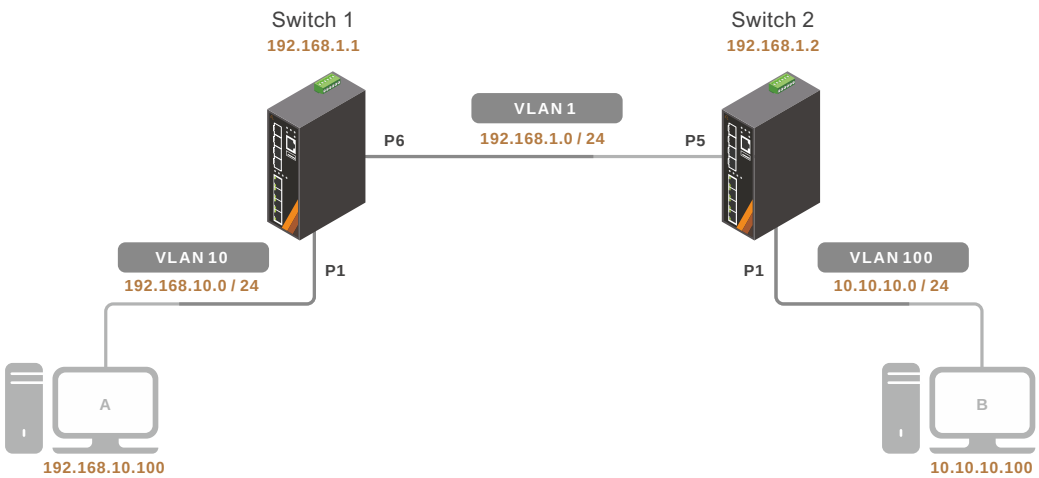
WAVESYS

SOFTWARE FEATURE

IP Routes (Static Routes)



IP Routes (Static Routes)

001.

IP routing is determined to build a suitable path for a network packet from a host on one network to another host on a different remote network, and selects a specific packet forwarding rules from the static routing table to determine how to deliver the packet to the target host.

DHCP Relay

002.

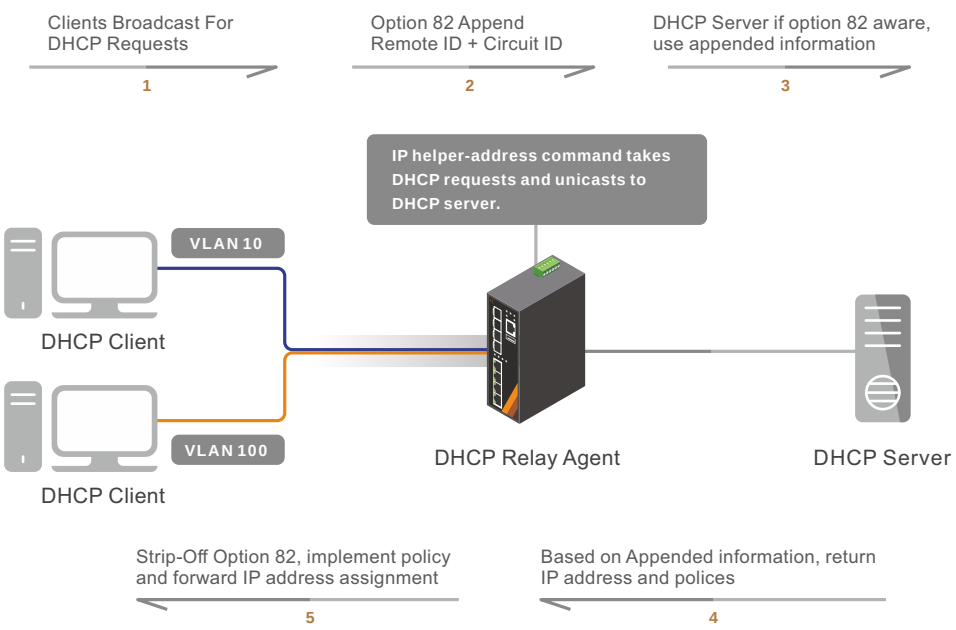
DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

DHCP Snooping

003.

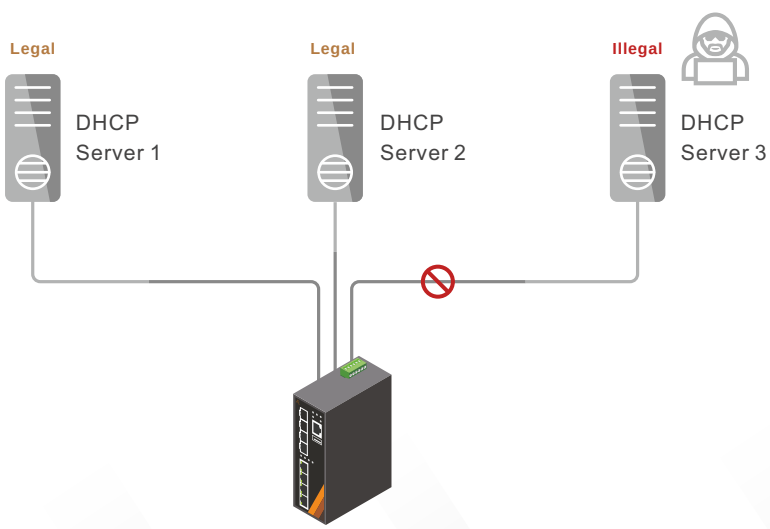
DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DHCP Relay

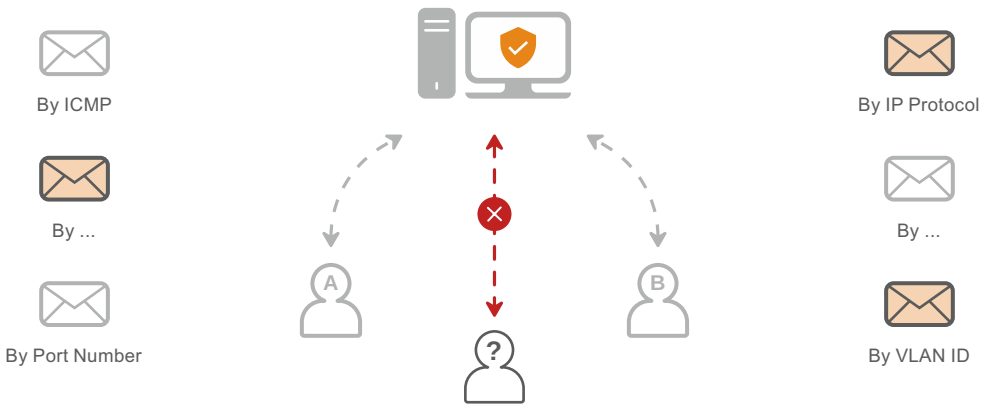


003.

DHCP Snooping

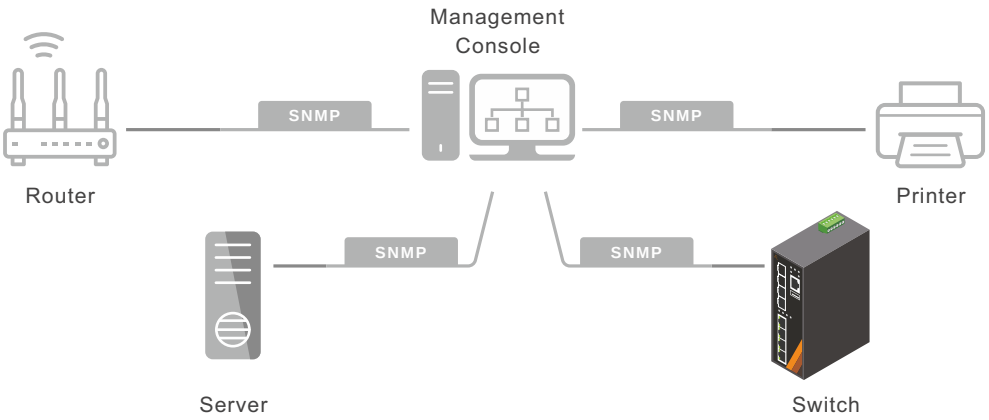


ACL



005.

SNMP



ACL

004.

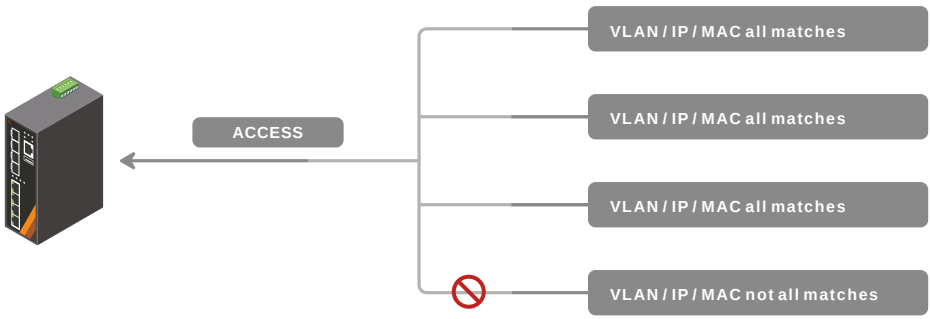
Access Control List (ACL) is a set of rules which used to filter network traffic. It can be configured on devices with packet filtering capabilities. ACL may include a list of conditions that determine when to allow the traffic or deny on the different packet of categories. It is applied for interfaces to filter leaving or entering packets.

SNMP

005.

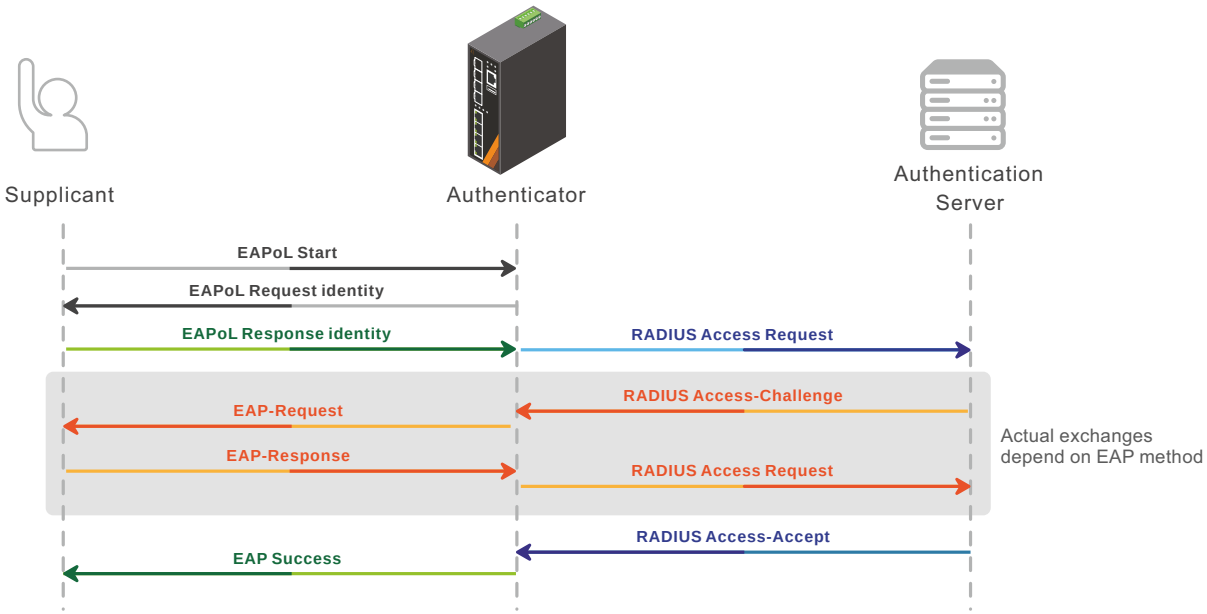
Simple Network Management Protocol (SNMP) is widely used in network management for collect ing and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

IP Source Guard



007.

IEEE 802.1X



IP Source Guard

006.

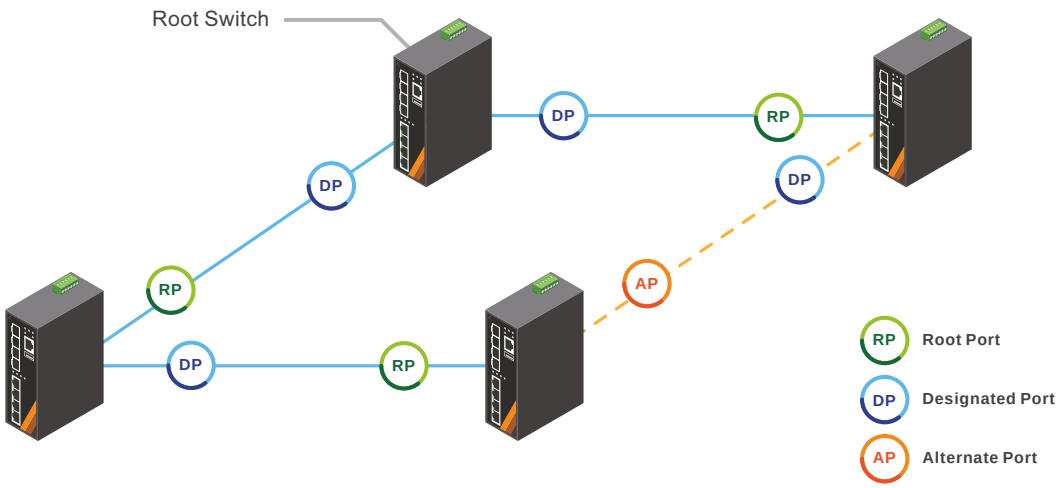
IP source guard is the solution for the IT adminis - trator, by restricting IP traffic, to prevent legitimate IP from being hacked by the malicious third party. Switching IP setting is a common way to avoid being blocked by the administrator, but this will eventually cause the whole network blocked. Therefore, the ultimate solution for the problem would be IP source guard.

IEEE 802.1X

007.

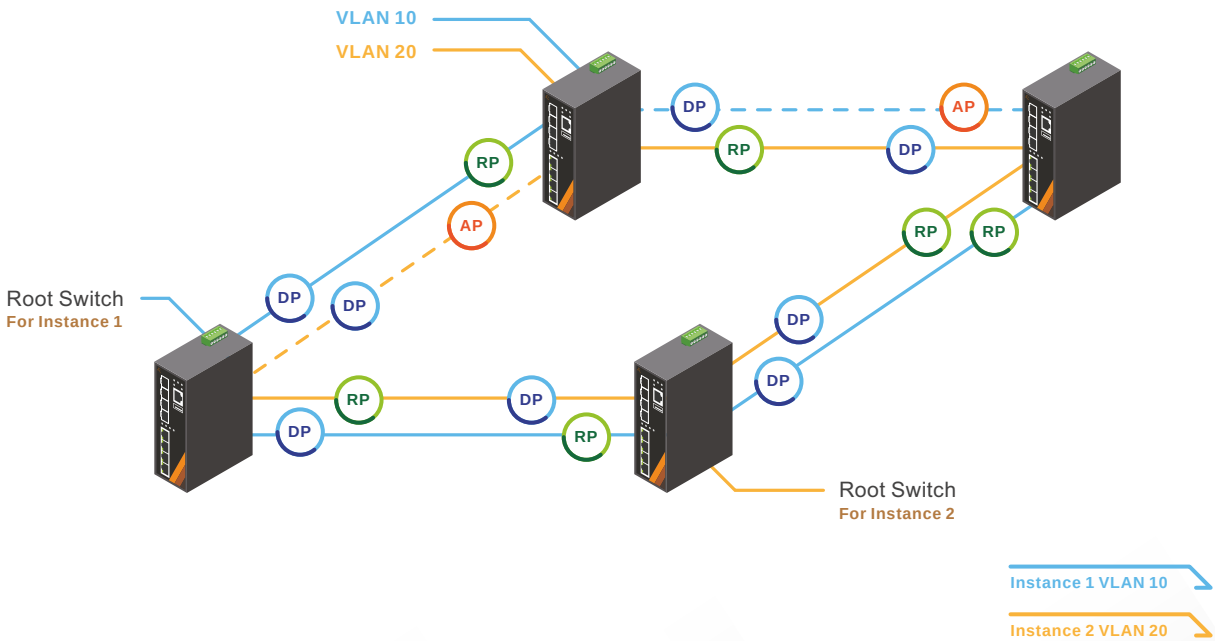
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to achieve more security on authenticated ports.

RSTP

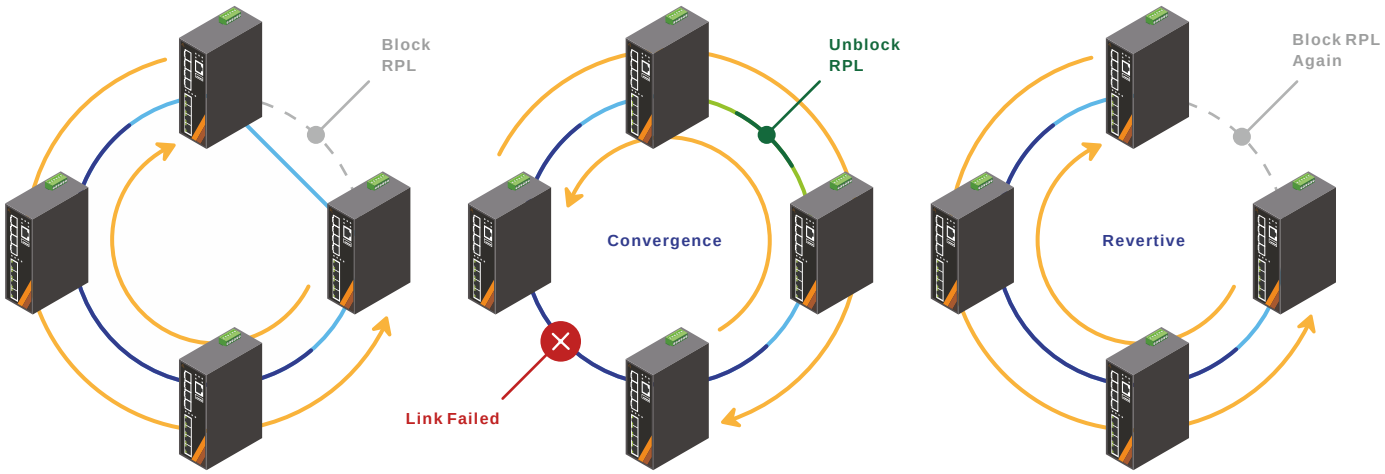


009.

MSTP



ERPS



RSTP

008.

RSTP is a useful link redundancy protocol which recovers the links without the need of manually enabling backup links to get rid of bridge loops danger. RSTP is available to address the STP convergence time gap issue. It uses discarding to replace STP disabled, blocking and listening ports status, and enables STP Root Ports and STP Designated Ports to change from the blocking to forwarding port state in a few seconds.

MSTP

009.

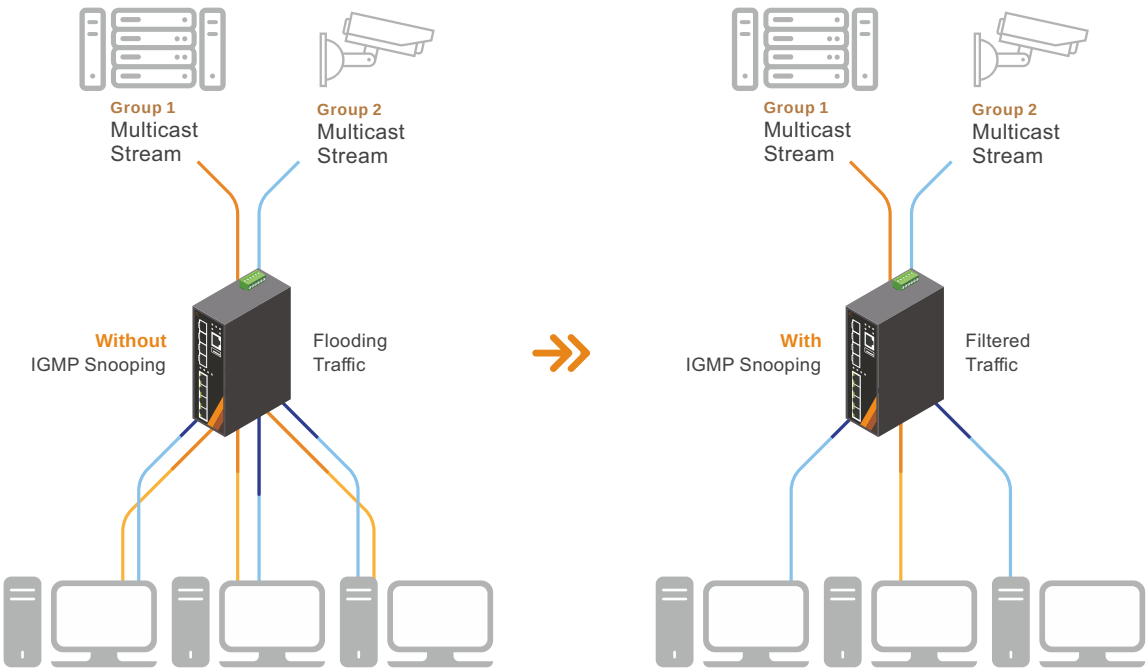
MSTP is the extension of RSTP. It allows frames to be assigned to different VLANs to separate instances of spanning tree. Each instance defines a single forwarding topology for a unique set of VLANs. Therefore, as a port belongs to multiple VLANs, it may be blocked in one spanning tree instance but forwarding in another instance.

ERPS

010.

ERPS is a fast ring redundancy protocol that is addressed by ITU-T under G.8032 to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and ensure that there are no loops formed at the Ethernet layer.

IGMP Snooping



IGMP Snooping

011.

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. This feature allows a switch to listen to the IGMP conversation between hosts and multicast routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. The switch will only forward multicast streams to the host, so it can reduce the unnecessary load in the traffic.

VLAN

012.

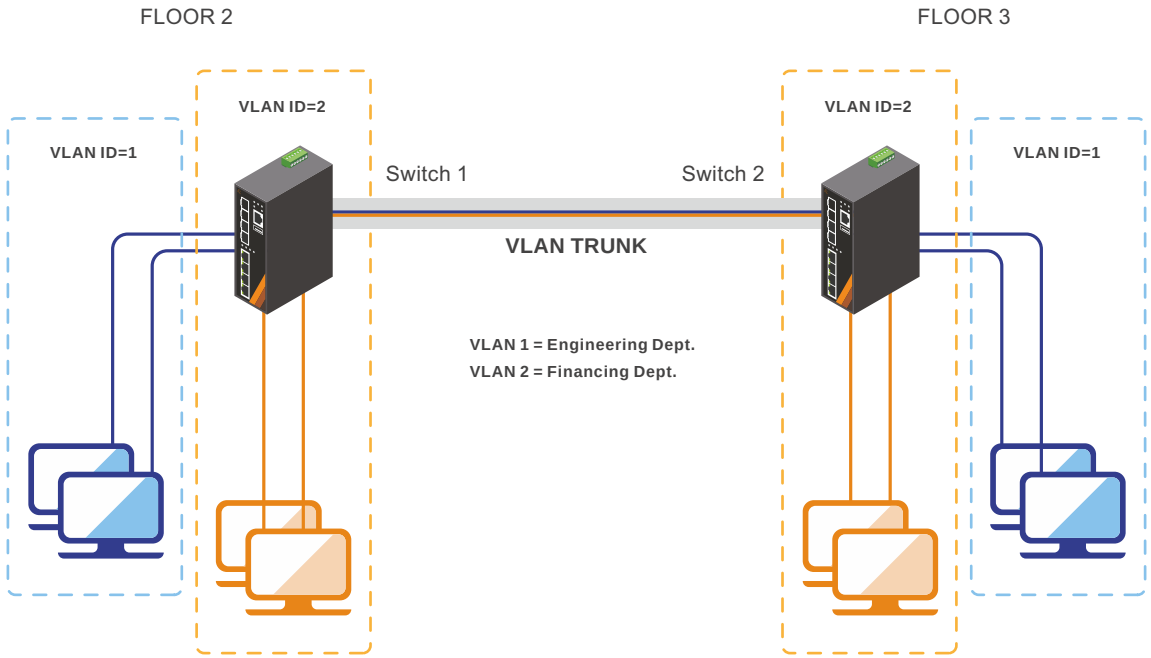
IEEE 802.1Q Virtual LAN (VLAN) defines a system of VLAN tagging for Ethernet frames and contains a VLAN Identifier that indicates the VLAN numbers. Users can use different VLAN settings to isolate network traffic.

QoS

013.

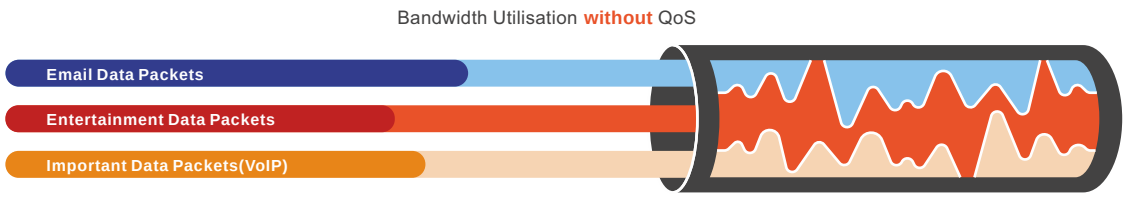
Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, users, or data flows, or to guarantee a certain level of performance to a data flow and application usage quality.

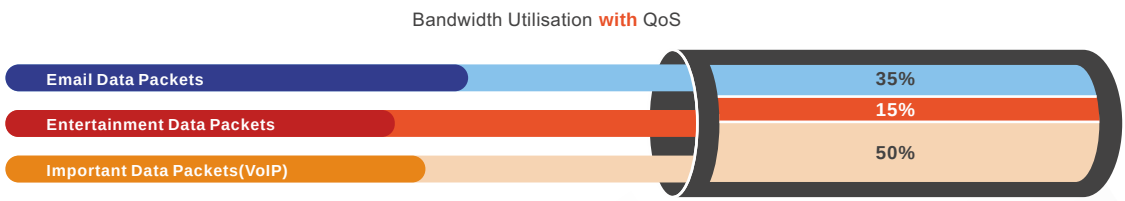
VLAN


FLOOR 2
FLOOR 3
VLAN ID=2
VLAN ID=2
VLAN ID=1
VLAN ID=1
Switch 1
Switch 2
VLAN TRUNK
VLAN 1 = Engineering Dept.
VLAN 2 = Financing Dept.

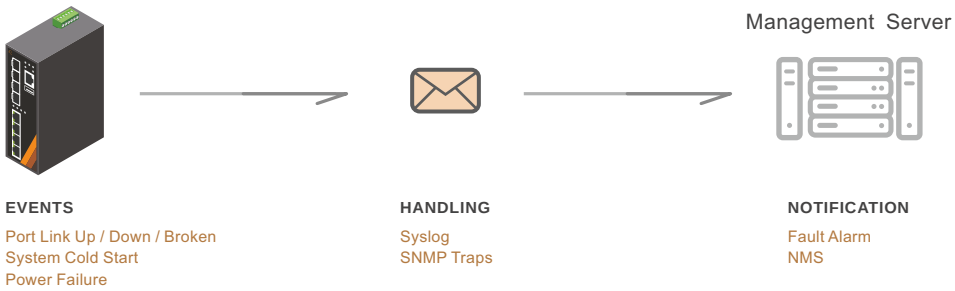
013.

QoS


Bandwidth Utilisation without QoS
Email Data Packets
Entertainment Data Packets
Important Data Packets(VoIP)

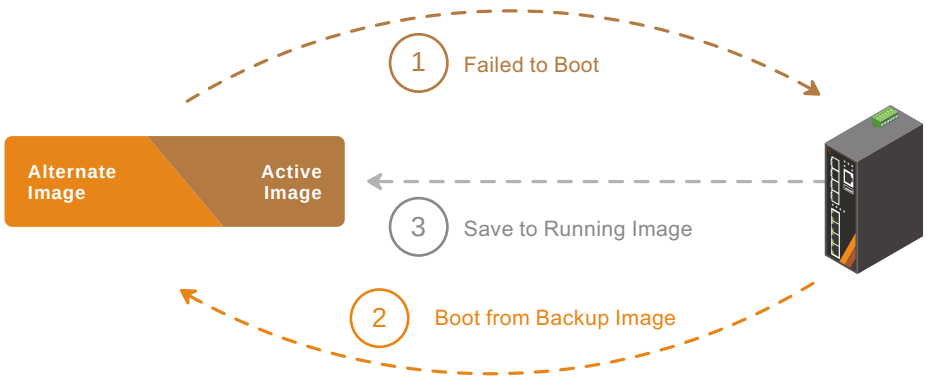

Bandwidth Utilisation with QoS
Email Data Packets
Entertainment Data Packets
Important Data Packets(VoIP)
35%
15%
50%

Fault Management



017.

Software Image Selection



Fault Management

016.

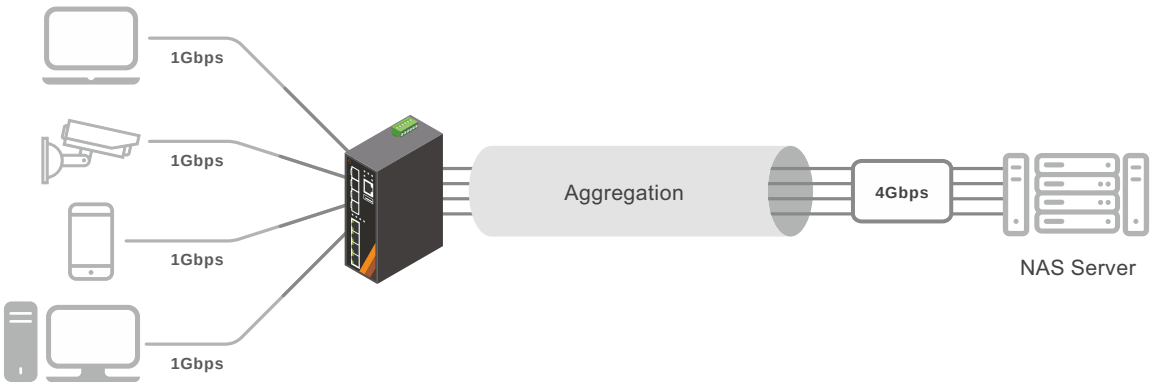
These messages are the main form of communication and recorded between a System Agent and a System Manager. They are used to inform a System manager when an important event happens at the Agent level. A benefit of using these messages for reporting alarms is that they trigger instantaneously, rather than waiting for a status request from the manager.

Software Image Selection

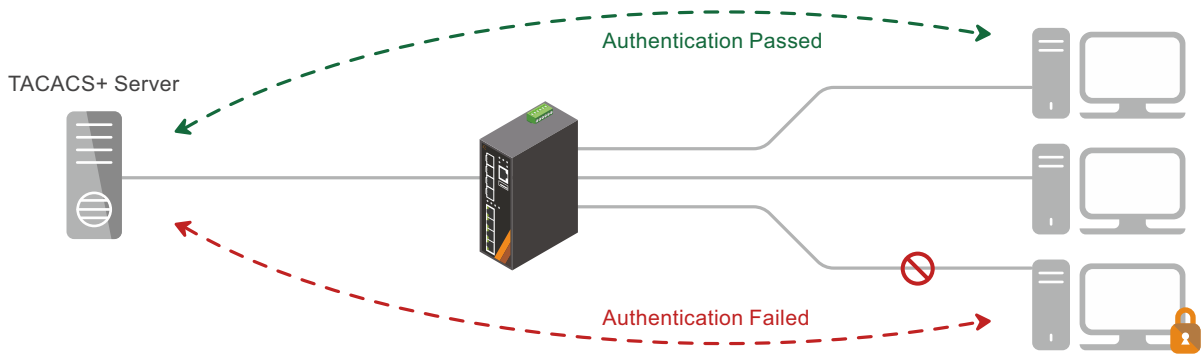
017.

The Software Image Selection feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as an alternate image.

Aggregation



TACACS+



Aggregation

Aggregation is a method of combining multiple network connections in parallel. It increases the throughput beyond what a single connection could sustain, and provides redundancy in case one of the links fails. For example, if the application requires a 4-Gigabit link, and each port supports only 1-Gigabit link, the “Aggregation” allows users to link 4 of 1-Gigabit ports to obtain a 4-Gigabit trunk feature.

TACACS+

TACACS+ is a networking protocol which provides access control for routers, network access servers and other network computing devices via one or more centralized servers.

Follow us on