Switches Glossary of Terms

Objective

This article contains the list of terms used in setting up, configuring, and troubleshooting the Cisco Small Business Switches.

Applicable Devices

Sx200 Series

Sx250 Series

Sx300 Series

Sx350 Series

SG300X Series

Sx500 Series

Sx550X Series

List of Terms

802.1X Supplicant — Supplicant is one of the three roles in the 802.1X IEEE Standard. The 802.1X was developed to provide security in Layer 2 of the OSI Model. It is composed of the following components: Supplicant, Authenticator, and Authentication Server. A Supplicant is the client or software that connects to a network so that it can access resources on that network. It needs to provide credentials or certificates to obtain an IP address and be part of that particular network. A Supplicant cannot have access to the network's resources until it has been authenticated.

ACL — An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device. The router or switch examines each packet to determine whether to forward or drop the packet, on the basis of the specified criteria within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

IGMP Snooping — Internet Group Management Protocol (IGMP) is a protocol that operates on switches that allows them to dynamically learn about multicast traffic. IGMP snooping is a feature that allows a network switch to listen to the IGMP conversation between hosts and routers. IGMP snooping performs a filtering mechanism that is enabled in the router to forward the multicast traffic of a group only to the ports that has joined the group. Thus with IGMP snooping, traffic on the network is reduced and enhancement in the performance of hosts behind the router is possible. Multicasts may be filtered from the links which do not need them.

IPv4 — IPv4 is a 32-bit addressing system used to identify a device in a network. It is the addressing system used in most computer networks, including the Internet.

IPv6 — IPv6 is a 128-bit addressing system used to identify a device in a network. It is the successor to IPv4 and the most recent version of the addressing system used in computer networks. IPv6 is currently being rolled out around the world. An IPv6 address is represented in eight fields of hexadecimal numbers, each field containing 16 bits. An IPv6 address is divided into two parts, each part composed of 64 bits. The first part being the Network Address, and the second part the Host Address.

Link Flap — Link flap is a situation in which a physical interface on the switch continually goes up and down, three or more times a second for duration of at least 10 seconds. The common cause is usually related to bad, unsupported, or non-standard cable or Small Form-Factor Pluggable (SFP), or related to other link synchronization issues. The cause for link flapping can be intermittent or permanent.

MAC-based ACL — Media Access Control (MAC)-based Access Control List (ACL) is a list of source MAC addresses. If a packet is coming from a wireless access point to a Local Area Network (LAN) port or vice versa, this device will check if the source MAC address of the packet matches any entry in this list and checks the ACL rules against the content of the frame. It then uses the matched results to permit or deny this packet. However, packets from LAN to LAN port will not be checked.

MLD Snooping — Multicast is the network layer technique that transmits data packets from one host to the selected hosts in a group. At the lower layer, the switch broadcasts the multicast traffic on all ports, even if only one host wants to receive it. Multicast Listener Discovery (MLD) Snooping is used to forward IPv6 multicast traffic only to the desired host(s). When MLD snooping is enabled on the switch, it detects the MLD messages exchanged between the IPv6 router and the multicast hosts attached on the interface. It then maintains a table that restricts IPv6 multicast traffic and forwards it dynamically to those ports that want to receive it.

MSTP — Multiple Spanning Tree Protocol (MSTP) is a protocol that creates multiple spanning trees (instances) for each Virtual LAN (VLAN) on a single physical network. This allows for each VLAN to have a configured root bridge and forwarding topology. This reduces the number of Bridge Protocol Data Units (BPDUs) across the network and reduces stress on the Central Processing Units (CPUs) of the network devices.

Port / VLAN Mirroring — Mirroring is a method used to monitor network traffic. With Port or VLAN Mirroring, copies of incoming and outgoing packets at the ports (source ports) of a network device are forwarded to another port (target port) where the packets are studied. This is used as a diagnostic tool by the network administrator.

Port Security — Configuring port security is one way to enhance network security. It can be configured on a specific port or Link Aggregation Group (LAG). A LAG combines individual interfaces into a single logical link, which provides an aggregate bandwidth of up to eight physical links. You can limit or allow access to different users on a given port/LAG. Port Security can also be used with dynamically learned and static MAC addresses to limit the ingress traffic of a port.

Protocol-based VLAN — Protocol based groups can be defined and bound to a port; therefore, every packet originating from the protocol groups is assigned to the configured VLAN on the page. Protocol-based VLAN divides the physical network into logical VLAN groups for each required protocol. In the inbound packet, the frame is checked and the VLAN membership can be determined based on the protocol type. The Protocol-Based Groups to VLAN mapping helps to map a protocol group to a single port.

QoS — Quality of Service (QoS) allows you to prioritize traffic for different applications, users or data flows. It can also be used to guarantee performance to a specified level, thus, affecting the quality of service of the client. QoS is generally affected by the following factors: jitter, latency, and packet loss.

RADIUS Server — Remote Authentication Dial-In User Service (RADIUS) is an authentication mechanism for devices to connect and use a network service. It is used for centralized authentication, authorization, and accounting purposes. A RADIUS server regulates access to the network by verifying the identity of the users through the login credentials entered. For example, a public Wi-Fi network is installed in a university campus. Only those students who have the password can access these networks. The RADIUS server checks the passwords entered by the users and grants or denies access as appropriate.

RSTP — Rapid Spanning Tree Protocol (RSTP) is an enhancement of STP. RSTP provides a faster spanning tree convergence after a topology change. STP can take 30 to 50 seconds to respond to a topology change while RSTP responds within three times the configured hello time. RSTP is backwards compatible with STP.

SNMP — Simple Network Management Protocol (SNMP) is a network standard for storing and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance.

Spanning Tree — Spanning Tree Protocol (STP) is a network protocol used on a Local Area Network (LAN). The purpose of STP is to ensure a loop-free topology for a LAN. STP removes loops through an algorithm that guarantees that there is only one active path between two network devices. STP ensures that traffic takes the shortest path possible within the network. STP can also automatically re-enable redundant paths as back up paths if an active path fails.

SSL Server — The Secure Sockets Layer (SSL) is a protocol used mainly for security management on the Internet. It uses a program layer which is located between the HTTP and the TCP layers. For authentication, SSL uses certificates which are digitally signed and bounded to the public key to identify the private key owner. This authentication helps during the time of connection. Through the use of SSL, the certificates are exchanged in blocks during the authentication process which are in the format described in ITU-T standard X.509. Then by the certification authority which is an external authority, X.509 certificates are issued which are digitally signed.

Syslog Aggregation — A Syslog service simply accepts messages, and stores them in files or prints them according to a simple configuration file. Syslog Aggregation means several syslog messages of the same type will not appear on the screen everytime an instance occurs. Enabling logging aggregation allows you to filter the system messages that you will receive for a specific period of time. It collects a few syslog messages of the same type so they won’t appear when they occur, but would rather appear on a specified interval.

TACACS+ — Terminal Access Controller Access Control System (TACACS+) is a Cisco proprietary protocol which is used for the implementation of enhanced security by providing authentication and authorization via username and password. To configure a TACACS+ server, the user must have privilege 15 access, which provides the user access to all the configuration features of the switch. Some switches can act as a TACACS+ client, where all the users connected can be authenticated and authorized in the network via a properly configured TACACS+ server. TACACS+ supports only IPv4.

TFTP Server — A Trivial File Transfer Protocol (TFTP) Server is a server that is used to automatically transfer configuration and boot files between devices on a LAN. The protocol is simple which allows low memory usage; however, this simplicity also allows the protocol to be easily compromised. For this reason, TFTP is rarely used with the Internet.

VLAN — A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application, without regard to the physical locations of the users. VLANs are a group of hosts or ports that can be located anywhere in a network but communicate as if they are on the same physical segment. VLANs help to simplify network management by letting you move a device to a new VLAN without changing any physical connections.