LEONTON

Software & Protocol

About

Leonton's industrial networking products are specifically designed and thoroughly tested to be utilized in extreme conditions and harsh environments. Leonton designs and tests all networking products with the highest industrial standard, including extended temperature, passive cooling, redundant power input, metal enclosure, lower voltage power input and more.

"Your Partner in Networking" is the slogan of Leonton, which conveys the idea and value we are determined to provide in the market by making the products with the highest quality and offering the best service in customization projects, creating networking environments with enhanced safety, efficiency, stability, and reliability.

leonton

Contents

Software & Protocol

04 LeNMS

05 TTDP (Train Topology Discovery Protocol)

06 RIP (Routing Information Protocol)

06 OSPF (Open Shortest Path First)

07 VRRP (Virtual Router Redundancy Protocol)

08 IP Routes (Static Routes)

09 DHCP Relay

09 DHCP Snooping

10 ACL

10 SNMP

11 IP Source Guard

11 IEEE 802.1X

12 RSTP

12 MSTP

13 ERPS

14 IGMP Snooping

15 VLAN

15 QoS

16 Aggregation

16 TACACS+

17 Fault Management

17 Software Image Selection

18 Modbus over Ethernet

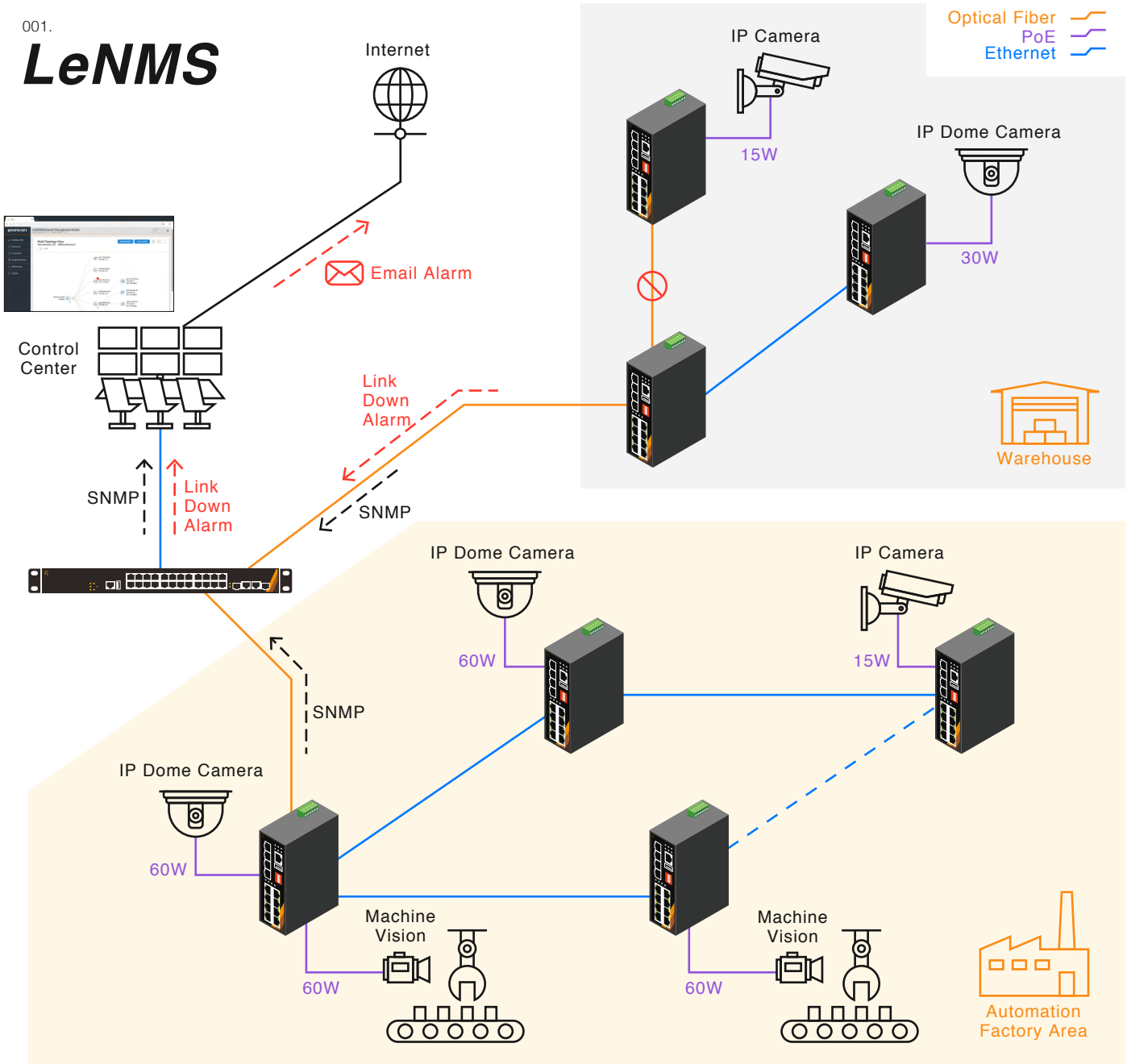
19 PoE Ping Alive

20 PoE Schedule

20 PoE Power Priority Management

001.

LeNMS



LeNMS

001.

Topology View

LeNMS automatically creates a network topology diagram. A device configuration does not require set up; the only step required is to configure the IP range in the network domain. LeNMS can discover the networked devices and automatically connect, monitor, and maintain from one central location. In the Topology View, LeNMS displays the topology of connections among all the switches and offers dynamic connectivity indicators, such as Port number, PoE power consumption, and Events.

Device List

Several columns show the device's information such as online status, PoE usage, and more. Alternative device names can be given as well in order to organize the devices for easier management. Devices can be located quickly by using the sort or search feature. To manage devices with web interfaces, simply click on the IP address which is hyperlinked to the GUI web interface.

E-map & Google map View

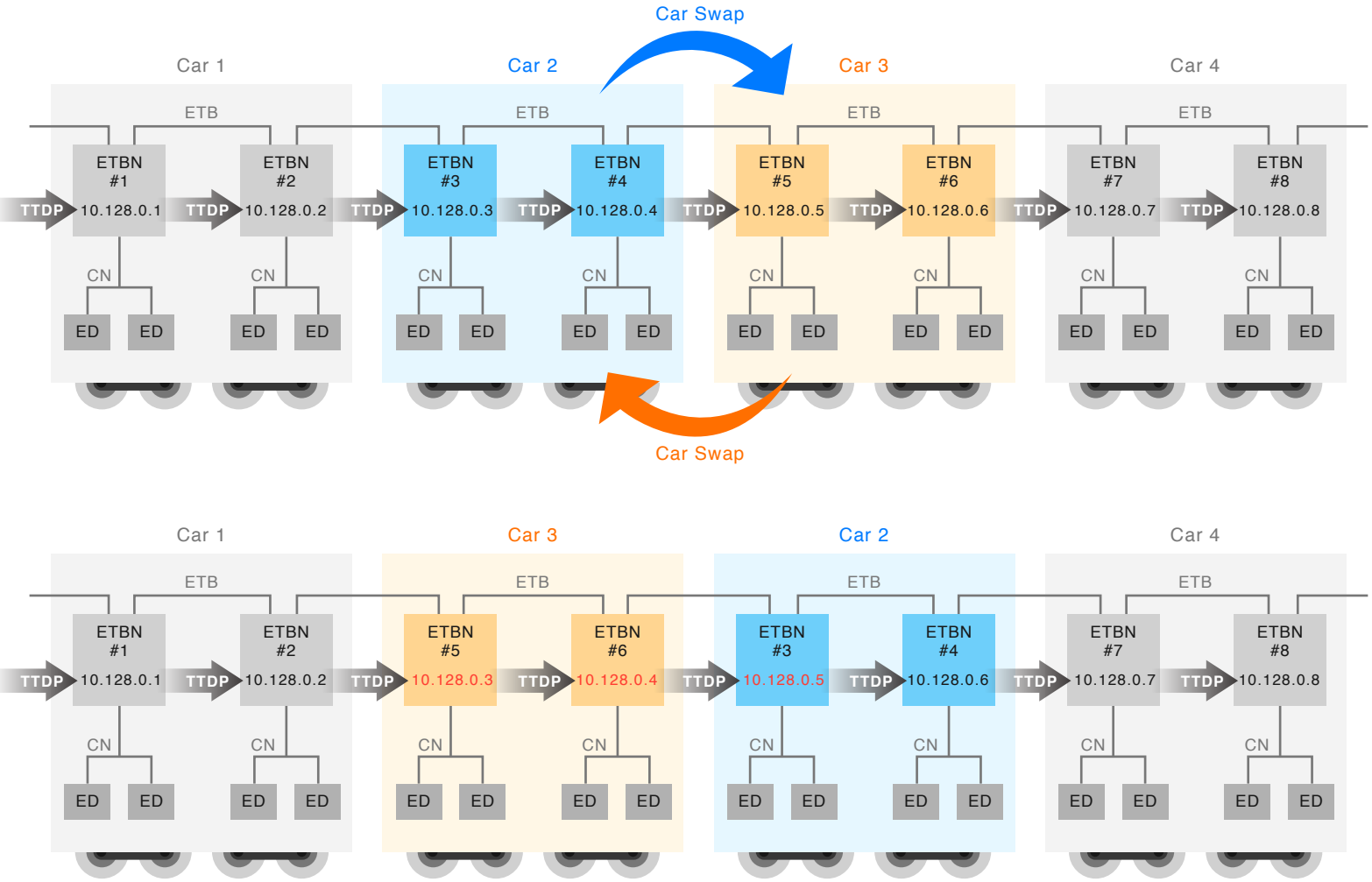
The E-map View allows floor plan images to be uploaded and devices can be positioned in locations where they are installed. If needed, the drawing on this page can be exported.
On the Google-Map View, users can add a location of a device onto the map where the longitude and latitude will automatically be set. Similar to the E-Map View, this allows administrators to monitor the complete picture of a large region. These features allows administrators to visually identify the location of a device quickly.

002.

TTDP

Railway

ETB: Ethernet Train Backbone
ETBN: Switch
CN: Consist Network
ED: End Device



TTDP (Train Topology Discovery Protocol)

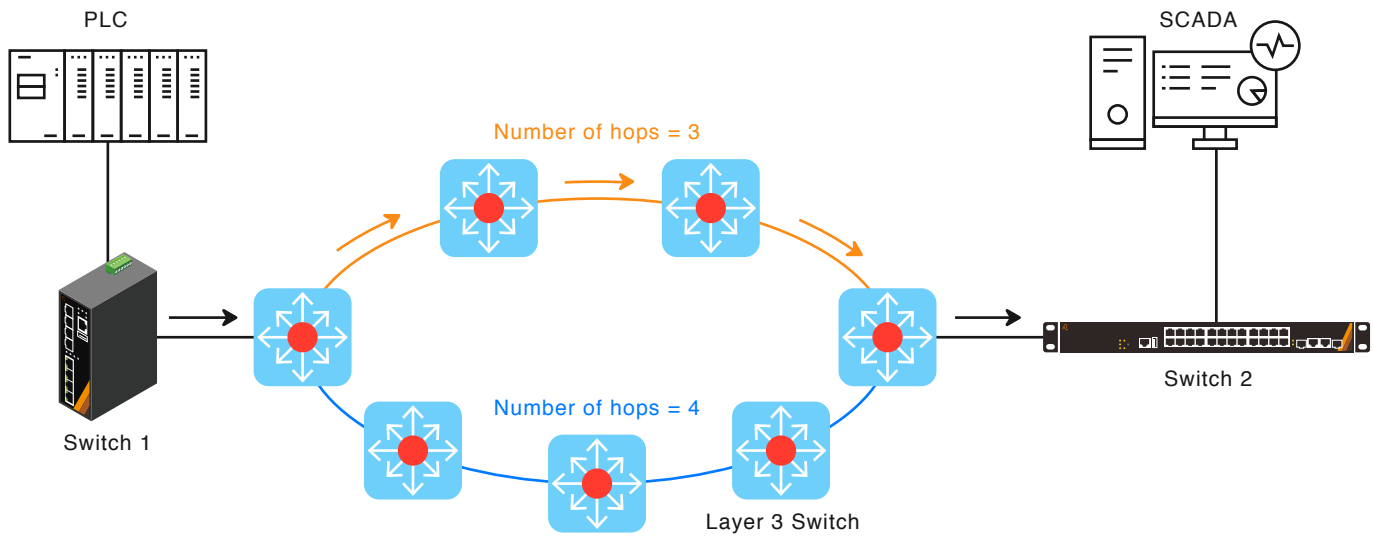
002.

Designed for the train inauguration applications, TTDP is primarily used to discover the network topology based on orientation identification of each railway carriage in a train in order to provide auto network configuration, such as assigning an ordered IP range, for all Ethernet switches deployed in the Train Network Communication Network (TCN). Each railway carriage contains some Ethernet Train Backbone Nodes (ETBN) along with some Consist Networks (CN) that are a part of the Ethernet Train Backbone (ETB). Without using TTDP, network operators must manually follow the correct order to perform IP configuration based on the change in orientation of a railway carriage each time when a railway carriage is rearranged from a train.

003.

RIP

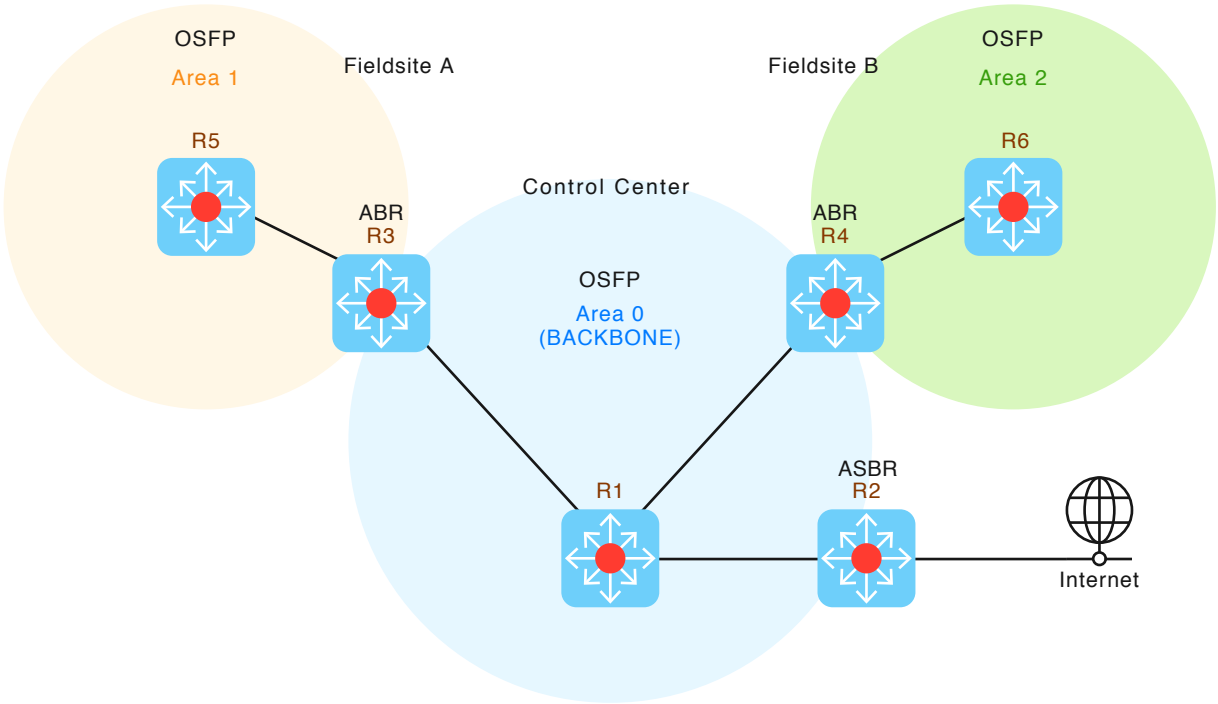
Layer 3



004.

OSPF

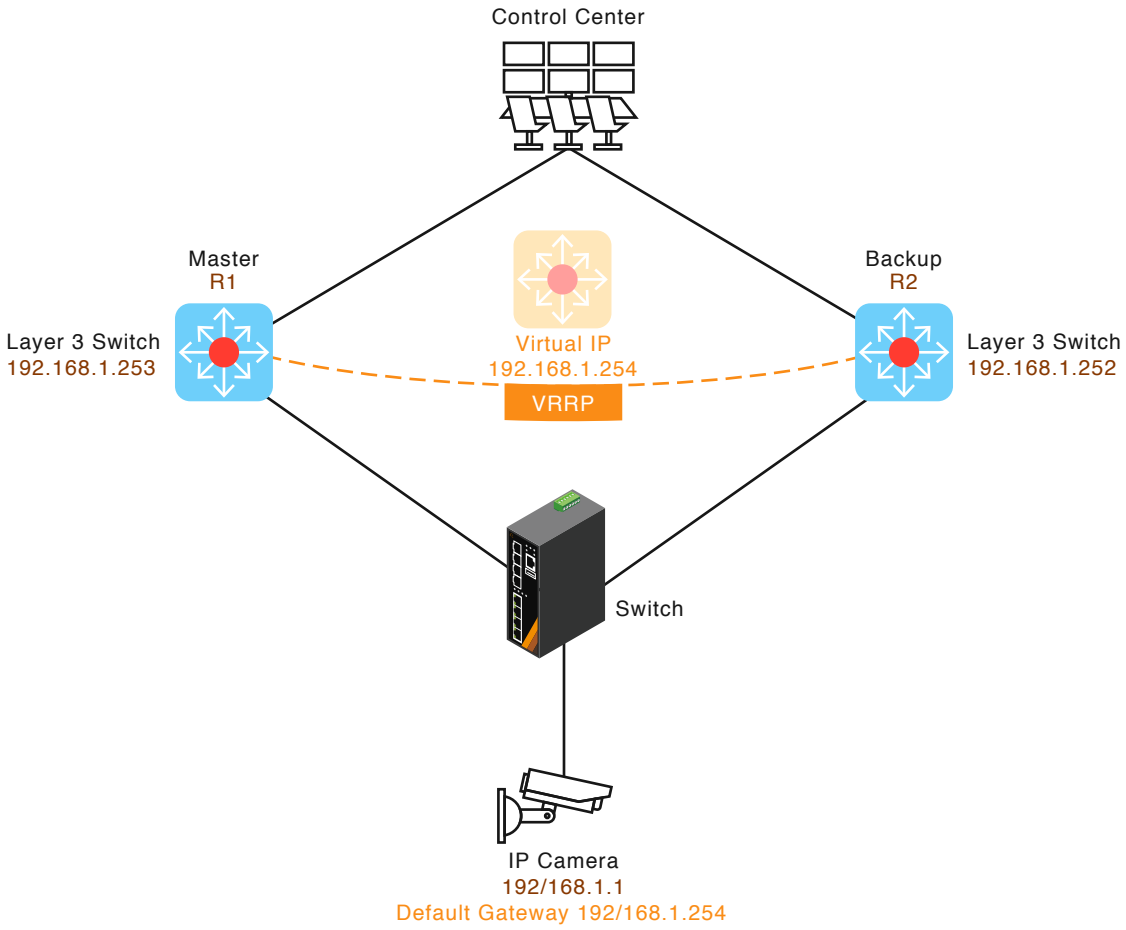
Layer 3



005.

VRRP

Layer 3



RIP (Routing Information Protocol)

003.

RIP is based on distance vectors, which relies on hop count to select the best possible route to a remote network. The best possible route is determined by the fewest number of hop count, which refers to the number of Layer 3 switches occurring in a route from any source to any destination network. RIP operates pretty well in fairly small networks, which only allows a maximum hop count of 15 switches. Hence, a hop count of 16 means that the route is considered unreachable. The big advantage of implementing RIP is that it has less complexity in terms of configurations.

OSPF (Open Shortest Path First)

004.

OSPF is based on a two-level hierarchical network design, which relies on the notion of different types of areas to segment a large network into multiple smaller networks. The main advantage of doing this is to keep routing entries to a minimum and retain the impact of any network topology changes within a specific area. Generally, the types of OSPF areas include Backbone Area, Standard Area, Stub Area, and Not So Stubby Area. These areas are connected by Area Border Routers that summarize a set of contiguous routes from its routing table into a single aggregate route and forward it to other areas.

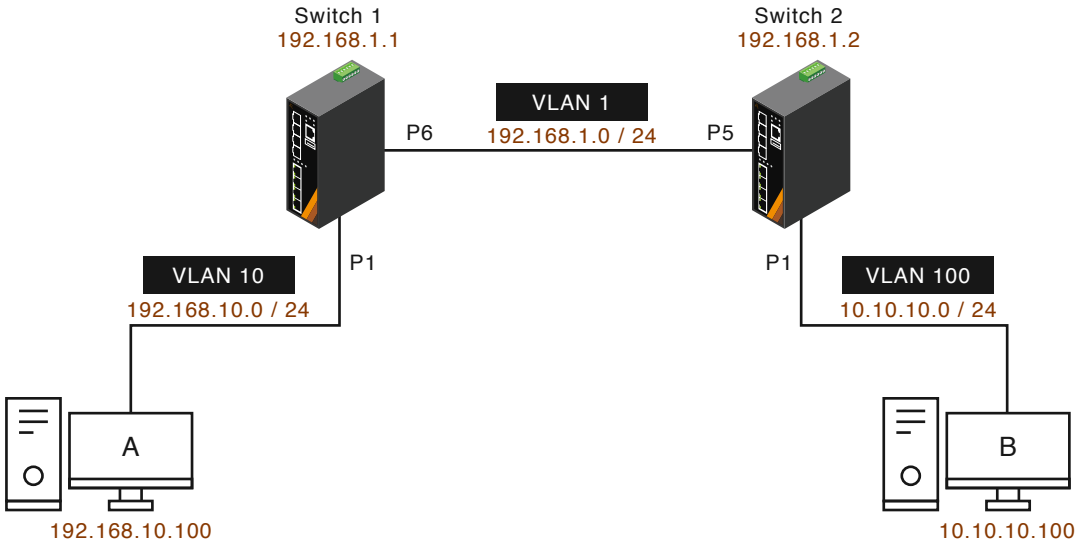
VRRP (Virtual Router Redundancy Protocol)

005.

With the support of gateway redundancy, the likelihood of a single point of network failure is greatly minimized. Therefore, implementing Layer 3 high availability can easily be accomplished by enabling two physical switches to form a single virtual group that acts as a default gateway to the remote control center for all connected end devices such as security cameras on a local network. If the primary switch becomes unavailable, then the backup switch steps in immediately and takes over responsibility for forwarding data.

006.

IP Routes



IP Routes (Static Routes)

006.

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

007.

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.

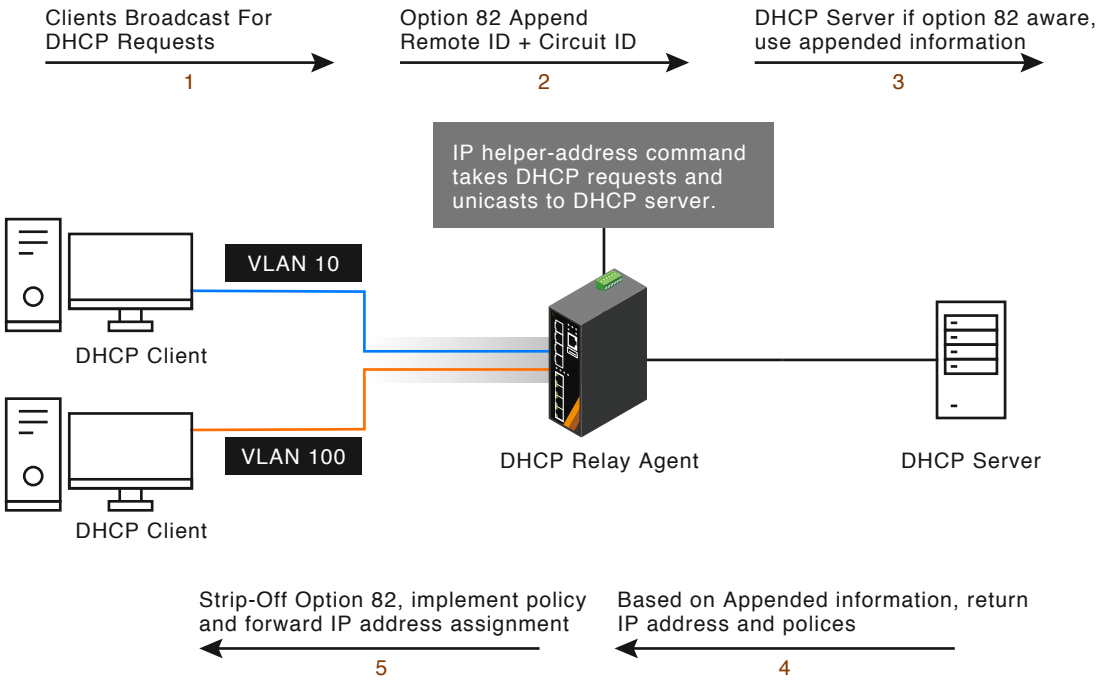
DHCP Snooping

008.

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.

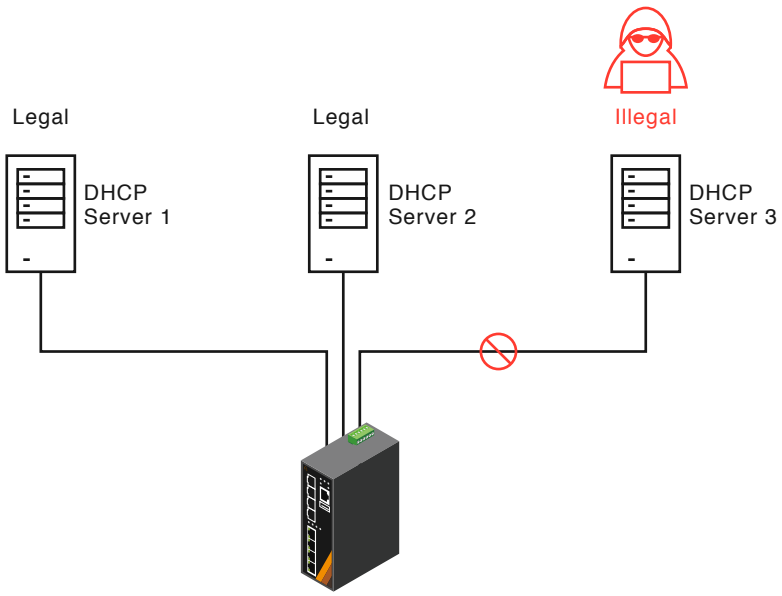
007.

DHCP Relay



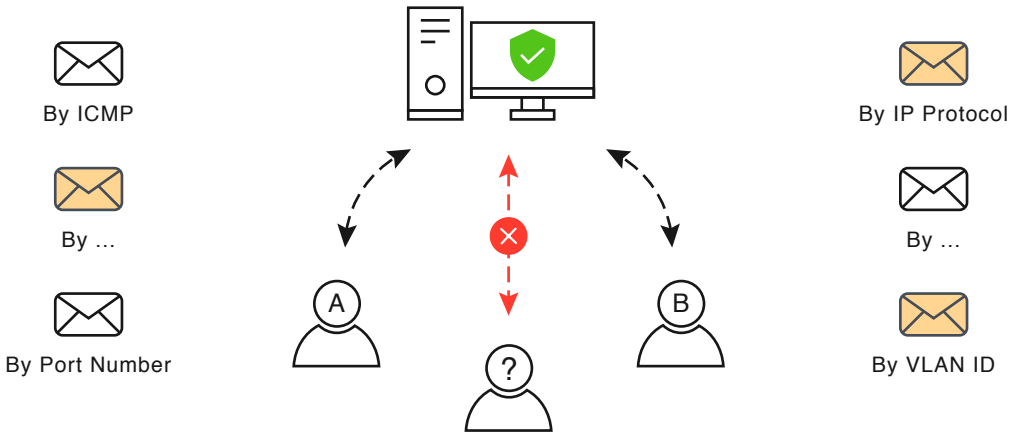
008.

DHCP Snooping



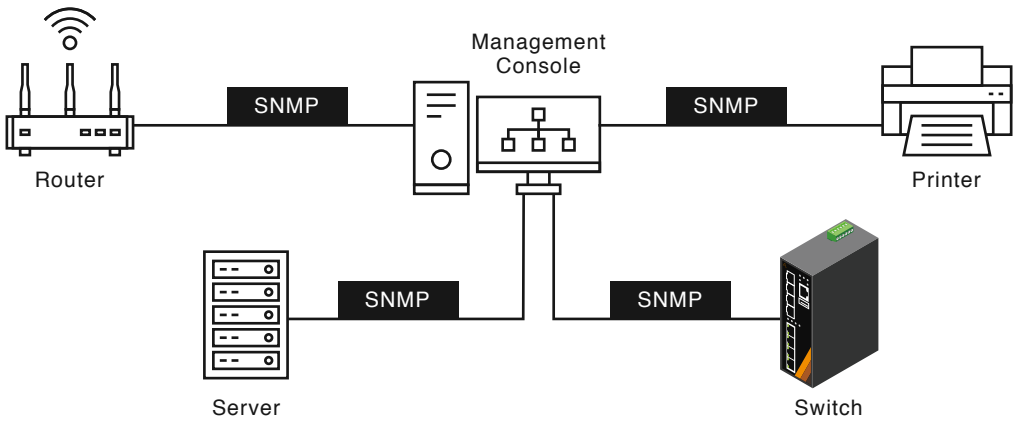
009.

ACL



010.

SNMP



ACL

009.

Access Control List (ACL) is a set of rules 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.

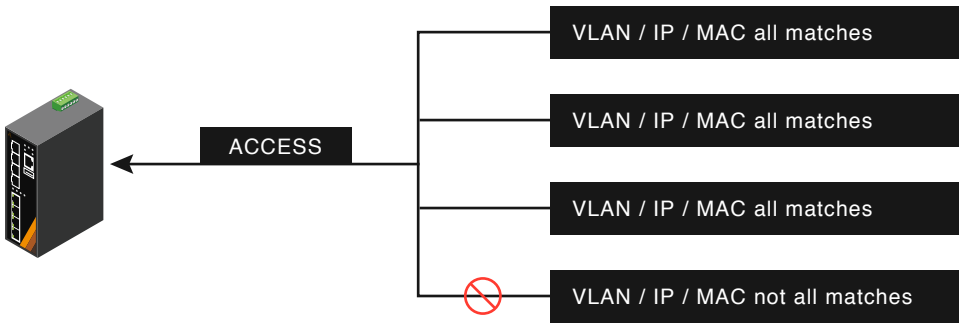
SNMP

010.

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

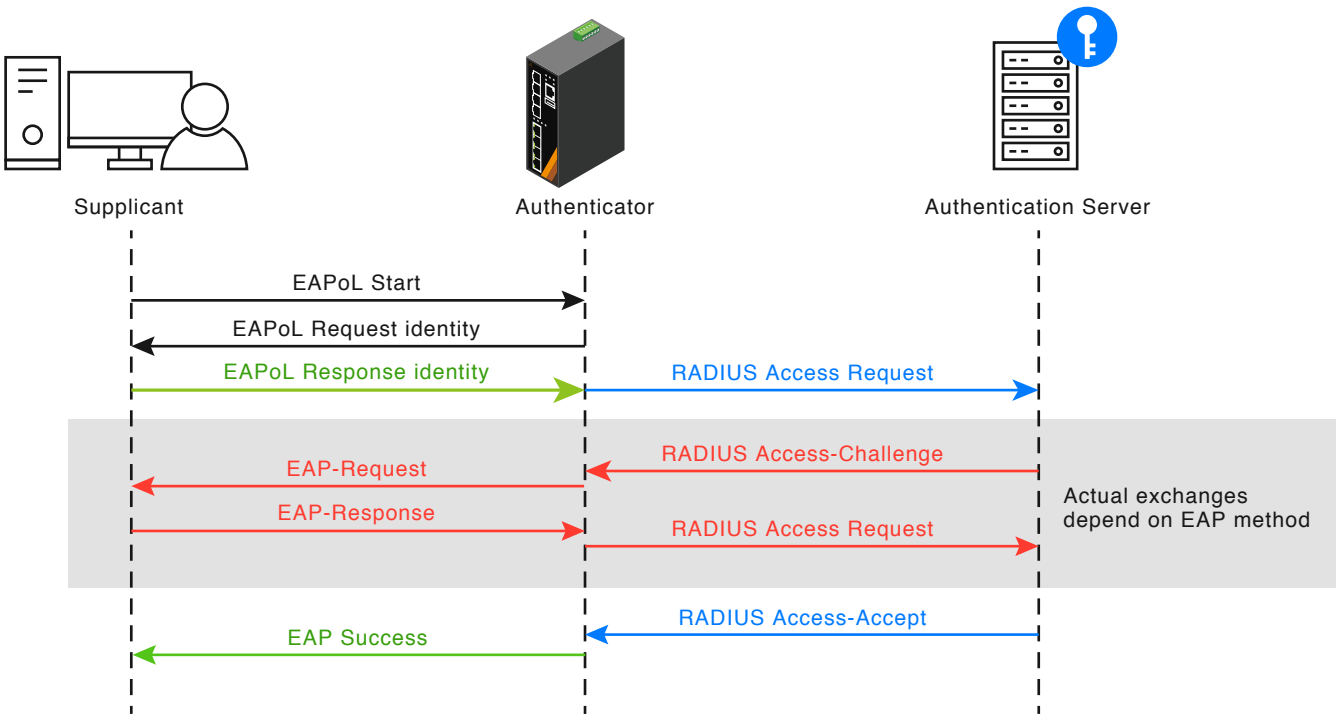
011.

IP Source Guard



012.

IEEE 802.1X



IP Source Guard 011.

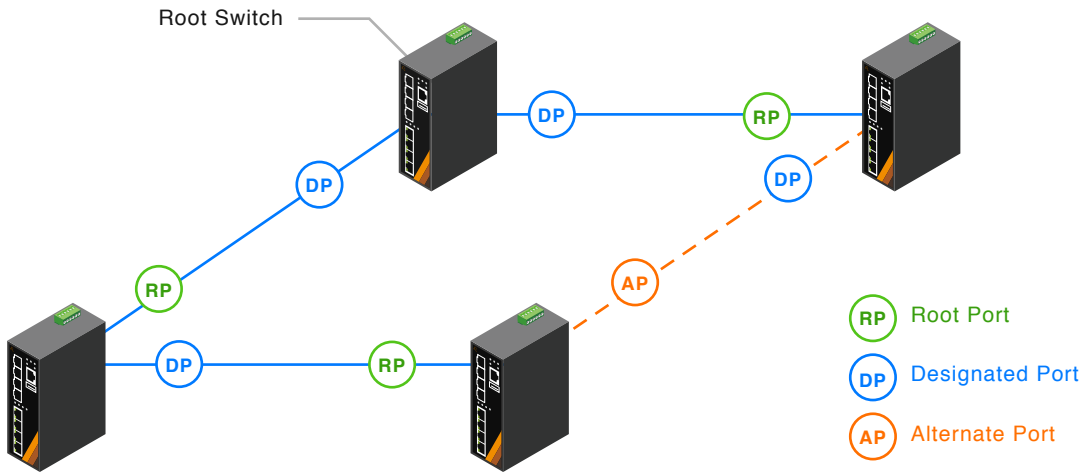
IP source guard is the solution for the IT administrator. By restricting IP traffic, it prevents legitimate IP from being hacked by the malicious third party. Switching IP setting is a common way to avoid being blocked by the administrator, but this will eventually cause the whole network blocked. Therefore,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

IEEE 802.1X 012.

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.

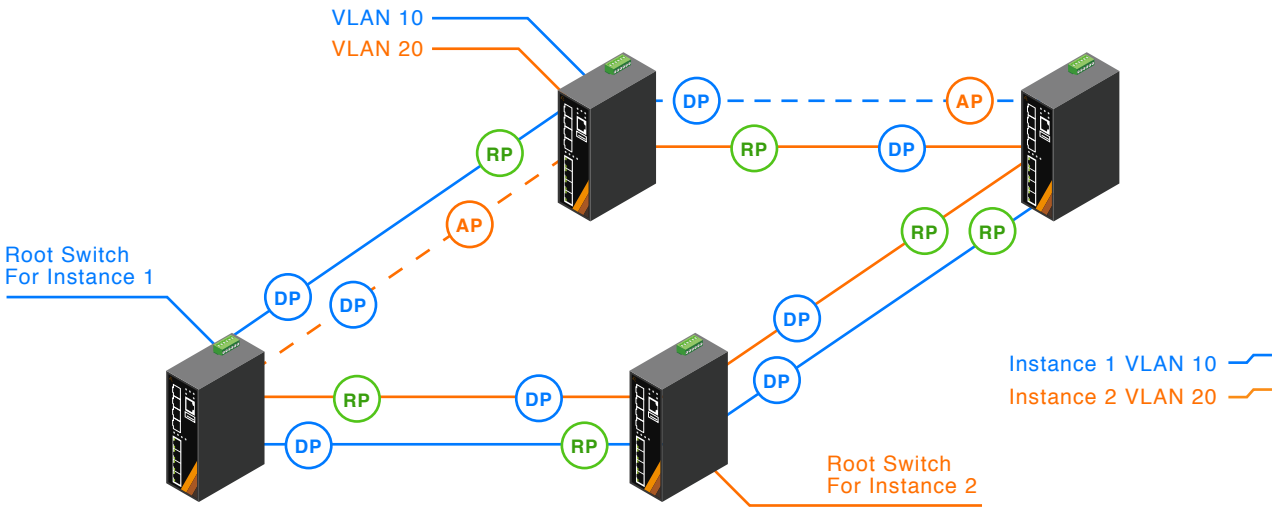
013.

RSTP



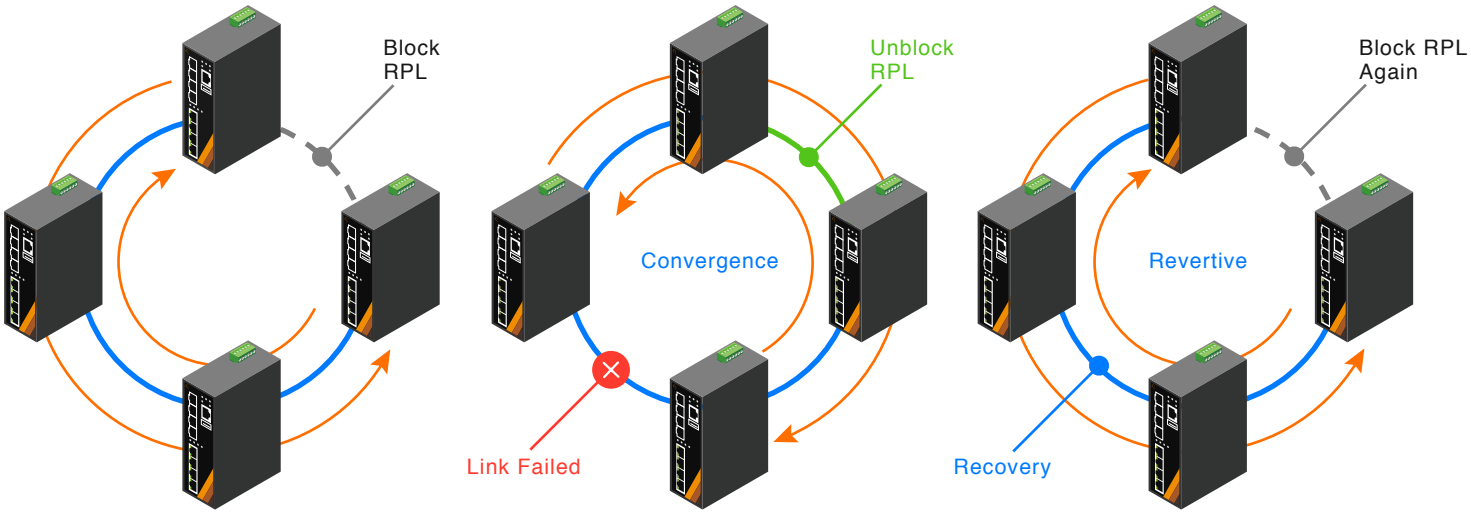
014.

MSTP



015.

ERPS



RSTP 013.

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 014.

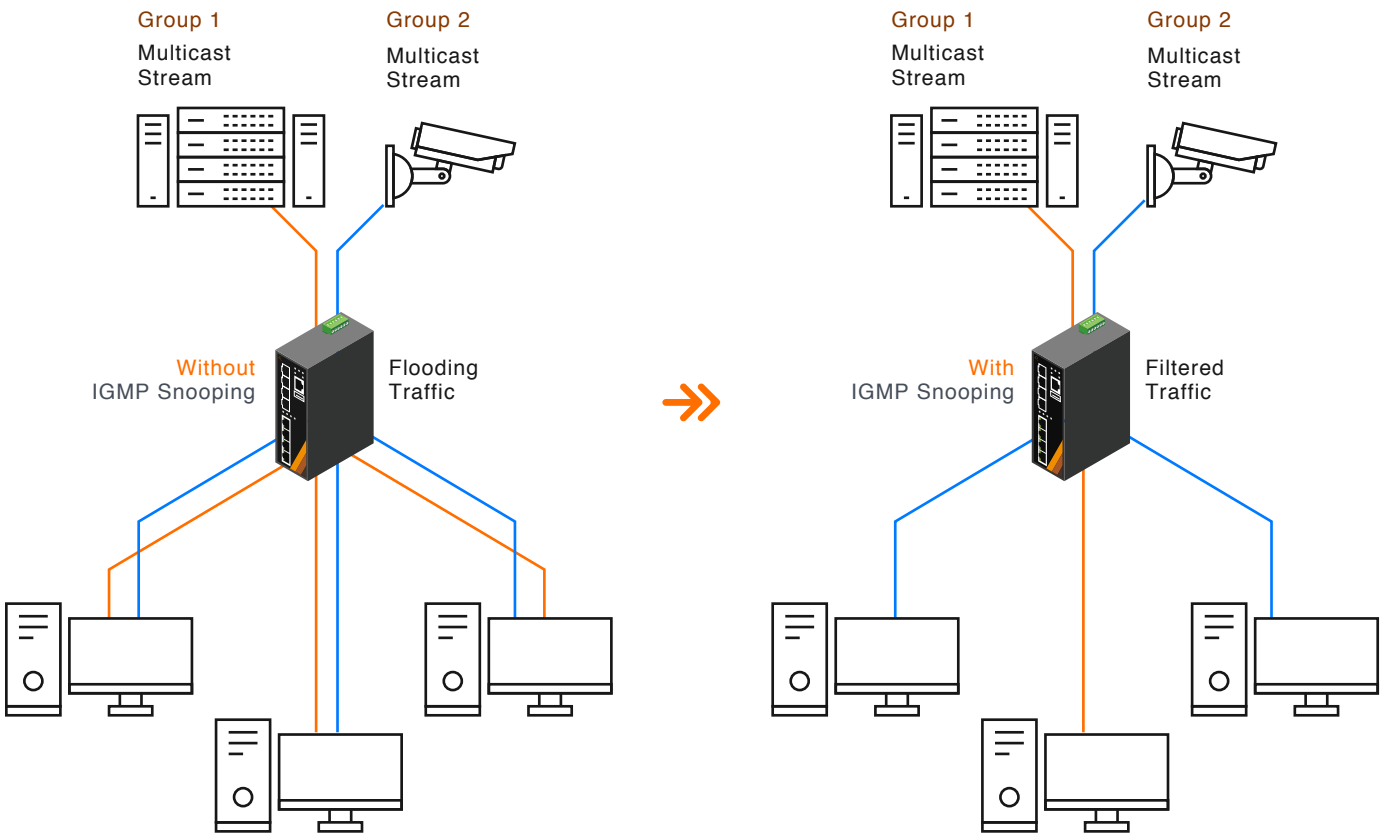
MSTP is the extension of RSTP. It allows frames to be assigned to different VLANs to separate instances of spanning tree. Each instance defines a single forwarding topology for a unique set of VLANs. Therefore, as a port belongs to multiple VLANs, it may be blocked in one spanning tree instance but forwarding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

ERPS 015.

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.

016.

IGMP Snooping



IGMP Snooping 016.

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 017.

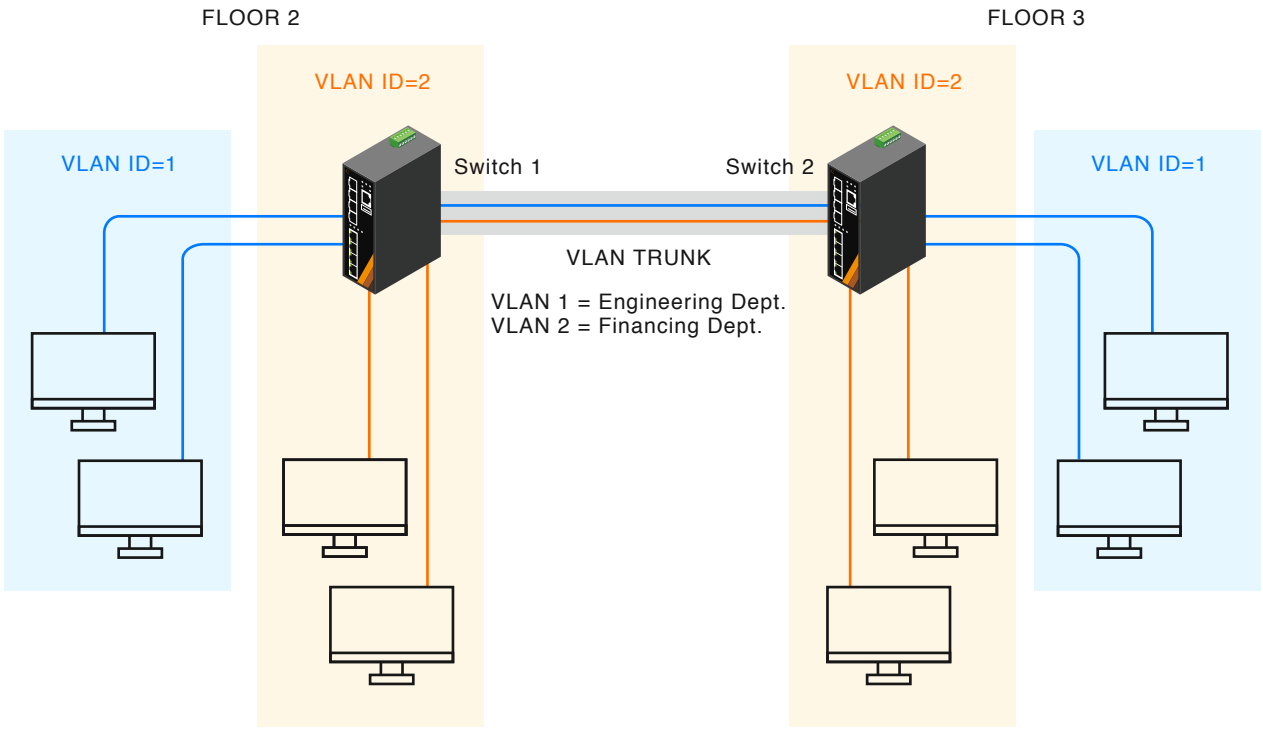
IEEE 802.1Q Virtual LAN (VLAN) defines a system of VLAN tagging for Ethernet frames and contains a VLAN Identifier that indicates the VLAN numbers. Users can use different VLAN settings to isolate network traffic.

QoS 018.

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.

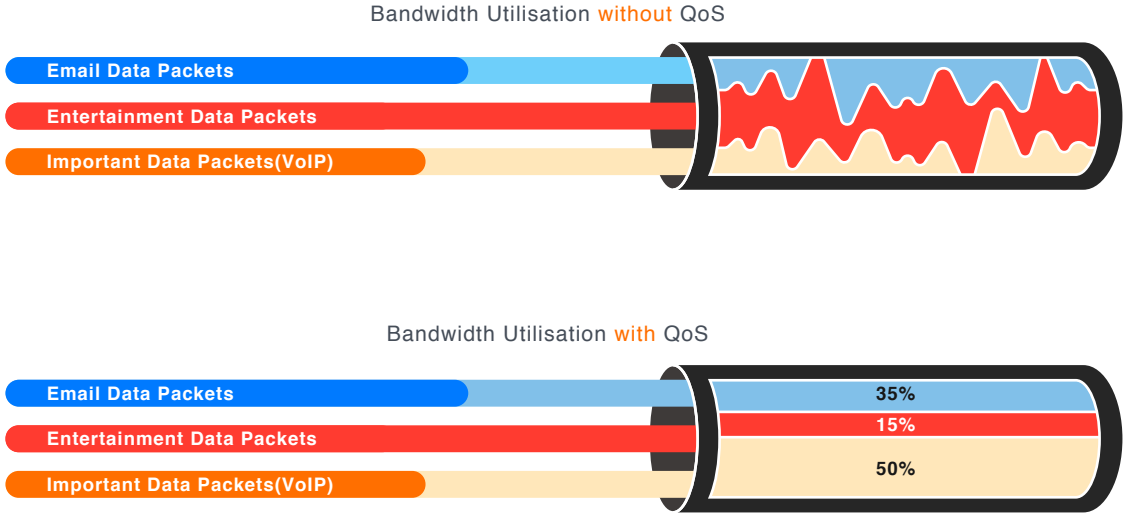
017.

VLAN



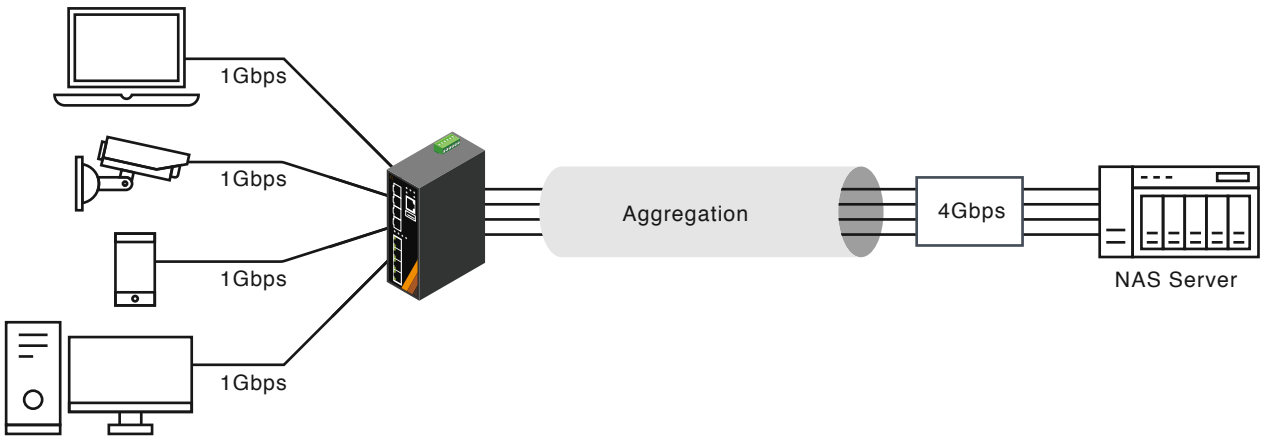
018.

QoS



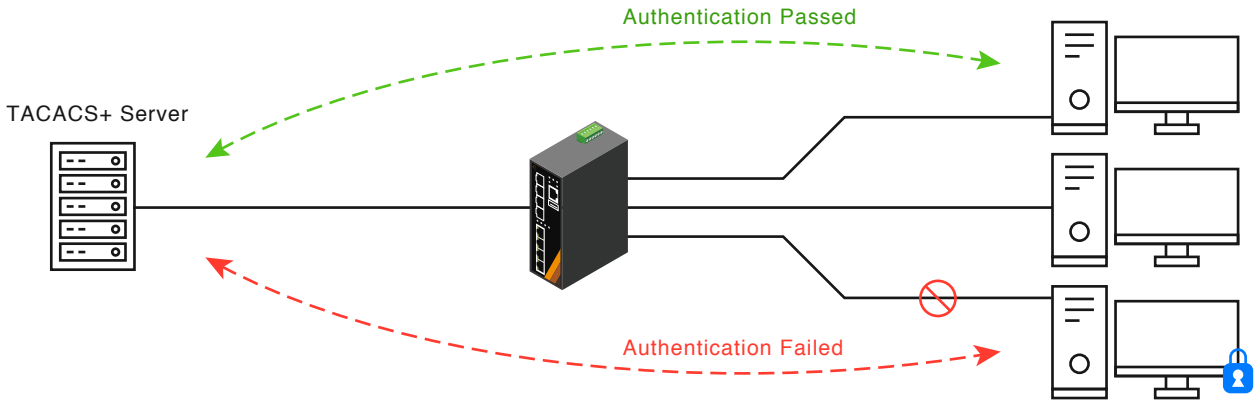
019.

Aggregation



020.

TACACS+



Aggregation 019.

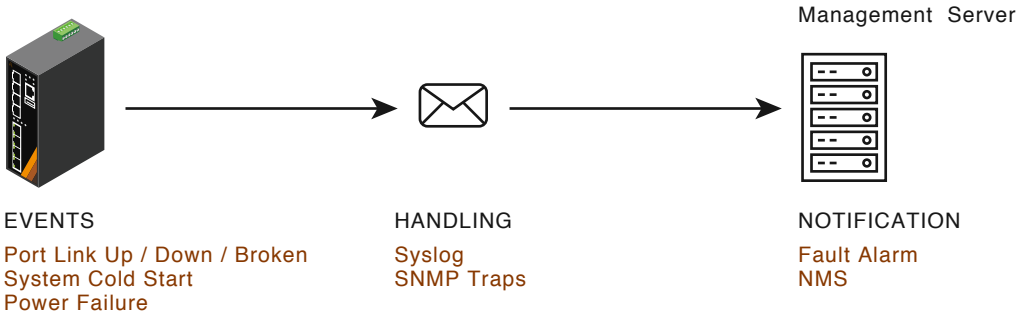
Aggregation is a method of combining multiple network connections in parallel. It increases the throughput beyond what a single connection could sustain, and provides redundancy in case one of the links fails. For example, if the application requires a 4-Gigabit link, and each port supports only 1-Gigabit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

TACACS+ 020.

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.

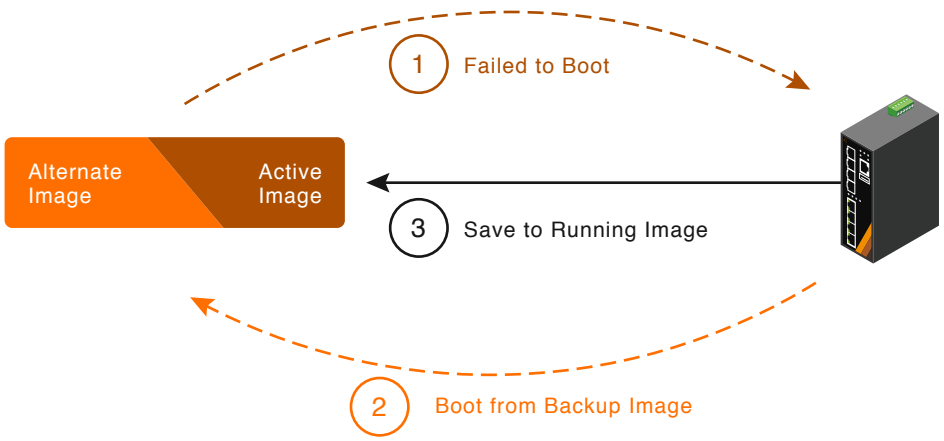
021.

Fault Management



022.

Software Image Selection



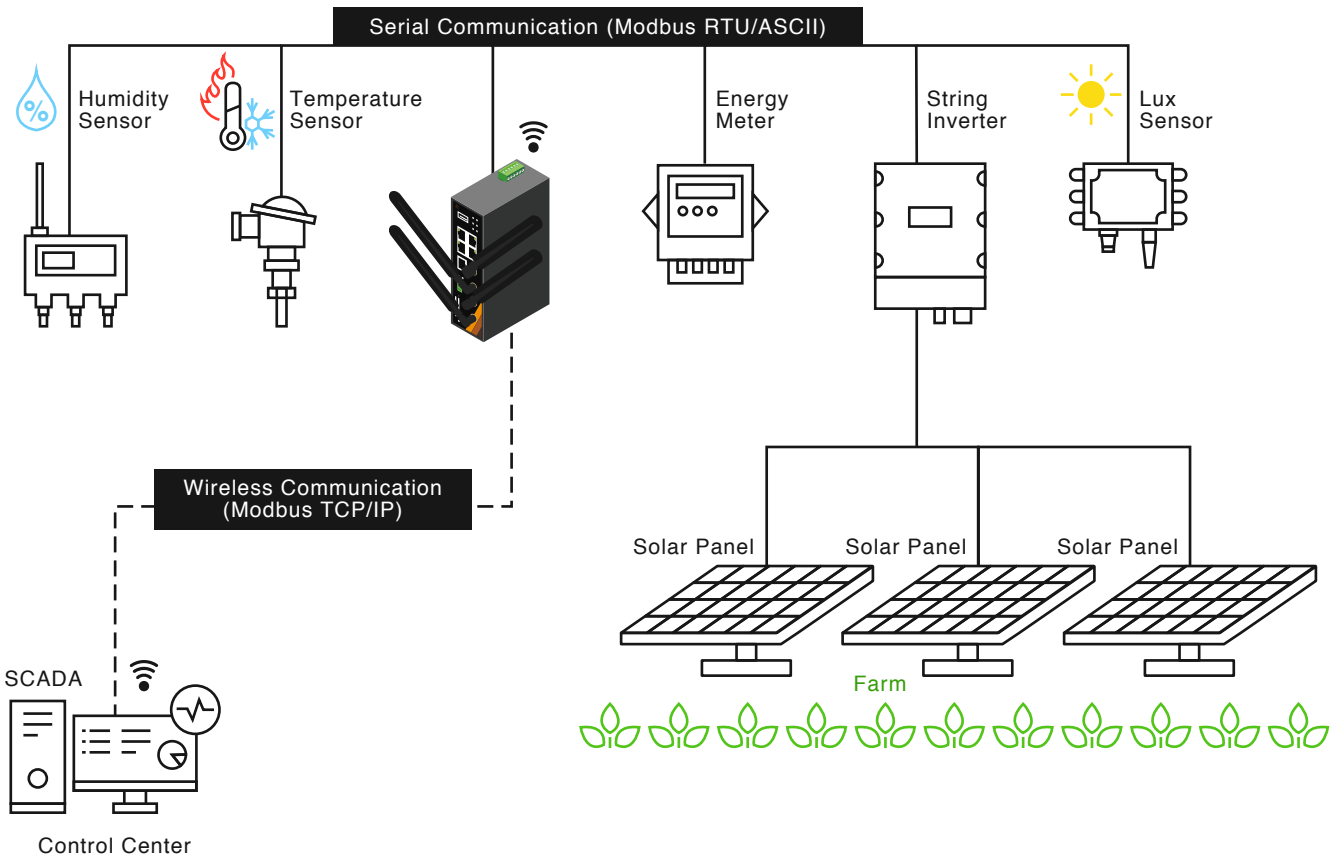
Fault Management 021.

These messages are the main form of communication and are 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 022.

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.

Modbus over Ethernet

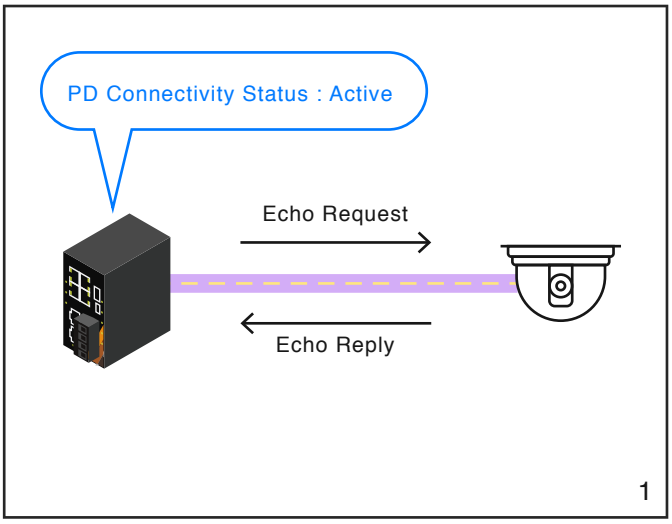


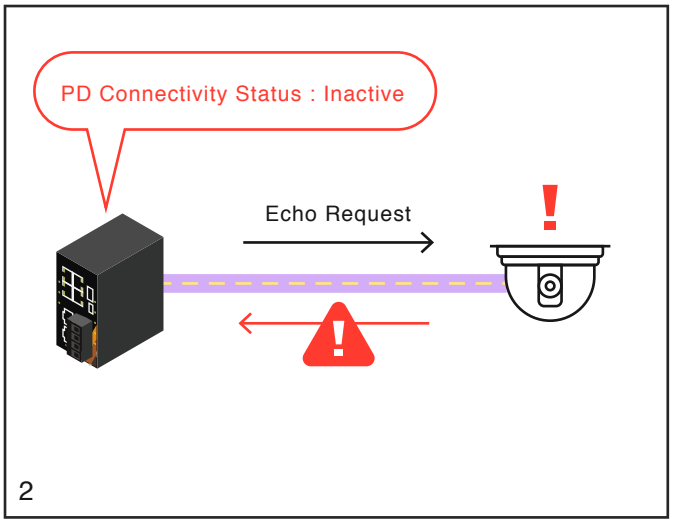
Modbus over Ethernet

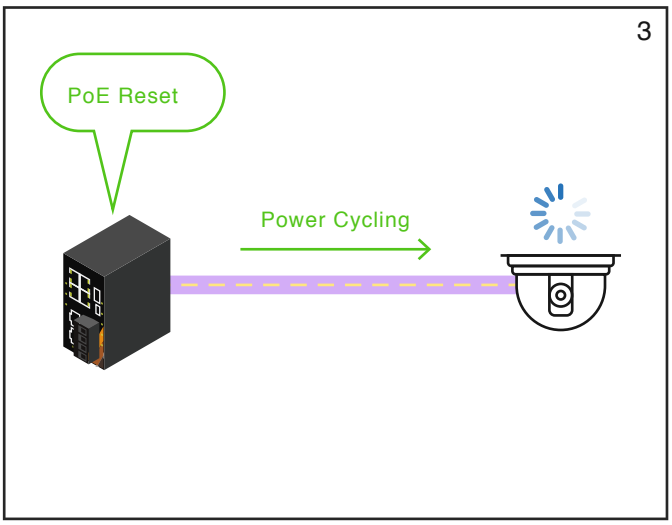
Nowadays, most Modbus applications require some implementations of protocol conversion, which brings serial communication into a TCP/IP environment. In a solar photovoltaic application, the IIoT gateway allows energy data such as light intensity, current, voltage, and power to be accesible through the Mobus RTU protocol in real-time. The serial data is then converted into the Modbus TCP/IP protocol before delivering it to the remote control center over the cellular network or Wi-Fi network depending on the transmission distance.

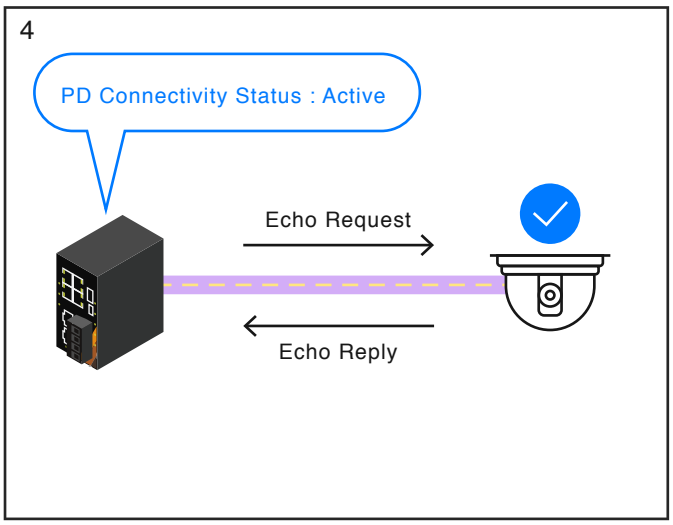
024.

PoE Ping Alive



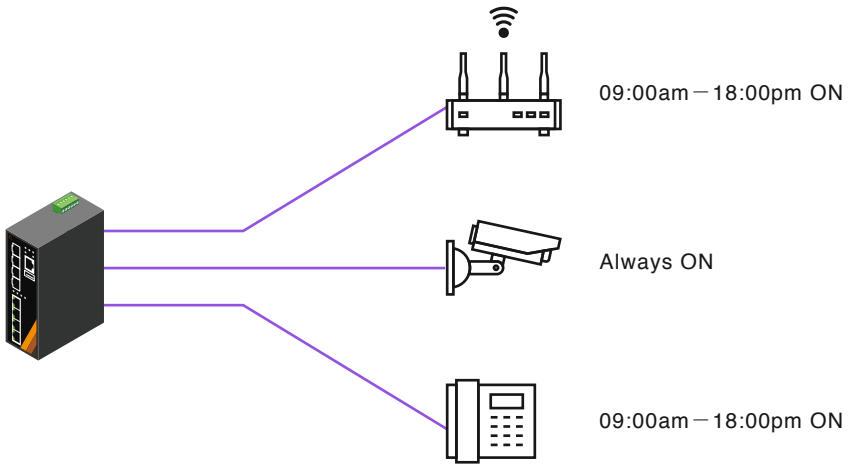






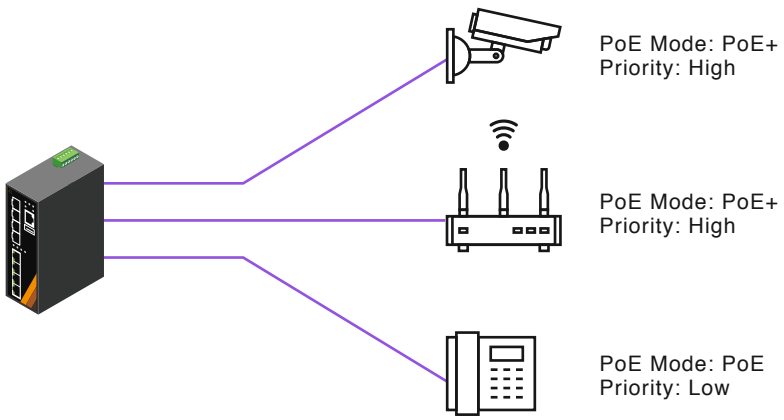
025.

PoE Schedule



026.

PoE Power Priority Management



www.leonton.com
info@leonton.com

Your Partner in Networking