WIRELESS TRANSMISSION SYSTEM FOR IP HD CAMERA

EXTERNAL TRANSMITTING-RECEIVING UNIT CDS-5IP

User's Manual



Copyright

Copyright © 2011 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual is intended to guide professional installer to install the CDS5-IP and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

Note:

• This indicates an important note that you must pay attention to.



• This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital Unit, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This Unit complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This Unit may not cause harmful interference, and (2) this Unit must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Warranty

Hardware warranty is for 24months from date of shipment. Distributor warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

IN NO EVENT SHALL DISTRIBUTOR BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE RISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Chapter 1 Introduction	
Introduction	
Appearance	
Key Features	
Typical Application	
Chapter 2 Hardware Installation	10
Preparation before Installation	
Professional Installation Required	
Safety Precautions	
Installation Precautions	11
Product Package	11
Hardware Installation	
Connect up	
Using the External Antenna	
Pole Mounting	
Chapter 3 Basic Settings	
Factory Default Settings	
System Requirements	
How to Login the Web-based Interface	
Time Settings	
RADIUS Settings	
Firewall Settings	
Basic Wireless Settings	
Site Survey	
VAP Profile Settings	
VLAN Tab	
Chapter 4 Advanced Settings	
Advanced Wireless Settings	

Content

Wireless Security Settings	
Data Encryption and Authentication Settings	40
Access Control	42
WDS Settings	
Chapter 5 Management	45
Remote Management	45
SNMP Management	
Configure SNMPv3 User Profile	47
Upgrade Firmware	
Backup/ Retrieve Settings	
Restore Factory Default Settings	
Reboot	50
Password	51
Chapter 6 Monitoring Tools	52
System Log	52
Site Survey	53
Ping Watch Dog	53
Date Rate Test	
Antenna Alignment	
Speed Test	55
Chapter 7 Status	57
View Basic Information	57
View Association List	57
View Network Flow Statistics	58
View ARP Table	59
View Bridge Table	60
View Active DHCP Client Table	60
View Network Activities	61
Chapter 8 Troubleshooting	62

Appendix A. ASCII	64
Appendix B. SSH Settings	65
Appendix C. GPL Declamation	73
Appendix D. Country Channel List	

Chapter 1 Introduction

Introduction

Designed for outdoor environment application, CDS-5IP is a high-performance solution that provides fast and reliable wireless network coverage. Designed with IEEE 802.11n draft 2.0 standard, high output power and built-in 16dBi dual-polarity antenna makes it possible to deliver several times faster data rate than normal wireless unit and higher bandwidth with longer range for outdoor applications. CDS-5IP supports four wireless communication connectivity (Master – main receiving point, Slave – camera point, Video Bridge and Master Repeater), allowing for various application requirements thus helping to get connection with almost each IP camera.

With high output power and reliable performance, CDS-5IP is an ideal wireless solution for IP HD cameras.

Appearance



Pic.1: External wireless Unit CDS-5IP

Key Features

- Support passive PoE which is supplied with 15V.
- High reliable watertight housing endures almost any harsh environments
- Four operating modes including MASTER, SLAVE, VIDEO BRIDGE, MASTER REPEATER
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2, WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- User-friendly Web management interface

Typical Application

This section describes the typical applications of the CDS5-IP – wireless external unit. By default, it is set to VIDEO BRIDGE mode which allows it to establish a wireless coverage. External wireless video unit CDS-5IP is able to deliver stable and efficient video, audio and data connectivity for various



applications.

Figure 1 Typical Application

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing the CDS-5IP.

Preparation before Installation

Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Safety Precautions

- 1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
- If you are installing the CDS-5IP Wireless External Unit for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
- 3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
- 4. When installing the CDS-5IP, please note the following things:
 - Do not use a metal ladder;
 - Do not work on a wet or windy day;
 - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- 5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

Installation Precautions

To keep the CDS-5IP - Wireless External Unit well while you are installing it, please read and follow these installation precautions.

- Users MUST use a proper and well-installed grounding and surge arrestor with the Wireless External Video Unit; otherwise, a random lightening could easily cause fatal damage to the unit.
 EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.
- Users MUST use the "Power cord & POE Injector" shipped in the box with the CDS-5IP. Use of other options will likely cause damage to the unit.
- 3. Users MUST power off the CDS-5IP Wireless External Video Unit first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto unit; otherwise, damage might be caused to the unit itself.

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

- CDS-5IP Wireless External Video Unit ×1
 Pole Mounting Ring ×2
 Power Cord & POE Injector ×1
 Product CD ×1
- Note:
 - Product CD contains User Manual!

Pole Mounting Ring



Power Cord & POE Injector





 Users MUST use the "Power cord & POE Injector" shipped in the box with the CDS-5IP - Wireless External Video Unit. Use of other options will likely cause damage to the unit.

Hardware Installation

Connect up

 The bottom of CDS-5IP - Wireless External Video Unit is a movable cover. Loosen the screw with a Philips screwdriver. Grab the cover and pull it back harder to take it out as the figure shown below.





Figure 2 Move the Cover

 Plug a standard Ethernet cable into the RJ45 port labeled "LAN 1". Do not plug the cable into the RJ45 port labeled "LAN 2".



Figure 3 Cable Connection

The secondary Ethernet port (labeled LAN 2) is for IP camera or next CDS-5IP Unit video integration. To use it you need to enable the secondary port in advance before connecting with the IP camera from the CDS-5IP's Web Management as shown below.

sat	C	DS-51	Prople	Ę
Status	System	Wireless	Management	Tools
Basic Settings »	Basic Setting	e		
TCP/IP Settings	Use this page to configure the		levice.	
Time Settings	Device Settings			
	Device Name:	CDS-5IP	(max. 15 characters and no spaces)	
	Network Mode:	Bridge 🔫		
	Ethernet 1 DataRate:	Auto	▼	
	Ethernet 2 DataRate:	Auto	* 3	
	Country/Region:	European Union		
	Secondary RJ45 Power:	🔘 Enabled 🛛 💿	Disabled	
	Spanning Tree:	Enabled	Disabled	
	STP Forward Delay:	1 (1~30 seco		

Take out the power cord and POE injector from the gift box, and plug the power cord into the DC port of the POE injector as the below picture shows.



Figure 4 Connect to POE Injector

4. Put what in the Step.2 and Step.3 together by plugging the other side of the Ethernet cable in into the POE port of the POE injector When you finish the Step.4, the set will be like the following picture:



Figure 5 Plug the Ethernet cable to the RJ-45 jack of the injector

5. Press the black PWR button beside the LAN 1 Ethernet port.



6. Attach and fasten the removable cover to the bottom of the unit with the screw.



7. Power on the CDS-5IP - Wireless External Video Unit by plugging the power adapter to the power socket.

Using the External Antenna

The CDS-5IP - Wireless External Video Unit provides two reverse SMA antenna connectors if you prefer to use the external antenna for your application instead of the built-in directional antenna, please follow the steps below.

1. Remove the two plugs as circled below:



 Connect your external antenna to the SMA-type connectors at the bottom of the Wireless External Video Unit.



A Warning:

 Users MUST power off the CDS-5IP - Wireless External Video Unit first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the unit; otherwise, damage might be caused to the unit itself.

Follow the steps described in **Connect Up** to finish the installation.

Pole Mounting

 Turn the Wireless External Video Unit over. Put the pole mounting rings through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through the CDS-5IP as the following right picture shows.





Figure 6 Pole Mounting – Step 1

 Mount the CDS-5IP - Wireless External Video Unit steadily to the pole by locking the pole mounting ring tightly. The mounting ring supports pole diameter 32mm to 70mm.



Figure 7 Pole Mounting – Step 2

3. Now you have completed the hardware installation of the CDS-5IP - Wireless External Video Unit .

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the CDS-5IP - Wireless External Video Unit factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "<u>Restore Factory Default</u> <u>Settings</u>".

Table 1 Factory Default Settings

Features	5	Factory Default Settings
Usernam	e	camsat
Passwor	d	camsat
Wireless	Unit Name	CDS-5IP
Operating	g Mode	Video Bridge
Data Rat	е	Auto
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
LAN	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning	j Tree	Enable
802.11 N	lode	802.11a/n
Country/	Region	European Union
Channel	Number	5500 MHz (CH100)
SSID		CAMSAT
Broadcas	st SSID	Enable
HT Prote	ct	Disable
Data Rat	е	Auto
Output P	ower	Full
Channel	Mode	20MHz
WMM		Enabled
RTS Thre	eshold (byte)	2346
Fragmen	tation Length (byte)	2346
Beacon I	nterval	100
DTIM Int	erval	1
Space in	Meter	0
Flow Cor	ntrol by AP	Disable

Security	Open System
Encryption	None
Wireless Separation	Disable
Access Control	Disable

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of the Wireless External Video Unit is 192.168.1.1. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape, Firefox, or Google Chrome.

How to Login the Web-based Interface

The CDS-5IP - Wireless External Video Unit provides you with user-friendly Web-based management tool.

• Open Web browser and enter the IP address (Default: **192.168.1.1**) of the Wireless External Video Unit into the address field. You will see the login page as below.



Name	camsat	
Password		
	Login	Reset

Figure 8 Login Page

• Enter the username (Default: camsat) and password (Default: camsat) respectively and click "Login" to login the main page of the Wireless External Video Unit. As you can see, this management interface provides 5 main options in the black bar above, which are Status, System,

Wireless,	Management and Tools.
-----------	-----------------------

Status	System	Wireless	Management	Tool
Information »				
Connections	Information			
Statistics	This page shows the curre	nt status and some basic sett	ings of the device.	
Statistics	System Information			
ARP Table	Device Name	CDS-5IP		
	MAC Address	00:19:70:00:fc:6	0	
Bridge Table	Country/Region	European Union		
DHCP Clients	Firmware Version	3.0.4(CS)2		
	LAN Settings			
Network Activities	IP Address	192 168 1 1		
	Subnet Mask	255.255.255.0		
	Gateway IP Address	0.0.0.0		
	MAC Address	00:19:70:00:fc:6	D	
	Wireless Settings			
	Operation Mode	Video Bridge		
	Wireless Mode	802.11A/N		
	Encryption	Open System		
	ACK Timeout	27 us		
	WMM Enable	On		
	Noise Floor	-96 dBm		

Figure 9 Main Page

Note:

• The username and password are case-sensitive, and the password should be no

more than 19 characters!

Basic System Settings

For users who use the CDS-5IP - Wireless External Video Unit for the first time, it is recommended

that you begin configuration from "Basic Settings" in "System" shown below:

tatus	System W	ireless	Management	Tool
Basic Settings »				
TCP/IP Settings	Basic Settings		of device	
Time Settings	Device Settings	buaic purumetera e		
	Device Name:	CDS-5IP	(max. 15 characters and no spaces)	
	Network Mode:	Bridge 🔻		
	Ethernet 1 DataRate:	Auto		
	Ethernet 2 DataRate:	Auto	×	
	Country/Region:	European Unior	n 💌	
	Secondary RJ45 Power:	C Enabled	Disabled	
	Spanning Tree:	Enabled	O Disabled	
	STP Forward Delay:	1 (1~30 se	econds)	
	GPS Coordinate Settings	3		
	Latitude:	N 🔻 0	° 0 ' 0 "	
	Longitude:	E ▼ 0	° 0 ' 0 "	

Figure 10 Basic System Settings

Basic Settings

Unit Name: Specify the Unit name, which is composed of no more than 15 characters with (0-9),

(A-Z), (a-z) or (-).

Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the unit when it is set to Router Mode.

Ethernet 1 Data Rate: Specify the transmission rate of data of LAN1. Default is Auto.

Ethernet 2 Data Rate: Specify the transmission rate of data of LAN2. Default is Auto.

<u>Country Region</u>: The availability of some specific channels and/or operational frequency bands are country dependent.

<u>Secondary RJ45 Power</u>: The secondary Ethernet port (labeled LAN 2) is for IP video integration. To use it you need to enable the secondary port via WEB UI in advance before connecting with the IP camera. **Spanning Tree**: Spanning Tree Protocol (STP) is a link management protocol for MASTER which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the MASTER points but establish the redundant link as a backup if the initial link fails.

<u>STP Forward Delay</u>: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

TCP/IP Settings

Open "**TCP/IP Settings**" in "**System**" as below to configure the parameters for LAN which connects to the LAN port of the CDS-5IP. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

	2	Million Louise		-
Status	System	Wireless	Management	Tool
Basic Settings				
TCP/IP Settings »	TCP/IP Settir	and a second		
Time Settings			ea network which connects to th or IP address, subnet mask, DH	
	IP Address Assignmen	it		
	Obtain IP Address A	Automatically		
	Use Fixed IP Addres	35		
	IP Address :	192.168.1.1		
	Subnet Mask:	255.255.255.0		
	Gateway Ip Address :	0.0.0		
	DNS 1:	0.0.0		
		0.0.0.0		

Figure 11 TCP/IP Settings (Bridge)

Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the CDS-5IP - Wireless External Video Unit is able to obtain IP settings automatically from that DHCP server.

Note:

• When the IP address of the Wireless External Video Unit is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the

client computer by running the "nbtstat –r" command before using the unit CDS-5IP name to access its Web Management page.

• In case the CDS-5IP - Wireless External Video Unit is unable to obtain an IP address

from a valid DHCP server, it will fall back to default static IP address.

<u>Use Fixed IP Address</u>: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the CDS-5IP manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

If the CDS-5IP - Wireless External Video Unit is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.

Basic Settings TCP/IP Settings Time Settings WAN Settings: WAN Access Type: Static IP IP Address: Default Gateway: 0.0.0.0 DNS 1: 0.0.0.0 DNS 2: 0.0.0.0 DNS 2: IP Address: IP Address: IP Address:	TCP/IP Settings ×	Use this page to configure the p	parameters for local a			
TCP/IP Settings >> Time Settings Use this page to configure the parameters for local area network which connects to the your Access Point. Here you may change the setting for IP address, subnet mask, DHO WAN Settings :	<u> </u>	Use this page to configure the p	parameters for local a			
Time Settings Use this page to configure the parameters for local area network which connects to the your Access Point. Here you may change the setting for IP address, subnet mask, DHO WAN Settings : WAN Access Type : Static IP ▼ IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0.0 DNS 1: 0.0.0.0 DNS 2: 0.0.0.0 LAN Settings : LAN Settings :	<u> </u>					
WAN Settings : WAN Access Type : Static IP • IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0.0 DNS 1 : 0.0.0.0 DNS 2 : 0.0.0.0 LAN Settings : LAN Settings :	Time Settings	your Access Former Here you hit	ay change the setting		innet mask DHCI	
WAN Access Type : Static IP IP Address : 192.168.1.1 Subnet Mask : 255.255.0 Default Gateway : 0.0.0.0 DNS 1 : 0.0.0.0 DNS 2 : 0.0.0.0		INCAN Contractor		ioi ii daaroooy oo		, , , , , , , , , , , , , , , , , , , ,
IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0.0 DNS 1 : 0.0.0.0 DNS 2 : 0.0.0.0		WAN Settings :				
Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0.0 DNS 1 : 0.0.0.0 DNS 2 : 0.0.0.0			ki kula ki kale da k	_		
Default Gateway: 0.0.0.0 DNS 1: 0.0.0.0 DNS 2: 0.0.0.0		IP Address :	192.168.1.1			
DNS 1: 0.0.0.0 DNS 2: 0.0.0.0 LAN Settings :		Subnet Mask :	255.255.255.0			
DNS 2: 0.0.0.0 LAN Settings :		Default Gateway :	0.0.0			
LAN Settings :		DNS 1:	0.0.0.0			
		DNS 2 :	0.0.0			
IP Address : 192.168.0.99		LAN Settings :				
		IP Address :	192.168.0.99			
Subnet Mask: 255.255.255.0		Subnet Mask :	255.255.255.0			
DHCP Server : Disabled 🔻		DHCP Server :	Disabled 💌			
DHCP IP Address Range : 0.0.0.0 - 0.0.0.0		DHCP IP Address Range :	0.0.0.0	0.0.0.0	1	
Lease Time : 0 (15-44640 Minutes)		Lease Time :	0 (15-4464	40 Minutes)	<u>5</u> 1	

Figure 12 TCP/IP Settings (Router)

<u>WAN Settings</u>: Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for the CDS-5IP manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range,

DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes). A DHCP relay agents is used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. To enable the DHCP relay agent, check the "**Enable DHCP Relay**" checkbox and enter the IP address of the DHCP server.

Warning:

- In AP mode, the CDS-5IP Wireless External Video Unit must establish connection with another wireless unit before it is set to Router mode. To access the unit in Router mode via wired port, please type the WAN IP address to enter the web page for WAN is on wired port and LAN is on wireless port. Or, you can access Unit through the wireless Unit connected with the CDS-5IP.
- In SLAVE mode, users can access the CDS-5IP via its wired port, for WAN is on wireless port and LAN is on wired port when unit is set to Router mode.
- Video Bridge mode and Master Repeater mode are similar to MASTER mode when unit is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect the CDS-5IP with another wireless unit before it is set to Router mode and access the CDS-5IP via the connected wireless unit.

Time Settings

Compliant with NTP, the CDS-5IP - Wireless External Video Unit is capable of keeping its time in complete accord with the Internet time. Make configuration in "**Time Settings**" from "**System**". To use this feature, check "**Enable NTP Client Update**" in advance.

		CD2-2	IP role	
Status	System	Wireless	Management	Tool
Basic Setting	s Time Settin		th a public time server over the Inter	net.
Time Setting	s >> Current Time: Time Zone Select:	14. 17	Day 1 Hr 16 Mn 10 Sec an Time: Dublin, Edinburgh, Lisbon, Lor	
	NTP server: Manual IP:	131.188.3.220 - Eur	ope 💌	

Figure 13 Time Settings

Current Time

Display the present time in Yr, Mon, Day, Hr, Min and Sec.

Time Zone Select

Select the time zone from the dropdown list.

NTP Server

Select the time server from the "**NTP Serve**r" dropdown list or manually input the IP address of available time server into "**Manual IP**".

Hit "Apply" to save settings.

RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open "RADIUS Settings" in "System" to make RADIUS configuration.

Status	System	Wireless	Management	Tools
Basic Settings	RADIUS S	ettings		
Time Settings	Use this page to set t Authentication R	ne radius server settings. ADIUS Server		
RADIUS Settings »	IP Address:	0.0.0.0		
Firewall Settings	Port: Shared Secret:	1812		
	🔄 Global-Key U	pdate		

Figure 16 RADIUS Settings

Authentication RADIUS Server

This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

IP Address: Enter the IP address of the Radius Server;

Port: Enter the port number of the Radius Server;

Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the

MASTER and RADIUS during authentication.

Re-authentication Time: Set the time interval between two authentications.

<u>Global-Key Update</u>: Check this option and specify the time interval between two global-key updates.

Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. CDS-5IP - Wireless External Video Unit has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under Router Mode.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data

packets from your local network to Internet through the CDS-5IP - Wireless External Video Unit. Use of

such filters can be helpful in securing or restricting your local network.

sat "	IRELESS TRA	CDS-5		HD CAMER
Status	System	Wireless	Management	Tools
Basic Settings	Source ID	Filtering		
TCP/IP Settings	Source IP	re used to restrict certain type	s of data packets from you	r local network to
Time Settings	Internet through the network.	Gateway. Use of such filters o	an be helpful in securing or	restricting your local
RADIUS Settings	W Constant of the	ce IP Filtering		
Firewall Settings	Local IP Address: Comment:			
Src IP Filtering »	-	Apply	Cancel	
Dst IP Filtering		C0224	Cancer	
Src Port Filtering	L	ocal IP Address 🗢 Con	ment 🗢 Select	Edit
Dst Port Filtering				
Port Forwarding		Delete Selected	Delete All Refresh	
DMZ Setting				

Figure 17 Source IP Filtering

Destination IP Filtering: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Check the "**Enable Destination IP Filtering**" checkbox and enter the IP address of the clients to be restricted. Hit **Apply** to make the setting take effect.

itatus	System	Wireless	Ma	inagement	Tool
Basic Settings	Destinati	on ID Filter	182		
TCP/IP Settings		on IP Filter		from accessing certain we	ebsites in WAN
Time Settings	according to IP add	dress.			
RADIUS Settings	Destination IP /	estination IP Filtering			
Firewall Settings	Comment:				
Src IP Filtering		A	pply Cancel		
Dst IP Filtering »	D	estination IP Addres\$	Comment 🗢	Select Edit	
Src Port Filtering					
		Delete Selecte	d Delete All	Refresh	

Figure 18 Destination IP Filtering

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through the CDS-5IP - Wireless External Video Unit. Use of such filters can be helpful in securing or restricting your local network.

sat "	RELESS TRANS	CDS-51	A Distance of the second	IP HD CA	UMERA
Status	System	Wireless	Managemen	it	Tools
Basic Settings	Course Dout	- 114 - alm			
TCP/IP Settings	Source Port	the second second second	s of data packate from	your local patwor	rk to
Time Settings	Internet through the Gatew network.	ay. Use of such filters ca	an be helpful in securin	ig or restricting yo	our local
RADIUS Settings	Enable Source Pol	t Filtering			
Firewall Settings	Port Range: Protocol:	Both +			
Src IP Filtering	Comment				
Dst IP Filtering		Apply	Cancel		
Src Port Filtering »	Source Port Ran	ige 🕈 Protocol\$	Comment +	Select Ed	lit
Dst Port Filtering					
Port Forwarding		Delete Selected	elete All Refresh		

Figure 19 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through the CDS-5IP - Wireless External Video Unit. Use of such filters can be helpful in securing or restricting your local network.

	148 H	100			1111 1
Status	System	Wireless	Managemen		Tool
Basic Settings	Destination	Dort Eiltori			
TCP/IP Settings	 Destination Entries in this table are us 			your local network	r to
Time Settings	Internet through the Gate network.				
RADIUS Settings	Enable Destination	on Port Filtering	<u>14</u>		
Firewall Settings	 Port Range: Protocol: 	Both 👻			
Src IP Filtering	Comment:				
Dst IP Filtering		Apply	Cancel		
2					

Figure 20 Destination Port Filtering

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind the router's NAT firewall.

1205 112	
Status	System Wireless Management Tools
Basic Settings	Dort Forwarding
TCP/IP Settings	 Port Forwarding Entries in this table allow you to automatically redirect common network services to a specific machine
Time Settings	behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
RADIUS Settings	Enable Port Forwarding
Firewall Settings	Protocol: Both ~
Src IP Filtering	Port Range:
	Comment:
Dst IP Filtering	
Dst IP Filtering Src Port Filtering	Apply Cancel

Figure 21 Port Forwarding

<u>DMZ</u>: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains Units accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

sar "	IRELESS TR	CDS-5	YSTEM FOR IP HD	CAMERA
Status	System	Wireless	Management	Tools
Basic Settings	DMZ			
TCP/IP Settings	A Demilitarized Zo	ne is used to provide Internet	t services without sacrificing unauthor	ized access to its
Time Settings		rk. Typically, the DMZ host o rs, FTP servers,SMTP (e-mail	ontains devices accessible to Internet) servers and DNS servers.	traffic, such as
RADIUS Settings	Enable DM	1		
Firewall Settings	DMZ Host IP Ac	dress: 0.0.0.0		
Src IP Filtering		Apply	Cancel	
Dst IP Filtering				

Basic Wireless Settings

Open "Basic Settings" in "Wireless" as below to make basic wireless configuration.

Status	System Wi	reless	Management	Tools
Deste Cambras				
Basic Settings »	Wireless Basic	Settings		
Profile Settings	Use this page to configure the p	1		
Advanced Settings	Point. Here you may change wir			
Access Control	Disable Wireless LAN	Interface		
	Wireless Mode:	Video Bridge	Site Survey	
WDS Settings	Frequency/Channel:	5500MHz (100) 🔻		
	Extension Channel:	None 💌		
	Channel Mode:	20 MHz 🔻		
	Antenna:	Internal (16 dBi)	SMA Connector	
	Maximum Output Power (per chain):	12 1	4 👝 14 dBm	
	Data Rate:	Auto	•	
	Extension Channel Protection	n: None 🔻		

Figure 14 Basic Wireless Settings

Disable Wireless LAN Interface

Check this option to disable WLAN interface, then the wireless module of the CDS-5IP will stop working and no wireless unit can connect to it.

Wireless Mode

Four operating modes are available on the CDS-5IP - Wireless External Video Unit.

MASTER: The CDS-5IP - Wireless External Video Unit establishes a wireless coverage and receives connectivity from other wireless units.

<u>SLAVE</u>: The CDS-5IP - Wireless External Video Unit is able to connect to the MASTER and thus join the wireless network around it.

<u>Video Bridge</u>: The CDS-5IP - Wireless External Video Unit establishes wireless connectivity with other CDS-5IP - Wireless External Video Units by keying in remote MAC address. Please refer to the "**WDS Setting**" for detailed configuration.

MASTER Repeater: The CDS-5IP - Wireless External Video Unit servers as AP and Bridge concurrently. In other words, it can provide connectivity services for CDS-5IPs under Bridge mode.

• Wireless Network Name (SSID)

This wireless network name is shared among all associated units in your wireless network. Keep it identical on all those units. Note that the SSID is case-sensitive and cannot exceed 32 characters.

HT Protect

Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, SLAVE can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

Frequency/Channel

Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation

Channel Mode

4 levels are available: 40MHz, 20MHz, 10MHz and 5MHz. 40MHz can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

Antenna

By default, the CDS-5IP - Wireless External Video Unit uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (16 dBi)" to "SMA Connector".

Warning:

• You are able to choose "SMA Connector" only from the WEB UI after you have physically installed the external antenna; otherwise, it might damage the unit itself.

Maximum Output Power (per chain):

Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.

Note:

- The output power here is counted from the RF single chain only not including the 16dBi internal antenna.
- You are able to choose "SMA Connector" only when you have well done installing the external antenna; otherwise, it might damage CDS-5IP Wireless External Video Unit

Data Rate

Usually "**Auto**" is preferred. Under this rate, the CDS-5IP - Wireless External Video Unit will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

Extension Channel Protection Mode

This is to avoid conflict with other wireless network and boost the ability of your unit to catch all legacy units transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Enable MAC Clone

Available in SLAVE mode, it hides the MAC address of the CDS-5IP while displays the one of associated SLAVE or the MAC address designated manually.

Site Survey

Under SLAVE mode, the CDS-5IP - Wireless External Video Unit is able to perform site survey, through which, information on the available access points will be detected.

Open "**Basic Settings**" in "**Wireless**", by clicking the "**Site Survey**" button beside "**Wireless Mode**" option, the wireless site survey window will pop up with a list of available wireless networks around. Select the MASTER you would like to connect and click "**Selected**" to establish connection.





VAP Profile Settings

Available in MASTER mode, the CDS-5IP - Wireless External Video Unit allows up to 16 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, you may check the **Enable** box of the profile and click on the profile (eg. Profile 2) to configure wireless and security settings. Hit **Apply** to active the profile.

Status	System	n	Wireless		Managen	nent	Too
Basic Settings Profile Settings »	VA	P Profile	Settings				
	define	each WLAN's attrib	ute.				
Advanced Settings	#	Profile Name \$	SSID	\$	Security \$	Vlan ID	Enable
Access Control	1	Profile1	CAMSAT		Open System	0	Always Enabled
WDS Settings	2	Profile2	CAMSAT		Open System	0	
	3	Profile3	CAMSAT	1	Open System	0	
	4	Profile4	CAMSAT	1	Open System	0	
	5	Profile5	CAMSAT	1	Open System	0	
	6	Profile6	CAMSAT		Open System	0	
	7	Profile7	CAMSAT	18	Open System	0	
	8	Profile8	CAMSAT	-	Open System	0	
	9	Profile9	CAMSAT		Open System	0	
	10	Profile10	CAMSAT	1	Open System	0	
	11	Profile11	CAMSAT	3	Open System	0	
	12	Profile12	CAMSAT	1.0	Open System	0	

Figure 16 VAP Profile Settings

Basic Settings				
basic settings				
	VAP Profile1 S	Settings		
Profile Settings »		276		
Advanced Settings	Basic Settings			
Access Control	Profile Name:	Profile1		
	Wireless Network Name (SSID):	CAMSAT		
WDS Settings	Broadcast SSID:	Enabled O E	Disabled	
	Wireless Separation:	C Enabled O C	Disabled	
	WMM Support:	Enabled	Disabled	
	Max. Station Num:	32 (0-32	2)	
	Security Settings			
	Network Authentication:	Open System	•	
	Data Encryption:	None 🔻		
	Key Type:	Hex 💌		

Figure 17 VAP Profile1 Settings

Basic Setting

Profile Name: Name of the VAP profile

Wireless Network Name: Enter the virtual SSID for the VAP

Broadcast SSID: In MASTER mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the CDS-5IP - Wireless External Video Unit, so that malicious attack by some illegal STA could be avoided.

<u>Wireless Separation</u>: Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except SLAVE mode, enable "Wireless Separation" can prevent the communication among associated SLAVES.

<u>WMM Support</u>: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under MASTER mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it

Max. Station Number: By checking the "Max. Station Num" the CDS-5IP will only allow up to 32 SLAVES to associate with

Security Setting:

To prevent unauthorized radios from accessing data transmitting over the connectivity, CDS-5IP -Wireless External Video Unit provides you with rock solid security settings. For detailed information please go to **Chapter 4 Wireless Security Setting**.

VLAN Tab

If your network uses VLANs, you can assign one SSID to a VLAN, and client Units using the SSID are grouped in that VLAN.

To allow users on the VLAN to access the WEB page of CDS-5IP - Wireless External Video Unit, you need to enable "**Enable 802.1Q VLAN**" and assign a management VLAN ID for your unit. Make sure the assigned management VLAN ID is identical to your network VLAN ID to avoid failures of accessing the Web page of the CDS-5IP - Wireless External Video Unit.
Status	System		Wireless	Manage	ment	Tools
Basic Settings	6	Protile6	CAMSAI	Open System	0	
	7	Profile7	CAMSAT	Open System	0	
Profile Settings »	8	Profile8	CAMSAT	Open System	0	
Advanced Settings	9	Profile9	CAMSAT	Open System	0	
Access Control	10	Profile10	CAMSAT	Open System	0	
WDS Settings	11	Profile11	CAMSAT	Open System	0	
wb5 Settings	12	Profile12	CAMSAT	Open System	0	
	13	Profile13	CAMSAT	Open System	0	
	14	Profile14	CAMSAT	Open System	0	
	15	Profile15	CAMSAT	Open System	0	
	16	Profile16	CAMSAT	Open System	0	
		nable 802.1Q		2001		

Figure 18 Management VLAN ID

Chapter 4 Advanced Settings

Advanced Wireless Settings

Open "Advanced Settings" in "Wireless" to make advanced wireless settings.

Status	System	Wireless	Management Tool
Basic Settings	Wireless Adv	anced Se	ettinas
			vanced users who have a sufficient knowledge about
Profile Settings			nged unless you know what effect the changes will
Advanced Settings »			
Access Control	A-MPDU aggregation:	Enabled	Disabled
Access control	A-MSDU aggregation:	© Enabled	Oisabled
WDS Settings	Short GI:	C Enabled	Disabled
	RTS Threshold:	2347	(1-2347)
	Fragment Threshold:	2346	(256-2346)
	Beacon Interval:	100	(20-1024 ms)
	DTIM Interval:	1	(1-255)
	IGMP Snooping:	Enabled	© Disabled
	RIFS:	Enabled	C Disabled
	Link Integration:	C Enabled	Oisabled
	TDM Coordination:	© Enabled	Disabled
	Space In Meter:	0	(0-15000 m)

Figure 19 Advanced Wireless Settings

A-MPDU/A-MSDU Aggregation

The data rate of your CDS-5IP except SLAVE mode could be enhanced greatly with this option enabled; however, if your SLAVE don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

Short GI

Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

RTS Threshold

The CDS-5IP - Wireless External Video Unit sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The

setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

• Fragmentation Length

Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor wireless video link performance. Leave it at its default of 2346 is recommended.

Beacon Interval

Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

DTIM Interval

DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

IGMP Snooping

Available in MASTER/Router mode, IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the MASTER will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

RIFS

RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

Link Integration

Available under MASTER/VIDEO BRIDGE/MASTER REPEATER mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating SLAVES as soon as the disconnection occurs.

TDM Coordination

Stands for "Time-Division Multiplexing Technique", this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in MASTER/CDS-5IP mode. It is highly recommended to enable TDM coordination when there are multiple CDS-5IPs needed to connect to the MASTER in your application.

LAN2LAN

LAN2LAN mode enables packet forwarding at layer 2 level. It is fully transparent for all the Layer2 protocols.

• Space in Meter

To decrease the chances of data retransmission at long distance, the CDS-5IP - Wireless External Video Unit can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

Flow Control

It allows the administrator to specify the incoming and outgoing traffic limit by checking "Enable Traffic Shaping". This is only available in Router mode.

Note:

 We strongly recommend you leave most advanced settings at their defaults except "Distance in Meters" adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless external video unit.

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the CDS-5IP -

Wireless External Video Unit provides you with rock solid security settings.

Data Encryption and Authentication Settings

Open "Profile Setting" in "Wireless" and enter "VAP Profile 1 Settings" as below.

sar "		DS-5	STEM FOR IP HD	CAMERA
Status	System	Wireless	Management	Tools
Basic Settings	VAP Profile1	Settings		
Advanced Settings	Basic Settings			
Access Control	Profile Name: Wireless Network Name	Profile1		
WDS Settings	(SSID): Broadcast SSID:	CAMSAT	Disabled	
	Wireless Separation:	Enabled	Disabled	
	WMM Support:		Disabled -32)	
	Security Settings			
	Network Authentication:	Open System		
	Data Encryption: Key Type:	Open System Shared Key Legacy 802.1x		
	Default Tx Key: WEP Passphrase:	WPA with Radius WPA2 with Radiu WPA & WPA2 w	us	
	Encryption Key 1:	WPA-PSK WPA2-PSK WPA-PSK&WPA2	2-PSK	

Figure 20 Security Settings

Network Authentication

Open System: It allows any unit to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication

Legacy 802.1x: Available in MASTER/SLAVE mode, it provides the rights to access the wireless video link and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless video link to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, MASTER and SLAVE.



 For first time users, if EAP type "TLS" is selected, you need to import valid user certificate given by CA in prior. To import user certificates, please refer to Chapter 5 Management/Certificate Settings for more details.

WPA with RADIUS: Available in MASTER/SLAVE mode, with warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

<u>WPA2 with RADIUS</u>: Available in MASTER/SLAVE mode, as a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.

WPA&WPA2 with RADIUS: Available in MASTER mode, it provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: Available in MASTER mode, it provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

Data Encryption

If data encryption is enabled, the key is required and only sharing the same key with other Wireless External Video Unit can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

<u>128 bits WEP</u>: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with

WPA-PSK, etc.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with Units using TKIP.

Note:

- We strongly recommend you enable wireless security on your wireless video link!
- Only setting the same Authentication, Data Encryption and Key in the CDS-5IP and other associated wireless units, can the communication be established!

Access Control

The Access Control appoints the authority to camera point on accessing the CDS-5IP - Wireless External Video Unit, thus a further security mechanism is provided. This function is available only under MASTER mode.

Open "Access Control" in "Wireless" as below.

Status	System	Wireless	Managemen	t Tools
Basic Settings	Wireless A	ccess Contro		
Profile Settings		Listed', only those clients v		
Advanced Settings	control list will be able		oint. When 'Deny Listed	is selected, these wireless
Access Control »	Access Control Mod	de: Disable 🗨		
WDS Settings	MAC Address:			
		Apply	Cancel	

Figure 21 Access Control

Access Control Mode

If you select "**Allow Listed**", only those clients whose wireless MAC addresses are in the access control list will be able to connect to your MASTER. While when "**Deny Listed**" is selected, those wireless clients on the list will not be able to connect the MASTER.

MAC Address

Enter the MAC address of the wireless point that you would like to list into the access control list, click "**Apply**" then it will be added into the table at the bottom.

Delete Selected/All

Check the box before one or more MAC addresses of wireless units that you would like to cancel, and click "**Delete Selected**" or "**Delete All**" to cancel that access control rule.

WDS Settings

Extend the range of your network without having to use cables to link the bridges by using the Wireless Distribution System (WDS): Simply put, you can link the bridges wirelessly. Open "**WDS Settings**" in "**Wireless**" as below:

ystem Wire	eless	Management	
		Contracting Protocology	Tool
-			PE 11 - 51
does. To do this, you must set the which you want to communicate v	ese APs in the same o with in the table and t	hannel and set MAC addre	sses of other APs
-		18 888 I	
Local MAC Address:			
Remote AP MAC Address 1:	00:19:70:00:fb:c5		
Remote AP MAC Address 2:			
Remote AP MAC Address 3:			
	does. To do this, you must set th which you want to communicate u in Bridge and AP Repeater mode. WDS Separation: Local MAC Address: Remote AP MAC Address 1: Remote AP MAC Address 2:	Wireless Distribution System uses wireless media to co does. To do this, you must set these APs in the same of which you want to communicate with in the table and the in Bridge and AP Repeater mode. WDS Separation: Local MAC Address: 00:19:70:00:fc:60 Remote AP MAC Address 1: Remote AP MAC Address 2:	Wireless Distribution System uses wireless media to communicate with other APs does. To do this, you must set these APs in the same channel and set MAC addre which you want to communicate with in the table and then enable the WDS.This fin Bridge and AP Repeater mode. WDS Separation:

Figure 22 WDS Settings

Enter the MAC address of another CDS-5IP in VIDEO BRIDGE mode you wirelessly want to connect

to into the appropriate field and click "Apply" to save settings.

Note:

- WDS Settings is available only under Video Bridge and MASTER Repeater Mode.
- Video Bridge uses the WDS protocol that is not defined as the standard thus

compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if radio Unit B and radio Unit C are specified as the WDS peers of radio Unit A, radio Unit B should not be specified as the WDS peer of radio Unit C and radio Unit C should not be specified as the WDS peer of radio Unit B in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

Chapter 5 Management

Remote Management

The CDS-5IP - Wireless External Video Unit provides a variety of remotes managements including Telnet, SNMP, FTP, SSH, HTTPS and exclusive WISE tool, making configuration more convenient and secure.

With **Normal** selected, Telnet, SNMP and FTP are activated as default remote management options. To use secure management tools such as SSH, HTTPS and WISE, please select "**Secure**". You may also choose "**Customized**" to enable any methods as desired.

Status	System	Wireless	Management	Tools
Remote Settings »	Pomoto Sott	inge		
CoovaChilli Settings	Remote Sett			
Firmware Upload	Management Privacy			
Configuration File	Normal Sec	ure 💿 Customized		
Password Settings		SNMP FTP		
Certificate Settings	SNMP Settings			
	Protocol Version: Server Port:	V2 • 161		
	Get Community:	public		
	Set Community:	private		
	Trap Destination: Trap Community:	0.0.0.0 public		
	Configure SNMPv3 U		-1	

Figure 32 Remote Management

SNMP Management

The CDS-5IP - Wireless External Video Unit supports SNMP for convenient remote management.

Open "Remote Settings" in "Management" shown below. Set the SNMP parameters and obtain MIB

file before remote management.

Status	System	Wireless	Management	Tools
Remote Settings »	Domoto Cott	linaro		
CoovaChilli Settings	Remote Sett	a terrar		
Firmware Upload	Management Privacy			
Configuration File	Normal Sec	ure 🖲 Customized		
Password Settings	V Telnet	SNMP FTP Force HTTPS WISE		
Certificate Settings	SNMP Settings			
	Protocol Version: Server Port. Get Community:	V2 V2 V2		
	Set Community:	private		
	Trap Destination:	0.0.0.0		
	Trap Community:	public		

Figure 33 SNMP Configuration

Enable SNMP

Check this box to enable SNMP settings.

Protocol Version

Select the SNMP version, and keep it identical on the CDS-5IP and the SNMP manager.

Server Port

Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

Get Community

Specify the password for the incoming Get and GetNext requests from the management station.

By default, it is set to public and allows all requests.

Set Community

Specify the password for the incoming Set requests from the management station. By default, it is set to private.

Trap Destination

Specify the IP address of the station to send the SNMP traps to.

Trap Community

Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Configure SNMPv3 User Profile

For SNMP protocol version 3, you can click "**Configure SNMPv3 User Profile**" in blue to set the details of SNMPv3 user. Check "**Enable SNMPv3 Admin/User**" in advance and make further configuration.

Enable SNMPv3Adr	min
User Name:	SNMPv3Admin
Password:	•••••
Confirm Password:	•••••
Access Type:	Read/Write 👻
Authentication Protocol:	MD5 -
Privacy Protocol:	None *
∉ Enable SNMPv3Use	er
User Name:	SNMPv3User
Password:	•••••
Confirm Password:	•••••
Access Type:	Read Only 👻
Authentication Protocol:	MD5 *
Privacy Protocol :	None -

Figure 34 Configure SNMPv3 User Profile

User Name

Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the CDS-5IP - Wireless External Video Unit.

Password

Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the CDS-5IP - Wireless External Video Unit.

Confirm Password

Input that password again to make sure it is your desired one.

• Access Type

Select "Read Only" or "Read and Write" accordingly.

Authentication Protocol

Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

Privacy Protocol

Specify the encryption method for SNMP communication. None and DES are available.

None: No encryption is applied.

DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Upgrade Firmware

Open "**Firmware Upload**" in "**Management**" and follow the steps below to upgrade firmware locally or remotely through the CDS-5IP's Web:

Status	System	Wireless	Management	Tools
Remote Settings				
	upgrade	Firmware		
CoovaChilli Settings			to a new version. Please do not nowe	r off the device
CoovaChilli Settings Firmware Upload	This page allows yo		e to a new version. Please do not power m.	r off the device

Figure 35 Upgrade Firmware

- Click "Browse" to select the firmware file you would like to load;
- Click "Upload" to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

Note:

• Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your Unit, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "Configuration File" in "Management" as below:

Status	System	Wireless	Management	Tools
CoovaChilli Settings	Configuratio	n Eile		
Configuration File »	Configuratio			
Password Settings			file or load the settings from the file rent configuration to factory defaul	
Certificate Settings	Save Settings to File:	Save		

Figure 36 Backup/Retrieve Settings

Save Settings to File

By clicking "**Save**", a dialog box will pop up. Save it, then the configuration file like **ap.cfg** will be saved to your local computer.

Load Setting from File

By clicking "**Browse**", a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click "**Upload**" to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The CDS-5IP - Wireless External Video Unit provides two ways to restore the factory default settings:

Restore factory default settings via Web

From "Configuration File", clicking "Reset Settings to Default" will eliminate all current

settings and reboot your Unit, then default settings are applied.

ation File		
ou to save current settings to a n	file or load the settings from the file w	hich was
Besides, you could reset the curr	rent configuration to factory default o	
o File: Save		
rom File:	瀏覽···· Upload	
	o File: Save rom File: to Default: Reset	rom File: 谢覽···· Upload

Figure 37 Restore Settings

Restore factory default settings via Reset Button

If software in the CDS-5IP is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

Reboot

You can reboot your CDS-5IP from "Configuration File" in "Management" as below:

Click "**Reboot**" and hit "**Yes**" upon the appeared prompt to start reboot process. This takes a few minutes.

nsat	7	CDS-5	YSTEM FOR IP HD	L
Status	System	Wireless	Management	Tools
CoovaChilli Settings	Configur	ration File		
Configuration File	>>		a file or load the settings from the file	
				e which was
Password Settings			current configuration to factory defaul	
Password Settings Certificate Settings	saved previously.	Besides, you could reset the c		t or reboot the

Figure 38 Reboot

Password

From "Password Settings" in "Management", you can change the password to manage your CDS-5IP.

Enter the new password respectively in "New Password" and "Confirm Password" fields; click

"Apply" to save settings.

Status	System	Wireless	Management	Tools
CoovaChilli Settings	Deceward	Sattinga		
Configuration File	Password S	password of this Access	Point	
Password Settings »	New Password:			
Certificate Settings	Confirm Password:			
		Apply	Cancel	
	Figu	ire 39 Passwo	rd	

Chapter 6 Monitoring Tools

System Log

System log is used for recording events occurred on the CDS-5IP, including station connection, disconnection, system reboot and etc.

Open "System Log" in "Tools" as below.

n sar "	RELESS	TRANSMIS	SION SYST	EM FOR IP HD CAM	IERA
Status	System	Wire	ess	Management	Tools
System Log »	Syste	m Log			
Site Survey		e to set remote log ser	ver and show the svs	tem log.	
Ping Watchdog		le Remote Syslog			
Data Rate Test	IP Addre	ara sa A			
Antenna Alignment	Port:		0.0.0.0 514		
Speed Test			Apply Cance	al]	
	#\$	Time 💠	Source \$	Message 💠	
	1	2011- 8- 1 15:58:05	00:19:70:00:FC:60	WLAN service stopped.	
	2	2011-8-1 15:58:06	00:19:70:00:FC:60	WLAN service started.	
	3	2011-8-1 15:58:06	00:19:70:00:FC:60	WLAN service stopped.	
	2				
	4	2011- 8- 1 15:58:06	00:19:70:00:FC:60	WLAN switch antenna from External to Internal.	
		2011- 8- 1 15:58:06 2011- 8- 1 15:58:06	00:19:70:00:FC:60 00:19:70:00:FC:60		
	4			Internal.	
	4	2011-8-1 15:58:06	00:19:70:00:FC:60	Internal. WLAN service started.	

Figure 23 System Log

Remote Syslog Server

Enable Remote Syslog: Enable System log to alert remote server.

IP Address: Specify the IP address of the remote server.

Port: Specify the port number of the remote server.

Site Survey

Only available under SLAVE mode, site survey allows you to scan all the MASTER points within coverage so that you may select a clean channel for your unit based on the scan result. Open "**Site Survey**" in "**Tools**" as below.

			and the second second	China			
Status	System		Wireless	Manag	gement		Tool
System Log							
	Wireless 6	2140	CURVAN				
Site Survey »			6750	work If any Acces	s Point or I	BSS is fou	nd you could
Site Survey » Ping Watchdog	Wireless S This page provides to choose to connect it r	ol to s	scan the wireless net		ss Point or I	BSS is fou	nd, you could
L	This page provides to	ool to s manual	scan the wireless net		Wireless Mode	BSS is fou Signal Strength	nd, you could Security

Figure 24 Site Survey Tool

Ping Watch Dog

If the link is somehow broken and cut off your ability the log in to the CDS-5IP, the ping watchdog has a

chance to reboot due to loss of connectivity.

sat	C)S-5	SYSTEM FOR IP HI	:
Status	System Wire	eless	Management	Tools
System Log				
Site Survey	Ping Watchdog	aure the Pina	Watchdog. If the failcount of the Pin	o reaches to a
Ping Watchdog »	specified value, the watchdog will			
	long land land land land land land land land			
Data Rate Test	Enable Ping Watchdog	192.168.3	173.30	
Data Rate Test Antenna Alignment		192.168. 300	seconds	
	IP Address to Ping:			

Figure 25 Ping Watchdog

Ping Watchdog

Enable Ping Watchdog: To activate ping watchdog, check this checkbox.

IP Address to Ping: Specify the IP address of the remote unit to ping.

Ping Interval: Specify the interval time to ping the remote unit.

<u>Startup Delay</u>: Specify the startup delay time to prevent reboot before the CDS-5IP is fully initialized.

Failure Count To Reboot: If the ping timeout packets reached the value, the unit will reboot automatically.

Date Rate Test

The Data Rate Test allows you test the current RSSI at each data rate between your CDS-5IP -

Wireless External Video Unit.

Data Rate Use this page to test t	the link qual	.7.	mote WDS	node.		
Use this page to test		.7.	mote WDS	node.		
	h					
	0	ndex \$		AC Address	+	
4- 		80 J.J.				
		Refre	sh St	cop		
		Pack	et Size	\$		Domoto
Rate 🗢	64 Bytes	256 Bytes [‡]	752 Bytes [‡]	1472 Bytets	Local RSS#	Remote RSSI +
Auto	95%	100%	99%	100%	-30	-26
6M	100%	100%	100%	100%	-30	-25
9M	100%	100%	100%	100%	-30	-25
12M	0%	0%	0%	0%	-37	-26
MCS0-6.5[13.5]	100%	100%	100%	100%	-30	-28
MCS1-13[27]	100%	100%	100%	100%	-30	-26
MCS2-19.5[40.5]	100%	100%	100%	100%	-30	-26
	Auto 6M 9M 12M MCS0-6.5[13.5] MCS1-13[27]	64 Bytes Auto 95% 6M 100% 9M 100% 12M 0% MCS0-6.5[13.5] 100% MCS1-13[27] 100%	Packa 64 Bytes 256 Bytes Auto 95% 100% 6M 100% 100% 9M 00% 0% 12M 0% 0% MCS0-6.5[13.5] 100% 100%	Packet Size Packet Size Packet Size 64 Bytes 256 Bytes 752 Bytes Auto 95% 100% 99% 6M 100% 100% 100% 9M 100% 100% 100% 12M 0% 0% 0% MCS0-6.5[13.5] 100% 100% 100% MCS1-13[27] 100% 100% 100%	Packet Size * 64 Bytes 752 Bytes 1472 Bytes Auto 95% 100% 99% 100% 6M 100% 100% 100% 100% 6M 100% 100% 100% 100% 9M 100% 100% 0% 0% 12M 0% 0% 0% 0% MCS0-6.5[13.5] 100% 100% 100% 100% MCS1-13[27] 100% 100% 100% 100%	Packet Size Packet Size 64 Bytes 256 Bytes 752 Bytes 1472 Bytes Local RSS* Auto 95% 100% 99% 100% -30 6M 100% 100% 100% -30 9M 100% 100% 100% -30 12M 0% 0% 0% 0% -37 MCS0-6.5[13.5] 100% 100% 100% -30 MCS1-13[27] 100% 100% 100% -30

Figure 26 Data Rate Test

Antenna Alignment

Under WDS mode, when the bridges are not easily visible from the location where the dish will be installed, the antenna alignment tool can help you evaluate the position of the unit and adjust the angle

of the antenna more precisely. Keep it that in real circumstances a lot of additional factors should be taken into account when your unit is installed. These factors include various obstacles (buildings, trees), the landscape, the altitude, transponder orientation, polarization, etc.

To use the tool, select the desired remote WDS bridge and click "Start", the web page will display the measured signal strength, RSSI and transmit/receive packets. If the signal quality is not quite good, try to adjust the antenna and see if the quality improves or not.

System Log Antenna				
	Aliann	nent		
Site Survey Use this page to alig	10220		y.	
Ping Watchdog	0	1	***	
Data Rate Test	0	Index \$	MAC Address 00:19:70:00:fc:60	\$
Antenna Alignment »	0			
Speed Test		Refresh	Wait3	

Figure 27 Antenna Alignment

Speed Test

The speed test is to monitor the current data transmission (TX) and data reception (RX) rate with the remote CDS-5IP - Wireless External Video Unit. Enter the IP address of the remote unit, type in the user name/password and click "**Test**". The result will display in the bottom **STATUS**. You may test single TX/RX or bi-direction.

Status	System	Wireless	Management	Tools
System Log				
Site Survey	Speed Tes		en this device and another termin	al.
Ping Watchdog				
Data Rate Test	Destination IP:	192.168.1.2		
Antenna Alignment	User Name: Password:	admin		
Speed Test »	Direction:	Transmit 💌		
opera rear n		Te	st	
	STATUS: Test comple			

Figure 28 Speed Test

Chapter 7 Status

View Basic Information

Open "Information" in "Status" to check the basic information of the CDS-5IP - Wireless External Video Unit, which is read only. Information includes system information, LAN settings, wireless setting and interface status. Click "Refresh" at the bottom to have the real-time information.

		CDS-5IP		
Status	System	Wireless	Management	Tools
Information »				
Connections	Information	nt status and some basic sett	ince of the device	
Statistics	System Information	nit status and some basic sett	ings of the device.	
ARP Table	Device Name	CDS-5IP		
Bridge Table	MAC Address Country/Region	00:19:70:00:fc:6 European Union	76	
DHCP Clients	Firmware Version	3.0.4(CS)2		
Network Activities	LAN Settings IP Address Subnet Mask Gateway IP Address MAC Address	192.168.1.1 255.255.255.0 0.0.0.0 00:19:70:00:fc:6/	D	
	Wireless Settings			
	Operation Mode Wireless Mode Encryption	Video Bridge 802.11A/N Open System		
	ACK Timeout WMM Enable	27 us On -96 dBm		

Figure 29 Basic Information

View Association List

Open "**Connections**" in "**Status**" to check the information of associated wireless CDS-5IP units such as MAC address, signal strength, connection time, IP address, etc. All is read only. Click "**Refresh**" at the bottom to update the current association list.

No. Server and America		11 (1997)	Distance Transmission				
Status	System	W	ireless		Managemer	it	Tools
Connections Statistics	**	shows the MAC Add		Noise	RSSI for each associat	ed device(s). Last IP	♦ Action
ARP Table	Index	MAC Address =	Strength	Floor	Connection Time	Lastip	Action
Alti Tubic		00:19:70:00:fb:c5	-23	-96	2011-8-1 16:23:47	192,168,1,2	

Figure 30 Connection

By clicking on the MAC address of the selected unit on the web you may see more details including unit name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, current TX/RX packets.

Association Node Details

The details information of association node.

MAC Address	00:19:70:00:fb:c5	Negotiated	Last Signal
Device Name	CDS-5IP	Rate	
Connect Time	2011-8-1 16:23:47	6M	-20 dBm
Signal Strength	-22 dBm	6.5M	-25 dBm
Noise Floor	-96 dBm	9M	-22 dBm
ACK Timeout	27	12M	-21 dBm
Link Quality	40%	13M	-22 dBm
Last IP	192.168.1.2	18M	-15 dBm
TX/RX Rate	52/104 Mbps	19.5M	-26 dBm
TX/RX Packets	14628/18240	24M	-12 dBm
Bytes Transmitted	21230137	26M	-21 dBm
Bytes Received	6849003	36M	-22 dBm
Dytes i tecelveu	0043003	39M	-25 dBm

Figure 31 Association Node Details

View Network Flow Statistics

Open "Flow Statistics" in "Status" to check the data packets received on and transmitted from the wireless and Ethernet ports. Click "Refresh" to view current statistics.

			eta) contra laterna		
itatus	System	Wirele	55	Management	Tool
Information					
Connections	Statis				
Statistics »	This page shi ethernet netv		for transmission and	reception regarding to wireles	s and
hannananan	Poll In	terval: 5	(0-65534) sec	Set Interval Stop	
ARP Table					
Bridge Table			Received	Transmitted	
a second to be a second second		Wireless		Prove server as in	
DHCP Clients		Unicast Packets	18045	14356	
Network Activities		Broadcast Packets	39	44	
Network Activities		Multicast Packets	170	83	
		Total Packets	18254	14483	
		Total Bytes	6849834	20846885	
		Ethernet 1			
		Total Packets	790	1155	
		Total Bytes	82122	1081426	
		Ethernet 2			
		Total Packets	0	0	
		Total Bytes	0	0	

Figure 32 Network Flow Statistics

Poll Interval

Specify the refresh time interval in the box beside "**Poll Interval**" and click "**Set Interval**" to save settings. "**Stop**" helps to stop the auto refresh of network flow statistics.

View ARP Table

Open "**ARP Table**" in "**Status**" as below. Click "**Refresh**" to view current table.

isat '	WIRELESS TRANSMISSION SYSTEM FOR IP HD CAMERA							
Status	System	Wireless	Man	agem	ent	Tools		
Information	4 D D T	- 6.1.2						
Connections	This table sho	able						
Statistics		IP Address 🔶	MAC Address	*	Interface \$			
ARP Table	*	192.168.1.88	20:6A:8A:2F:D5:BE	•	br0			
Bridge Table								
DHCP Clients			Refresh					
Network Activities								

View Bridge Table

Open "Bridge Table" in "Status" as below. Click "Refresh" to view current connected status.

Status	System	Wireless	Manag	ement	Tools
Information					
	Bridge	Table			
Connections	This table shows	bridge table.			
Statistics					
400 T 11		MAC Address \$	Interface \$	Ageing Timer(s)\$	
ARP Table		00:19:70:00:fc:60	Bridge		
Bridge Table »		20:6a:8a:2f:d5:be	LAN	0.00	
Dingo iubio		00:19:70:00:fb:c5	LAN	0.49	

Figure 34 Bridge Table

View Active DHCP Client Table

Open "**DHCP Client**" in "**Status**" as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click "**Refresh**" to view current table.

Status	System	Wireless	Man	agement	Tools
Information	DUCD	Cliente			
Connections	DHCP (s. MAC address and tim	ne expired for each DHCP	eased client
Statistics		IP Address \$			
ARP Table		None		Time Expired(s)	
ARP Table Bridge Table			1785(53) 517517.52		

Figure 35 DHCP Client Table

View Network Activities

The network activities allows you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Web of the Wireless External Video Unit. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. Throughput statistics can be updated manually using the "**Refresh**" button.



Figure 36 Network Activities

Chapter 8 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the CDS-5IP. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of the CDS-5IP?

MAC Address distinguishes itself by the unique identity among network Units. There are two ways available to know it.

• Each Unit has a label posted with the MAC address. Please refer below.



Figure 37 MAC Address

 On the CDS-5IP's Web-based management interface, you can view the MAC Address from "<u>View Basic Information</u>".

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in "Configuration File" from "Management".

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in "**Configuration File**" from "**Management**".

Q 4. What if I cannot access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.

• Hardware reset the unit.

Q 5. In wireless client mode, what if the wireless connection is not stable after associating with an AP?

- Since the CDS-5IP comes with a built-in directional antenna, it is recommended make it face to the direction where the MASTER is to get the best connection quality.
- In addition, you can start "Site Survey" in "Wireless Basic Settings" to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available unit for better connection.

Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ACSII).

As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F,

a-f or punctuation. Each one consists of two-digit hexadecimal.

ASCII	Hex	ASCII	Hex	ASCII	Hex	ASCII	Hex
Character	Equivalent	Character	Equivalent	Character	Equivalent	Character	Equivalent
!	21	9	39	Q	51	i	69
"	22	:	ЗA	R	52	j	6A
#	23	,	3B	S	53	k	6B
\$	24	<	3C	Т	54	-	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
"	27	?	3F	W	57	0	6F
(28	@	40	Х	58	р	70
)	29	А	41	Υ	59	q	71
*	2A	В	42	Z	5A	r	72
+	2B	С	43	[5B	s	73
,	2C	D	44	١	5C	t	74
-	2D	Е	45]	5D	u	75
	2E	F	46	٨	5E	v	76
/	2F	G	47	I	5F	w	77
0	30	Н	48	`	60	х	78
1	31	I	49	а	61	у	79
2	32	J	4A	b	62	Z	7A
3	33	К	4B	С	63	{	7B
4	34	L	4C	d	64		7C
5	35	М	4D	е	65	}	7D
6	36	Ν	4E	f	66	2	7E
7	37	0	4F	g	67		
8	38	Р	50	h	68		

Table 2 ACSII

Appendix B. SSH Settings

Table 3 SSH Settings

get	set	del	Keyword				Descriptions
	\checkmark		time				time setting
\checkmark				-now			current system time
\checkmark	\checkmark			-zone			time zone
	\checkmark			-NTPUpdate			NTP Update
\checkmark	\checkmark			-servertype			server type
\checkmark	\checkmark			-IP			-IP
\checkmark	\checkmark			-Manual IP			-Manual IP
	\checkmark		system				system setting
\checkmark				-swversion			system firmware version
\checkmark	\checkmark			-systemmac			system MAC address
	\checkmark			-devname			system name
	\checkmark			-country			country/region
	\checkmark			-ethernet1DataRate			ether port 1 data rate
	\checkmark			-ethernet2DataRate			ether port 2 data rate
\checkmark	\checkmark			-macclone			mac clone enable
\checkmark	\checkmark			-clonedmac			cloned mac address
	\checkmark			-poepower			secondary RJ45 power
	\checkmark			-stp			Spanning Tree
	\checkmark			-stpForwardDelay			STP forward delay
	\checkmark			-gpslatitude			gps latitude
\checkmark	\checkmark			-gpslongitude			gps longitude
\checkmark	\checkmark		ipset				
\checkmark				-networkmode			network mode select
v	v			-networkmode			(bridge or router)
\checkmark	\checkmark			-bridge			bridge mode ip settings
	\checkmark				-iptype		fixed/dynamical ip(dhcp
'	•				iptype		client)
\checkmark	\checkmark				-ipaddr		ip address
\checkmark	\checkmark				-netmask		subnet mask
\checkmark	\checkmark				-gateway		gateway ip address
\checkmark	\checkmark				-dns1		dns1
\checkmark	\checkmark				-dns2		dns2
\checkmark	\checkmark			-router			router mode ip settings
\checkmark	\checkmark				-wan		wan ip settings
\checkmark	\checkmark					-accesstyp e	router mode access type
		l		1	1	-staticipadd	static ip address

	ĺ				r	
\checkmark	\checkmark				-staticnetm ask	static subnet mask
\checkmark	\checkmark				-staticgate way	static gateway ip address
\checkmark	\checkmark				-staticdns1	static dns1
\checkmark	\checkmark				-staticdns2	static dns2
\checkmark	\checkmark				-dhcpclient hostname	dhcp client hostname
\checkmark					-pppoecon nectstatus	pppoe connect status
\checkmark					-pppoelocal ip	obtains IP from pppoe server
\checkmark	\checkmark				-pppoestati cipaddr	pppoe static ip address
\checkmark	\checkmark				-pppoeuser name	pppoe username
\checkmark	\checkmark				-pppoepass word	pppoe password
\checkmark	\checkmark				-pppoeserv ername	pppoe server name
\checkmark	\checkmark				-pppoecon nectmode	pppoe connect mode
\checkmark	\checkmark				-pppoeidleti me	pppoe idle time
\checkmark	\checkmark			-lan		lan ip settings
\checkmark	\checkmark				-ipaddr	lan ip address
\checkmark	\checkmark				-netmask	lan subnet mask
\checkmark	\checkmark				-dhcpserve renable	dhcp server enable
\checkmark	\checkmark				-dhcpserve ripstart	dhcp server ip start
\checkmark	\checkmark				-dhcpserve ripend	dhcp server ip end
\checkmark	\checkmark				-dhcpserve rleasetime	dhcp server leasetime
\checkmark	\checkmark				-dhcprelay enable	dhcp relay enable
\checkmark	\checkmark				-dhcpserve rip	dhcp server ip
\checkmark	\checkmark	wlan				wlan setting
\checkmark	\checkmark		-operationmode			operation mode
\checkmark	\checkmark		-ssid			wireless network name
\checkmark	\checkmark		-ssidhided			wireless SSID broadcast

\checkmark	\checkmark			-type	wireless wep key type
	\checkmark	\checkmark	-key		wireless wep key setting
\checkmark	\checkmark		-encryption		 wireless data encryption
\checkmark	\checkmark		-authentication		wireless authentication type
\checkmark	\checkmark		-среТуре		СРЕ Туре
\checkmark	\checkmark		-stdm		stdm setting
	\checkmark		-IGMP		IGMP
	\checkmark		-preamble		 preamble
\checkmark	\checkmark		-DTIM		DTIM
\checkmark	\checkmark		-beacon		beacon
\checkmark	\checkmark		-fragment		 fragment
\checkmark	\checkmark		-RTS		RTS
\checkmark	\checkmark		-RIFS		rifs
\checkmark	\checkmark		-shortGI		short GI
\checkmark	\checkmark		-A-MSDU		A-MSDU
\checkmark	\checkmark		-A-MPDU		A-MPDU
	\checkmark		-extension		 extension
	\checkmark		-channelOffset		channel offset of 40MHz
\checkmark	\checkmark		-channelMode		channel mode
	\checkmark		-LinkIntegration		class setting
1	,				meter setting wireless bwa coverage
\checkmark	\checkmark		-spaceInMeter		wireless bwa space in
\checkmark	\checkmark		-StaNumLmt		Whether manually limit the number of station
\checkmark	\checkmark		-maxStaNum		max sta connection number
N	V		-Isolation		communication between clients
					wireless isolate
			-wmm		wmm settings
			-antennaGain		antenna gain setings
			-antenna		antenna type
			-rate		rate
	√ √		-frequency/channel		(depends on country and wireless mode) power
					-wireless frequency/channel
	\checkmark		-HTprotect		HT protect
\checkmark	\checkmark				
	\checkmark		-wirelessmode		wireless mode

\checkmark				-ssid		ssid of this vap
\checkmark	\checkmark			-profileName		Name of profile
	\checkmark			-active		on/off this vap
\checkmark	\checkmark		vapprofile 1(2, 3,etc)			VAP setting
\checkmark				-association		list of associated wireless clients
\checkmark	\checkmark			-wdsSeparation		WDS Separation
√					-remote4	remote macAddr4
√					-remote3	remote macAddr3
<u>√</u>					-remote2	remote macAddr2
<u>√</u>					-remote1	remote macAddr1
√					-local	local macAddr
√	\checkmark			-wdsMac		WDS Remote Mac
√					-upburst	Outgoing Traffic Burst
√					-uplimit	Outgoing Traffic Limit
<u>√</u>					-downburst	Incoming Traffic Burst
<u>√</u>					-downlimit	Incoming Traffic Limit
√					-enable	enable Traffic Shaping
√				-trafficshaping		traffic shaping
					password	
					-privatekey	WPA private key password
\checkmark	\checkmark				-usercert	WPA cert file
√					-password	WPA password
√					-loginname	WPA login name
√					-username	WPA user name
					pe	
					-innereapty	WPA inner EAP Type
	\checkmark	\checkmark		-	-eaptype	WPA EAP Type
	\checkmark			-eap		WPA EAP setting
\checkmark	\checkmark				-keyupdate	enable wireless WPA global key update
\checkmark	\checkmark				-reauthtime	wireless WPA re-auth period (in seconds)
\checkmark	\checkmark	\checkmark			-psk	wireless pre-shared key (PSK) for WPA-PSK
\checkmark	\checkmark	\checkmark		-wpa		wireless WPA setting
√					-4	wireless wep key 4
√					-3	wireless wep key 3
√					-2	wireless wep key 2
√			ļ		-1	wireless wep key 1
V	V				-default	wireless wep default key index

\checkmark	\checkmark		-ssidhided		Broadcast SSID Enable or
	√				Disable
$\frac{}{}$			-vlanID		vlanID of this vap
			-Isolation		wireless separation
<u>√</u>			-wmm		WMM Support
\checkmark	\checkmark		-MaxStaNum		Max Station Number
	\checkmark		-StaNumLmt		Whether manually limit the
					number o f station
	\checkmark		-authentication		wireless authentication
1	1				type
\checkmark	\checkmark		-encryption		wireless data encryption
	\checkmark		-default		wireless wep default key
	,				index
	\checkmark		-wpa		wireless WPA setting
			-association		list of associated wireless
					clients
	\checkmark	vlan			vlan setting
	\checkmark		-active		enable 802.1Q VLAN
	\checkmark		-manageID		Management VLAN ID
	\checkmark	radius			radius setting
	\checkmark		-IPaddr		IP address
\checkmark	\checkmark		-port		port
	\checkmark		-shared secret		Shared Secret
	\checkmark	firewall			firewall setting
	\checkmark		-srcipfilter		source ip filter settings
	\checkmark			-enable	source ip filter enable
	\checkmark			-addrule	add a source ip filter rule
	\checkmark			-delerule	delete source ip filter rule
1					show source ip filter rule
				-rulelist	lists
	\checkmark		-destipfilter		destination ip filter settings
	\checkmark			-enable	destination ip filter enable
1	1				add a destination ip filter
	\checkmark			-addrule	rule
	,				delete destination ip filter
	\checkmark			-delerule	rule
1					show destination ip filter
				-rulelist	rule lists
	\checkmark		-srcportfilter		source port filter settings
	\checkmark			-enable	source port filter enable
					add a source port filter
	\checkmark			-addrule	rule
	+				delete source port filter
	\checkmark			-delerule	

				-rulelist	show source port filter rule lists
\checkmark	\checkmark		-destportfilter		destination port filter settings
\checkmark	\checkmark			-enable	destination port filter enable
\checkmark	\checkmark			-addrule	add a destination port filter rule
	\checkmark			-delerule	delete destination port filter rule
\checkmark				-rulelist	show destination port filter rule lists
	\checkmark		-portforward		port forward settings
	\checkmark			-enable	port forward enable
	\checkmark			-addrule	add a port forward rule
	\checkmark			-delerule	delete port forward rule
\checkmark				-rulelist	show port forward rule lists
			-dmzenable		dmz enable
			-dmzipaddr		dmz ip address
\checkmark	\checkmark	remote			remote management setting
	\checkmark		-privacy		radius IP address
	\checkmark		-telnet		enable telnet
	\checkmark		-snmp		enable snmp
	\checkmark		-ftp		enable ftp
			-ssh		enable ssh
			-forcehttps		force https
			-wise		enable wise tools
	\checkmark	snmp			SNMP setting
	\checkmark		-version		Protocol Version
	\checkmark		-port		Server Port
	\checkmark		-getCommunity		SNMP Read Community
			-setCommunity		SNMP Write Community
			-trapdestination		Trap Destination
	\checkmark		-trapcommunity		Trap Community
	\checkmark		-v3Admin		v3Admin
				-on	Enable SNMPv3Admin
	\checkmark			-name	name
				-password	password
\checkmark				-accessTyp e	access type
				-authentica	Authentication Protocol

		1			tion	
\checkmark	\checkmark				-Privacy	privacy protocol
\checkmark	\checkmark			-v3User		-v3User
	\checkmark				-on	Enable SNMPv3User
					-name	name
					-password	password
1	1				-accessTyp	
\checkmark	\checkmark				е	access type
I	1				-authentica	
\checkmark	\checkmark				tion	Authentication Protocol
\checkmark	\checkmark				-Privacy	privacy protocol
	\checkmark		coovachilli			CoovaChilli setting
				-coovaChilliEnable		Coovachilli Enable
1	1			-primaryRadiusServ		
\checkmark	\checkmark			er		Primary RADIUS Server
1	1			-secondaryRadiusSe		Secondary RADIUS
	\checkmark			rver		Server
1	1					RADIUS Authentication
	\checkmark			-radiusAuthPort		Port
	\checkmark			-radiusAcctPort		RADIUS Accounting Port
				-radiusSharedSecret		RADIUS Shared Secret
				-radiusNasid		RADIUS Nasid
\checkmark				-radiusAdminUserna me		RADIUS Admin Username
				-radiusAdminPassw ord		RADIUS Admin Password
				-uamPortalUrl		UAM Portal URL
	1			-uamSecret		UAM Secret
			syslog			syslog
			e yeleg	-client		enable syslog client
				-ipaddr		syslog server IP address
				-port		syslog server port number
•				-clear		syslog clear
	1		pingwdg			ping watchdog
v √	v √		Pingway	-enable		enable
$\sqrt{\frac{v}{\sqrt{v}}}$	v √			-interval		interval
v √	v √			-startdelay		startup delay
v √	v √			-failcount		failure count
$\frac{N}{}$	$\sqrt{\frac{1}{\sqrt{2}}}$					
	$\sqrt{\frac{1}{\sqrt{2}}}$	\checkmark		-ip		ip address
	N	N	acl			access control
\checkmark	\checkmark			-mode		enable wireless access control (ACL)
		\checkmark		-delete		delete a local ACL

						address	
\checkmark				-list		delete or display all local	
v		v		-1151		ACL address	
	\checkmark			-MacAddr		add mac address to	
	'						Current Access Control List
\checkmark			statistics			statistics	
\checkmark				-Wireless		Wireless LAN	
\checkmark				-Ethernet		Ethernet LAN	
\checkmark		\checkmark	log list			syslog list	
	\checkmark		password			system password	
	\checkmark		reset			restore factory	
	\checkmark		reboot			reboot system	
	\checkmark		exit			logout from CLI	

Appendix C. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there may contains some public software, if it is, please read below carefully:

1. Definition

"**Public Software**", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in <u>the Section 5</u>, the indicated <u>website</u>, the complete license terms can be found.

"Public Software" shall mean each of:

(a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and

(b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2.

Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and

conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in <u>its presentation on website</u>.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table	2 Public	Software	Name and	d Description	
-					

Program	Copy Right	Origin Sour	Licenses or	License Terms
Name	Description	Code	Distribution Models or	Website
			its special license	Reference
			terms	
U-boot	Wolfgang Denk,	ftp://ftp.denx.de/	GNU GENERAL	GNU GENERAL
	DENX Software	pub/u-boot/	PUBLIC LICENSE	PUBLIC
	Engineering,		Version 2	LICENSE Version
	wd@denx.de			2
Busybox		http://www.busy	GNU GENERAL	http://www.gnu.or
		box.net/downloa	PUBLIC LICENSE	g/licenses/old-lice
		ds/busybox-1.01	Version 2	nses/gpl-2.0.html
		.tar.bz2		

Goahead	Copyright (c)	http://data.goahe			
	GoAhead	ad.com/Software			
	Software Inc.,	/Webserver/2.1.			
	1992-2000.	8/webs218.tar.g			
		Z			
hostapd	Copyright (c)	http://hostap.epit	GNU	GENERAL	http://www.gnu.or
	2002-2006, Jouni	est.fi/releases/h	PUBLIC	LICENSE	g/licenses/old-lice
	Malinen	ostapd-0.4.8.tar.	Version 2		nses/gpl-2.0.html
	<jkmaline@cc.hut< th=""><th>gz</th><th></th><th></th><th></th></jkmaline@cc.hut<>	gz			
	.fi> and				
	contributors				
wpa_suppl	Copyright (c)	http://hostap.epit	GNU	GENERAL	http://www.gnu.or
icant	2003-2005, Jouni	est.fi/releases/w	PUBLIC	LICENSE	g/licenses/old-lice
	Malinen	pa_supplicant-0.	Version 2		nses/gpl-2.0.html
	<jkmaline@cc.hut< th=""><th>4.7.tar.gz</th><th></th><th></th><th></th></jkmaline@cc.hut<>	4.7.tar.gz			
	.fi> and				
	contributors				
ntpclient	Copyright 1997,	http://doolittle.ica	GNU	GENERAL	http://www.gnu.or
	1999, 2000, 2003	rus.com/ntpclien	PUBLIC	LICENSE	g/licenses/old-lice
	Larry Doolittle	t/ntpclient_2003	Version 2		nses/gpl-2.0.html
		_194.tar.gz			
net-snmp	Copyright(c)	http://prdownloa	GNU	GENERAL	http://www.gnu.or
	2001-2003,	ds.sourceforge.n	PUBLIC	LICENSE	g/licenses/old-lice
	Networks	et/net-snmp/net-	Version 2		nses/gpl-2.0.html
	Associates	snmp-5.4.1.tar.g			
	Technology, Inc	z			
	All rights				
	reserved.				
			1		

<i></i>		ft = // = ft = 1 = = = = f			
vsftpd	Author: Chris	ftp://vsftpd.beast	GNU	GENERAL	http://www.gnu.or
	Evans	s.org/users/ceva	PUBLIC	LICENSE	g/licenses/old-lice
		ns/vsftpd-1.1.2.t	Version 2		nses/gpl-2.0.html
		ar.gz			
linux		ftp://ftp.kernel.or	GNU	GENERAL	http://www.gnu.or
		g/pub/linux/kern	PUBLIC	LICENSE	g/licenses/old-lice
		el/v2.6/linux-2.6.	Version 2		nses/gpl-2.0.html
		15.tar.bz2			
iptables	Copyright	ftp://ftp.netfilter.o	GNU	GENERAL	http://www.gnu.or
	2000-2004	rg/pub/iptables/i	PUBLIC	LICENSE	g/licenses/old-lice
	netfilter project	ptables-1.3.6.tar.	Version 2		nses/gpl-2.0.html
	http://www.netfilter	bz2			
	.org/				
openssl	Copyright (c)	http://www.open	GNU	GENERAL	http://www.gnu.or
	1998-2008 The	ssl.org/source/o	PUBLIC	LICENSE	g/licenses/old-lice
	OpenSSL Project.	penssl-0.9.8k.tar	Version 2		nses/gpl-2.0.html
	All rights	.gz			
	reserved.				
Igmpproxy	Copyright (C)	http://sourceforg	GNU	GENERAL	http://www.gnu.or
	2005 Johnny	e.net/projects/ig	PUBLIC	LICENSE	g/licenses/old-lice
	Egeland	mpproxy/files/ig	Version 2		nses/gpl-2.0.html
	<johnny@rlo.org></johnny@rlo.org>	mpproxy/0.1/igm			
		pproxy-0.1.tar.gz			
		/download			
Dnrd	Copyright (C)	http://sourceforg	GNU	GENERAL	http://www.gnu.or
	1998 Brad M.	e.net/projects/dn	PUBLIC	LICENSE	g/licenses/old-lice
	Garcia	rd/files/dnrd/2.12	Version 2		nses/gpl-2.0.html
	<garsh@home.co< th=""><th>/dnrd-2.12.tar.gz</th><th></th><th></th><th></th></garsh@home.co<>	/dnrd-2.12.tar.gz			
	m>	/download			

iproute	Stephen	http://developer.	GNU	GENERAL	http://www.gnu.or
	Hemminger	osdl.org/dev/ipro	PUBLIC	LICENSE	g/licenses/old-lice
	shemminger@osd	ute2	Version 2		nses/gpl-2.0.html
	l.org				
	Alexey Kuznetsov				
	kuznet@ms2.inr.a				
	c.ru				
Pppd	Paul Mackerras	ftp://ftp.samba.or			
	<paulus@linuxcar< th=""><th>g/pub/ppp/</th><th></th><th></th><th></th></paulus@linuxcar<>	g/pub/ppp/			
	e.com>				

Appendix D. Country Channel List

The CDS-5IP - Wireless External Video Unit supports country selection. Channels may vary upon each country's regulation. The following tables list the channel with country code in each bandwidth.

Table 3 FCC Countries

Country	Mode	Channel list			
		40MHz	20MHz	10MHz	5MHz
United States Chile China Columbia Mexico Panama Philippines Taiwan Uruguay Venezuela	(5725~5850)	149/153/157/ 161	149/153/157/161/ 165	149/151/153/155/ 157/159/161/163/1 65	149/150/151/152/ 153/154/155/156/ 157/158/159/160/ 161/162/163/164/ 165

Table 4 CE Countries

Country	Mode	Channel list				
		40MHz	20MHz	10MHz	5MHz	
Albania					100/101/102/103/	
Algeria	11a					
Australia	(5470~5725)			100/100/100/1000/	104/105/106107/	
Austria	Excluded	Excluded	100/104/108/	100/104/108/112	100/102/104/106/ 108/110/112/114/	108/109/110/111/
Belgium	CH120~CH131		116/132/136/140	116/118/132/134/1	112/113/114/115/	
Bulgaria	011120 011101	112/132/136		00/400/440	116/117/118/119/	
Cyprus	Meteorology			36/138/140		
Czech	Radars				131/132/133/134/	
Republic					135/136/137/138/	
Denmark						

Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Latvia
Liechtenstein
Lithuania
Luxembourg
Macedonia
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United
Kingdom

Table 5 Other Countries

Country	Mode	Channel list				
		40MHz	20MHz	10MHz	5MHz	
India	11a 5725-5875MHz			149/151/153/155/ 157/159/161/163/1 65/167/169/171/17 3	149/150/151/152/ 153/154/155/156/ 157/158/159/160/ 161/162/163/164/ 165/166/167/168/ 169/170/171/172/ 173	

Korea Russia	11a 5470-5650MHz 5725-5825MHz	100/104/108/ 112/149/153/ 157/161 *Russia: Does not support HT40.	100/104/108/112/ 116/149/153/157/ 161	100/102/104/106/ 108/110/112/114/ 116/149/151/153/1 55/157/159/161/	100/101/102/103/ 104/105/106107/ 108/109/110/111/ 112/113/114/115/ 116/149/150/151/ 152/153/154/155/ 156/157/158/159/ 160/161/
South Africa	11a 5470-5725MHz 5725-5875MHz	112/116/132/	116/132/136/140/ 149/153/157/161/	100/102/104/106/ 108/110/112/114/ 116/118//132/134/1 36/138/140//151/15 3/155/157/159/161/ 165	135/136/137/138/