

User Manual

EKI-1334



Copyright

The documentation and the software included with this product are copyrighted 2015 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

- Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
- All other product names or trademarks are properties of their respective owners.

Product Warranty (5 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for five years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For outof-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

- 1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
- 2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
- 3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
- 4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
- 5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. Printed in Taiwan Edition 1 October 2015

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

Technical Support and Assistance

- 1. Visit the Advantech web site at http:support.advantech.com.cn where you can find the latest information about the product.
- 2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
 - Product name and serial number
 - Description of your peripheral attachments
 - Description of your software (operating system, version, application software, etc.)
 - A complete description of the problem
 - The exact wording of any error messages

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com.

Safety Instructions

- 1. Read these safety instructions carefully.
- 2. Keep this User Manual for later reference.
- 3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- 4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- 5. Keep this equipment away from humidity.
- 6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- 7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- 8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- 9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- 10. All cautions and warnings on the equipment should be noted.
- 11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- 12. Never pour any liquid into an opening. This may cause fire or electrical shock.
- 13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- 14. If one of the following situations arises, get the equipment checked by service personnel:
 - The power cord or plug is damaged.
 - Liquid has penetrated into the equipment.
 - The equipment has been exposed to moisture.
 - The equipment does not work well, or you cannot get it to work according to the user's manual.
 - The equipment has been dropped and damaged.
 - The equipment has obvious signs of breakage.
- 15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40° C (-40° F) OR ABOVE 80° C (140° F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
- 16. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.
- 17. The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

- To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
- Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

EKI-1334 User Manual

Contents

Chapter	1	Overview	1
	1.1 1.2 1.3	Introduction Package Checklist Product Features 1.3.1 Interfaces 1.3.2 Functions 1.3.3 Environmental Limits 1.3.4 Power Requirements 1.3.5 Physical Characteristics 1.3.6 Advanced Industrial Characteristics 1.3.7 Warranty	2 4 4 4 5 5 5 5
Chapter	2	Hardware Installation	7
	2.1 2.2 2.3 2.4 2.5	Typical ApplicationPanel LayoutQuick Connection to Internet.2.3.1 Insert SIM Card2.3.2 Antenna Installation2.3.3 Power Supply.2.3.4 Connect.2.3.5 Build Connection between EKI-1334 and PC2.3.6 Start to configure your EKI-1334 (Optional)2.3.7 Connect EKI-1334 with InternetQuick IPSec VPN ConfigurationReset to Factory Defaults2.5.1 Hardware Approach2.5.2 Web Approach	
Chapter	3	Advanced Configuration	21
	3.1 3.2	Configuration on Web3.1.1Preparation3.1.2System3.1.3Network3.1.4Service3.1.5Firewall3.1.6QoS3.1.7VPN3.1.8Tools3.1.9StatusCLI Configuration3.2.1CLI Operation3.2.2CLI command	22 24 29 36 40 43 43 53 54 57 57 59
Appendix	хА	FAQ	61
	A.1 A.2	FAQ Support	62 63

EKI-1334 User Manual



Overview

Sections include:

- Introduction
- Package Checklist
- Features & Specifications
- Product Models

1.1 Introduction

EKI-1334 are M2M wireless routers that integrate 3G network and virtual private network (VPN) technologies. The products meet fundamental needs of field communication in industry, support international commercial UMTS (HSPA+) and GPRS network.

The design of the EKI-1334 fully incorporated the requirements of industrial users, adopted multi-level software detection mechanism. Multiple VPN protocol ensures security in data transmission, preventing malicious access and tampering of data. The humanized WEB configuration interface is easy for customer to use. It also supports connection to multiple network devices, enabling multi service processing.

The EKI-1334 are the ideal choice for industrial usage, having low power consumption, wide working temperature range from -20° C to 70° C, small size and light weight that is easy for application in harsh, narrow industrial environment.

Important Safety Information

This product is not intended for use in the following circumstances

- Area(s) where radio transmission equipment (such as cell phone) are not permitted.
- Hospitals, health care facilities and area(s) where cell phones are restricted by law.
- Gas stations, fuel storage and places where chemical are stored.
- Chemical plants or places with potential explosion hazard.
- Any metal surface that may weaken the radio signal level.

RF safety distance

- For GPRS router, the compliance boundary distance is r=0.26 m for GSM 900 MHz and r=0.13 m for DCS 1800 MHz.
- For HSUPA router, the compliance boundary distance is r=0.26 m for GSM 900 MHz and r=0.13 m for DCS 1800 MHz, r=.0.094 for WCDMA 900 MHz, r=0.063 for WCDMA 2100 MHz.

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Notice

The Directive on Waste Electrical and Electronic Equipment (WEEE), which entered into force as European law on 13th February 2003, resulted in a major change in the treatment of electrical equipment at end-of-life.

The purpose of this Directive is, as a first priority, the prevention of WEEE, and in addition, to promote the reuse, recycling and other forms of recovery of such wastes so as to reduce disposal.

The WEEE logo (shown at the left) on the product or on its box indicates that this product must not be disposed of or dumped with your other household waste. You are liable to dispose of all your electronic or electrical waste equipment by relocating over to the specified collection point for recycling of such hazardous waste. Isolated collection and proper recovery of your electronic and electrical waste equipment at the time of disposal will allow us to help conserving natural resources. Moreover,

proper recycling of the electronic and electrical waste equipment will ensure safety of human health and environment.



For more information about electronic and electrical waste equipment disposal, recovery, and collection points, please contact your local city centre, household waste disposal service, shop from where you purchased the equipment, or manufacturer of the equipment.

1.2 Package Checklist

We put each EKI-1334 cellular router in a box with standard accessories. Additionally, there're optional accessories can be ordered. When you receive our package, please check carefully, and if there're items missing or appearing to be damaged, please contact with your Advantech sales representative.

Items in package include:

Standard Accessories:

Accessories	Description	
EKI-1334 Cellular Router	1	
Cable	1 Cross line, CAT-5,1.5M	-
Antenna	3 m Cellular Antenna	

1.3 Product Features

1.3.1 Interfaces

WAN

Cellular WAN:

- Band Options: GSM/GPRS/EDGE: 850/900/1800/1900 MHz
- UMTS /HSPA/HSPA+: 850/900/1900/2100 MHz

Ethernet WAN:

- Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX
- Magnetic Isolation Protection: 1.5 KV built-in

LAN

- Number of Ports: 3
- Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX
- Magnetic Isolation Protection: 1.5 KV built-in

DMZ

- Number of Ports: 1
- Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX
- Magnetic Isolation Protection: 1.5 KV built-in

Serial

- Serial Type: RS232
- Data bit: 5/6/7/8
- **Stop bit:** 1/2
- Check bit: N/O/D
- **Baud rate:** 3,200 bit/s ~ 115, 200 bit/s

SIM Interface

SIM Control: 3 V

1.3.2 Functions

- PPP:
 - Support VPDN/APN, fast access to virtual private dial-up network (VPDN) provided by mobile operator, ensure high-security data transmission.
 - Support CHAP/PAP/MS-CHAP/MS-CHAP V2 authorization
 - Support Connection Detection, auto-recovery, auto-link, ensure reliable communication.
 - Support On-demand connection, SMS Activity
- Dynamic IP: Support DHCP, applied as Server/Client
- Dynamic DNS:
 - Support Dynamic DNS-IP Binding
 - Provide DDNS analyze to help access dynamic data center
- **Flux Management:** Support rate limiting,

Firewall Function:

- Package filtering
- Port Mapping

- Virtual Address Mapping
- DMZ zone
- MAC addresses binding.
- Route function: Support Static Routing Table
- VPN: IPSec/SSL VPN, L2TP/PPTP VPN, GRE
- Link Backup:
 - VRRP: Support VRRP protocols, realizing immediate link backup
- **DNS Forwarding:** Support DNS Forwarding, support DNS record
- Network tools: Support Ping, Trace Route and Telnet

1.3.3 Environmental Limits

- Operating Temperature: -20 to 70° C (-4 to 158° F)
- **Operating Humidity:** 5 to 95% RH
- **Storage Temperature:** -40 to 85° C (-40 to 167° F)

1.3.4 Power Requirements

- Power Inputs: 1 terminal block, including power jack and serial
- Input Voltage: 9 ~ 26 V_{DC}

1.3.5 Physical Characteristics

- Housing: Steel, providing IP30 protection
- Dimensions (mm):







Front View

1.3.6 Advanced Industrial Characteristics

Physical Characteristics: Shell: Metal, IP30

1.3.7 Warranty

- Warranty Period: 5 year
- Ш

EKI-1334 User Manual



Hardware Installation

Sections include:

- Typical Application
- Panel Layout
- Quick Connect to Internet
- Quick IPSec VPN Configuration
- Reset to Factory Defaults

2.1 Typical Application

EKI-1334 can be used to connect your device (with RS232/Ethernet Interface) to Internet via GPRS/ 3G cellular network. Meanwhile, to ensure the security and access, EKI-1334 support VPN, enabling remote access and secure data transmission through Internet.

2.2 Panel Layout



The Reset bottom, SIM card slot and power supply are on above panel.

Signal Status LED Description



5 ----- Signal: 10-19 (Router can work under this signal level)

------ Signal: 20-31 (Perfect signal level)

2.3 Quick Connection to Internet

2.3.1 Insert SIM Card

Open EKI-1334 SIM/UIM card case at the bottom, insert the SIM card and close the case.

2.3.2 Antenna Installation

After install the EKI-1334, connect the interface of enhanced antenna to the interface of skin antenna and screw tightly. Put the amplifier of enhanced antenna to where it can receive the signal well.

Caution! Position and angle of the antenna may influence the quality of signal.



2.3.3 Power Supply

Connect EKI-1334 to power supply with the power supply cord in the package, observe whether the Power LED on the panel of EKI-1334 goes on. If not, please contact Advantech for technical support.

You can start to configure EKI-1334 after the Power LED turns on.

2.3.4 Connect

Link EKI-1334 with PC:

- 1. Using a cable to link EKI-1334 with a PC;
- 2. After the connection, you can see one LED of RJ45 Interface turns green and the other flashes.

2.3.5 Build Connection between EKI-1334 and PC

EKI-1334 Router can auto-distribute IP address for PC. Please set the PC to automatically obtain IP address via DHCP. (Based on Windows Operation System):

- 1. Open "Control Panel", double click "Network Connections" icon, and enter "Network Connections" Screen.
- 2. Double click "Local Area Connection", enter "Local Area Connection Status" screen:

ieneral	Support		
Conn	ection		
Stat	us:		Connected
Dura	stion:		00:18:12
Spe	ed		1.0 Gbps
Activi	ty		
		Sent —	Received
Byte	¢.	33,920	107,297
Prop	eties	Disable	
Prop	erties	Disable	

3. Click "Properties", enter "Local Area Connection Properties" screen

ieneral Advanced	
Connect using:	
VMware Accelerated AMD PCNet Ad	Configure
This connection uses the following items:	
Clent for Microsoft Networks File and Printer Sharing for Microsoft Network O O Packet Scheduler Contennet Photocol (CCP/IP)	rks -
Igstal	Properties
Description	
	he default
Transmission Control Protocol/Internet Protocol. T wide area network protocol that provides commun across diverse interconnected networks.	ication
Transmission Control Protocol/Internet Protocol. T wide area network protocol that provides commun across diverse interconnected networks. Show icon in notification area when connected Notify me when this connection has limited or no	connectivity

Choose "Internet Protocol (TCP/IP)", click "properties" button, ensure your PC can obtain IP and DNS address automatically. (Or you can set your PC in the subnet: 192.168.2.0/24, for example, set IP: 192.168.2.10, Net Mask: 255.255.255.0, Default Gateway: 192.168.2.1)

Seneral	Alternate Configuratio	n		
You can this capi the appr	get IP settings assign ability. Otherwise, your opriate IP settings.	ed automatically need to ask your	il your network s network adminis	upports trator for
⊙ 0b	tain an IP address aut	omatically		
OUD	e the following IP addr	ess:		
Pad	diess:			
Subro	et madic			
Deta	il gateway.			
@ 0b	tain DNS server addre	ss automatically		
OUs	e the following DNS se	ever addresses:		
Piele	red DNS server:			
Abri	ate DNS server.			
			Adv	anced

Click "OK", EKI-1334 will allocate an IP address: 192.168.2.x, and a gateway: 192.168.2.1(the default address of EKI-1334).

After configure TCP/IP protocols, you can use ping command to check whether the link between PC and Router is built correctly. Below is an example to execute Ping command under Windows XP:

Ping 192.168.2.1

If the screen shows:

Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\inhand>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms ITL=128 Reply from 192.168.2.1: bytes=32 time=1ms ITL=128 Reply from 192.168.2.1: bytes=32 time=1ms ITL=128 Reply from 192.168.2.1: bytes=32 time<1ms ITL=128
Ping statistics for 192.168.2.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 1ms, Average = Oms
C:\Documents and Settings\inhand>ping 192.168.2.1

Then the PC and EKI-1334 are correctly connected. Else if it shows:



The connection is not built, you need to check step by step starting from Section 2.3.4.

2.3.6 Start to configure your EKI-1334 (Optional)

After you have finished the former steps, you can configure the EKI-1334:

1. Open IE browser, input the default IP address of the Router: http://192.168.2.1, you can see the login page as below:

EKI-1334	Login
Username	
Password	
	Login

Input "username" (default: adm) and the "password" (default: 123456), then click "login" to enter the operation screen.

2. Change the IP configuration:

Caution! After updating the configuration, please click "apply" to activate your configuration.



If you want to set your own IP of EKI-1334, please follow the instructions below:

System	Betwork	Services	Fireval1	QoS	12.8	Teels	Statur
					System 3	tatus	
Fane		Router					
Rodel .		100954001					
Serial States	() ()	89095111129500	90				
bearrightion		www.inhand.com	6 CD				
Ourrent Versi	ion.	1.2.0.12462(to	(#th				
Oureaut Boot	loader Version	1.1.3.13121					
Router Time		2000-01-01 08:	104:10				
PC Time		2012-03-20 08:	50:00 Sy	NO. TANK			
Tp tian		0 day, 00:04:1	52				
CPE Load to /	9 / 15 mina)	0.00 / 0.01 /	0.00				
Beauty consul	ption	28,9080 / 17,9	1000 (dz. 201	0 2			

Click "Network"=>"LAN", change the IP address to 192.168.1.254:

System	Network	Services	Firewall	QoS
MAC Address		00:18:05:00:	45:C6	Default
IP Address		192.168.1.25	4	
Netmask		265.265.255	0	
MTU		Default 💌 1	600	
Detection host		0.0.0.0		
LAN Mode		Auto Negotia	tion 💌	

3. Click "Apply", then you will see:

Executing	
Please wait for 8 Seconds	
and the second sec	

Now the IP address of EKI-1334 has been reset, and in order to enter the configuration page, you need to set your PC in the same subnet as EKI-1334, for example: 192.168.1.10/24 then input the updated IP address (192.168.1.254) in your IE Browser.

2.3.7 Connect EKI-1334 with Internet

Follow the configuration steps below to enable EKI-1334 to connect to the internet.

1. Click "Network"=>"Dialup", enter dialup configuration interface:

	Enabling	z an Intellig	gent Plane	*				
System	Network	Services	Firewall	QoS	VPN	Tools	Status	
						Dialup)	
Enable								
Time schedule	2	ALL . Sch	edule Managen	nent				
PPPoE Bridge								
Shared Connection(NAT)		8						
Default Route								
Network Provider (ISP)		Custom		 Mana 	age			
APN		internet						
Access Numbe	er	*99#						
Username		web						
Password		•••						
Network Selec	t Type	3G Only *						
Band		ALL			•			
Static IP								
Connection Me	ode	Always Online 🔻						
Redial Interval		30	Seconds					
Show Advand	ced Options	8						

2. Please check the APN, Dialup Number, Username and Password: Dialup Number, Username and Password are provided by local mobile operator. The following examples show parameters provided by China Mobile, Vodafone. Please contact with local operator for details.

1: China Mobile APN: CMNET Phone Number: *99# User Name: web Password: web

2: Vodafone APN: internet Phone Number: *99# User Name: web Password: web 3. After correctly configuring, EKI-1334 can now access Internet. Open IE Browser, input www.google.com, you should see the Google home page:



2.4 Quick IPSec VPN Configuration

If you need to build a VPN tunnel to access to your remote PLC through Internet or you need to ensure security of the data transmission, here's a quick configuration guide of IPSec for EKI-1334.



Connect PC with Router to enter router configuration interface, select "VPN" => "IPSec setting":

System	Network	Services	Firewall	QoS	VPN
				IPS	ec Settings
Enable NAT-T	raversal (NATT)	2			
Keep alive time interval of NATT		60	Seconds		
Enable Compr	ession				
Debug					
Force NATT					

Enable NAT-Traversal (NATT): select enable.

Keep alive time interval of NATT: set the "Keep alive time interval of NATT", default is 60 seconds.

Enable Compression: select enable.

Please change the parameters according to actual situation.

Click "Apply" to complete the configuration.

 Select "VPN"=> "IPSec Tunnels" to check or modify parameters of IPSec Tunnels.



2. Click "Add" to add a new IPSec Tunnel:

	Enabling	g an Intellig	gent Plane	<i>r</i>			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
dit IDCas tur						IPSec Tun	nels
uit if sec tuni	ner						
Show Advance	ed Options						
Basic Parame	ters						
Tunnel Name	е	IPSec_tunne	L1				
Destination A	Address	23.34.45.56					
Startup Mode	es	Auto Activat	ed 🔻				
Restart WAN	when failed						
Negotiation N	Mode	Main Mode	٠				
Tunnel Type		Subnet - Sul	onet 🔻				
Local Subnet	t	192.168.2.1					
Local Netma	sk	255 255 255	0				
Remote Subi	net	0.0.0.0					
Remote Netr	nask	255 255 255	0				

Basic Parameters: basic parameters of IPSec tunnel.

Tunnel Name: name IPSec tunnel, the default is IPSec_tunnel_1.

Destination Address: set to VPN server IP/domain, e.g.: the domain provided by GJJ is gjj-ovdp.3322.org.

Startup Modes: select Auto Activated.

Negotiation Mode: optional between Main Mode and Aggressive Mode. Generally, select Main Mode.

IPSec Protocols: optional among ESP, AH. Generally, select ESP.

IPSec Mode: optional between Tunnel Mode and Transport Mode. Generally, select Tunnel Mode.

Tunnel Type: optional among Host-Host, Host-Subnet, Subnet-Host and Subnet-Subnet.

Local Subnet: IPSec local subnet protected. E.g.: 172.16.16.0.

Local Net Mask: IPSec local Net Mask protected. E.g.: 255.255.255.252.

Remote Subnet: IPSec remote subnet protected. E.g.: 172.16.0.0.

Remote Net Mask: IPSec remote Net Mask protected. E.g.: 255.240.0.0.

Phase 1 Parameters: configuration parameters during Phase 1 of IPSec negotiation.

IKE Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IKE Lifetime: the default is 86400 seconds.

Local ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Remote ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Authentication Type: optional between Shared Key and Certificate, generally choose Shared Key.

Key: set IPSec VPN negotiating key.

Phase 2 Parameters: configuration parameters during Phase 2 of IPSec negotiation.

IPSec Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IPSec Lifetime: the default is 3600 seconds.

Perfect Forward Encryption: Optional among None, GROUP1, GROUP2 and GROUP5. This parameter should match with the server, generally, select "None". Click "Save" to finish adding IPSec Tunnel:

AD.	ANT	ECH								
1	mabling	an Intelli	gent Plane	1						
System 1	Network	Services	Frendt	QoS	VPN	Tools	Status			
						IPSec Tun	inels			
Name	Tursel	Description						Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters
PSec_tancel_1	192 16 65P: Tr	8 2 1055 255 251 unnel Mode, Main	Örnrecker 23 Mode Auto Acto	la 45.56+++0.0.0 alled	62562562556			Authentication Type Bhaved Key Policy: Jose-md5- modp 1524 Lidetime Bi6000seconds Disated Perfect Formad Serecy(PF3)	Policy 3des-eid5-96 L/More 3600Seconds	Enable OPD, Interval 603econds, Tameout 1603econds Disabled (CMP Detection
Add		Show Detail St.	fut.							

You can click "Show Detail Status" to observe the specific connection details, or click "Add" to add a new tunnel.

Now you have successfully built a high-security IPSec tunnel.

And the PC in IPSec client subnet can get access to the server's subnet. Open command in your PC, then ping a PC in the server's subnet:

C: Doo	cunent	s and	Setting	s Jason	Hu>pin	g 192.16	8.123.256
Pingin	ng 192	2.168.	123.250	with 32	bytes	of data:	
Reply	from	192.1	68.123.2	50: byt	es=32 t	ine=428n	s TTL=63
Reply	from	192.1	68.123.2	50: byt	es=32 t	ine=395n	s TTL=63
Reply	from	192.1	68.123.2	50: byt	es=32 t	ine=397n	s ITL=63
Reply	from	192.1	58.123.2	50: byt	es=32 t	ine=393n	s TTL=63

2.5 Reset to Factory Defaults

2.5.1 Hardware Approach

Legend: On-- 🔵 Off-- 🔘 Blink-- 🖉

1. Press and hold RESET button while turning on EKI-1334:



2. When you see ERROR LED turns on (about 10 seconds after power on), release the RESET button:



3. After a few seconds, the ERROR LED will turn off, now press RESET button again:



4. Then you will see ERROR and STATUS LED blink, which means reset to factory defaults succeed!



Factory default settings: IP: 192.168.2.1 Net Mask: 255.255.255.0 Serial parameter: 19200-8-N-1

2.5.2 Web Approach

1. Login the web interface of EKI-1334 , select "System"-->"Config Management":

	Enabling	an Intellig	gent Plane	1			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
outer Config	uration					Config Manag	gement
遺擇檔案 未述	羅擇任何檔案	Imp	ort Bac	kup			
Restore defau	It configuration						
etwork Provi	der (ISP)						
	19 / 19 /	Imm	Bac	kun			

2. Click "Restore default configuration" to Reset EKI-1334.

EKI-1334 User Manual



Advanced Configuration

Sections include: ■ Configuration on Web ■ CLI Configuration

3.1 Configuration on Web

EKI-1334 must be correctly configured before use. This chapter will show you how to configure EKI-1334 via Web interface.

3.1.1 Preparation

1. First, connect your devices to EKI-1334 with a cable or a HUB (switch), then set the IP of PC and EKI-1334 in the same subnet, for example: Set PC IP to 192.168.2.50, net mask: 255.255.255.0, gateway (default IP of EKI-1334: 192.168.2.1):

e Edit View Percettes Tools Advanced Help	
🕽 Back 🔹 🕥 - 🎓 🔎 Search 💫 Folders 🛄 -	
dress 🔍 Network Connections	× 🗗
Local Area Connection Properties 🛛 💈 🔀	Internet Protocol (TCP/IP) Properties
Seneral Advanced	General
Connect using Will ware Accelerated AMD PCNet Ad Configure This connection uses the following items:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Bent for Microsoft Networks File and Printer Sharing for Microsoft Networks GoS Packet Scheduler Soft Scheduler Soft Scheduler	IP address: 192 . 169 . 2 . 50 Subnet mask: 255 . 255 . 255 . 0 Default gateway: 192 . 168 . 2 . 1
Instal Unimit Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network, protocol that provides communication across diverse interconnected networks. Show icon in notification area when connected	Obtain DNS server address extendically OUse the following DNS server addresses: Preferred DNS server: Alternate DNS server:
Notify me when this connection has limited or no connectivity OK Cancel	Advanced

 Open IE browser, input the IP address of EKI-1334: http://192.168.2.1 (default IP of EKI-1334).

Then you'll see the Login Window pop up, you need to login as Administrator. Input the username and password (default: adm/123456).

					dista.	- 0 - X
EKI-1334 -> Login x					-	
← → C ㎡ 🗋 192.168.2.3	1/logout.cgi		00	A 📕	0	🖸 🖌 🗉
11 應用程式 🕒 ICOM - Advantech	Agile Product Lifec.	. 🚼 Employee Portal	S Google	🗀 從 IE 🗷,	λ	
-						
	EKI-1334 Lo	ain				
		1011				
	Username					
	Password		1			
		Login				
						٨

3. Click "Login" to enter configure interface:

AD	NANT	ECH					
	Enabling	an Intellig	gent Plane	1			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						System St	atus
Name		EKI-1334					
Model		EKI-1334					
Serial Number		RP6151412	250228				
Description		www.advant	ech.com.tw				
Current Versio	n	1.2.0.r3559					
Current Bootlo	ader Version	1.1.3.r2421					
Router Time		2000-01-01	08:41:00				
PC Time		2015-02-17	10:25:00 Sy	nc Time			
Up time		0 day, 00:26	5:38				
CPU Load (1/	5 / 15 mins)	0.00/0.00/	0.00				
Memory const Total/Free	umption	28.89MB / 2	0.37MB (70.50	%)			

3.1.2 System

System settings include the 9 parts: Basic Setup, Time, Serial Port, Admin Access, System Log, Config Management, Update, Reboot and Logout.

1. Basic Setup

	Enabling	g an Intellig	gent Plane	¢			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						Basic Set	up
anguage		English	•				
Hostname		EKI-1334			1		

Parameters Name	Description	Default	Example
Language	Choose language of configuration web	Chinese	English
Router Name	Set name of EKI-1334	Router	My Router
Host Name	Name the device/PC linked with EKI-1334	Router	My Router

2. Time

	Enabling	z an Intellig	gent Plane	1			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						Time	5
Router Time	uter Time 2000-01-01 08:42:18						
PC Time		2015-02-17	10:26:18 Sy	nc Time			
'imezone		Custom					•
Custom TZ S	String	CST-8			1		
uto Update T	ime	Disabled	*				

Name	Description	Default
Router Time	Display router time	2000-01-01 8:00:00
PC Time	Display PC time (or the time of device linked with router)	
Time Zone	Set time zone	Custom
Custom TZ string	Set the string of time zone of Router	CST-8
Auto Update Time	Time Update Interval	Disabled
NTP Time Servers (after enable the Auto Update Time)	Setting for NTP Time server. (Three at the most)	pool.ntp.org

Chapter 3 Advanced Configuration

3. Serial Port

	Enabling	; an Intellig	gent Plane	r			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						Serial Po	ort
laudrate		115200 •					
ata Bits		8 🔻					
arity		None •					
stop Bit		1 •					
Software Flow Control		E					

Name	Description	Default
Baud Rate	Serial baud rate	19200
Data Bit	Serial data bits	8
Parity	Set parity bit of serial data.	None
Stop Bit	Set stop bit of serial data.	1
Hardware Flow Control	Enable Hardware Flow Control	Disable
Software Flow Control	Enable Software Flow Control	Disable

4. Admin Access

Syst	em N	etwork S	ervices	Firew	all QoS	VPN	Tools	Status
Iseman	me / Passwo	d					Admin Ac	cess
Userna	ime	a	idm					
	ssword	1						
olu ras								
New Pa	assword	Г						
New Pa Confirm	assword n New Passw	ord [
New Pa Confirm Manage Enable	assword n New Passw ment Service Type	ord [Local	Remote	Allowed addresses fr (Octional)	om WAN	Description	
New Pa Confirm Manage Enable	assword n New Passw ment Service Type HTTP	Service Port	Local access	Remote access	Allowed addresses fr (Optional)	om WAN	Description	
New Pa Confirm fanage Enable	assword n New Passw ment Service Type HTTP HTTPS	Service Port 80 443	Local access	Remote access	Allowed addresses fr (Optional)	om WAN	Description	
New Pa Confirm fanage Enable	assword n New Passw ment Service Type HTTP HTTPS TELNET	ord Service Port 80 443 23	Local access	Remote access 2 2 2	Allowed addresses fr (Optional)	om WAN	Description	

Name	Description Defau	ult	
	Username/Password		
Username	Username for configuration web login		adm
Old Password	To change the password, you need to input the one	e old	123456
New Password	Input new password		
Confirm New Password	Input the new password again		
Management			
	HTTP/HTTPS/TELNET/SSHD/Const	ole	
Enable	Select to enable		Enable
Service Type	HTTP/HTTPS/TELNET/SSHD/Console		80/443/23/22/Blank
Local Access	Enable—allow manage Router by LAN(e.g.: H Disable—forbid manage Router by LAN.	ITTP)	Enable
Remote Access	Enable—allow to manage EKI-1334 by WAN. HTTP) Disable—forbid to manage EKI-1334 by WAN. (HTTP)	(e.g.: e.g.:	Enable
Allowed Access from WAN (Optional)	Set the range of allowed IP address for WAN (HTTP/HTTPS/TELNET/SSHD)		Control services server can be set at this time, for example 192.168.2.1/30 or 192.168.2.1- 192.168.2.10
Description	Describe the parameters of management (nor influence to EKI-1334)	ז-	
	Other Parameters		
Log Timeout	Set the Log Timeout, configuration web will be connected after timeout	e dis-	500 seconds

5. System Log

	Enabling	g an Intellig	gent Plane	r			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						System L	og
og to Remote	e System						
IP Address /	Port(UDP)		: 51	4			
og to Console		0					

Name	Description	Default
Log to Remote System	Enable remote log server	Disable
IP address/Port (UDP)	Set the IP and Port of remote log server	Port: 514
Log to Console	Enable remote log server	Disable

6. Config Management

AD	NANT	IECH					
	Enabling	g an Intellig	gent Plane	1			
System	Network	Services	Firewall	QoS	VPN	Tools	Status
outer Config	uration					Config Mana	gement
選擇檔案 未如	國任何檔案	Imp	ort Bad	kup			
Restore defaul	t configuration						
letwork Provi	der (ISP)						
資標檔案 未清	推住间缆宽	Imp	ort Bac	kup			

Name	Description
Router Configuration	Import/Backup configuration file
Restore default configu- ration	Click to reset EKI-1334 (to enable RESET, you need to reboot EKI-1334)
Network Provider (ISP)	Used to configure the APN, username, password and other parameters of major operators

7. System Upgrade

AD	NANT	ECH					
	Enabling	g an Intellig	gent Plane	(
System	Network	Services	Firewall	QoS	VPN	Tools	Status
						Upgrad	e
Select the file t	to use:						

To upgrade the system, click "System"=>"System upgrade" to enter update page, then follow the steps below:

Click "Browse", choose the upgrade file;



Click "update", and then click "sure" to begin update, the window will show as below.

< 0:01

Upgrading system... It will take about 1-5 minutes depending on network. Please wait and don't interrupt!

Upgrade firmware succeed, and click "reboot" to restart EKI-1334 .

8. Reboot

If you need to reboot system, please click "System"=>"Reboot", then click "OK" to restart system.



9. Logout

If you need to logout system, click "System"=>"Logout", and then click "OK".


3.1.3 Network

Network settings include Dialup, LAN, DNS, DDNS, Static Route, and etc.

1. Dialup

Dustan	Mahurati	Convine	Eiround	0.00	VON	Toolo	Otatio
System	Network	Services	Firewall	Qos	VPN	TOOIS	Statu
						Dialup	
nable		۲					
ime schedule	2)	ALL V Sch	edule Managen	nent			
PPoE Bridge							
hared Conne	ection(NAT)	8					
efault Route		8					
etwork Provid	der (ISP)	Custom			 Mana 	ge	
PN		uninet					
ccess Numbe	er	*99***1#					
sername		gprs					
assword							
letwork Selec	t Type	Auto •					
and	08055.00	ALL			•		
tatic IP							
onnection Me	ode	Always Onli	ne 🔻				
tedial Interval	6	30	Seconds				
			-				
now Advanc	ed Options						
nitial Comma	ands						
PIN Code			1				15
Dial Timeout		120	Seconds				
MTU		1500					
MDU		1500					
MRO		1500					
TX Queue Le	ength	64					
Authenticatio	n Type	Auto 🔻					
-whenticado	ad compression						
Enable IP he		1000					
Enable IP he	isyncmap						
Enable IP he Use default a Use Peer DN	isyncmap IS			201			
Enable IP he. Use default a Use Peer DN Link Detectio	asyncmap IS n Interval	 ■ 55 	Seconds(0: dis	able)			
Enable IP he Jse default a Jse Peer DN Link Detectio	asyncmap IS n Interval n Max Retries	55 3	Seconds(0: dis	able)			
Enable IP he Use default a Use Peer DN Link Detectio Link Detectio Debug	asyncmap IS n Interval n Max Retries	© 55 3	Seconds(0: dis	able)			-111
Enable IP he Jse default a Jse Peer DN Link Detectio Link Detectio Debug Expert Option	isyncmap IS n Interval n Max Retries ns	■ 55 3 ■ nomppe nom	Seconds(0: dis	able) xsdcomp novj n	ovjccomp noccp		
Enable IP he Use default a Use Peer DN Link Detectio Link Detectio Debug Expert Option CMP Detecti	isyncmap IS n Interval n Max Retries ns ion Server	S5 3 nomppe nom	Seconds(0: dis	able) 25dcomp novj n	ovjccomp noccp		
Enable IP he Use default a Use Peer DN Link Detectio Link Detectio Debug Expert Option ICMP Detecti ICMP Detecti	isyncmap IS n Interval n Max Retries ns ion Server ion Interval		Seconds(0: dis	able) xsdcomp novj n	ovjccomp noccp		
Enable IP he Use default a Use Peer DN Link Detectio Link Detectio Debug Expert Option (CMP Detection) (CMP Detection)	asyncmap IS n Interval n Max Retries ns ion Server ion Server ion Interval ion Timeout	 ■ 55 3 ■ nomppe nom 30 20 	Seconds(0: dis	able) xsdcomp novj n	ovjccomp noccp		

Name	Description	Default
Enable	Enable PPP dialup	Enable
Time Schedule	Set time for online and offline	ALL
SHARED	Enabled—device linked with Router Can access to internet. Disable—device Can NOT access to internet via Router.	Enable
ISP	Select local ISP, if not listed here, please select "Customer"	Customer
Network Select Type	Choose mobile network type	HSDPA (or GPRS)
APN	APN parameters provided by Local ISP, you can set TWO different group of dialup param- eters (APN/Username/Password) and set one as backup	cmnet/uninet
Access Number	Dialup parameters provided by Local ISP	"*99#""*99***1#" or #777
Username	Dialup parameters provided by Local ISP	"GPRS" or "CDMA"
Password	Dialup parameters provided by Local ISP	"GPRS" or "CDMA"
Static IP	Enable Static IP if your SIM card can get static IP address	Disable
Connection Mode	Optional Always Online,	Always Online
Redial Interval	When Dial fails, EKI-1334 will redial after the interval	30 seconds
Show Advanced Options	Enable configure advanced options	Disabled
Initial Commands	Used for advanced parameters	Blank
Dial Timeout	Set dial timeout (IR700 will reboot after timeout)	120 seconds
MTU	Set max transmit unit	1500
MRU	Set max receive unit	1500
TX Queue Length	Set length of transmit queue	3
Enable IP header com- pression	Enable IP header compression	Disabled
Use default asyncmap	Enable default asyncmap, PPP advanced option	Disabled
Using Peer DNS	Click Enable to accept the peer DNS	Enabled
Link Detection Interval	Set Link Detection Interval	30 seconds
Link Detection Max Retries	Set the max retries if link detection failed	3
Debug	Enable debug mode	Enable
Expert Option	Provide extra PPP parameters, normally user needn't set this.	Blank
ICMP Detection Server	Set ICMP Detection Server, blank represents none	Blank
ICMP Detection Interval	Set ICMP Detection Interval	30 seconds
ICMP Detection Timeout	Set ICMP Detection Timeout (IR700 will reboot if ICMP time out)	5 seconds
ICMP Detection Max Retries	Set the max number of retries if ICMP failed	5

Chapter 3 Advanced Configuration

Dialup----Time Schedule Management:

	Ena	bling	an In	telligen	Plane	1					
System	Netw	ork	Servic	es F	irewall	Q	oS	VPN	Tools	Status	
chedule Man	agement								Dialup	,	
Name	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Time Range 1	Time Range 2	Time Range 3	Descriptio
schedule 1	0	1	1	×	3		8	9:00-12:00	14:00-18:00	0.00-0.00	

Name	Description	Default
Name	Name the schedule	schedule 1
Sunday		Blank
Monday		Enable
Tuesday		Enable
Wednesday		Enable
Thursday		Enable
Friday		Enable
Saturday		Blank
Time Range 1	Set Time Range 1	9:00-12:00
Time Range 2	Set Time Range 2	14:00-18:00
Time Range 3	Set Time Range 3	0:00-0:00
Description	Describe configuration	Blank

2. WAN

System	Network	Services	Firewall	QoS	Tools	Status	
			WAN				
Туре		Disabled	~	1			
		Static IP Dynamic Ad ADSL Dialup	dress (DHCP) (PPPoE)]			
		Disabled					

This page is to set the type of WAN port:

Name	Description	Default
Туре	Static IP; Dynamic Address(DHCP); ADSL Dialup(PPPoE); Disabled	Disabled

Caution! There can only be one WAN type at one time, enabling one type WAN will disabled another.



WAN—Static IP

		WAN	
Туре	Static IP	×	
SHARED	1		
MAC Address	00 18 05 00 5	51:44 Default Clone	
IP Address	192.168.1.29		
Netmask	255.255.255	0	
Gateway	192.168.1.1		
MTU	Default 💌 1	500	
Multi-IP Settings	Netmask	Description	
			Add

Name	Description	Default
Туре	Static IP	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
IP Address	Set WAN port IP	192.168.1.29
Net Mask	Set WAN port Net Mask	255.255.255.0
Gateway	Set WAN Gateway	192.168.1.1
MTU	Set Max Transmission Unit, optional between default and manual	1500
Multi-IP Settings(ca	an set 8 additional IP address at the most)	
IP address	Set the additional IP address of LAN	Blank
Net Mask	Set Net Mask	Blank
Description	Describe the settings	Blank

WAN-Dynamic Address (DHCP)

samic Address (DHCP) 💌	
8.05:00-51:44 Default Clone	
aut 🛩 1500	
	namic Address (DHCP) 💌 18.05:00:51:44 Default Clone ault 👻 1500

- C	
	7
	τ.
- 0)
-	
D)
- 11	_
	-
	J)
	>
- C	2
<	
0	5
	5
)
à	5
- U)
C	5
	_
	1
- C	٦.
_)
	-
(5
	-
0	ς.
Ц	J
-	÷.
)
	÷.
)

Name	Description	Default
Туре	Dynamic Address (DHCP)	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
MTU	Set Max transmission unit, optional between default and manual	1500

WAN --ADSL

		WAN	4
Туре	ADSL Dialup (PPPoE)	~	
SHARED	Ø		
MAC Address	00 18 05 00 51 44	Default Clone	
MTU	Default M 1482		
ADSL Dialup (PPPoE) Settings			
Usemane			
Password			
Static IP	Ø		
IP Address			
Peer Address	0.0.0.0		
Connection Mode	Always Online	1	
Show Advanced Options	8		
Service Name			
TX Queue Length	3		
Enable IP head compression			
Use Peer DNS	S		

Name	Description	Default
Туре	ADSL Dialup (PPPoE)	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
MTU	Set Max Transmission Unit, optional between default and manual	1500
ADSL Dialup (PPPoE)	Settings	
Username	Set username for dialing up	Blank
Password	Set password for dialing up	Blank
Static IP	Enable Static IP	Disabled
IP address	Static IP Address	Blank
Peer IP	Set Peer IP	Blank
Connection Mode	Set connection mode (Connect on Demand/Always Online/ Manual)	Always Online
Advanced Options		
Show advanced options	Enable advanced configuration	Disabled
Service Name	Name the service	Blank
TX Queue Length	Set TX Queue Length	3

Enable IP head com- pression	Click to enable IP head compression	Disabled
User Peer DNS	Enable User Peer DNS	Disabled
Link Detection Interval	Set link detection interval	55 seconds
Link Detection Max Retries	Set link detection max retries	10 (times)
Debug	Select to enable debug-mode	Disabled
Expert Options	Set expert parameters	Blank
ICMP Detection Server	Set ICMP Detection Server	Blank
ICMP Detection Time	Set ICMP Detection Time	30
ICMP Detection Time- out	Set ICMP Detection Timeout	3
ICMP Detection Max Reties	Set ICMP Detection Max Reties	3

3. LAN

		LAN	
MAC Address	00 18 05 00 5	6:10 Default	
IP Address	192.168.2.1		
Netnask	255 255 255)	
NTU	Default 💌 1	500	
Detection host	0.0.00		
WOL MAC Address	EE EE EE E	E4F 25 Device List	
ulti-IP Settings			
IP Address	Tetaask	Description	
			484
Apply Ca	ancel		

Name	Description	Default
MAC Address	The MAC address in LAN	00:10:A1:86:95:02 (Provided by Advan- tech) , for manufactures
IP Address	Set IP Address in LAN	192.168.2.1 (If Changed, you need to input the new address for entering the configuration web)
Net Mask	Set Net Mask of LAN	255.255.255.0
MTU	Set MTU length, optional between Default and Manual	1500
Detection Host	Set Detection Host Address	0.0.0.0
WOL MAC Address	Set the MAC of PC in the LAN of router, for Wakeup Over LAN (WOL) function, you should also set "Networks"à "Dialup" and change dialup mode into "Trigger by SMS".	Blank
Multi-IP Setting	gs (Support additional 8 IP addresse	s at the most)
IP Address	Set additional IP Address of LAN	Blank
Description	Description about this IP address	Blank

4. DNS

System	Network	Services	Firewall	QoS	Tools	Status	
			DNS				
Primary DNS		0.0.0.0					
Secondary DNS		0.0.0					

Name	Description	Default
Primary DNS	Set Primary DNS	Blank
Secondary DNS	Set Secondary DNS	Blank

5. DDNS (Dynamic DNS)

System	Network	Services	Firewall	QoS	Tools	Status	
			DDNS				
Dynamic DNS ==	> Dialup						
Current Address							
Service Type		Disabled	~				

Name	Description	Default
Current Address	Show the current IP address	Blank
Service Type	Select DDNS Provider	Disabled

System	Network	Services	Firevall	QoS	VPN	Tools	Status
					DDNS		
namic DNS	=> WAN						
urrent Addre	122	10.5.1.40					
ervice Type		DynDNS - D	ynamic 🔄				
URL.		http://www.	dyndns.com/				
Isernane		test					
assword							
iostname		test					
Wildcard							
X							
Backup MX							
orce Update							
ast Update							
ant Remance		1076					

Name	Description	Default
Service Type	DynDNS - Dynamic	
URL	http://www.dyndns.com/	
Username	Registered username for DDNS	
Password	Registered password for DDNS	
Hostname	Registered hostname for DDNS	

6. Static Route

			Static Route			
Destination	Netmask	Gateway	Interface	Description		
0.0.0.0	255 255 255 0	0.0.0.0		×		
						Add

Name	Description	Default
Destination	Set IP address of destination	Blank
Net Mask	Set subnet Mask of destination	255.255.255.0
Gateway	Set the gateway of destination	Blank
Interface	Optional LAN/WAN port access to destination	Blank
Description	Describe static route	Blank

3.1.4 Service

Service settings include DHCP Service, DNS Forwarding, VRRP and other related parameters.

1. DHCP Service

NAME: P				202.1			
				9	BCP Service		
inable DOCP		2					
IP Pool Starting	Address	10, 5, 1, 90					
IP Pool Ending A	diress	10.5.1.254					
Lease		60 3	linutes				
DMS						Edit	
Windows Nume Serv	ver (WINS)	0.0.0.0					
tatic DHCP							
	and the second second	Heat				•	
BAC Address	IF Address						
BAC Address 00:00:00:00:00:00	10.5.1.90						
BAC Address 00100100100100100	10.5.1.90)[7	

()
0
\bigcirc
_
\mathbf{O}
6.5
\mathbf{O}
01
_
-
()
()
\mathbf{O}
\square
oi
Q
a b
ati
atic
atio
ation

Name	Description	Default
Enable DHCP	Click to enable DHCP	Enable
IP Pool Starting Address	Set the starting IP address of DHCP pool	192.168.2.2
IP Pool Ending Address	Set the ending IP address of DHCP pool	192.168.2.100
Lease	Set the valid time lease of IP address obtained by DHCP	60 minutes
DNS	Set DNS Server	192.168.2.1
Windows Name Server	(WINS)	Set WINS
Blank	Static DHCP (can set 20 des- ignated IP address at the most)	MAC Address
Set the MAC address of a designated IP address	Blank	IP address
Set the static IP address	192.168.2.2	Host
Set the hostname	Blank	

2. DNS Relay

			4	DWS Rolmy		banks -
able 185 Helay						
		1				
the Lip addre	THE STA DOBALS RAD	er Patring				
Address	Rest	Bearript				
Address	Rest	Beseript				
Address	Rest	Buseript				

Name	Description	Default
Enable DNS Relay	Click to enable DNS Relay	Disabled
Design	ate IP address<=>DNS couples (20 at the second	ne most)
IP Address	Set IP address <=> DNS couples	Blank
Host	Set the name of IP address <=> DNS couples	Blank
Description	Describe IP address <=> DNS couples	Blank

3. VRRP

System	Network	Services	Pirewall	005	VP/N	Tools	Status
					VBBP		
Enable VRRP-I	8						
Group ID		1 -					
Priority		20 • (254	highest)				
Advertisemen	it Interval	60 • Sec	onds				
Virtual IP		13					
Authentication	n Type	None	•				
Virtual MAC		15					
Monitor		None 🔻					
Enable VRRP-I		123					

Name	Description	Default
VRRP-1	Select to enable VRRP	Disable
Group ID	Select group id of routers (range 1-255)	1
Priority	Select priority for router (range 1—254)	10 (bigger number stands for higher priority)
Advertisement Interval	Set ad interval	60 sec
Virtual IP	Set Virtual IP	Blank
Authentication Type	Optional: None/Password type	None
Virtual MAC	Set Virtual MAC	Blank
Monitor	Set Monitor	None
VRRP-II		

4. DTU

		DTU	
Enable	10		
DTU Protocol	Transparent -		
Protocol	UOP -		
Mode	Client .		
Frame Interval	100 mseconds		
Serial Buffer Frames	4		
Mutti-Server Policy	Parallel •		
Vin Reconnect Interval	15 Seconds		
Max Reconnect Interval	180 Seconds		
DTU ID			
Source IP			
luiti Server			
Server Address		Server Po	rt

Name	Description	Default
Enable	Click to enable DTU	Disable
DTU Protocol	Set DTU protocol, Please see more in related Quick Guide	Transparent
Protocol	Optional between TCP/UDP	UDP
Mode	Set DTU as client or server	Client
Frame Interval	Set Frame Interval	100
Serial Buffer Frames	Set Serial Buffer Frames	4
Multi-Server Policy	Optional between Parallel/Poll	Parallel
Min Reconnect interval	Set Min Reconnect interval	15
Max Reconnect interval	Set Max Reconnect interval	180
DTU ID	Set ID of DTU	Blank
Source IP	Set Source IP	Blank
Multi Server	Set the IP address and Port of server to receive data.	Blank

5. SMS

				5	a s		(Column
inable		2					
Status Query		show status	(Engl	ish Only)			
Reboot		reboot	(Engl	ish Only)			
Default Pol	icy	Block 💌		rtim		Beservation	
CANNE STRAFT			Ā	ccept			
15201697607							
15201697607 15201697807			14	Accept	v		

Name	Description	Default
Enable	Click to enable SMS control	Disable
Status Query	Set Status Query SMS, and you can see status of router by send SMS (e.g.: show status).	
Reboot	Let the router reboot	
SMS Access Control		
Default Policy	Block or Accept control SMS from cer- tain Phone	Block
Phone List	Include phone numbers accepted or blocked to send SMS to router	

Note!

Before using this function, please make sure you have a SIM card in the EKI-1334 that has SMS function. Otherwise, please contact local mobile operator to get one.

SMS you will get in your mobile phone: Host: (SN); Uptime: (the uptime of router for this time of reboot); State: (Online/Offline) (Cellular WAN IP)

3.1.5 Firewall

This page is to configure the firewall parameters.

1. Basic Configuration

Default Filter Policy	Accept 🛩	
Block Anonymous WAN Requests (ping)		
Filter Multicast	R	
Defend DoS Attack	8	

Name	Description	Default
Default Filter Policy	Optional between Accept / Refused	Accept
Block Anonymous WAN Request (ping)	Click to enable filer ping request	Disable
Filter Multicast	Click to enable filter multicast	Enable
Defend DoS Attack	Click to enable Defend DoS Attack	Enable

2. Filtering

inable	Proto		Source	Source Port	Destination	Destination Port	Action		Log	Description	
Ø	ALL	×	00000	10	1.5	10°	Accept	٠			
											A

Name	Description	Default
Enable	Click to enable filtering	Blank
Protocol	Optional among TCP/UDP/ICMP	All
Source IP address	Set Source IP address	Blank
Source Port	Set Source Port	Blank
Destination IP	Set destination IP	Blank
Destination Port	Set destination port	Blank
Action	Accept/Deny	Accept
Log	Click to enable login	Disable
Description	Describe your configuration	Blank

3. Port Mapping

(=)e		ing	ort Mapp	P					
	Description	Log	Internal Port	Internal Address	Service Port	Source		Proto	Enable
	<u> </u>		8080)[]	8080	0.0.0.0/0	*	TCP	
Ad									

Name	Description	Default
Enable	Click Enable Port Mapping	Disable
Source	To fill with source IP	0.0.0/0
Service Port	Fill the port of service	8080
Internal Address	Set the internal IP for mapping	Blank
Internal Port	Set the Port mapping to internal	8080
Log	Click to enable log about port mapping.	Disable
Description	Describe meanings of each mapping	Blank

4. Virtual IP Mapping

			Virtu	al IP Mapping		(color)
Intual IP for Rou	ter [
ource IP Range	6 E					
nable Virtual P	Real P	Log	Description			
Ø	100004	0				
		1.58				AM

An internal PC's IP can match to a virtual IP, and external network can access the internal PC via this virtual IP address.

Name	Description	Default
Virtual IP for Router	Set Virtual IP for Router	Blank
Source IP Range	Set range of source IP address	Blank
Virtual IP	Set virtual IP	Blank
Real IP	Set real IP	Blank
Log	Enable logging concerned with virtual IP	Disable
Description	Describe this configuration	Blank

5. DMZ (All Port Mapping)



Mapping all the ports and then external PC can get access to all the ports of internal device behind EKI-1334.

Caution! This function cannot map the admin port of EKI-1334 (e.g.: 80 TCP) to the device's port.



6. MAC-IP Bundling

Stand	- ALLER A		10.000	MLC	JP Bundling	1000	 1010
MAC Address	P Addres	a De	scription				
00 00 00 00 00 00 00	192,168	22					
							- Adl

When firewall denies all access to the external network, only PC with MAC-IP Bundling can access external network

Name	Description	Default
MAC Address	Set Bundling Mac address	Blank
IP Address	Set Bundling IP address	192.168.2.2
Description	Describe this configuration	Blank

3.1.6 **QoS**

1. Banwidth Control

				Bandy	width Control
Enable					
Outbound Limit. N	Ask Bandwidth	100000	kbit/s		
Inbound Limit Ma	x Bandwidth	100000	kbit/s		

Name	Description	Default
Enable	Click to enable	Disable
Outbound Limit Max Bandwidth	Set the limit speed of out- bound bandwidth	100000kbit/s
Inbound Limit Max Bandwidth	Set the limit speed of inbound bandwidth	100000kbit/s

2. IP BM Limit

						IP BW L	imit	
nable IP Add	ress	Rate(kbit/s)	Priority		Description			
	1440.000	100	Medium	•	and shall be all			
		100	Medium					
		100						

Name	Description	Default
Enable	Click to enable	Disable
IP Address	Set IP Address	Blank
Rate	Set Rate	100 kbit/s
Priority	Set the Priority	Medum
Description	Describe this configuration	Blank

3.1.7 VPN

This page introduces the parameters in EKI-1334 Web.

1. IPSec Settings

To build an IPSec VPN Tunnel, you need to first set IPSec properties on this page, then go to IPSec Tunnels to add your VPN:

System	Network	Services	Firewall	QoS	VPN	Tools	Status	
				IPS4	c Settings			(CONTRACT)
Enable NAT-T	raversal (NATT)	2						
Keep alive tim NATT	e interval of	60	Seconds					
Enable Compr	ession	P						
Debug								
Force NATT								

IPSec Settings

Description:

- 1. Select to Enable or Disable NATT, normally we need to enable, unless you ensure there is no NAT routers in the network.
- 2. Select to enable Compression Mode or Debug

Name	Description	Default
Enable NAT Transversal (NATT)	Click to enable NATT	Enable
Keep alive time interval of NATT	Set live time for NATT	60 sec
Enable Compression	Click to enable	Enable
Enable Debug	Click to enable	Disable
Force NATT	Click to enable	Disable

2. IPSec Tunnels

				IPS	ic Tunnels				C-P
Name	Tunnel	Description				Phase	1 Parameters	Phase 2 Parameters	Link Detection Parameters
Add		Show Detail Sta	stute						
A0		onow permissio	ens j						

Click "Add" and enter the configuration page:

Edit IPSec tunnel		il dec runners
Show Advanced Options	V	
Basic Parameters		
Tunnel Name	IPSec_tunnel_1	
Destination Address	0.0.0.0	
Startup Modes	Auto Activated	×
Restart WAN when failed		
Negotiation Mode	Main Mode	
IPSec Protocol	ESP 💌	
IPSec Mode	Tunnel Mode 💌	
Tunnel Type	Subnet - Subnet 👻	
Local Subnet	192.168.2.1	
Local Netmask	255.255.255.0	
Remote Subnet	0.0.0.0	
Remote Netmask	265 255 255 0	
Phase 1 Parameters		
IKE Policy	3DES-MD5-DH2	×
IKE Lifetime	86400	Seconds
Local ID Type	IP Address 💌	
Remote ID Type	IP Address 💌	
Authentication Type	Shared Key 💌	
Key		
Phase 2 Parameters		
IPSec Policy	3DES-MD5-96	
IPSec Lifetime	3600	Seconds
Perfect Forward Serecy(PFS)	None 🛩	
Link Detection Parameters	-	
DPD Time Interval	60	Seconds(0: disable)
DPD Timeout	180	Seconds
ICMP Detection Server		
ICMP Detection Local IP		
ICMP Detection Interval	60 Seconds	
ICMP Detection Timeout	5 Seconds	
MP Detection Max Retries	0	
Cont Count		
Save Cancel		

Name	Description	Default
Show Advanced Options	Click to enable advanced options	Disable
	Basic Parameters	
Tunnel Name	To name the tunnel	IPSec_tunnel_1
Destination Address	Set the destination address of IPSec VPN Server	Blank
Startup Mode	Auto Activate/Trigged by Data/ Passive/Manually Activated	Enable
Negotiation Mode	Optional: Main Mode or Aggressive Mode	Main Mode

IPSec Mode (Enable Advanced options)	Optional: ESP or AH	ESP
IPSec Mode (Enable Advanced options)	Optional: Tunnel Mode or Transport Mode	Tunnel Mode
Tunnel Type	Optional: Host—Host, Host—Subnet, Subnet—Host, Subnet— Subnet	Subnet——Subnet Mode
Local Subnet	Set IPSec Local Protected Sub- net	192.168.2.1
Local Subnet Net Mask	Set IPSec Local Protected Sub- net Net Mask	255.255.255.0
Remote Subnet Address	Set IPSec Remote Protected Subnet	Blank
Remote Subnet Net Mask	Set IPSec Remote Protected Subnet Net Mask	255.255.255.0
	Phase 1 Parameters	
IKE Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IKE Lifetime	Set IKE? Lifetime	86400 sec
Local ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Local ID (Only for FQDN and USERFQDN)	Set the ID according to ID type	Blank
Remote ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Remote ID (Only for FQDN and USERFQDN)	Set the ID according to ID type	Blank
Authentication Type	Optional: Shared Key or Certificate	Shared Key
Key (While choosing Shared Key Authentica- tion Type)	Set IPSec VPN Negotiation Key	Blank
Phase 2 Parameters		
IPSec Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IPSec Lifetime	Set IPSec Lifetime	3600sec
Perfect Forward Secrecy (PFS)	Optional: Disable, GROUP1, GROUP2, GROUP5	Disable ((Enable Advanced options)
Link Dete	ction Parameters (Enable Adva	inced options)
DPD Time Interval	Set DPD Time Interval	60sec
DPD Timeout	Set DPD Timeout	180sec
ICMP Detection Server	Set ICMP Detection Server	Blank
ICMP Detection Local IP	Set ICMP Detection Local IP	
ICMP Detection Interval	Set ICMP Detection Interval	30sec
ICMP Detection Timeout	Set ICMP Detection Interval	5sec
ICMP Detection Max Retries	Set ICMP Detection Max Retries	3

3. GRE Tunnels

			GRE Tunnels				Contract
me Local virtual I	P Peer Addr	ess Remote virtual I	P Remote Subnet	Remote Netmask	Key	NAT	Description
0.0.0	0.0.0.0	0.0.0	0.0.0	255.255.255.0		13	
							Add
nin Vic	e Local virtual II 0.0.0.0	e Local virtual IP Peer Addre	e Local virtual IP Peer Address Remote virtual I 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	e Local virtual IP Peer Address Remote virtual IP Remote Subnet 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	e Local virtual IP Peer Address Remote virtual IP Remote Subnet Remote Netmask 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	e Local virtual IP Peer Address Remote virtual IP Remote Subnet Remote Netmask Key 0.0.0.0 0.0.0 0.0.0 0.0.0 255 255 255 0	e Local virtual IP Peer Address Remote virtual IP Remote Subnet Remote Netmask Key NAT 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

GRE Tunnels

Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set GRE Tunnel Name	tun0
Local Virtual IP	Set Local Virtual IP	0.0.0.0
Remote Address	Set Remote Address	0.0.0.0
Remote Virtual IP	Set Remote Virtual IP	0.0.0.0
Remote Subnet Address	Set Remote Subnet Address	0.0.0.0
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Кеу	Set Tunnel Key	Blank
NAT	Click Enable NAT Function	Disable
Description	Add Description	Blank

4. L2TP Clients

dit L2TP Tunnel	L2TP Clients	
Enable		
Dunnel name	L2TP_TUNNEL_1	
LOTP Server		
Deername		
Pastword		
2TF Server Name	12tpserver	
Startup Modes	Auto Activated 💓	
Authencation Type	CRup 🛩	
Enable Challenge Secrets	8	
Challenge Secrets		
Local IP Address		
Remote IP Address		
Remote Submet		
Renote Netnack	255. 255. 255. 0	
Link Detection Interval	60 Seconds	
Max Setries for Link Detection	8	
Enable NAT		
actu	1500	
ETU EUU Enuble Dabus	1500	

Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	L2TP_TUNNEL_1
L2TP Server	SetL2TP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server Password	Blank
Server Name	Set Server Name	l2tpserver
Startup Modes	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP	СНАР
Enable Challenge secrets	Set to enable Challenge secrets	Disable
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Disable
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Disable
Expert Options	Set Expert Options	Blank

5. PPTP Clients

idit PPTP Tunnel		PPTP Clients
Enable	2	
Tunnel name	PPTP_TUNNEL_1	
PPTP Server		
Username		
Password	5	
Startup Modes	Auto Activated	v
Authencation Type	Aut o 💌	
Local IP Address		
Remote IP Address		
Remote Subnet		
Remote Netmark	255. 255. 255. 0	
Link Detection Interval	60	Seconds
Max Retries for Link Detection	5	
Enable NAT		
Enable MPPE		
Enable MPPC		
etu	1500	
IRU)	1500	
Enable Debug		
Expert Options(Expert Only)		

Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	PPTP_TUNNEL_1
PPTP Server	Set PPTP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server's Password	Blank
Startup Mode:	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP, MS-CHAPv1, MS- CHAPv2	Auto
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Blank
Enable MPPE	Click Enable MPPE	Blank
Enable MPPC	Click Enable MPPC	Blank
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Blank
Expert Options	For Advantech R&D only	Blank

6. OpenVPN Settings

		OpenVPN Tunnels
dit OPENVPN Tunnel		
Tunnel name	OpenVEX_1_1	
Enable		
Mode	Client 💌	
Protocol	UDP 💌	
Port	1194	
OPENVPN Server	211.189.3.69	
Authencation Type	User/Password	×
Username	test	
Password		
Pre-shared Key		
Parata Subrat	102 168 8 0	
Nemote Subnet	192.100.0.0	
Remote Netmask	255. 255. 255. 0	
Link Detection Interval	60	Seconds
Link Detection Timeout	300	Seconds

Renegotiate Interval	86400	Seconds
Enable NAT		
Enable L20	V	
Encryption Algorithms	Blowfish(128) 💌	
UTU	1500	
Max Fragment Size		
Debug Level	Warn 🛩	
Expert Options(Expert Oply)		

This page is to configure the OpenVPN settings, including Tunnel Name, Work Mode, Protocol, Port No. and other items.

Name	Description
Tunnel name	default
Enable	Enable this configuration
Mode	Client or Server
Protocol	UDP or TCP
Port	Import or Export Certificate (CRL)
OPEN VPN Server	OPEN VPN Server's IP or DNS
Authencation Type	 None for host to host connection (not available when 700 as server) Pre-shared Key for host to host connection (not available when 700 as server) User/Password For multi users to access CA needed: Client: root CA (ca.crt) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key) X.509 Cert (multi-client) CA mode for multi users to access CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key) X.509 CertCA mode for host to host tunnel CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) X.509 CertCA mode for host to host tunnel CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) User+X.509 modeusername + password + CA cer- tificate CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) User+X.509 modeusername + password + CA cer- tificate CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key)
Pre-shared Key	Set shared key or TLS-AUTH static password
Remote Subnet, Remote Net mask	Set the static route of the router, always towards the subnet of its peer
Link Detection Interval, Link Detection Timeout	Always use default
Renegotiate Interval	Always use default

Enable NAT	Set NAT mode, meanwhile it will disable route mode
Enable MPPE	Enable MPPE, always set in server
Enable LZO	Enable LZO compression
Encryption Algorithms	Set encryption algorithms, must match with the server
MTU, Max Fragment Size	Always use default

7. OpenVPN Advanced Settings

				OpenW	/W Advanced		
Enable (Server	Client-to-Client Mode Only)						
Client	Ranagement						
Inable	Tunnel nume Voornam	*/ConnenNane	Password	Client IF (6th byte must be 4m*1)	Local Static Route	Remote Static Route	
M	Open/VPN_T_						
							A44

This page is to configure the OpenVPN advanced settings.

Name	Description
Enable Client-to-Client	Enable client access to other clients
	Client Management
Tunnel Name	Tunnel Name of the Client
Username/Common Name	Username (using Username/password mode) or Common Name in CA (CA mode)
Local Static Route	The client subnet
Remote Static Route	The server subnet

Caution! CA can only be produced by customer's PC; EKI-1334 cannot produce CA.



EKI-1334 User Manual

8. Certificate Management of OpenVPN Settings

ertificate Management		Certificate Hana	gement
Enable SCEP (Simple Certificate Enrollment Protocol)			
Protect Key			
Protect Key Confirm			
	1000		
	Browse.	Import CA Certificate	Export CA Certificate
	Browse.	Import CML	Export CNL
	Browse. Browse.	Import CRL	Export CML Export Public Key Certifica

Name	Description	Default
Enable SCEP (Simple Certificate Enrollment Protocol)	Click Enable	
Certificate Protected Key	Set Certificate Protected Key	Blank
Certificate Protected Key Confirm	Confirm Certificate Protected Key	Blank
Import/Export CA Certificate	Import or Export (CA) Certificate	Blank
Import/Export Certificate (CRL)	Import or Export Certificate (CRL)	Blank
Import/Export Public Key Certificate	Import or Export Public Key Certificate	Blank
Import/Export Private Key Certificate	Import or Export Private Certificate	Blank

3.1.8 Tools

Tools contain PING Detection, Route Trace, Link Speed Test and etc.

1. PING

System	Network	Services	Firevall	QoS	VFN	Tools	Status
					PING		
Host					Ping		
Ping Count		4					
Packet Size		32 By	rtes				
Expert Optics	15						

Name	Description	Default
Host	Destination for PING	Blank
Ping Count	Set PING Counts	4 times
Packet Size	Set PING Packet Size	32 Bytes
Expert Options	Advanced parameters	Blank

2. Trace Route

System	Network	Services	Firewall	QoS	VPN	Tools	Status
					Traceroute		
East					Irace		
Макімца Норл		20					
Tinecut		3 Seconds					
Protocol		UDP 💌					
Expert Option	3			1			

Name	Description	Default
Host	Destination for Trace Route	Blank
Max Hops	Set Max Hops	20
Time Out	Set Time Out	3 sec
Protocol	Optional: ICMP/UDP	UDP
Expert Options	Advanced parameters	Blank

3. Link Speed Test

System	Network	Services	Firevall	Qo5	Abla	Tools	Statu
				L	ink Speed Test	8	
			Browse	upload	download		

Test link speed via unload or download

3.1.9 Status

Status contains System, Modem, WLAN, Network Connections, Route Table, Device List and Log.

1. System Status

System	Network	Services	Firewall	965	YPH	Tools	Status	
					System St	tatur		
Nane		Router						
Model		1909590801						
Serial Number	1	RW0061111295	000					
Description		www.inhand.c	OR. CTL					
Current Versi	on	1.2.0.x2462(test)					
Current Bootl	oader Version	1.1.3.x2421						
Router Time		2000-01-01 0	8104131					
PC Time		2012-03-20 0	5:59:09 5	NO TIME				
Up time		0 day, 00:04	: 32					
CPU Lond to /	8 / 18 mine)	0.00 / 0.01	/ 0.00					
Remory consus Total/Free	grion	28.9085 / 17	. post 162.20	40				

This page shows the status of system, including Name, Model Type, Current Version and etc.

2. Modem Status

System	Network:	Services	Freval	QoS	VPN	Tools	Status		
Dialup					Mod	em			
Modem Type Status Manufacturen Product Signal Level Register Stat MEI(ESH) Co MASI Code NASI Code NASI Code NASI Code PLMN LAC Cell ID	as de	MC2716 resetting 21E MC2716 - (0) no registe 0x80AA45	red (48)						
								() Steconds	· Stop

This page shows the status of Modem, including signal level.

3. Network Connections

		Network Connections
WAN.		
MAC Address	00:18:05:00:55:10	
Connection Type	Static IP	
IF Address	203, 86, 43, 190	
Netaask	255, 255, 255, 0	
Gateway	203, 86, 43, 185	
DBS		
NTU	1500	
Status	Connected	
Connection time	0 day, 17:26:19	
Dislup		
Connection Type	Disabled	
IP Address	0,0.0,0	
Netmark	0,0,0,0	
Gateway	0.0.0.0	
DINS	0,0,0,0	
NTU	1500	
Status	Disconnected	

This page shows the network connections via WAN or LAN

4. Route Table

	Status	Tools	FW		Qo5	Firewall	Services	Network	System.
			Table	Route					
			Interface	Retric		Galeway	sk	Retar	Destination .
			CestD	0		0.0.0.0	15.255.255	255 25	10.8.0.2
			1 km0	0		0.0.0.0	5.255.0	255.25	192.168.5.6
			tran0	0		10.8.0.2	15.255.0	255.25	192 166 3.0
			Tear	0		0.0.0.0	6.255.0	155.25	203.06.43.0
			tranD	Ú.		10 6 0 7	15.255.0	255.25	10.0.0.0
			trad	0		10.0.0.2	8.255.0	255.21	192.168.9.0
			1+	0		0.0.0.0	0.0	255.0	127.0.0.0
			+ic0	0		203.88.43.185	0	0.0.0	default
wal Refresh									

This page shows the route table of EKI-1334 .

5. Device List

System	Betwork	Services	Fizevall	Qo5	V98	Tools	Statur		
				p	evice List				
Interface		ess	n	Address		· Rest			Lesse
***0	00:15:46	17 53.17	10	0.06.42.105					
								C Iltientale	- Stop

This page shows the devices linked with EKI-1334 .

6. Log

.

			Log	66
Level	Time	Redale	Centent	
			Two many logs, ald logs are not displayed. Flasse download log file to shack more logs!	
debug	Jun 19 13:06:49	InAgent	TRST 012345678948CER	
info	Jun 19 13-06.49	InAgan1	Firmware Version(1.3.0.r1773):Botity Config Timestamp(a-1275632530021):Systemfig Timestamp(0000000000000)	
infe	Jun 19 13:06:59	InAgent.	Try ts legin(8th/10)	
infe	Jun 19 13:06:59	InAgent	norma spicesf_timestamp act from()	
debug	Jun 19 13:06:58	InAgent	IRST 0123456709ABCEE	
infe	Jun 19 13:06:59	InAgent	Firmware Version(1.3.0.r1773), Entity Config Timestamp(w-1075630533001), Systemfig Timestamp(000000000000)	
info	Jun 19 13:07:09	InAgent	Try ts legis(10th/10)	
info	Jun 19 13:07:09	InAgent	sorum systemsEstimestamp ant Erand)	
debug	Jun 19 13:07:09	InAgent	INCI 0123496789ABCBE	
into	Jun 19 13:07:09	InAgent	Fireware Version(L.3.0.r1773); Enkity Config Timestamp (#-1275632530021) Systemfig Timestamp (0000000000000)	
info	Jun 19 13:07:19	InAgent.	Try to connect 040F AF (10.8.0.6.9000)	
inf+	Jun 19 15:07:19	InAgent	Try to Legin(1th/10)	
info	Jun 19 13:07:19	InAgent	serum syscend_timestamp sot found!	
debing	Jun 19 13:07:19	InAgent.	2852-0123456T09ABC08	
info	Jun 19 13:07:19	InAgent	Firmware Version(J. 3. 0. r1773):Entity Config Timestamp(w-1275632533021).Systemfig Timestamp(000000000000)	
infe	Jun 19 13:07:29	InAgent	Try ts Legin (2th/10)	
info	Jun 19 13:07 29	InApent	serve syscelf_timestamp set found!	
debug	Jun 19 13:07:29	InAgent	INST 0123456709ABCBE	
info	Jun 19 13-07-29	InAgent	Firmware Version(0.3.0.v1773);Entity Config Timestamp(a-1275632533021);Synconfig Timestamp(D0000000000000)	
			Clear Log Download Log File Download System Diagnosing Data	

This page shows the log of system, including download log file.

Under certain situation when there're problems that can't be diagnosed at the moment, you'll be asked to provide the diagnose log to Advantech engineers.

3.2 CLI Configuration

This chapter will show you how to configure via CLI.

3.2.1 CLI Operation

1. Input telnet LAN IP to login CLI configuration. For example:



2. After connection is succeed, input username and password of EKI-1334 . The default username/password is adm/123456.

Caution! Password will not be showed.





3. Login to User Mode

an Telnet 192.	168. 2. 1	- O X
Wel Inhand Copyrigh http://w	uxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
Model Serial Number Description Current Versio Current Bootlo get help for c	: IR711WH70 : RW7911003117964 : www.inhand.com.cn : 1.3.5.r2275 ader Version : 1.1.6.r1730 commands	
type '?' for d help language show exit ping telnet traceroute enable Router>	<pre>letail help at any point get help for commands set language show system information exit current mode/console ping test telnet to a host trace route to a host turn on privileged commands</pre>	

This screenshot is the config-view of IR700.

4. Enter privileged mode, password is 123456



5. Login to privileged mode successfully



 Enter configured mode, then you could configure parameters you want to set up.

Router# conf terminal Router(config)#

3.2.2 CLI command

Configure username and password

```
Router(config)# nvram set adm_user adm
set adm_user=adm
Router(config)# nvram set adm_passwd 123456
set adm_passwd=123456
Router(config)#
```

Enable serial function

```
Router<config)# nvram set console_enable 1
set console_enable=1
```

Configure serial port parameters, like baudrate, parity, stop bit and so on.

Router(config)# nvram set com4_config 192008n1 set com4_config=192008n1

Enable advanced options of dialup

Router(config)# nvram set advanced 1 set advanced=1

Configure ICMP server

```
Router(config)# nvram set wan1_icmp_host www.sina.com
set wan1_icmp_host=www.sina.com
```

Configure LAN IP

Router(config)# nvram set lan0_ip 192.168.2.1 set lan0_ip=192.168.2.1

Enable DHCP function

Router(config)# nvram set dhcpd_enable 1 set dhcpd_enable=1

Configure DHCP IP pool: 192.168.2.10-192.168.2.20

```
Router(config)# nvram set dhcpd_start 192.168.2.10
set dhcpd_start=192.168.2.10
Router(config)# nvram set dhcpd_end 192.168.2.20
set dhcpd_end=192.168.2.20
```

Enable HTTP function

Router(config)# nvram set http_enable 1 set http_enable=1

Configure HTTP service port

Router(config)# nvram set http_port 80 set http_port=80

Enable HTTP local access

```
Router(config)# nvram set http_local 1
set http_local=1
```

Enable HTTP remote access

```
Router(config)# nvram set http_remote 1
set http_remote=1
```

Check device ID

```
Router(config)# nvram get ovdp_device_id
ovdp_device_id=711122732
```

After configuration, please don't forget to commit and reboot router!

```
Router(config)# nvram commit
% command ok!
Router(config)# reboot
are you sure to reboot system?[Y¦N] y<sub>m</sub>
```



FAQ

A.1 FAQ

1. EKI-1334 is powered on, but can`t access Internet through it? Please check?

- Whether the EKI-1334 is inserted with a SIM card.
- Whether the SIM card is enabled with data service, whether the service of the SIM card is suspended because of an overdue charge.
- Whether the dialup parameters, e.g. APN, dialup number, username and password are correctly configured.
- Whether the IP Address of your computer is the same subnet with EKI-1334 and the gateway address is EKI-1334 LAN address.
- 2. EKI-1334 is powered on, have a ping to detect EKI-1334 from your PC and find packet loss?

Please check if the network crossover cable is in good condition.

3. Forget the setting after revising IP address and can`t configure EKI-1334 r? Method 1: connect EKI-1334 with serial cable, configure it through console port.

Method 2: within 5 seconds after EKI-1334 is powered on, press and hold the Restore button until the ERROR LED flashes, then release the button and the ERROR LED should goes off, press and hold the button again until the ERROR LED blinks 6 times, the EKI-1334 is now restored to factory default settings. You may configure it now.

4. After EKI-1334 is powered on, it frequently auto restarts. Why does this happen?

Please check:

- Whether the module works normally.
- Whether the EKI-1334 is inserted with a SIM card.
- Whether the SIM card is enabled with data service, whether the service of the SIM card is suspended because of an overdue charge.
- Whether the dialup parameters, e.g. APN, dialup number, username and password are correctly configured.
- Whether the signal is normal.
- Whether the power supply voltage is normal.

5. Why does upgrading the firmware of my EKI-1334 always fail?

Please check:

- When upgrading locally, check if the local PC and EKI-1334 are in the same network segment.
- When upgrading remotely, please first make sure the EKI-1334 can access Internet.
- After EKI-1334 establishes VPN with the VPN server, your PC under EKI-1334 can connect to the server, but the center can't connect to your PC under EKI-1334?

Please make sure the firewall of your computer is disabled.

7. After EKI-1334 establishes VPN with the VPN server, Your PC can't connect to the server?

Please make sure "Shared Connection" on "Network=>WAN" or "Network=>Dialup" is enabled in the configuration of EKI-1334.

- 8. EKI-1334 is powered on, but the Power LED is not on?
- Check if the protective tube is burn out.
- Check the power supply voltage range and if the positive and negative electrodes are correctly connected.
- 9. EKI-1334 is powered on, but the Network LED is not on when connected to PC?
- When the PC and EKI-1334 are connected with a network cable, please check whether a network crossover cable is used.
- Check if the network cable is in good condition.
- Please set the network card of the PC to 10/100M and full duplex.
- 10. EKI-1334 is powered on, when connected with PC, the Network LED is normal but can't have a ping detection to the EKI-1334?
- Check if the IP Address of the PC and EKI-1334 are in the same subnet and the gateway address is EKI-1334 LAN address.
- 11. EKI-1334 is powered on, but can't configure through the web interface?
- Whether the IP Address of your computer is the same subnet with EKI-1334 and the gateway address is EKI-1334 LAN address.
- Check the firewall settings of the PC used to configure EKI-1334, whether this function is shielded by the firewall.
- 12. The EKI-1334 dialup always fails, I can't find out why?

Please restore EKI-1334 to factory default settings and configure the parameters again.

- 13. How to restore EKI-1334 to factory default settings?
- Press and hold the Restore button, power on EKI-1334;
- Release the button until after the STATUS LED flashes and the ERROR LED is on;
- After the button is released, the ERROR LED will go off, within 30s press and hold the Restore button again until the ERROR LED flashes;
- Release the button, the system is now successfully restored to factory default settings.

A.2 Support

In case you have problems with the installation and use, please address them to us by e-mail:

icg.support@advantech.com.tw.



www.advantech.com.cn

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© Advantech Co., Ltd. 2015