TiFRONT

Cloud Security Switch
for CCTVs

PIOLINK

TiFRONT
Cloud Security Switch for CCTVs

Are you planning to install IP cameras?
Enhance the security with the proprietary switch

Security for the CCTV Network and Password Management for IP Cameras

With the Common Criteria certification, PIOLINK's TiFRONT Cloud Security Switch for CCTVs is the specialized switch for the internal network security and IP cameras' password management.

TiFRONT Cloud Security Switch for CCTVs

TiController

- the switch for CCTVs
- supporting the ERPS

- Security for the CCTV/ Internal Network
- Preventing Ransomware from Spreading

+

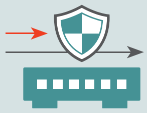
- Managing Information of IP Cameras
- Managing Passwords for IP Cameras

Security measures are needed for the CCTV network, too.

Security Policies on Threats toward the CCTV Network

Security Incidents due to Users' Carelessness

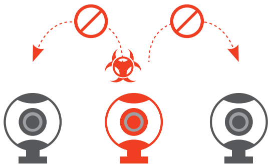
Even if you separate the network to prevent CCTV hacking, security threats can occur. This is because IP camera account manager or outsourced staff can become unintentional attackers when they access the network. The switch for CCTVs is the next-generation switch with internal network security technology.



TiMatrix, a High-Performance Security Engine

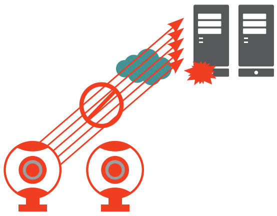
- applying proprietary security algorithm for the internal network security
- blocking malicious traffic, attempts of snatching video, and access from unauthorized terminals
- responding to zero-day threats with no signatures
- maintaining the maximum line speed while running the security features

Blocking Malicious Traffic



Preventing the Spread of Ransomware through IP Cameras

Ransomware is the most frequent malicious code attack in recent years, and the damage is large as well. The switch for CCTVs can minimize the damage by preventing ransomware from spreading through IP cameras.



Blocking DoS Attacks Which Use IP Cameras as Bots

The switch for CCTVs detects and blocks large volumes of traffic from IP cameras and IoT devices. This can prevent internal network failures caused by traffic surges, and block DoS attacks on target hosts.

Access Controls

Preventing IP Camera Video and PC Screens from Leakage

Private data and trade secrets are protected by blocking attacks (e.g. ARP spoofing) which hijack IP camera video and user PC screens.

Internal network access control for unauthorized terminals

It identifies various terminals such as IP cameras, laptop computers, smart phones, etc. using IP/MAC addresses and blocks access to the internal network if they are not registered.

IP Camera Management, TiController Makes It Simple

IP cameras became important not only for security purposes, but also for big data collection sensors in the 4th Industrial Revolution era. In particular, users need to change passwords to prevent IoT hacking attempts as IP cameras have increased industrial utilization by combining AI–based image recognition and analysis technologies.

IP Camera Security Threats and Management Issues

Anybody can try to access an IP camera with a matching IP address.

You can become a target if you use the camera without changing the password.

work efficiency problems such as time and engineers for managing passwords

The Korean government announced plans on the security for IP cameras.
(December, 2017)

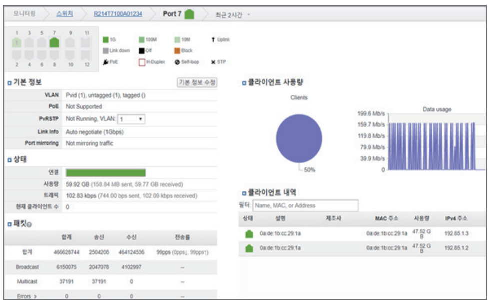
- It is mandatory to set an IP camera password for each terminal and to operate it by changing the password.
- The IP camera security checklist and security certification system are implemented.

Total Management on IP Camera Passwords

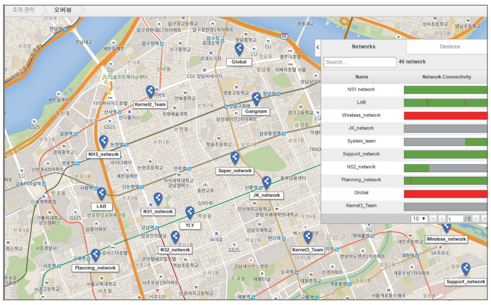
With TiController, the management system of switches for CCTVs, you can change the passwords of multiple cameras at once.

With TiController, you can not only manage passwords, but also use various convenient features to manage internal networks.

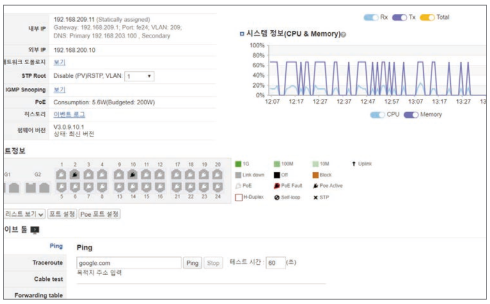
Checking the Statuses of IP Cameras at a Glance



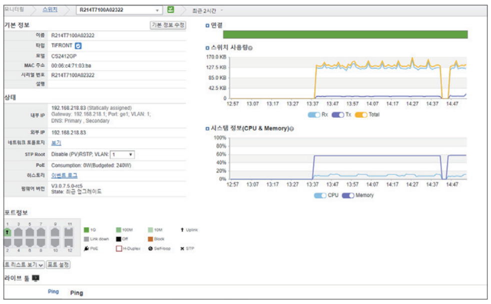
managing information of IP camera management switches



checking locations of IP camera management switches



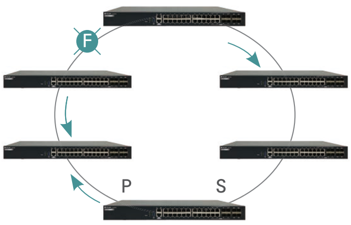
managing problems on IP camera management switches



analyzing traffic statuses in real time

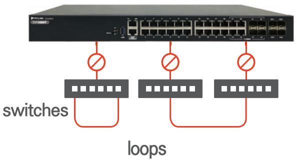
The Optimal Switch for Installing CCTV Networks

Maintaining the Network Stability



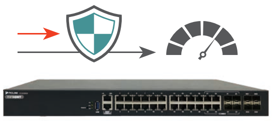
ERPS (Ethernet Ring Protection Switching)

Loops are prevented by blocking specific links on a ring-shaped network.



Preventing Loops for the Non-STP Configurations

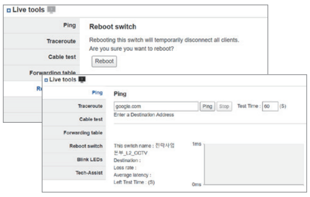
The STP feature is supported as the default. If a loop occurs on a network which does not support the STP, the service can be maintained as traffic overloads are prevented by automatically blocking the ports.



Maintaining the Wire-Speed Performance While Running Security Features

With the high-performance multi-core hardware security engine, the maximum wire speed can be maintained with no latency on the traffic even while checking the security.

Remote Troubleshooting



Reboot switch

Rebooting this switch will temporarily disconnect all clients.
Are you sure you want to reboot?

Reboot

Ping

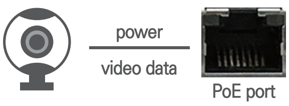
google.com Ping Stop Test Time : 60 (S)
Enter a Destination Address

This switch name : 전략사업본부_L2_CCTV
Destination :
Loss rate :
Average latency :
Left Test Time : (S)

Troubleshooting and Remote Power Controlling with TiController

Without visiting each site, you can check problems on the network and cables with the commands such as “ping” and “traceroute”. Especially if there is a problem on a switch, it is very convenient to restart the system remotely.

PoE



Multiple PoE+ Ports for Connecting to IP Cameras

With a LAN cable, it is possible to support the power supply and video transmission for a pan-tilt-zoom camera at once. From 8 to 24 PoE+ ports (IEEE 802.3at) which support the power of 30 watts.

Noiseless

Fanless Switches

You can use switches even at workplaces as there are no fans with noise.
(available for CC2510G, CC2510GP, and CC2528GXP)

Switches for CCTVs

TiFRONT	CC2510G	CC2510GP	CC2528GX	CC2528GXP
Switch Fabric	20 Gbps	20 Gbps	128 Gbps	128 Gbps
Forwarding Rate	29.76 Mpps	29.76 Mpps	190.48 Mpps	190.48 Mpps
DRAM Memory	256 MB	256 MB	512 MB	512 MB
Flash Memory	288 MB	288 MB	256 MB	272 MB
Ethernet Ports (total)	10	10	28	28
1GbE Copper	8	8	24	24
1GbE Fiber (SFP)	2	2	4 (dual media SFP)	–
10GbE Fiber (SFP+)	–	–	4	4
PoE	–	802.3af, 802.3at	–	802.3af, 802.3at
Power Input	DC 12–48 V	DC 48–57 V	AC 100–240 V (50/60 Hz)	
Power Supplies	external (optional)	external (optional)	single/dual	single
Power Consumption (W)	17	17	30.1 (S) / 30.6 (D)	26 (S)
Dimension (WxDxH, mm)	72 × 118 × 145	72 × 118 × 145	440 × 215 × 44	440 × 331 × 44
Weight (kg)	0.85	0.88	2.75 (S) / 2.9 (D)	6.0 (S)
Fan	fanless	fanless	fans	fanless
IPv6	IPv6 ready logo (Phase II)			
RoHS Compliant	RoHS compliant			
Security Certification	CC (EAL2)			

Details

L2	
Port Management	• auto negotiation / speed / duplex • flow control
VLAN	• port-based/protocol/MAC/subnet VLAN • 802.1Q • hybrid VLAN • private VLAN • ingress/egress tagging • maximum VLAN (4K)
Spanning Tree	• STP, RSTP, MSTP, PvST+, PvRST+
MAC Learning	• MAC address aging • MAC filtering • duplicate MAC address learning prevention • reserve MAC learning prevention • static entry support • independent VLAN learning • maximum MAC entry (16 K / 32 K)
Port Mirroring	• port mirroring (N:N)
Link Aggregation	• LACP • link trunking • LACP load balancing • trunk groups (8) • members per group (8) • static trunk load balancing
IGMP Snooping	• join/leave, multicast group (1K) • v1/v2/v3
QoS	• L2, L3, L4 header-based classification • 8 CoS queues per port • differentiated services • IEEE 802.1p priority • CoS, DSCP, IP precedence • priority marking/remarking • rate limiting/shaping
ACL	• L2/L3/L4-based filtering • VLAN ACL • ACL filter naming • time-based ACL
PoE	• supporting the PoE+ standard (802.3at) • enabling/disabling it for each port • setting priorities of the power supply for each port • blocking the PoE power supply for each port • scheduling the PoE power • monitoring the operation status
Network Redundancy	• ERPS (Ethernet Ring Protection Switching)
Jumbo Frame	• supported

Security	
Anomalous Traffic	• 1-to-1 flooding, random flooding, IP scanning, port scanning, IP spoofing, ARP spoofing, neighbor spoofing, MAC flooding, counting & logging • supporting the IPv4/IPv6 security features • automatically detecting/blocking/cancelling • blocking for each source MAC/IP address • setting exceptions for detection
Protocol Anomaly	• DAD attacks, LAND attacks, teardrop attacks, abnormal L4 source port ranges, same ports (source/destination port number), abnormal TCP flags, TCP fragment attacks, ICMP flood attacks, Smurf attacks
Port Protection	• storm control • limiting the number of MAC addresses
Account Management	• login/logout history • history of running commands
Others	• IP source guard, dynamic ARP inspection, embedded RADIUS, detecting unauthorized wireless routers, detecting devices, DHCP filtering, NetBIOS filtering, detecting self-loops, system access

Management	
SNMP	• SNMP v1/v2c/v3 • public MIB (system, interface, IP address, UCD, router (RFC-1213), protocol (TCP, UDP, SNMP, ICMP), RFC1573 private interface MIB) • private MIB (learning MAC address tables, security configurations) • SNMP trap (authentication, port link up/down)
CLI Interface	• Telnet, SSH, consoles
EMS Interface	• SNMP, syslog, SSH
Authentication	• RADIUS, TACACS+
User Management	• logging in with a password, session timeout configuration, multiple users, authority for each user, multiple configurations
Configuration and OS Management	• updating the OS via TFTP
Logging In/Out	• syslog server, monitoring, log threshold management, backing up logs, monitoring system/security logs
Monitoring	• port statistics, usage rates of the CPU/memory, fans, the watchdog, temperature sensors
Others	• UDLD

TiController (extra options)

Installation	• Zero-Touch Installation: DHCP/static networks, the cellular network • Plug-In: updating the OS and configurations with a USB flash drive • switches' web GUIs
Management	• Multitenancy: role-based • Devices: topology, ports, traffic • Traffic: statistics on traffic usage per network/port/host • Ports: port scheduling • Maps: locations of switches with the network information • Firmware: overall/scheduled updates • Backing up Configurations: automatically backing up configurations • Alarms: notifications about problems on the system • Remote Troubleshooting: live tools, technical assistant • Passwords for IP Cameras • bulk updates on passwords and managing usage history
Passwords for IP Cameras	• bulk updates on passwords and managing usage history
TiMatrix Security	• security level setting (high/middle/low) • flooding / scanning / protocol anomaly setting • ARP spoofing / MAC flood setting • SMB tracing / scanning setting
Others	• traffic storm control • system ACLs
Virtual Configurations	• configuring in advance from TiController even without an actual switch
Virtual Stacking	• managing switches as one without physically connecting them • configuring switches within a network at once

Device Replacement	• applying current configurations without backing them up
Device Configurations (Layer 2)	• VLAN, voice VLAN • MAC learning • port settings • RPVSTP • mirroring • self-loops • ACL • QoS • LACP • LLDP • IGMP snooping • RSPAN (remote mirroring)
Remote Connection	• connecting from a remote console
Topology	• topology map
Host Management	• collecting host information and configuring policies
IT Asset Management	• collecting/sorting/updating asset information
IPT Line Number Chart	• filling out the IPT line number chart
Dashboard	• component-type and alarming dashboard • information on the performance of the device • traffic statuses on hosts and ports • network alarms
Log Management	• security logs, event logs, audit logs
Reports	• user-defined reports • scheduled reports

Recommendations for Deployed TiController

	TiController 100	TiController 500	TiController 1000
Type	hardware appliance	hardware appliance	hardware appliance
CPU	1 x Intel Xeon 3.0 GHz	1 x Intel Xeon 3.0 GHz	2 x Intel Xeon 2.1 GHz
Memory	16GB	64GB	128GB
HDD	1 x SATA-Ⅲ 1TB	4 x SATA-Ⅲ 1TB	8 x SATA-Ⅲ 1TB
Size	1RU	1RU	1RU
Managed Switches	up to 100 units	up to 500 units	up to 1000 units
LAN	2 x gigabit Ethernet	2 x gigabit Ethernet	2 x gigabit Ethernet

PIOLINK

PIOLINK, Inc. | global@piolink.com | www.PIOLINK.com

- Depending on the product's upgrade and correction of printing errors, PIOLINK, Inc. reserves the right to change specifications at any time without notice.
- The images may vary from the actual appearances.
- All names of the companies, products, and service are registered.
- All products can be purchased from authorized partners. All information is available at PIOLINK's sales department or website.