Factsheet

Test Agents – Whitebox

Whitebox

SamKnows Whitebox

The Whitebox is a purpose-built hardware measurement agent manufactured by SamKnows, capable of measuring fixed-line broadband connections of up to 1Gbps. It supports a wide range of network and application-specific measurements, and can detect the presence of user-generated cross traffic.

Specifications

The current generation of Whitebox (8.0) is capable of measuring 1Gbps downstream and upstream over both TCP and UDP.

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
- USB 2.0 port
- DC power (12V @ 2000mA)

Firmware

The Whitebox runs 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. SamKnows publishes its firmware source code in compliance with the GPL.

Remote updates

The Whitebox communicates with the SamKnows cloud to retrieve its test schedule and configuration. These updates occur automatically, approximately once per hour. The Whiteboxes retrieve configuration updates using the IETF LMAP protocol, and communicate over HTTPS using TLS 1.2.

Additionally, SamKnows will periodically issue firmware updates which are applied automatically by the Whitebox.

No user interaction is required for the Whitebox to retrieve software or configuration updates.

Placement within the home network

Whiteboxes are typically installed in-line (i.e. "man in the middle") in the user's home network. This is required in order to identify the presence of cross-traffic. Modern versions of the Whitebox utilise a hardware switch internally, with the SamKnows applications only having access to port counters via the switch's API. User-generated cross-traffic does not pass across the CPU, so is unavailable to packet capture applications.

In some cases it is possible (through cooperation with the ISP/client) to deploy the Whitebox out-of-band, i.e. as a regular network client. In this scenario an alternative mechanism is used to capture the presence of cross-traffic (e.g. UPnP, HTTP or SNMP polling of the router).

Whitebox 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.

The following steps guide end-users through the installation of the Whitebox.

Within 24 hours of installing the SamKnows Whitebox we will send you an automated email once we have detected that your Whitebox is operational and working correctly. You should be able to see data being displayed in SamKnows One within a few hours.

1. Connect one end of the network cable to the port marked “WAN” on the back of the Whitebox.
2. Plug the other end into a spare port on your router (not the USB port), it may also be marked “WAN”.
3. Connect the power cable to the Whitebox and press the power button on the back labelled ON/OFF.
4. The green working light (two revolving arrows icon above it) will flicker for approx. 30-60 seconds. The light will then stay solid once a connection is made.
5. Within 48 hours of installing your Whitebox we will send you an email with your personal SamKnows One login details to your analytics dashboard.
6. Wired devices plugged into your router should be connected to LAN1 - LAN4 ports on the Whitebox instead. If your devices connect via WiFi ignore this step.
7. Get in touch if you need some help with anything or to let us know how you are getting on.

Supported tests and metrics

Please refer to the tests and metrics section to find the list of test clients that are supported by the Whitebox.

Cross-traffic detection (inline)

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, by default, set to 64kbps downstream and 32kbps upstream, although this can be modified. 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. Breaches of these thresholds are reported and can be viewed within the SamKnows One platform.

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.

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).

The Whitebox includes support for out-of-band UPnP cross-traffic detection out of the box. This uses the libminiupnpc library to interrogate the CPE's WANConnectionInfo status. Note that many consumer-grade CPE appear to support UPnP counters, but do no not implement them correctly.

To determine if your CPE adequately provides UPnP counters, follow the following instructions:

1. Download miniupnpc (the client) from http://miniupnp.free.fr/files/ and compile. Or use ‘yum’ or ‘apt-get’ to install it from your distribution of choice.
2. Execute the following (note that you may need to change the interface in use):

```
# ./upnpc-static -m eth0 -s
    upnpc : miniupnpc library test client. (c) 2005-2013 Thomas Bernard
    Go to http://miniupnp.free.fr/ or http://miniupnp.tuxfamily.org/
    for more information.
    List of UPNP devices found on the network :
    desc: http://192.168.2.254:2869/upnp/dslip.xml
    st: urn:schemas-upnp-org:device:InternetGatewayDevice:1

    Found valid IGD : http://192.168.2.254:2869/upnp?control=WANIPConn1
    Local LAN ip address : 192.168.2.50
    Connection Type : IP_Routed
    Status : Connected, uptime=148s, LastConnectionError : ERROR_UNKNOWN
     Time started : Mon Nov  4 17:28:00 2013
```

MaxBitRateDown : 17254174 bps (17.2 Mbps) MaxBitRateUp 2013291 bps (2.0 Mbps)
ExternalIPAddress = 46.65.6.101
Bytes: Sent: 64931 Recv: 76507
Packets: Sent: 22778539 Recv: 0

1. Download a large file and repeat the command in step 2, verifying that the byte counters have increased by the same size as the file you downloaded.

Legacy whiteboxes
(Please see page 5)

Legacy Whiteboxes

Model	Platform reference	Release date	Maximum measurable speed	Wireless capabilities
Whitebox 6.0	ac1750v2	2015	550Mbps down, 550Mbps up	802.11a/b/g/n/ac, 2.4Ghz and 5Ghz
Whitebox 5.0	wdr4900	2014	800Mbps down, 800Mbps up	802.11a/b/g/n, 2.4Ghz and 5Ghz
Whitebox 3.0	wdr3600	2013	450Mbps down, 250Mbps up	802.11a/b/g/n, 2.4Ghz and 5Ghz
Whitebox 2.0	wr1043nd	2011	200Mbps down, 200Mbps up	802.11b/g/n, 2.4Ghz
Whitebox 1.0	wr741ndv4	2011	100Mbps down, 100Mbps up	802.11b/g/n, 2.4Ghz
Whitebox 0.5	wnr3500l	2010	150Mbps down, 100Mbps up	802.11b/g/n, 2.4Ghz