DOCUMENT REFERENCE:
SQ303-002-EN

FIXED BROADBAND WHITEBOX SAMKNOWS BRIEFING

August 2015

SAMKNOWS QUALITY CONTROLLED DOCUMENT.					
SQ	REV	LANG	STATUS	OWNER	DATED
303	003	EN	DRAFT	SC	20150810
REVISION HISTORY					
DATED	REV	AUTHOR	COMMENTS		
20150810	003	LR	General Updates		
20131204	002	KR	General Updates		
20130701	001	SC	Original.		

Contents

1 Important Notice

IMPORTANT NOTICE

Limitation of Liability

The information contained in this document is provided for general information purposes only. Whilst care has been taken in compiling the information herein, SamKnows does not warrant or represent that this information is free from errors or omissions. To the maximum extent permitted by law, SamKnows accepts no responsibility in respect of this document and any loss or damage suffered or incurred by a person for any reason relying on the any of the information provided in this document and for acting, or failing to act, on any information contained on or referred to in this document.

2 THE ARCHITECTURE

SamKnows offers hardware probes (termed herein as "Whiteboxes") for the purpose of accurately measuring end-user broadband performance. There are three types of probes: two for fixed-line broadband, and one for mobile broadband. This document focuses upon the fixed-line Whiteboxes.

The Whiteboxes execute a series of software tests over their broadband connection they are connected to. The results of these tests are reported securely up to hosted backend infrastructure.

The majority of tests run against SamKnows's network of test nodes. These are dedicated servers either on-net (on the local ISP's network) or off-net (on the public Internet). Some tests will execute against real applications hosted on the Internet, mimicking their behaviour and measuring key performance variables.

When a testing cycle has completed, the results are encrypted and transmitted over SSL to hosted backend infrastructure for processing and presentation through a web interface to each panellist and other interested parties.

Panellists are, as part of the terms of service, required to leave their Whitebox and other networking equipment permanently powered on and connected to ensure consistent testing.

2.1 Firmware

All SamKnows Whiteboxes run a custom distribution of Linux, derived from OpenWrt. Many standard OpenWrt features have been removed to save space on the device, and some additional features have been added to support the measurements.

The custom firmware is flashed at the factory and is not directly upgradeable by the user hosting the Whitebox. The firmware is remotely upgradeable by SamKnows.

This cut-down operating system provides network connectivity and the measurement applications alone – there is no web interface and the Whitebox provides no routing functionality. Panellists have no ability to disable, reconfigure or influence the SamKnows software in any way through normal usage.

SamKnows' firmware makes use of GPL v2.0 licenced code. The source code for SamKnows' firmware build is available at:

`https://files.samknows.com/~gpl/`

2.2 Whitebox Communications

All communications between the Whitebox and the Data Collection Service on the backend hosted infrastructure are initiated by the Whitebox, encrypted over SSL and subject to authentication

The Whitebox communicates with the target test nodes over a variety of TCP and UDP ports. The Whitebox will also communicate with some unmanaged services over both TCP and UDP.

2.3 Software Updates

The SamKnows software suite has the ability to auto-update itself, downloading updated binaries and testing schedules from the Data Collection Service and storing locally in RAM or flash.

Because these devices are installed on a consumer's broadband connection (which will likely be in use through normal day-to-day activity), it is necessary for the Whitebox to take some precautions in order to protect the validity of the gather data. In order to determine when it is safe to execute tests, the end user's traffic levels are monitored continuously. In fact, this is the reason for connecting all Ethernet devices through the Whitebox.

2.4 Whitebox 1.0 (SK-TL-WR741ND)

The SK-TL-WR741ND can accurately measure fixed-line broadband connections of up to 100Mb/s.

The specifications of the device are as follows:

- Functions as an Ethernet bridge
- Passively monitors wireless activity
- 4x 100Mbps LAN interfaces
- 1x 100Mbps WAN interface
- Single 2.4GHz 802.11bgn radio
- Single DC power (9V @ 750mA)
- Power draw: 4W
- 243mm x 160.6mm x32.5mm Dimensions
- Weight: 500g

2.5 Whitebox 5.0 (SK-TL-AC1750)

The SK-TL-AC1750 can accurately measure fixed-line broadband connections of up to 600 Mb/s downstream and 300 Mb/s upstream. This device uss a new Linux 3.10.49 kernel.

The specifications of the device are as follows:

- 2x 802.11a/b/g/n/ac wireless interface, 3 antennas
- 720Mhz MIPS CPU
- 128MB RAM
- 5x1 Gbps Ethernet
- Single DC power (12V @ 1500mA)
- Power draw: 5W
- Weight: 700g
- Functions as an Ethernet bridge
- Passively monitors wireless activity
- 4x 1Gbps LAN interfaces
- 1x 1Gbps WAN interface

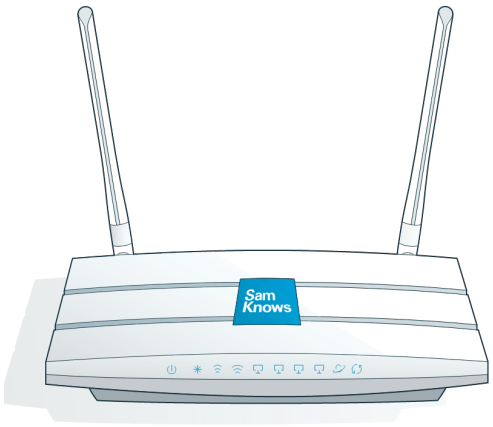


Fig1: SamKnows Whitebox

2.6 Whitebox 8.0

The latest SamKnows Whitebox, the Whitebox 8.0, is capable of measuring 1000Mb/s downstream and upstream.

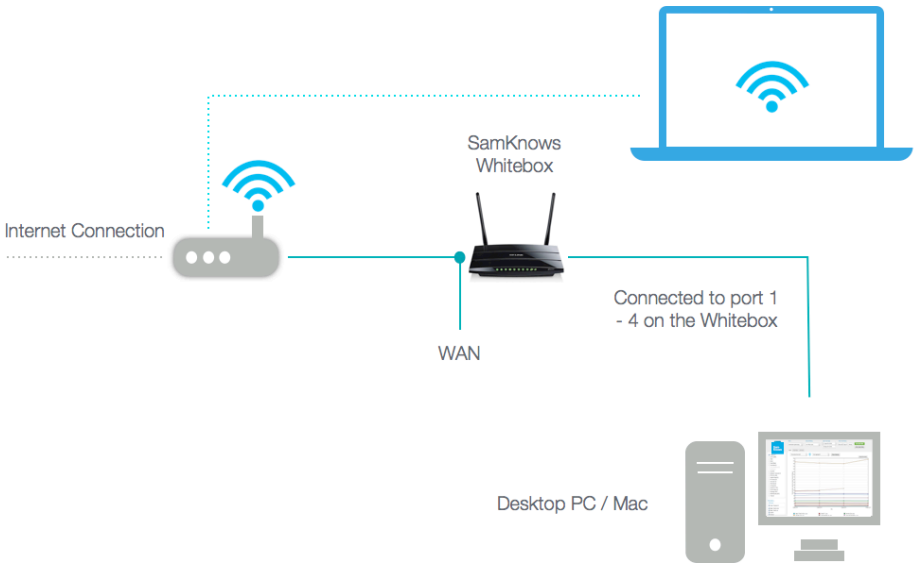
The specifications of the device are as follows:

- Dual 2.4 GHz and 5GHz WiFi radios, supporting 802.11a/b/g/n/ac
- Dual-core 880MHz CPU
- 128MB RAM
- 16MB flash storage
- 4x 1Gbps LAN interfaces
- 1x 1Gbps WAN interfaces

Fig 2: SamKnows Whitebox 8.0

2.7 Installation

The Whitebox operates as an Ethernet bridge, co-existing with an existing modem/router. All wired devices should connect through the Whitebox. Wireless devices should continue to connect to their existing router:



2.8 Cross-traffic detection (Inline / pass-through)

A key benefit to the Whitebox approach is the fact that 'cross-traffic' (other traffic in the participant's home) can be accounted for. This means we can avoid running tests when the user is using their connection, resulting in (a) cleaner results for us and (b) a happy participant (because their use of the Internet is not being interrupted).

Participants are instructed to connect their wired devices via the Whitebox and leave their wireless devices unchanged.

Prior to and between tests, a threshold manager service monitors the inbound and outbound traffic across the WAN interface of the Whitebox to calculate if a panellist is actively using the Internet connection. The threshold for traffic is set to 64kbps downstream and 32kbps upstream. If these thresholds are breached prior to the test starting or between tests, the test will be delayed for a minute and the process repeated. If the connection is being actively used throughout, this pause and retry process will occur up to 5 times before the entire test cycle is abandoned.

A similar process is performed for wireless clients. Wireless users are not asked to make any changes. As with the wired approach, measurements are not conducted when there is wireless activity detected. Wireless activity is determined by

passively monitoring the traffic from the user's wireless SSID(s). There are two techniques used to determine the user's wireless SSID:

1) Perform a scan for wireless networks in the vicinity of the Whitebox. Search for an access point that has a MAC address adjacent to the MAC of the LAN interface on the volunteer's CPE. In a user's home environment, this is typically a combined modem/router/WAP. This takes advantage of the fact that most CPE use similar MACs on their Ethernet and WiFi interfaces. This provides significantly improved confidence in high density wireless environments (like apartment blocks).
2) Where no adjacent wireless MAC is found, the Whitebox falls back to the old approach of choosing the device with the strongest signal, whereby the SamKnows Whitebox passively monitors the strongest nearby wireless network for traffic.

Once an SSID has been identified, the Whitebox passively monitors all traffic that the SSID exchanges and records volume information. Note that it does not matter if the wireless network is encrypted; the Whitebox does not need to join the wireless network, it simply cares about volumes of data (it makes a conservative assumption that all wireless traffic is destined for the Internet).

If a wireless AP is broadcasting multiple SSIDs on the same channel, then the Whitebox will catch traffic from all, because they will use the same or adjacent MAC addresses. It does not matter if the user has hidden their SSID or encrypted their wireless network; the Whiteboxes are simply passively monitoring packet volume and do not need access to the data contained within the packets.

The wireless monitoring process described above is repeated in both the 2.4GHz and 5GHz channels, for applicable Whitebox models.

2.9 Cross-traffic detection (Out-of-band)

Some ISPs may use services that require the user to connect devices directly to the CPE, meaning that the inline approach described above is not suitable. In those cases we can still support cross-traffic detection by interrogating the CPE out-of-band. We can do this using UPnP, SNMP, HTTP or any other protocol (custom development may be required).

[DOCUMENT ENDS]