block. Using ARP inspection can block several types of attacks in which hosts or devices connected to a Layer 2 network can become susceptible to the “poisoning” of ARP caches.

Auto-Negotiation

Auto-negotiation is an automatic process in which two different devices establish a common mode of operation and speed settings in order to create a link between them.

C

CC

Continuity check (CC). CC is a *MEP* functionality that is able to detect loss of continuity in a network by transmitting *CCM* frames to a peer MEP.

CCM

Continuity check message (CCM). CCMs are *OAM* frames transmitted from a MEP to its peer MEP and used to implement *CC* functionality.

CDP

Cisco Discovery Protocol (CDP).

COS

Class of Service (CoS). A type of *QOS* class used to classify each incoming frame and provide queuing, scheduling, and congestion control guarantees to that frame based on the CoS configuration. There is a one-to-one mapping between CoS, queue, and priority. A CoS value of **0** (zero) has the lowest priority.

COS ID

Class of Service ID (CoS ID). An identifier assigned to every incoming frame that can later be used as a basis for rewriting different parts of the frame.

D

DDMI

Digital Diagnostics Monitoring Interface (DDMI). An interface used to provide enhanced digital diagnostic monitoring for optical transceivers that allows real-time access to device operating parameters.

DEI

Drop Eligible Indicator (DEI). A 1-bit field in *VLAN* tags.

DES

Data Encryption Standard (DES). A security standard that provides a complete description of a mathematical algorithm for encrypting and decrypting binary-coded information. Encrypting data converts it an unintelligible form called a cipher. Decrypting the cipher converts the data back to its original plain text form. The algorithm described in this standard specifies both encrypting and decrypting operations using a binary number as a key.

DHCP

Dynamic Host Configuration Protocol (DHCP). A protocol used for assigning dynamic IP addresses to devices on a network. DHCP is used by clients to obtain IP addresses and other parameters (such as default gateways, subnet masks, and IP addresses of *DNS* servers) from a *DHCP Server*. The DHCP server ensures that all IP addresses are unique (for example, that no IP address is assigned to a second client while the first client's assignment is still valid) and manages IP address pools without the need for a human network administrator. Using DCHP for dynamic addressing simplifies network administration by reducing the need for manually assigning unique IP addresses when adding new clients to the network.

DHCP Server

Server used to allocate network addresses and deliver configuration parameters to dynamically configured hosts (DHCP clients) via DHCP.

DHCP Snooping

DHCP snooping is a feature used to block intruders on untrusted ports of the switch device. When used, this feature discovers and blocks bogus DHCP reply packets being injected into legitimate conversations between the DCHP client and server.

DNS

Domain Naming System (DNS). A system that stores and associates many types of information with domain names. In addition, DNS translates human-friendly domain names and computer host names into computer-friendly IP addresses. For example, the human-friendly domain name **www.example.com** might be translated to **192.168.0.1** by DNS.

DOS

Denial of Service (DoS). An attack type in which an attacker attempts to prevent legitimate users from accessing information or services in the network. By targeting network sites and connections, attackers can prevent network users from accessing email, websites, online accounts, or other services used on the affected computer.

Dotted Decimal Notation

A format used to write IP addresses using decimal numbers and dots as separators between octets. For example, an IPv4 address, when expressed in dotted decimal notation, has the form **x.y.z.w**, where x, y, z, and w are decimal numbers between **0** and **255**.

DPL

Drop Precedence Level (DPL). Every incoming frame on the switch is classified with a DPL value, which is then used throughout the device to provide congestion control guarantees to the frame depending on the DPL's configuration. A DPL with a value of **0** (zero) corresponds to **Committed** (green) frames, whereas a DPL with a value greater than **0** (zero) corresponds to **Discard Eligible** (yellow) frames.

DSA

Digital Signature Algorithm (DSA). DSA is a Federal Information Processing Standard (FIPS) used for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August of 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.

Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.

DSCP

Differentiated Services Code Point (DSCP). A field in IP packet headers used to classify packets.

E

ECE

EVC Control Entry (ECE). ECEs are rules ordered in a list to control the preferred classification of packets.

EEE

Energy Efficient Ethernet (EEE). An Ethernet standard defined in IEEE 802.3az.

EPS

Ethernet Protection Switching (EPS). A switching standard defined in ITU/T G.8031.

ERPS

Ethernet Ring Protection Switching (ERPS). A switching standard defined in ITU/T G.8032 that provides fast protection and recovery switching for Ethernet traffic in a ring topology, while also ensuring that the Ethernet layer remains free of loops.

EtherType

An specific field in the Ethernet media access control (MAC) packet header (defined by the Ethernet networking standard) that is used to indicate which protocol is being transported in an Ethernet frame.

EVC

Ethernet Virtual Connection (EVC). EVCs are an association of two or more user network interfaces (UNIs). UNIs are interfaces at which customer services are provided in the Metro Ethernet Forum (MEF) standardized network. Inside these provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs) and connections between service providers are completed using External Network-to-Network Interfaces (E-NNIs).

F

FTP

File Transfer Protocol (FTP). A transfer protocol that uses Transmission Control Protocol (*TCP*) to provide file writing and reading. It also provides directory service and security features.

Fast Leave

Fast leave processing is used in multicast snooping and allows the switch to remove the member interface that receives the leave message from the multicast forwarding table without sending last member query messages. The specific member interface is also pruned from the multicast tree for the multicast group specified in the original leave message. Fast leave processing also ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMPv2 and MLDv1. The feature should only be enabled when a single IGMPv2/MLDv1 host is connected to the specific interface.

G

GARP

Generic Attribute Registration Protocol (GARP). A generic protocol used for registering attributes with other participants as defined in IEEE 802.1D-2004, clause 12.

GVRP

GARP VLAN Registration Protocol (GVRP). A protocol used for dynamically registering virtual local area networks (VLANs) on ports as defined in IEEE 802.1Q-2005, clause 11.

H

HQOS

Hierarchical Quality of Service (HQoS). A specific method of *QOS* that is configured on a service level.

HTTP

Hypertext Transfer Protocol (HTTP). A protocol used to transfer or convey information on the worldwide web (WWW). HTTP defines how messages are formatted and transmitted and what actions web servers and browsers should take in response to various commands. For example, when entering a URL in a browser, an HTTP command is sent to the web server directing it to fetch and transmit the requested web page.

Any web server machine contains an HTTP daemon (in addition the web page files it can serve). The HTTP daemon is a program designed to wait for HTTP requests and handle them when they arrive. The web browser is an HTTP client, sending requests to server machines. An HTTP client initiates requests by establishing a Transmission Control Protocol (*TCP*) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send the request message.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). A protocol used to indicate a secure HTTP connection. HTTPS provides authentication and encrypted communication and is widely used on the world wide web for sensitive communication (such as payment transactions and corporate logins).

HTTPS employs the use of the Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. HTTPS uses port 443 instead of port 80 in its interactions with the lower layer TCP/IP protocols. SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchanges.

I

ICMP

Internet Control Message Protocol (ICMP). A protocol that generates error responses for diagnostic or routing purposes. These ICMP messages generally contain information about routing difficulties or simple exchanges such as time stamp or echo transactions. For example, issuing a **ping** command causes ICMP to test and Internet connection.

IEEE 802.1x

An IEEE standard used for port-based network access control. This standard provides authentication to devices attached to a local area network (LAN) port and establishes point-to-point connections or prevents access from that port if authentication fails. With 802.1x, access to all switch ports can be centrally controlled from a server, thus allowing authorized users to use the same credentials for authentication at any point within the network.

IGMP

Internet Group Management Protocol (IGMP). A communications protocol used to manage membership of IP multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships and is an integral part of the IP multicast specification (like *ICMP* for unicast connections). IGMP can be used for online video and gaming and allows more efficient use of resources for those applications.

IGMP Querier

When a router sends IGMP query messages onto a particular link, the router is called the querier. *Querier Election* determines which single IGMP querier is used on a particular link.

IMAP

Internet Message Access Protocol (IMAP). A protocol used by email clients to retrieve email messages from a mail server. IMAP is used by IMAP clients to communicate with the servers, and *SMTP* is used to transport the mail to an IMAP server.

The current version of IMAP is IMAP4. It is similar in function to the Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, IMAP4 leaves email messages on the server, rather than downloading them to the computer. To remove email messages from the server, the mail client mused by used to generate local folders, copy messages to the local hard drive, and then delete and expunge the messages from the server.

IP

Internet Protocol (IP). A protocol used for communicating data across an Internet network. IP is a “best effort” system, indicating that no packet of information sent over the network is assured to reach its destination in the same condition in which it was sent. Each device connected to a local area network (LAN) or wide area network (WAN) is given an IP address, and this address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the IP protocol is version 4 (IPv4), which has IP addresses of 32-bits that allow for an excess of four billion unique addresses. This number is reduced drastically by the practice of web masters taking addresses in large blocks, even when the bulk of those remain unused. The next version of the IP protocol is version 6 (IPv6), which provides 128-bit IP addresses (represented roughly by a 3 with 39 zeros after it). For the moment, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IP Multicast (IPMC). IPMC supports both IPv4 and IPv6 multicasting.

IPMC Profile

IP Multicast (IPMC) profile. ICMP profiles are used to deploy the access control parameters on IP multicast streams.

IP Source Guard

A security feature used to restrict IP traffic on untrusted ports by filtering traffic based on the *DHCP Snooping* table or manually configured IP source bindings. This feature helps prevent IP spoofing attacks, in which a host tries to spoof and use the IP address of another host.

IVL

Independent *VLAN* Learning (IVL). A feature of ASE devices in which every VLAN uses its own logical source address table (as opposed to *SVL*, in which two or more VLANs share the same part of the MAC address table).

J

JSON

JavaScript Object Notation (JSON). A lightweight, data interchange format used as an alternative to XML. JSON transmits dynamic data between web servers and applications using human-readable text consisting of one or more attribute-value pairs.

L

LACP

Link Aggregation Control Protocol (LACP). A protocol defined in IEEE 802.3ad that allows the bundling of several physical ports together to form a single logical port.

LLC

Logical Link Control (LLC) protocol. A protocol defined in IEEE 802.2 that provides a link mechanism for upper layer protocols. Residing in the upper sub-layer of the Data Link layer, it provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network. LLC headers consist of 1 byte of Destination Service Access Point (DSAP) information, 1 byte Source Service Access Point (SSAP) information, and 1 or 2 bytes of a Control field information followed by LLC information.

LLDP

Link Layer Discover Protocol (LLDP). A protocol defined in IEEE 802.1ab that allows stations attached to an IEEE 802 LAN to advertise information to other stations attached to the same IEEE 802 LAN. Information advertised includes the major capabilities provided by the system in which the station resides, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station’s point of attachment to the IEEE 802 LAN required by those management entities. Information distributed by LLDP is stored by its recipients in a standard management information base (MIB), making it possible for the information to be accessed by a network management system (NMS) using the Simple Network Management Protocol (*SNMP*).

LLDP-MED

An extension of the IEEE 802.1ab standard defined by the telecommunication industry association (TIA-1057).

LLQI

Last Listener Query Interval (LLQI). The maximum response time used to calculate the maximum response code inserted into specific queries. These queries are used to detect the departure of the last listener for multicast addresses or sources. In IGMP, this term is called last member query interval (LMQI).

LOC

Loss of Connectivity (LoC). Detected by *MEP*s when devices are indicating lost connectivity in the network; can also be used as a switch criteria by *EPS*.

M

MAC Table

A table built by the switch that maps Media Access Control (MAC) addresses to specific switch ports; the table is used to know to which ports the frames should go, based upon the destination MAC (DMAC) address included in the frame. The MAC table contains both static and dynamic entries. Static entries are configured by the network administrator if fixed mapping between the DMAC and the switch port is required.

Incoming frames also contain a source MAC (SMAC) address that indicate the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been received after a configurable time.

MEP

Maintenance Entity Endpoint (MEP). An endpoint in a maintenance entity group (ITU-T Y.1731).

MD5

Message Digest Algorithm 5 (MD5). A message digest algorithm used for cryptographic has functions with a 128-bit hash value. Designed by Ron Rivest in 1991, MD5 is officially defined in RFC 1321 (The MD5 Message-Digest Algorithm).

Mirroring

A feature in which the switch system is configured to mirror frames from multiple ports to a mirror port (basically copying the frame to another port). Mirroring can be useful for debugging network problems or monitoring network traffic. Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

Multicast Listener Discovery (MLD). A protocol used by IPv6 routers to discover multicast listeners on a directly-attached link; it is used similarly to how *IGMP* is used in IPv4. The MLD protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier

A router that sends MLD query messages on a particular link is called an MLD querier. *Querier Election* determines which single MLD querier is used on a particular link.

MPLS

Mulitprotocol Label Switching (MPLS). MPLS is a protocol that uses Layer 2 switching labels to forward packets, thus speeding up network traffic transmission. By using Layer 2 switching, instead of Layer 3 routing, complex destination lookups in the routing table can be avoided. MPLS uses a variety of protocols to establish the network path (Label Switched Paths (LSPs)) and then forwards the packet using the network paths. The packet itself is labeled at the edge of the service provider’s network, and service providers can use the label information to specify the best method for traffic flow forwarding.

A Mulitprotocol Label Switching Transport Profile (MPLS-TP) is being designed by the IETF as an extension to MPLS using requirements provided by service providers. It will be used as a network-layer technology in transport networks and will give service providers a reliable packet-based technology that uses circuit-based transport networking and aligns with current organization processes and large scale work procedures of other packet transport technologies. MPLS-TP is expected to be a low cost Layer 2 technology that will provide *QOS*, end-to-end *OAM*, and protection switching.

MSTP

Multiple Spanning Tree Protocol (MSTP). A protocol that provides for multiple spanning tree instances while maintaining *RSTP* and *STP* compatibility. MSTP was defined originally in IEEE 802.1s, but has since been incorporated into IEEE 802.1D-2005.

MRP

Multiple Registration Protocol (MRP). A protocol providing a generic registration framework that defines the dynamic registration and de-registration of attributes across a bridged LAN. Attributes include *VLAN* identifiers or multicast group MAC addresses. MRP was originally defined in IEEE 802.1ak and has since been incorporated in IEEE 802.1Q-2014.

MVR

Multicast *VLAN*Registration (MVR). A protocol used in Layer 2 (IP) networks that enables multicast traffic from a source VLAN to be shared with subscriber VLANs. Typically MVR is used to save bandwidth by preventing duplicate multicast streams from being sent in the core network. Instead, with MVR, streams are received on the MVR VLAN and forwarded to the VLANs where they have been requested by hosts.

MVRP

Multiple VLAN Registration Protocol (MVRP). A protocol that defines the dynamic registration and de-registration of VLAN identifiers across bridged LANs. MVRP uses the *MRP* framework to define its operation and is therefore also called an *MRP* application. MVRP was originally defined in IEEE 802.1ak and has since been incorporated into IEEE 802.1Q-2014.

N

NAS

Network Access Server (NAS). A server that acts as a gateway guarding access to a protected source. As clients connect to the NAS, the NAS communicates with another resource to verify the client’s supplied credentials. Based on the verification, the NAS permits or denies access to the protected resource. An example of NAS implementation is *IEEE 802.1x*.

NetBIOS

Network Basic Input/Output System (NetBIOS). A program that allows applications on separate computers to communicate within a local area network (LAN). NetBIOS provides each computer on the network a name and IP address corresponding to a different host name, as well as provides the session and transport services described in the Open Systems Interconnection (OSI) network model. NetBIOS is not supported on a wide area network (WAN).

NFS

Network File System (NFS). A system that allows hosts to mount partitions on a remote system and use them as though they are local file systems. In addition, NFS allows system administrators to store resources in a central location on the network where authorized users can continually access them. NFS supports the sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

Network Time Protocol (NTP). A network protocol used to synchronize the clocks of computer systems using the User Datagram Protocol (*UDP*) as a transport layer.

O

OAM

Operation, Administration, and Maintenance (OAM). A protocol described in ITU-T Y.1731 that implements carrier Ethernet functionality. *MEP* functionality, like *CC* and *RDI* are based on OAM.

Optional TLVs

Optional Type Length Value (*TLV*). *LLDP* frames contain multiple TLVs, and some of the TLVs within those frames can be configured to be included or not. Configurable TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LDDP frame.

OUI

Organizationally Unique Identifier (OUI). An OUI address is a globally unique ID assigned to a vendor by IEEE. It can be determined to which vendor a device belongs according to the OUI address that forms the first 24 bits of a MAC address.

P

PCP

Priority Code Point (PCP). A 3-bit field storing the priority level for an 802.1Q frame (known as *User Priority*).

PD

Powered Device (PD). A remote device powered by power sourcing equipment (PSE) in a *PoE* system.

PHY

Physical Interface Transceiver (PHY). A device that operates in the Ethernet physical layer (IEEE 802.3).

Ping

A program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The computer responds with an acknowledgment that it received the packets. Using the ping functionality verifies whether a specific computer on a network or the Internet exists and is connected using *ICMP* packets. Ping requests are packets from the origin computer, and Ping replies are packet responses from the target.

PoE

Power Over Ethernet (PoE). A method of transmitting electrical power to remote devices over standard Ethernet cables. PoE can power IP phones, wireless LAN access points, or other equipment and can be useful in situations where it is difficult or expensive to connect the equipment to a main power supply.

Policer

Limits the bandwidth of received frames before they reach the ingress queue.

POP3

Post Office Protocol version 3 (POP3). A protocol used by email clients to retrieve messages from a mail server. POP3 is designed to delete mail on the server as soon as it has been downloaded; however, some implementations allow users or administrators to specify that mail is saved for a specific period of time. POP3 can be thought of as a “store-and-forward” service.

An alternative to POP3 is *IMAP*. IMAP provides more capabilities for retaining and organizing emails on the server. IMAP can be thought of as a remote file server.

Both POP3 and IMAP focus on the receiving of email and should not be confused with Simple Mail Transfer Protocol (*SMTP*). Emails are sent with SMTP, and a mail handler receives it on the recipient’s behalf. The email is then read using POP3 or IMAP. Both POP3 and IMAP are the most prevalent Internet standard protocols for email retrieval, and virtually all modern email clients and servers support both.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE). A network protocol used to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. PPPoE is typically used with ADSL services in which individual users connect tot he ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

POST

Power On Self Test (POST). A self-test run automatically when various components are powered on. POSTs can be used to test the basic hardware and include ready-made tests (such as BIST) embedded in hardware ASICs, such as memory test, serdes tests, internal loopback tests, etc.

Private VLAN

Private *VLAN*s (PVLANs) provide Layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of a PVLAN cannot communicate with each other while ports that are members of the PVLAN can communicate with each other.

PSFP

Per-Stream Filtering and Policing (PSFP). A feature that allows filtering and policing decisions, and subsequent frame queuing decisions, on a per-stream basis. PSFP is supported by a table of stream filters that determine the filtering and policing actions that are applied to frames received on ingress ports.

PTP

Precision Time Protocol (PTP). Network protocol used to synchronize clocks of computer systems.

Q

QCE

QOS Control Entry (QCE). A QCE is a combination of keys and actions. The keys can be configured to match specific parts of a frame, and the actions can be configured to override the default classified values of *COS*.

QCL

QOS Control List (QCL). A list of *QCE*s to which each every frame is compared. The comparison starts with the first entry in the list and continues until there is a match between the frame and key parameters or the end of the list is reached. If a match occurs, the frame is reclassified according to the action parameters specified in the QCE.

QL

Quality Level (QL). Used in *SyncE* to specify the quality level of a given clock source. The QL value is received on a port in an *SSM*.

QOS

Quality of Service (QoS). A method used to guarantee bandwidth relationships between individual applications or protocols. As communications networks transport a multitude of applications and data, including high-quality video and delay-sensitive date such as real time voice, these networks must provide secure, predictable, measurable, and sometimes guaranteed services. QoS configurations are used as a set of techniques used to manage network resources to provide reliable services.

QOS Class

See Class of Service (*COS*).

Querier Election

Querier election is a process in which the querier becomes the single router allowed to send Query messages on a particular link. Querier election rules define that the *IGMP Querier* or *MLD Querier* with the lowest IPv4 or IPv6 address wins the election.

R

RARP

Reverse Address Resolution Protocol (RARP). A protocol used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of *ARP*.

RADIUS

Remote Authentication Dial In User Service (RADIUS). A networking protocol that provides centralized access, authorization, and accounting management for people or computers connecting to network services.

RDI

Remote Defect Indication (RDI). An *OAM* functionality that is used by a *MEP* to indicate to a remote peer MEP that a defect has been detected.

RFC2544

An RFC that describes a number of test that can be run to assess the performance characteristics of a network interconnecting devices. In this context, it is specialized towards determining whether a network section conforms to a service level agreement (SLA) and is usually run during service activation.

Router Port

A router port is a pot on the Ethernet switch that leads the switch towards a Layer 3 multicast device.

RSA

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA). One of the first public-key cryptography systems widely used for secure data transmission. In RSA, the encryption key is public and differs from the decryption key, which is kept secret. This asymmetry is based on the difficulty of factoring the product of two large prime numbers. Rivest, Shamir, and Adleman first publicly described the RSA algorithm in 1977.

RSTP

Rapid Spanning Tree Protocol (RSTP). An updated version of *STP* documented by the IEEE in 802.1w in 1998 that provides faster spanning tree convergence after topology changes. Standard IEEE 802.1D-2004 incorporates RSTP, obsoletes STP, and yet allows RSTP to be backwards-compatible with STP.

S

Samba

A program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Windows, IBM OS/2, and other SMB client machines by using the Server Message Block (SMB) protocol and Common Internet File System (CIFS) which are underlying protocols used in Windows networking. Samba can be installed on a variety of operating system platforms including Linux, most common Unix platforms, OpenVMS, and IBM OS/2 and can also register itself with the master browser on the network so that it appears in the listing of hosts in a Window's "Neighborhood Network."

sFlow

An industry standard technology used for monitoring switched networks through a random sampling of packets on switch ports and time-based sampling of port counters. Sampled packets (flow samples) and counters (counter samples) are sent as sFlow *UDP* datagrams to a central network traffic monitoring server (sFlow receiver/collector). Additional information about sFlow can be found online at https://sflow.org.

SHA

Secure Hash Algorithm (SHA). An algorithm designed by the National Security Agency (NSA) and published by the NIST as a US Federal Information Processing Standard (FIPS). Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence of any length (the message).

Shaper

Limits the bandwidth of transmitted frames (after packets have passed through the ingress queues).

SMTP

Simple Mail Transfer Protocol (SMTP). A text-based protocol that uses *TCP* to provide mail services modeled on the *FTP* file transfer service. SMTP transfers mail messages between systems and creates notifications for incoming mail.

SNAP

Subnetwork Access Protocol (SNAP). A protocol used for multiplexing more protocols can than can be distinguished using the 8-bit 802.2 Service Access Points (SAP) fields on networks using IEEE 802.2 LLC. SNAP supports identifying protocols by *EtherType* field values or vendor-private protocol identifiers.

SNMP

Simple Network Management Protocol (SNMP). A protocol that allows diverse network objects to participate in a network management architecture and enables network management systems to learn of network problems by receiving traps or change notices from network devices using SNMP. SNMP is part of the Transmission Control Protocol/Internet Protocol (*TCP/IP*).

SNTP

Simple Network Time Protocol (SNTP). A network protocol used to synchronize the clocks of computer systems. SNTP employs *UDP* as a transport layer.

SR

Seamless Redundancy (SR). A feature used to provide high fault tolerance to link failures with zero fail over time. SR operates by generating duplicate streams from the stream source (talker) to listener(s) across statically configured redundant paths and then merging the streams at the listening devices.

SSID

Service Set Identifier (SSID). A unique identifier applied to a particular 802.11 wireless LAN. Client devices receive broadcast messages from all access points within range advertising their SSID and are then connected to a particular SSID based on device configuration or by manually selecting an SSID to which to connect.

SSH

Secure Shell (SSH). A network protocol that encrypts data between two networked devices. SSH provides a secure channel for data exchange and maintains the confidentiality and integrity of that data over an insecure network. SSH replaces Telnet and RSH protocols which do not provide as much data security.

SSM

Synchronization Status Message (SSM). Used in SyncE to deliver *QL* indications.

STP

Spanning Tree Protocol (STP). A Layer 2 protocol that ensures no loops occur in a bridged LAN. STP was replaced by *RSTP*.

SVL

Shared *VLAN* Learning (SVL). A feature in which frames that are initially classified to a particular VLAN based on port VLAN ID or VLAN tag information can be bridged on a shared VLAN. In SVL, two or more VLANs are grouped in order to share common source address information in the *MAC Table*. The common entry in the MAC table is identified by a Filter ID (FID). SVL is useful when configuring more complex, asymmetrical cross-VLAN traffic patters (like E-TREE and multi-netted servers).

The alternative VLAN learning mode to SVL is *IVL*. IVL is the default VLAN learning mode, and not all switches support SVL.

Switch ID

Switch IDs are used to uniquely identify switches in a stack. Switch IDs are displayed on the front of the switch itself and are also widely used in GUI pages and CLI commands associated with ASE devices.

SyncE

Synchronous Ethernet (SyncE). A functionality used to make network clock frequencies synchronized. Note that SyncE is different than real time clock synchronization (IEEE 1588).

T

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+). A networking protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

TAS

Time Aware Shaper (TAS). Based on an amendment captured in 802.1Qbv, this feature adds time-aware queue-draining procedures, managed objects, and extensions to existing protocols that enable bridges and end stations to schedule the transmission of frames (based on the timing derived from IEEE standard 802.1A).

Tag Priority

A 3-bit field storing the priority level of an 802.1Q frame.

TCP

Transmission Control Protocol (TCP). A communications protocol that uses IP to exchange messages between computers. TCP guarantees reliable and in-order deliver of data from the sender to the receiver, and also distinguishes data for multiple connections using concurrent applications (for example, a web server and also an email server) running on the same host.

TCP connections can be used to connect applications on networked hosts and is known as a “connection-oriented” protocol, which means that a connection is established and maintained until such a time as the message or messages to be exchanged by the applications at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets managed by IP and then reassembled back into a complete message at the destination. Common network applications that use TCP include the world wide web (WWW), email, and File Transfer Protocol (*FTP*).

Telnet

Teletype Network (Telnet). A terminal emulation protocol that uses *TCP* to provide a virtual connection between the telnet server and client. The telnet protocol enables the client to control the server and also communicate with other servers on the network. Telnet sessions require a client user to log into a server by entering a valid user name and password, and then they are able to enter commands through the program just as if they were entering commands directly on the server console.

TFTP

Trivial File Transfer Protocol (TFTP). A file transfer protocol that uses *UDP* to provide file reading and writing features, but does not provide directory service and security features.

ToS

Type of Service (ToS). A priority control implemented in IPv4 that operates by decoding the 6-bit ToS field in an IP header to determine the packet priority. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (**0** to **63**).

TLV

Type Length Value (TLV). Pieces of information included in *LLDP* frames are known as TLVs.

TKIP

Temporary Key Integrity Protocol (TKIP). A protocol used in *WPA* to replace *WEP* with a new encryption algorithm. TKIP uses the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

TT-Loop

Traffic Test Loop (TT-Loop). A firmware module that provides methods for performing tests defined in RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and *Y.1564* (remote end).

U

UDLD

Unidirectional Link Detection (UDLD). A protocol that monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links and provides mechanisms for detecting one way connections before they create a loop or other protocol malfunctions. RFC 5171 specifies the method to detect unidirectional links at the data link layer.

UDP

User Datagram Protocol (UDP). A communications protocol that uses the Internet Protocol to exchange messages between computers. An alternative to Transmission Control Protocol (*TCP*), UDP does not provide the service of dividing messages into packet datagrams and it does not provide the reassembling and sequencing of packets. Applications that use UDP must be able to ensure that entire messages arrive in the right order, but using UDP can save processing time if the applications use small data units in message exchanges. UDP provides two services not provided by the IP layer. Port numbers, used to distinguish different user requests, and optional checksum capabilities help to verify that data has arrived intact.

Common network applications that use UDP include *DNS*, streaming media applications such as IPTV, Voice over IP (VoIP), and *TFTP*.

UPnP

Universal Plug-and-Play (UPnP). A feature that allows devices to connect seamlessly to a network providing simplified connection for home or enterprise data sharing, communications, and entertainment.

User Priority

A 3-bit field storing the priority level for 802.1Q frames; also known as *PCP*.

V

VLAN

Virtual Local Area Network (VLAN). A Layer 2 network partition that restricts communication between switch ports by creating multiple, distinct, and manually isolated broadcast domains.

VLAN ID

A 12-bit field specifying the *VLAN* to which the frame belongs.

Voice VLAN

A *VLAN* configured specifically for voice traffic. By adding the ports with voice devices attached to a specific voice VLAN, QoS-related configuration for voice data can be performed. Using a separate voice VLAN helps to ensure the transmission priority of voice traffic and quality.

W

WEP

Wired Equivalent Privacy (WEP). A deprecated algorithm used to secure wireless networks; its design is based on the IEEE 802.11 standard. WEP was intended to provide security comparable to that of traditional wired networks for wireless networks.

WiFi

Wireless Fidelity (WiFi). A generic term defined by the Wi-Fi Alliance; used to refer to any type of 802.11 network (whether 802.11b, 802.11a, dual-band, etc.).

WPA

WiFi Protected Access (WPA). A replacement for *WEP*, WPA is a security algorithm designed according to the IEEE 802.11i standard. Although WPA implements the majority of the IEEE 802.11i standard, only with WEP2 is the full standard available. WPA provides more security for wireless networks than WEP, but less than WPA2. WPA is backwards compatible with pre-WPA wireless interface cards, but WPA2 is not.

WPA-PSK

WiFi Protected Access Pre-Shared Key (WPA-PSK). A security algorithm for wireless networks that employs WPA along with a pre-shared key (PSK). In enterprise networks, WPA is used in conjunction with an IEEE 802.1X authentication server to provide different keys to each client (as with *WPA-RADIUS*), while in personal networks, every client is given the same passphrase (or the pre-shared key). When using WPA-PSK, the security depends upon the strength and secrecy of the passphrase.

WPA-RADIUS

WiFi Protected Access RADIUS (WPA-RADIUS). This form of the WPA security algorithm relies on the use of an 802.1x authentication server to distribute different keys to each client in an enterprise environment.

WPS

WiFi Protected Setup (WPS). A security standard used to simplify the creation of a wireless home network and connect home devices to that network.

WRED

Weighted Random Early Detection (WRED). An active queue management mechanism, used in *QOS* configurations, that provides preferential treatment of higher-priority frames when traffic builds up within a queue. A frame's *DPL* value is used by WRED to determine the priority of the frames; a higher DPL value results in a higher probability that the frame is dropped during times of congestion.

WTR

Wait to Restore (WTR). The time in which a failed resource must remain inactive ("not active") before restoration to the failed resource is completed.

Y

Y.1564

An Ethernet service activation test methodology (SAM), defined by ITU-T as a testing methodology to be used in assessing Ethernet services prior to delivering network elements to customers. It can be used for turning up, installing, and troubleshooting Ethernet-based services. The Y.1564 testing methodology completely validates Ethernet service level agreements (SLAs) in a single test and is designed around three main objectives: validating SLAs, verifying that network-carried services meet SLA objectives, and providing ongoing service tests to confirm that network elements can continue to carry all services as outlined in the SLAs.