7180 SW Fir Loop. #100
Portland, Oregon 97223
phone: 503-290-0110
fax: 503-290-0111
web: www.ipcopper.com

IPCopper USC1030 / USC2030 Packet Capture Appliance Product Manual

For firmware versions 2.03 and later

Table of Contents

OVERVIEW 1

INSTALLATION.....2

POWERING THE UNIT ON AND OFF 4

UNDERSTANDING THE FRONT PANEL 6

RETRIEVING DATA.....7

TROUBLESHOOTING.....9

WATCHDOG TIMER 11

INDEX 12

SPECIFICATIONS 13

ADDITIONAL RESOURCES.....13

The following paragraph does not apply to any country where such provisions are inconsistent with local law: IPCopper, Inc. provides this publication "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products described may be made at any time.

IPCopper is a trademark of IPCopper, Inc., registered in the United States and/or other countries. Other trademarks are the property of their respective owners and are used here for reference purposes only.

© IPCopper, Inc. 2013. All rights reserved.

The text of this publication, illustrations, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, such as photocopying, recording, storage in an information retrieval system, or otherwise, without the prior written permission of IPCopper, Inc.

United States government restricted rights
This documentation is provided with restricted rights. Use, duplication or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in applicable FAR provisions: IPCopper, Inc., Portland, OR 97205.

What's in the Box

1	IPCopper unit
1	Cat-5e patch cable
1	power cord
1	black USB stick, which is your external key
1	white USB stick, containing the product manual and IPCD1030 / USC2030 utility

Overview

The IPCopper USC1030 is a forensic-class full packet capture appliance with 1 TB recording capacity, 1 Gbps peak capture speed and 400 Mbps minimum sustained capture speed for recording Ethernet / IP traffic. Some of its key features include:

- Electronic invisibility: The USC1030 uses neither an IP address nor MAC address. This stealthiness increases the security of the appliance, while at the same time making installation as easy as connecting a few cables.
- Permanent recording: **WARNING! The USC1030 / USC2030 will cease passing, processing and recording traffic once it reaches its 1 TB capacity.** The USC1030 and USC2030 feature forensic-class recording, meaning that once captured and recorded the data cannot be altered, modified or erased. When the unit reaches capacity, the FULL light will illuminate, and the unit will no longer capture IP / Ethernet packets or pass Ethernet / IP traffic.
- No configuration: The appliance is truly plug-and-play. Once connected and powered up, the unit begins recording all Ethernet / IP activity that passes through it automatically, with no user intervention. Additionally, installing the unit on your network will not affect traffic flow, speed or topology.
- Compact footprint: Weighing less than 4lbs and measuring 3" x 9" x 7.5", the USC1030 is portable and fits tight spaces.

This product manual is for USC1030 and USC2030 units running firmware versions 2.03 and later. If you need the product manual for earlier versions of the firmware, please contact IPCopper support at support@ipcopper.com.

Installation

1. Location / Placement

The USC1030 / USC2030 may record the activity of an entire internet connection, a single computer, a group of computers or other networked equipment. The placement of the packet capture appliance determines which network traffic would be recorded.

- To record all traffic that passes through the internet connection, place the packet capture appliance between the internet source (generally a modem) and all other equipment.
- To record only the internet or ethernet traffic to and from one computer or other device, place the packet capture appliance between that specific piece of equipment and the rest of the network.
- To record only the internet or ethernet traffic to and from a specific group of computers or other networked equipment, place the packet capture appliance between the group of computers/devices and the rest of the network.

2. Connect Ethernet Cables

The USC1030 / USC2030's two Ethernet ports are located on the front panel of the unit. The USC1030 / USC2030 may be used as either pass-through (a.k.a. inline) or on a SPAN/mirror port.

- For PASS-THROUGH/INLINE: Connect one Ethernet cable to one of the ports on the front of the USC1030 / USC2030. Connect the second Ethernet cable to the other port. The order in which the ports are connected does not matter.
- For SPAN/MIRROR: Connect an Ethernet cable from the switch or router's SPAN or "mirror" port to either port (it does not matter which one is used). Please note: You can only connect one SPAN / mirror port to the USC1030 / USC2030.

The USC1030 / USC2030 will automatically detect whether it is connected

inline or to a SPAN/mirror port. No configuration is required for either method other than the connecting of the cables.

Each Ethernet port has two lights, one green and one yellow. The green light, when shining, indicates that the link is up. The yellow light indicates that the port is operating at gigabit speed.

3. Insert the External Key

Before connecting the USC1030 / USC2030 to power, insert the external key into the USB slot. The unit will not boot up unless the key is present when the unit is powered on or re-booted. Please see the next section for information on powering the appliance on and off.

IMPORTANT! YOU MUST INSERT THE EXTERNAL USB KEY BEFORE CONNECTING THE USC1030 / USC2030 TO AC POWER.

POWERING THE UNIT ON AND OFF

To protect the packet capture appliance from power surges and other electrical fluctuations, we suggest that you connect the unit to power using a surge protector or UPS (uninterruptible power supply). Power surges may damage the USC1030 / USC2030 and/or cause it to malfunction.

Powering up the USC1030 / USC2030

IMPORTANT! YOU MUST INSERT THE EXTERNAL USB KEY BEFORE CONNECTING THE USC1030 / USC2030 TO AC POWER.

The USC1030 / USC2030 powers on when connected to power (i.e., when the power cable is connected). This allows the unit to power on automatically once power is restored after an electrical outage. When powering on the USC4060, please use the following sequence:

1. Insert the external key fully into its slot.
2. Connect the power cable to both the back of the unit and the AC power source.

DO NOT PRESS THE POWER BUTTON WHILE THE UNIT IS BOOTING UP. The unit will boot up automatically once connected to AC power. It could take up to a minute and a half for the USC1030 / USC2030 to boot up. For the first 15 seconds, the unit checks its internal systems and the lights on the front panel may blink in a random pattern or shine steady. After that, the unit will turn off all lights on the front panel except the power light for about 15-20 seconds. Once the unit becomes fully operational the green REC light will turn on and shine steady and the Ethernet port lights will illuminate.

If the packet capture appliance does not appear to boot up properly, check the following:

- Make sure the external USB key is fully inserted into the USB port.
- Connect the packet capture appliance to power via a surge protector or UPS (uninteruptible power supply).

If the red "Error" LED illuminates, press the reset button to reboot the appliance after first checking that the power and Ethernet cables are fully connected and the external USB key is fully inserted into the USB port. If the red error light persists, please turn to the Troubleshooting section for further suggestions.

Powering down the USC1030 / USC2030

To power down the appliance, press the power/shutdown button, then wait for the unit to begin blinking the power/shutdown button's blue light. Once the blue light is blinking, unplug the power cable.

Pressing the power/shutdown button initiates the following sequence:

1. The REC light begins to blink.
2. The unit ceases passing traffic and flushes all internal caches to disk, to ensure that all data is saved prior to shutdown.
3. When all data in the cache has been saved, the blue power/shutdown button light will begin blinking, indicating that it is safe to unplug the unit from the power source.

Once in shutdown mode, you must unplug the unit from the AC power source before booting it up again.

IMPORTANT: DO NOT PRESS THE POWER BUTTON WHILE THE UNIT IS BOOTING UP OR IF THE EXTERNAL USB KEY IS NOT INSERTED IN ITS SLOT ON THE FRONT PANEL. Instead, wait until the unit is operational before pressing the power button (indicated by the steady illumination of the REC light). If you press the power button while the unit is booting up or the external key is not present, the unit will enter a non-operational state and may flash all lights every few seconds. To exit this state, insert the external USB key (if not already in place) and press the power button. The unit will resume booting up. DO NOT LEAVE THE APPLIANCE IN THIS STATE WITH ALL THE LIGHTS FLASHING TO AVOID POSSIBLE DAMAGE TO THE UNIT. ANY DAMAGE RESULTING FROM LEAVING THE APPLIANCE IN THIS STATE IS NOT COVERED BY THE WARRANTY.

Understanding the Front Panel

The front panel of the USC1030 / USC2030 has several LED lights and a small number of buttons, for use in determining the status of your device and preparing it to retrieve data. The diagram below outlines what each of these lights and buttons are, and what they are for.

INDICATOR LIGHTS

- REC: indicates unit is operational and ready to record
- RET: lights up when toggled into retrieve mode; indicates that unit is in retrieve mode
- COM: lights up when communicating during data retrieval
- FULL: shines red once capacity has been reached (at this point the unit will no longer pass or record traffic)
- ERR: indicates an error (see Troubleshooting section)
- HDD: indicates that hard drive is engaged

RETRIEVE BUTTON

RESET BUTTON
press to reboot

KEY

ETHERNET PORTS

- GREEN: indicates link is up
- YELLOW: indicates port operating at gigabit speed

POWER/SHUTDOWN BUTTON

Retrieving Data

You MUST press the RETRIEVE button on the front panel before attempting to retrieve data.

When the unit is in retrieve mode, the green RET light (second from the left) will illuminate. When the RET light is illuminated you may proceed with data retrieval using either the provided IPCD1030 / IPCD2030 command-line utility (preferred method) or the optional server-authenticated retrieval method (see below). The RET light will automatically turn off and the unit exit retrieve mode when the unit powers down or restarts.

Switching back and forth between the two data retrieval methods may create unnecessary vulnerabilities, therefore we recommend using only one data retrieval method on a permanent basis.

When using the command-line utility, the data stream between the unit and the utility is encrypted. The command-line utility is the preferred method as it is the most secure for checking status and downloading data.

Although the authentication process on our servers is secure, we recommend that the server-authenticated data retrieval method be reserved for situations where using the command-line utility is not practical.

1. Data Retrieval with Command-Line Utility *(preferred method)*

To retrieve recorded data from the USC1030 / USC2030 using the command-line utility, please consult the instructions for the IPCD1030 / IPCD2030 utility included with your unit. *Please note that the utility is keyed to the specific unit with which it came; this copy of the utility cannot be used with a different unit*.

When using the utility, data may be retrieved from the unit by date/time range. Please consult the separate IPCD1030 / IPCD2030 instructions that came in the box for more information.

The utility connects directly to the unit and all communications are encrypted. During the retrieval process the unit remains in “stealthy” mode

and continues to capture and record the network traffic as normal. The unit may slow down the data retrieval process if the sustained packet capture speed reaches and/or exceeds 400 Mbps.

2. Server-Authenticated Data Retrieval

By default, server-authenticated data retrieval is disabled. It may be enabled via the utility that came with the unit. Instructions on how to do this are included in the utility's documentation.

To retrieve recorded data from the USC1030 / USC2030 using the server authentication method, go to www.ipcopper.com and follow the directions to register your unit. During the registration process you will be asked to provide some personal information and will need to have physical access to the unit as well as to a telephone.

Once you have registered, toggle the unit into retrieve mode using the RETRIEVE button and log into the web-based interface. This interface is only used to authenticate the retrieval session and protect against unauthorized retrieval. The data from the unit will be downloaded directly to a PCAP file on your computer.

This method is optional and not recommended for new deployments. It is currently offered only for compatibility purposes for existing customers.

Troubleshooting

We are committed to your satisfaction. The tips below should help resolve most issues that may arise with the USC1030 or USC2030, but we are here to help if you need further assistance.

If you have any questions or concerns about operating your USC1030 / USC2030, even if the unit is not longer within the warranty period, please contact support@ipcopper.com. Please include your unit's serial number in the email; the serial number is located on the "warranty void if tampered" sticker on the back of the unit. You will receive an automated acknowledgment that your email was received and most questions are answered the same business day or within 24-48 business hours.

Error light is on.

1. Try restarting the unit (press the reset button). This will re-boot the unit and in most cases clear the error.
2. Try changing the power cable and/or electrical outlet and reboot the unit.
3. Try changing all Ethernet cables and rebooting the unit.
4. Try disconnecting all Ethernet cables and rebooting the unit.

If the error light persists after several attempts to reboot the unit, changing cables and changing the power source, there may be a problem with the unit's hard drive or other internal part. Please contact IPCopper technical support for further assistance.

Cannot connect to Internet.

1. Is the error light on? If yes, see "Error light is on" above.
2. Make sure that the Ethernet cable(s) are firmly connected at both ends and that the unit is connected to power.
3. Check that there are no loose network cables between your computer and the unit.
4. Check the status lights on your modem, to see if your internet connection has gone down.
5. If the unit has just been rebooted or is booting up for the first time or for

the first time after a power outage, make sure that the USB key is firmly inserted into the USB port. The presence of the USB key is necessary when booting up; if it is missing, the unit will not function.

7. Check your modem's connectivity.

Please note that if you are connecting the USC1030 / USC2030 between your router and the modem, neither the router nor the modem would be able to detect the presence of the unit. As such, no MAC address alterations would occur.

When I connect the unit to power, nothing happens and no lights come on.

1. Make sure that the power cable is connected securely at both ends.
2. Try using a different electrical outlet.
3. Try using a different surge protector or UPS (uninterruptible power supply).
4. Try using a different power cable.

If none of the above makes a difference, please contact technical support for further assistance. If you have recently experienced power fluctuations, such as a power spike due to a recent storm, some of the unit's internal components may have been affected. It is highly recommended that the unit always be connected to power using a surge protector and/or UPS (uninterruptible power supply) for protection against power spikes, surges or other fluctuations in the electrical grid.

All lights are flashing.

1. Make sure the external USB key is fully inserted into its slot, then press the power button.
2. Unplug the unit from AC power, make sure the external USB key is fully inserted into its slot, then re-connect to AC power.

DO NOT LEAVE THE UNIT IN THIS STATE TO AVOID POSSIBLE DAMAGE. ANY DAMAGED RESULTING FROM LEAVING THE UNIT IN THIS STATE IS NOT COVERED BY THE WARRANTY.

Watchdog Timer

The USC1030 and USC2030 come equipped with a watchdog timer. In the unlikely event that a software or hardware malfunction causes the unit to become unresponsive, the watchdog timer will re-boot the unit after an interval of 1-3 minutes.

Please note that if the watchdog timer reboots the unit when the external USB key is not present, the unit will wait until the key is re-inserted before booting up.

Index

automatic power on 4
capacity 1
command-line utility 3, 7
forensic recording 1
data retrieval 3, 7, 8
electronic invisibility 1
error lights 4, 9
ethernet ports 2, 3, 6
external key 3, 6
front panel 6
indicator lights 6
inline 2
installation 2
IPCD1030 / IPCD2030 utility 7, 8
IP address 1
location 2
MAC address 1
mirror 2, 3, 8
pass-through 2
placement 2
power 4
power button 5
power down 5
shutdown 5
SPAN 2, 3
watchdog timer 11

Specifications

Peak capture speed	1 Gbps
Min. sustained capture speed	400 Mbps
Min. sustained packet rate	150,000 packets per second
Memory capacity	1 TB
Capture rate	100%
Network interface	2 x RJ-45 GbE
Encryption	Dual, with 20,000 bit key
Encrypted data access	Yes
Flow control	Supported
Jumbo frames	Supported, up to 9 KB
Power supply	95 - 250 VAC 48Hz-100Hz
Non-operating temperatures:	-20 °C to +70 °C
Operating temperatures:	0 °C to +50 °C
Weight	4 lbs
Dimensions	3 in x 9 in x 7.5 in

Additional Resources

General . . . . . www.ipcopper.com

Hardware Troubleshooting . . . . . www.ipcopper.com/support.htm

Other Support. . . . . www.ipcopper.com/support.htm

Warranty Claims . . . . . www.ipcopper.com/warranty.htm