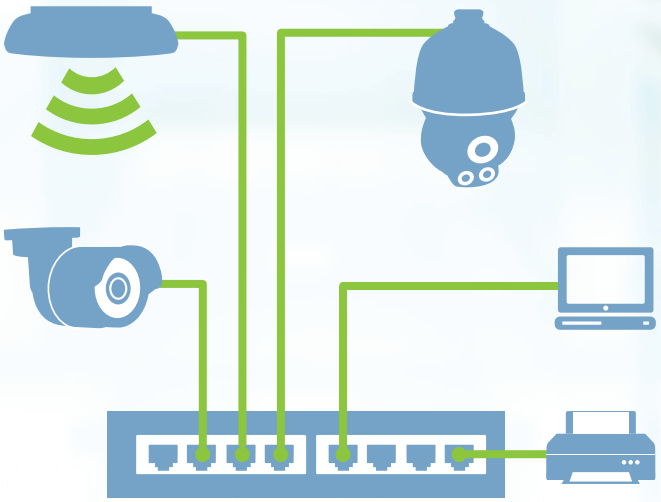
Managed Switches 101

A network switch's basic function is to connect devices together on your computer network. Network switches are available with varying amounts of ports and features to meet the needs and demands of your working project.

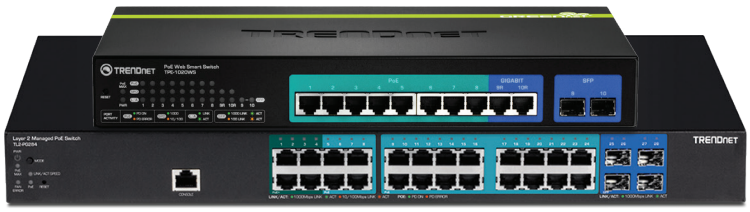
Switches are already "smart" devices; after receiving data, the switch sends that data to a specific device on the network (and not a blanket transmission to all connected devices). This is particularly useful as the switch is able to receive data from all connected devices and transmit that data to specific devices simultaneously.



TRENDnet

Managed vs Unmanaged Switches

Managed switches



Unmanaged switches

There are two types of switches: unmanaged and managed. Amongst those, managed switches are further broken down by varying sub-categories. Simply put, managed switches feature network controls that allow you to customize, manage, and monitor your network. Conversely, unmanaged switches are “plug and play” solutions, designed only to increase port density and cannot be further configured.

TRENDnet offers both unmanaged and managed switches (Layer 2/Layer2+ and Web Smart). Today, not much differs between Layer 2 and Web Smart switches; both Layer 2 switches and Web Smart switches feature a graphical user interface (GUI), however, only Layer 2 switches offer a command line interface (CLI).

The CLI and GUI each have their own advantages and disadvantages. However, a command line interface is generally viewed as more efficient, allows for more control over the system, and is easier to use for remote access. However, it is designed for more advanced network administrators.

Important Managed Switch Features

SNMP
Simple Network Management Protocol is for monitoring the status and management of devices connected to the network.

VLAN
Virtual LAN configurations group devices together to isolate traffic, improve network performance, add an extra layer of security, and reduce unnecessary network traffic.

QoS
Quality of Service allows you to prioritize your network traffic and improve performance (commonly used in VoIP and video applications).

RSTP/STP
Rapid Spanning Tree Protocol and Spanning Tree Protocol are used for redundancy in the network and to prevent looping. RTSP recovers the network from a failed link and locates a new network path in significantly less time than STP.

Port Mirroring
Port mirroring helps to identify and troubleshoot network problems by mirroring data traffic to a designated port on the switch.

IGMP Snooping
IGMP snooping eliminates network congestion caused by multicast traffic. IGMP snooping ensures that multicast data is only forwarded to specific devices that exclusively request the multicast data rather than sending that data to all the devices connected to the network (commonly used in IPTV applications).

TRENDnet