

# ITAC10120 ITAC10130



# User manual Web Management

Originalbedienungsanleitung in deutscher Sprache. Für künftige Verwendung aufbewahren.

This user manual contains important information for installation and operation. This should be also noted when this product is passed on to a third party. Therefore look after these operating instructions for future reference!

CE

Version 05/2019

# Inhalt

1	Ac	cess	to Web Management	. 5
	1.1	Acc	ess to Web Management	. 5
	1.2	Acc	ess to Web Management via CLS Port	. 5
2	Re	set		. 5
3	We	eb Ma	anagement	.7
	3.1	Sys	tem Status	.7
	3.2	Por	t setting	. 8
	3.2	2.1	Port speed limit	.9
	3.3	VL	AN settings	10
	3.3	.1	VLAN Forwarding	11
	3.4	Tru	nk Management	12
	3.5	RS	ГР	13
	3.5	5.1	STP Basic Concept	13
	3.5	5.2	RSTP	15
	3.6	Por	t Security	16
	3.6	5.1	802.1X certificates	17
4	We	eb Ma	anagement	19
	4.1	SNI	MP Settings	19
	4.2	Ema	ail Alarm	20
	4.3	Por	t Mirror	21
	4.4	IGN	AP Snooping	22
5	Ne	tworl	k Statistics	23
	5.1	MA	C Address	24
6	Sys	stem	Management	25
	6.1	IP A	Address	25
	6.2	Log	Information	26
	6.3	File	Management	27
7	Po	E Ma	nagement	28
8	Qo	S Ma	anagement	30

# 1 Access to Web Management

### 1.1 Access to Web Management

To connect to the web management interface, connect a network cable to any of 1-16/1-24 RJ45 port and enter the following data into browser.

The default factory settings are:IP-Address:192.168.1.200User:adminPassword:admin

# 1.2 Access to Web Management via CLS Port

To connect to the web management interface, connect a console cable (RJ45 -> R232 serial port 115200,8, N, 1) to the CLS port, to the PC at the serial port (DB9) and enter the following data into the browser.

The default factory settings are:

IP-Address:	192.168.1.200
User:	admin
Password:	admin



# 2 Reset

### Restart:

Press the reset button to restart the switch.

### Reset to default factory settings:

Press the reset button for more than 10 seconds to reset the switch to default factory settings.

GB

The factory default settings of the device are as following:

	Options	Default Configuration
System	Username / password	admin/admin
	IP-Address	IP-Address : 192.168.1.200
		Subnet Mask : 255.255.255.0
	MAC address table aging time	300 Seconds
Port	Ports Status	Enable
	Ports Speed Rate	Auto-negotiation
	Ports duplex mode	Auto-negotiation
	Flow Control	Open
	Trunking	Port does not converge
	Port Speed Limitation	No limitation for Speed
	Port Link Type	Access
	Management VLAN	VLAN 1
	VLAN Function Mode	Port-based VLAN
М	AC Binding	No Binding
RSTP	RSTP Function	Close
Network Management	SNMP	Close

# 3 Web Management

# 3.1 System Status

	Description
Word Time Zone	Select your time zone or select "Automatically". Select "Adjust Daylight Saving Time" for automatically DST correction.
Time Configuration	Select "Local Time" or use NTP function.
NTP Server	Enter the correct NTP server's IP address to start the sync.
System Time	The current time of the device, if you did not get the NTP updated time, then it will start to count from 0:00,1970.
PC Time	Computer current time.
Device Name	Enter the Name of the device. Network identification device used to facilitate the integrated management tools such as SNMP to judge different equipment.
Contacts	Enter maintenance personnel's contact information.
Contact Address	Enter maintenance personnel's contact information.
MAC Address	MAC Hardware address of the device.
Hardware, Software Version	Current running / installed version of hardware and firmware.
Running Time	The total time device has been running. When the device is restarted, the time is reset.

# 3.2 Port setting

On the [Port security / Port Settings] page, you can observe the status and make different settings for ports.

	System stat	tus   Port setting   PoE   VLAN   QoS   L	ACP   Port security   Netv	vork managemer	nt   Network statistics   Sy	Eng stem manage	alish 🛩 ment   Exit
Port setting>	>Port setting						
Port setting							
Port enable		Enable					
Port rate		Auto negotiation 💉 Dug	plex mode Auto negotiation	~			
Flow control		Enable 💌					
Port range		Ок	Refresh				
	1000000		Current status	1	Port status		
	Port	Port mark(Double-click to modify)	(speed/duplex)	Port property	Port rate(speed/duplex)	Flow control	Port enable
	1	port1	no link	Copper	100M/Auto	enable	enable
	2	port2	no link	Copper	Auto/Auto	enable	disable
	3	port3	no link	Copper	Auto/Auto	enable	disable
	4	port4	no link	Copper	Auto/Auto	enable	enable
	5	port6	no link	Copper	Auto/Auto	enable	enable
	6	port6	no link	Copper	Auto/Auto	enable	enable

	Description
Port Enable / Disable	Enabled by default.
	Enable or disable a certain port.
	If a port is disabled, you cannot transmit any data on this port.
Port Speed Rate	Auto-negotiation mode by default.
	Possible speed settings: 10M, 100M, 1000M, Auto-negotiation.
	Auto-negotiation means, that the port can automatically negotiates the port speed with the other connected device
Duplex Mode	Auto-negotiation mode by default.
	Possible settings: including full-duplex mode, half-duplex mode, and Auto-negotiation mode
Flow Control	Enabled by default.
	Enable or disable Flow control.
	When two switches have enabled the flow control function, if one of the two switches are congested, it will send a message to the other switch to notify it to temporarily stop sending messages or slow down the sending speed. After receiving the message, the other switch will stop sending or slow down the sending speed of messages to avoid packet loss and ensure normal operation of notwork sendices

# Attention:

- Uplink optical port 25 and 26 are fixed at 1000Mbps.
- Uplink ethernet ports 27 and 28 are fixed at 10/100 / 1000Mbps adaptive.

# 3.2.1 Port speed limit

Users can restrict every port traffic flow. Port restrictions including Unicast packets, Multicast packet and broadcast packets. The accuracy is 1Mbps.

The range is:

- For downlink ports 1~1000Mbps
- For uplink ports 1~ 1000Mbps

Syst	tem status   F	Port setting   PoE   VLAN	QoS LACP Port see	curity   Network mana	agement   Network st	English atistics   System management
Port setting>> Spee	d limit					
Bandwidth setting		🛛 Enable 💿 Disable				
Port range		1				
nput speed			Mbps			
Limited type		Broadcast packet	The unknown multicast	Unknown Unicast	Known multicast	Known item on Edit
	Port	Port	mark	Input speed		Limited type
	1	po	rt1	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	2	aaaa	aport2	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
<b></b>	3	po	rt3	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	4	port4	SSSS	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	5	po	rt5	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	6	SSSS	Sport6	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	7	po	rt7	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	8	DDD	DDDD	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	9	DDDDD	DDDDD	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast
	10	po	t10	50Mbps	Broadcast	UknMcast UknUcast Mcast Ucast

	Description
Bandwidth	Off by default.
Settings	
on / off	Enable or disable the port speed limit.
Port Range	The port for speed limit.
Input Rate	The max. input rate of each port.
Limited type	Port limited type, including all Unicast packets and multicast

# 3.3 VLAN settings

The switch supports two VLAN modes:

#### Port-based VLAN mode:

Define VLAN members according to device port. After you specify the port to a VLAN, specified VLAN Packets can be forwarded by the port.

#### 802.1Q VLAN mode:

Defined by IEEE802.1Q protocol. Process the packets by identifying the packets tags.

On the [VLAN / Port VLAN] page, you can observe and change the VLAN settings.

-	System st	atus   Port setting   PoE   V	LAN   QoS   L	ACP   Port security   N	etwork management   Network :	English 💌 statistics   System management   Exi
VLAN>>Port	/LAN					
Port range						
Link type		Direct connect terminal 💌				
Default VLAN	ID					
VLAN forward	ing list					
Vlan-untagge	d mark list		ОК			
	Port	Port mark	Link type	Default VLAN ID	VLAN forwarding list	Vian-untagged mark list
	1	port1	Access	123		
	2	port2	Access	123		
	3	port3	Access	123		
	4	port4	Access	123		
	5	port5	Access	123		

	Description
Link type	Access: port belongs to one VLAN, which is normally used for connecting devices. By default, all ports are Access ports.
	Trunk : port belongs to multiple VLANs and can receive and send multiple VLAN packets. It is normally used to connect network devices.
Default VLAN ID	Enter the ID number (generally 1 – 4094).
VLAN Forwarding list	Enter the ports that VLAN packets can be transferred.
VLAN untagged mark list	Port forwarded packets can be set in VLAN.

# 3.3.1 VLAN Forwarding

On the [VLAN / VLAN forwarding] page, you can observe the current port VLAN forwarding settings.



	Description
VLAN ID	Change VLAN ID.
VLAN Name	Change VLAN name.

# 3.4 Trunk Management

TRUNK means port convergence. After configuration two or more physical ports to become a logical path to increase the bandwidth between switches and network nodes.

On the [LACP / TRUNK] page, you can observe the current port link convergence settings.

Network manageme	1t>>LACP			
LACP Setting				
Load Balance	SRC MAC	*		
Trunk Group	Trunk-			
Trunk Mode	Manual LACP 👻			
Port Range		Add Del		
Index	Trunk Group Mode	Port Range	Port Status	

# Attention:

Each convergence group supports up to eight ports. Ports with the following cases cannot be added to an convergence group:

- Port with 802. 1X function
- The mirror port
- Port with MAC address binding

In the same convergence group, the port speed, duplex mode, and basic configuration must be consistent.

STP consistent configuration, including STP ports on / off, STP priority, STP cost, whether to open loop guard and root guard, or edge ports.

QoS configuration is consistent.

VLAN consistent configuration, including permitted VLAN, the default port of VLAN ID. Link type on the ports is consistent.

# 3.5 RSTP

STP (Spanning Tree Protocol) is established in accordance with IEEE 802.1D standard. It is developed for the elimination of the data link layer loops in the LAN protocol. Devices running this protocol exchange packets with each other to find loops in the network and choose to block some certain ports. This will eventually make the loop network structure into a loop-free tree pruning network structure. Thus it prevents packet proliferation and infinite cycling in loop network, avoiding declined processing capacity and receiving same messages repeatedly.

STP contains two meanings, narrow meaning of STP is defined in IEEE 802. 1D, board meaning of STP includes IEEE 802.1D defined STP and various enhanced spanning tree protocol produced on the basis of STP (such as RSTP protocol).

# 3.5.1 STP Basic Concept

The root bridge

STP introduces the concept of root bridge, since network structure tree must have a root. Only one root bridge and the root bridge will change when the network topology changes, so the root bridge is not fixed.

### The path cost

Path cost is a reference value for STP to select a link. By calculating the path cost of STP, STP chooses stronger links to block redundant links and cut the network into a loop- free tree topology.

### The port role

Root port:	Responsible for forwarding data to the root port.
Designated port:	Responsible for forwarding data to the downstream of network segment or switch port.
Block Port:	Port suppressed by other' s specific ports.

Port status	
Forwarding:	Forwarding user traffic, only the root port or designated port have this condition.
Learning:	The switch builds the MAC address table according to user traffic received (but not forwarding traffic).
Listening:	The completion of the root bridge, select the root port and designated ports.
Blocking:	Only BPDU is received and processed, no user traffic forwarded.
Disabled:	Consider blocking or link disconnection.

# The designated bridges and designated ports

Classification	Designated Bridge	Designated Port
For equipment	Equipment connecting directly with switch and responsible to transfer BPDU message to switch.	Port used by designated bridge to transfer BPDU message to switch.
For LAN	Responsible to transfer BPDU message to local network segment equipment.	Port used by designated bridge to transfer BPDU message to local network segment.

# 3.5.2 RSTP

RSTP (Rapid Spanning Tree Protocol) is an optimized version of STP. It is" fast" because the delay is shortened under certain conditions when a port is selected as the root port and designated port to enter to the forwarding state, thus the time to reaching topology stability is greatly reduced.

On the [LACP / RSTP] page can observe the current port RSTP settings.

	System stat	lus   Port setting   PoE	VLAN   QoS   LACP   Port sec	urity   Network manage	ment   <u>Network statistics</u>   S	English ystem management   E			
LACP>>RS	TP				Flow statistics MAC table				
RSTP settir	lg 🛛	• Enable • Disable							
Device prior	ity								
Sending me	essage interval	2	second (1-10)						
laximum m	nessage lifetime	6	second (6-40)						
Changing port status delay 🗄 second (4-30)									
Network bri	dge information	RSTP							
		Path expenditu	re Port priori	ty Po	int to point port	Edge port			
modily c	oninguration	0	0						
Por	rt range		Modify						
	Port	Por mark	Path expenditure	Port priority	Point to point port	Edge port			
	1	port1	automatic detection	128	NO	YES			
	2	port2	automatic detection	128	NO	YES			
	3	port3	automatic detection	128	NO	YES			
	4	port4	automatic detection	128	NO	YES			
	6	portE	automatic detection	128	NO	VES			

	Description
Device priority	As the network bridge priority, network bridge and network bridge MAC address combined as bridge ID, of which minimum bridge ID will become the root network.
Sending message interval	The interval needed to send a BPDU data packet.
Maximum message lifetime	Means the validity of a BPDU data package received from another switch.
Changing port status delay	The forward delay of a switch port status in transition status (listening and learning).
Path expenditure	Setting port path cost, only setting when port default path cost on "off" status. Port link cost, with port priority and port ID form port ID to compare Value range 1~200000000. "0" means automatic check.
Port priority	By default port priority is 128. The priority of port in network bridge, with port priority and port ID form port ID to compare.
Point to point port	Switch port and switch connected directly, then this port is P2P port, RSTP adopts negotiation mechanism for P2P port so as to achieve quick transformation of port status.
Edge port	The network edge switch generally connects with terminal equipment's, such as PC workstation. To configure these terminal ports to Edge ports can achieve status of transformation port without discarding Learning and forwarding transformation course.
RSTP	Check RSTP information and port information.
mormation	

# 3.6 Port Security

# Statics Address Latch

Statics MAC address is to limit computer operation. The computer with binding computer MAC and ports cannot communicate with other ports, while other computer can do that.

On the [Port security/Stastic address lock] page displays switch information of statics address latch.

Port security>> Stastic addre	ss lock		Flow statistics MAC table	
Stastic address lock	Enable Oisable			
MAC address				
VLAN ID				
Port				
		OK Cancel		
	No.	MAC	VLAN ID	Port

	Description
MAC Address	Static MAC address differs from the general MAC address. Once a static address is added, the address will remain in effect until be deleted.
VLAN ID	Port-corresponding VLAN ID number.
Port	Select a static MAC address to forward a port. You can only specify one forwarding port.

# Attention:

This feature is a security mechanism which requires high attention to the settings.

- Do not use a multicast address.
- Do not enter the reserved MAC address, such as local MAC address. For a port which has already been added to an aggregation group, it is not allowed to set binding function between port and MAC address.

#### 3.6.1 802.1X certificates

IEEE 802.1X certification system adopted the "controllable port" and "uncontrolled ports" logic functions. It can realize the separation of business and certification. After passing certification, the business flow and the certification flow separation, it has no special requirement for the following subsequent packets. Business can be flexible, especially in develop broadband multicast business, it has a lot of advantages. All the business is not restricted by authentication.

802.1X Three Main Parts :

Application supplicant: User and Client which want to get the certification.

Authentication server:

A typical example for the RADIUS server.

#### Certification System authenticator:

Between the end devices, such as wireless access points, switches, etc. They can play at the same time equipment system and authentication server two characters, you can also use the additional authentication server, at the same time support the billing system.

In the [port security / 802.1X authentication] page, you can modify / 802.1X authentication function settings.

						English		
S	ystem status	Port setting   Po	E   VLAN   QoS   LACE	P   Port security   Network man	agement   Network statisti	cs   System management   Ex		
Port security>>80	1.x certificatio	n						
Global setting		🔍 Enable 🎯 🛙	isable					
iming update cer	tification	3600	Second [60 - 40,000,00	10]				
ladius server		Local  Re	mote					
		IP address						
Hadius server setting		Share secret ke	Y .					
Convor part cotting		Billing server p	ort [0 - 65535]					
server port seming		Certification se	IO - 6553	5]				
Port setting		Control mode		Port control n	nethod	Maximum user quantity		
		Auth	orized-force	MAC Based	-			
ort range			Edit	]				
-	Dire			Setting status				
-	Port		Portmark	Control mode	Control method	Maximum user quantity		
	1		port1	Authorized-force	MAC Based	4096		
E3	2		aaaaaport2	Authorized-force	MAC Based	4096		
	3		port3	Authorized-force	MAC Based	4096		
13	4		port4ssss	Authorized-force	MAC Based	4096		
	5		port5	Authorized-force	MAC Based	4096		
	6		SSSSSSport6	Authorized-force	MAC Based	4096		
	7		0.047	Authorized force	MAC Based	4006		

	Description
802.1X config	The is default off.
	Turn 200 4V contification On/Off
Regularly	The certification cycle time, used to enhance the security of
update the	authentication.
certification	
Radius Server	If you select internal Radius server, applicants will only be used inside the Radius database users and password.
	If you select external Radius server, you will need to fill in the authentication server IP address and Ports.
	If you need to use the AAA billing system, fill in server setting IP address and Ports.
Authentication	The default port is 1812.
server IP	
address	Radius Remote access authentication server.
	Set the IP address/domain is device can access to.
Shared key	For device access authentication server Shared password string.
Service port	The default port is 1813.
settings	
	Server implementation is the function of billing, set the IP
	address/domain is equipment can access to.
Control mode	Compulsory licensing model respectively, and the automatic
	mode, mandatory unauthorized mode.
Port Control	MAC Based.
mode	
Max ID list	Scope :1-4096.

### Attention:

Between the applicant and the authentication system using MD5 - inquiry, do not support others.

If the network connection properties are without "authentication" option, please select "attachment" - > "management tools" - > "component services" - > "service", set "Wired AutoConfig" to "automatic".

Billing server setup error will also lead the applicant cannot be authenticated. No billing server needs to be set up.

All uplink or downlink ports must be forced through the authentication, or prohibit the use of certification, otherwise can't use the remote server, unless you use the internal authenticated server.

When using the remote server, the administrator can access the remote server, be sure to confirm equipment displaying device address of the gateway set up correctly. If you use the domain name the DNS must be set correctly.

# 4 Web Management

### 4.1 SNMP Settings

SNMP is used to ensure the management information transferred between any two points, so that network administrators can easily retrieve information on any node on the network to modify information, fault search, troubleshooting, capacity planning and report generation.

SNMP contains NMS and Agent, of which NMS is a workstation running the serverside program, while Agent is the client software running on network device. NMS can send request message to Agent, after Agent receive request message from NMS, it starts to read or write and generate response packets and send the response packets back to the NMS.

On the [Network management / SNMP Settings] page, you can enable / disable the SNMP settings.

System status	Port setting   PoE	VLAN   QoS   L	ACP   Port security   N	etwork management   I	Network statistics   Syste	English m management   E	<b>∽</b> ×it
Network management>> SNMP	setting						
SNMP setting	• Enable • Disa	able					
SNMP gateway							
SNMP version							
Read-only community name	oublic						
Read-write community name	privale .						
SNMP V3							
Username			Read-w	rite method			
identify authentication			Verify p	assword		3	
Encryption protocol			Encrypt	ed password	1		
				6			
🔲 No. User na	ame Identify a	uthentication	Verify password	Encryption protocol	Encryption password	Read-write metho	d
		R	efresh Save	Help			

	Description
SNMP Gateway	Agent send the network IP address from receiver who send abnormal alert.
SNMP version	Only support V1/V2/V3 version.
Read-only community name	A SNMP community named after a string, the group only has permission to operate.
Read-write community name	A SNMP community named after a string, the group has permission to Get and Set operations.

# Attention:

Community name: used to define the relationship between the SNMP manager and an SNMP agent. If the community name SNMP packets have not been recognized by the device, the packet is discarded. You can use the standard community name (public or private) or a user-defined group name.

# 4.2 Email Alarm

The device if it is running an event supervision, the supervision sends an alert message to defined Email recipients when something wrong about defining time and some abnormal event occurs. Supervision also periodically send all log messages to predefined recipients.

On the [Network management / Email alarm] page, you can turn on / off Email alarm settings.

System	status   Port setting   PoE   VLAN   QoS   LACP   Port security   Network management   Network statistics   System management	Ex
Network management>	>Email alarm	
Email alarm	Enable O Disable	
Mail server		
Mail accountant		
Mail password		
Receiver address		
Mail reply address		
Mail interval		

	Description
Mail Server	The host computer's IP address or the host computer that provide
	POP3 Email delivery service to our devices.
Email	The account name for logging in email server.
Accounts	
E-mail	The password to the account name for logging in email sever.
Password	
Recipient	The email address used to inform recipients of abnormal events.
Address	
Email Reply	The email address that can help solve abnormal events.
Address	
Mail interval	The interval time that regularly send log and weekly reports.

# Attention:

Some email service system requires that the "email reply address" should match the "email account". When sending system test email, the password should be in plain text. The test mail cannot be sent if the password is "empty".

# 4.3 Port Mirror

Port mirroring refers to copying the monitor port data to a designated monitoring port for data analysis and monitoring. The Ethernet Switch supports multiple mirroring to one mirroring, which Copy packets from multiple ports to a monitor port. User can also specify the direction of monitored packets, such as only monitor designated ports message. Equipment using port mirroring group way to configure port mirroring. Every port Mirror include monitoring port and be monitored port.

In the [network management/ port Mirror] page, which could modify [port Mirror] function settings.

	Description
Port Mirror	The default is off.
	Turn Port Mirror Function on/off.
Monitor Port	Select Port for monitoring.
Mirror Port	These ports collect designated direction data from be monitored
	ports.
<b>Data Collection</b>	Specifies the monitor port data direction:
	"all data", "data import" and "export data"

### Attention:

This feature must be turned off in normal use, otherwise, all based on advanced management capabilities port can use such as RSTP, IGMP, SNOOP.

Mirroring only handles normal packet FCS, cannot handle all kinds of erroneous data frame.

To replace the mirror port or monitor port, directly input monitoring port number or Mirror port number.

# 4.4 IGMP Snooping

Switch IGMP membership report message to the router IGMP membership through intercepting mainframe. Form Corresponding relationship between group members and switch interfaces. Switch transfer multicast packets be received to member group ports according to Correspondence.

The [Network Management/ IGMP Snooping] Page, Modify and setting [ IGMP Snooping] function.

System status	Port setti	ng   PoE   VLAN   (	QoS LACP Poi	t security	Network management	Network statistics   System m	English 📃 💌 anagement   Exit
Network management>>IGMP S	nooping						
IGMP snooping function	O Enat	ole 🔵 Disable					
IGMP inquiry	• Enal	ole O Disable					
IGMP inquiry interval	125	Second (60-1000)					
Group members life time	300	Second (120-5000	1				
Stastic multicast table configura	ition						
Stastic multicast MAC address	1		VLAN ID				
Port range			Add	Delete			
No.		multicas	t address		VLAN ID	Port number	Туре
			Refresh	Save	Help		

	Description
IGMP	The default is disabled.
Snooping	Enchle en dischle the Multicest Openning function
	Enable of disable the Multicast Shooping function.
IGMP Inquiry	Enable or disable the IGMP Multicast Inquiry function.
IGMP Query	Set interval for query interval.
interval	
Member	Set Existing multicast Member survival time.
Existing Time	
Unknown	How to transfer those ports when the received multicast address
multicast	does not exist in the address table.
group	
forwarding	
table	

# 5 Network Statistics

On the [Network statistics / Flow statistics] page, you can view the number of data packets and bytes transferred for each port.

ork states	ibcs>>>tow statistics	1.5000						
Port	Classics and the skines	Sent In	mo	Canada and a second	Cincil a sect on a log and	Received	frame	Free sectors
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	o	0	0	0	0	0
5	0	0	o	0	0	o	0	0
6	0	0	o	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

	Description
Receive Frame	The received address is the number of packets in the unicast
Singlecast	address.
Package	
Receive Frame	The received address is the number of packets in the multicast
Multicast	address.
Package	
Receive Frame	The sent received address is the number of packets in the
Broadcast	broadcast address.
Package	
Receive Frame	Error package numbers due to various wrong reasons sent and
Error	received by ports.
Package	
Send Frame	The sent address is the number of packets in the unicast address.
Singlecast	
Package	
Send Frame	The sent address is the number of packets in the multicast
Multicast	address.
Package	
Send Frame	The sent address is the number of packets in the broadcast
Broadcast	address.
Package	
Send Frame	Error package numbers due to various wrong reasons sent and
Error Package	received by ports.

# 5.1 MAC Address

MAC (Media Access Control) address is the hardware identification of network equipment. Switches could transfer message according to MAC address. The MAC address is unique ,which ensures the correct message. Every switch maintains a MAC address table, in which, the MAC address corresponds to switch ports. The switch could decide to filter this data frame or transfer data frame to corresponding port according to MAC address table when the switch receives data frame. MAC address is the basic and premise for data frame fast forwarding.

On the [Network statistics /MAC table] page, you could check MAC address of each port.

System statu	s   Port setting   PoE   VLAN   QoS   Li	ACP   Port security   Net	work managemer	nt   Network statistics	System management   E
letwork statistics>>MAC tabl	e			MAC table	
IAC table inqury					
nquiry by physical port					
nquiry by MAC address type	All type				
		Inquiry			
No.	Source address	VLAN ID	Туре	Port	Process mode
1	20:4E:7F:89:DB:97	1	Dynamic	28	forward
2	00:24:8C:95:AD:4C	1	Dynamic	28	forward
3	50 E5:49 AF:46:97	1	Dynamic	28	forward
4	54:04:A6:D5:BB:6F	1	Dynamic	28	forward
5	14:DA:E9:93:02:64	1	Dynamic	28	forward
6	00:0C:29:29:D2:60	1	Dynamic	28	forward
7	00:1F:29:9A:88:E6	1	Dynamic	28	forward

	Description
Inquiry by	Enter MAC address to check/filter.
physical port	
Inquiry by MAC	MAC address type consists of static MAC address and dynamic
address type	MAC address.

# Attention:

Multicast MAC address table is displayed in IGMP snooping table. All these address tables are unicast addresses. The permanent static address is configured in static MAC address port table. You need to modify corresponding entries when the port changes. The aging time of MAC address is 300s, after port disconnected , the upper port operation procedures clear all correspond port entries.

# 6 System Management

#### 6.1 IP Address

On this page, you can check the IP address for this device.

System management	>>IP address	
Access	Static IP    Dynamic IP	
IP address	192.168.1.184	
Subnet mask	255.255.255.0	
Default gateway	192.168.1.1	
DNS address	202.96.134.133	

### Attention:

Please fill in correct DNS address when using it for NTP and Email.

#### User Management

On this page, you can modify or add one user with password.



	Description
User Index	User index indicates the group of users. There are three user indexes in drop down table.
Visit Level	Administrator:View and set all settings.User:View and set only some functions.
User name	The identification of the user.
Input Password	Enter user password.
Confirm Password	Confirm above entered password.

# 6.2 Log Information

The log function allows users to access information of the system operation. When this function is enabled, corresponding events are recorded to the log:

- System restart
- Port Link Down/UP
- Power supply status
- Login information
- Broadcast storm
- System action and operation record
- NTP time synchronization information
- Other system information

On the [System management/ Log information] page you could check the time and type of event.

tomoto lon sen	or O Engli	la O Dimabia	
.og server addre	tas		Record lowest grade notifications N
nformation proc	essing Dow	nioad Delete	
No.	Type	Time	Evont
1	LINK	2014-11-06 13:21:30	Port G0/28 Link Up!
2	CONFIG	2014-11-07 16:30:45	User login successful - IP-217-23.89.110 Name:admin
3	CONFIG	2014-11-07 16:28:26	System time is changed as Local - IP.217.23.89.110 Name admin
4	CONFIG	2014-11-10 11:24:20	User login successful - IP:192.168.1.16 Name admin
5	CONFIG	2014-11-11 10 12 46	User login successful - IP: 192.168.1.16 Name.admin
6	CONFIG	2014-11-11 10:37:51	User login successful - IP:192.168.1.16 Name:admin
7	CONFIG	2014-11-11 16:38:06	User login successful - IP:192.168.1.16 Name:admin
8	CONFIG	2014-11-19 09 30:46	User login successful - IP 192 168.1.16 Name admin
9	CONFIG	2014-11-19 09:47:51	User login successful - IP 192 168 1 16 Name admin

	Description
Log Sever address	The server address receiving the log information.
Record lowest grade	There are eight optional levels: error information, notification information to be logged, information in need of quick reaction, serious information, information that cannot be used in system, normal but important information, information in debug, warning information.
Download	Download all information (File format *.cfg).
Delete	Deleted all information.

# 6.3 File Management

On the [System management/ File management] page you can check configure document, software upgrade, restore factory setting and reboot system.



	Description				
Configuration File	Backup switch configuration (File format *.cfg)				
	Restore switch configuration (File format *.cfg)				
Software	Select file to perform firmware update.				
Update					
Restore	Set switch to default settings, except for IP address, user name				
Factory	and password.				
Defaults					
System Reboot	Restart system and return to system status page.				

# 7 PoE Management

On PoE management page, you can turn on/off PoE function, set input power, maximum overload, reservation power etc.

PoE							
Power settin	ng (Be careful for modif	cation)					
Power provid	ted 360 W	Overload limit 5 %	Reserved rate 15 %	ОК			
Power statu	s						
Consumed	sumed W Remaining NaN		Reserved 54 W	Provided	Provided 360 W		
Port status a	and control						
Portrange		Priority Low	Power limit 25 W (0-99	W) ON	OFF	OK	
	Dent	Destaurt		Setting			
-	Pon	POILINAIK	Consumed (vv)	Power limit (W)	Priority	Port status	
	1	port1		25	Low	open	
	2	port2		30	Low	open	
	3	port3		30	Low	open	
	4	port4		30	Low	open	
	5	port5		30	Low	open	

### Attention:

Please do not modify the input power, if the setting value is more than the actual power of the built-in power, there will be a risk of overload burning. If the setting value is less than the actual power for the built-in power supply, it cannot be fully allocated out.

Each port of the product is to provide maximum output power of 30W, if user setting exceeds 30W, 30W is still the maximum power output only.

	Description				
Power	Determined by built-in power supply module and cannot exceed				
provided	maximum power supply.				
Overload limit	The default is 5%.				
	Built-in power supply allows overload rate. Setting range 0% $\sim$				
	10%. If actual output power is overlarge, the system will power off ports with lower priority.				
Reserved rate	Reservation power cannot be used for distribution, but can be used for PD consumption caused by overload change. The default is 15% of the total power. The larger this number, the smaller the risk of system overload. So the usable power for distribution and PD quantity become less. On the contrary, the more the number of PD access, the greater risk of system overload.				
Consumed	Actual total power output.				
Remaining	Means power that could be used for redistribution. Surplus = input - actual output - reservation. Please note that when insert a new PD equipment, the power will be distributed based on the detected PD power level instead of the actual power of inserted PD , for example : when surplus power is 20W, the system still cannot distribute power nor supply power if insert power level of PD is 25 5W and the actual power only				
	requires 10W.				
Reserved	Used for PD consumption with overload changes. It stems from the set menu "input power rate * reserve power".				

Provided	Total power for system setting.			
	It stems from the set menu "input power".			
Priority	There are three levels for port power: "low", "middle", "high".			
	Supply priority: when the system is overloaded, the power supply			
	of the port with low priority will be turned off firstly.			
Power limit	Set the output power limit for single port. The port will power off			
	when actual output power exceeds limit.			
On / Off	Turn PoE Port Power on / off.			
Setting	Set port priority for maximum power consumption.			

# 8 QoS Management

On the [QoS management/QoS Settings] page you can modify the QoS function.



	Description				
QoS Setting	The default is Off.				
	Turn QoS function on / off.				
802. 1P QoS	Set traffic priority.				
Setting	The highest priority is 7, then to 6、5、4、3、2、1、0				
802. 1P Scope	The default is 0.				
	Possible values 0-7.				
Priority	Set que priority.				
	The highest priority is 7, then to 6、5、4、3、2、1、0				

# DSCP7TOS QoS

On the [QoS Setting/ DSCP/TOS QoS] page you can modify the setting [DSCP/TOS QoS.

								English
Syste	em status   P	ort setti	ng   PoE   VLAN   Q	oS   LACP   Port s	ecurity   Network mai	nagement   Netwo	rk statistics   System	management   E
QoS>>DSCP/TOS Qo	s							
DSCP/TOS QoS setti	ng	O Ena	ble 🔍 Disable					
DSCP mark range								
DSCP priority		0	- Set					
DSCPMark	Priority	ŝ. Î	DSCPMark	Priority	DSCPMark	Priority	DSCPMark	Priority
0	0		1	0	2	0	3	0
4	0		5	0	6	0	7	0
8	1		9	1	10	1	11	1
12	1		13	1	14	1	15	1
16	2		17	2	18	2	19	2
20	2		21	2	22	2	23	2
24	3		25	3	26	3	27	3

	Description
DSCP/TOS QoS	The default is off.
	Turn DSCP/TOS QoS function on / off.
DSCP Scope	Identifies TOS scope (0-63)
DSCP Priority	Set TOS Priority.

# Impressum

Diese Bedienungsanleitung ist eine Publikation der ABUS Security-Center GmbH & Co. KG, Linker Kreuthweg 5, 86444 Affing. Alle Rechte einschließlich Übersetzung vorbehalten. Reproduktionen jeder Art, z.B. Fotokopie, Mikroverfilmung, oder die Erfassung in elektronischen Datenverarbeitungsanlagen, bedürfen der schriftlichen Genehmigung des Herausgebers.

Nachdruck, auch auszugsweise, verboten.

Diese Bedienungsanleitung entspricht dem technischen Stand bei Drucklegung. Änderung in Technik und Ausstattung vorbehalten.

# Imprint

These operating instructions are published by ABUS Security-Center GmbH & Co.KG, Linker Kreuthweg 5, 86444 Affing, Germany. No reproduction (including translation) is permitted in whole or part e.g. photocopy, microfilming or storage in electronic data processing equipment, without the express written consent of the publisher.

The operating instructions reflect the current technical specifications at the time of print. We reserve the right to change the technical or physical specifications.

#### © Copyright 05/2019 by ABUS Security-Center