Sparrow IQ Quick Start Guide

Release 1.3.4

Table of Contents

1 Introduction

This document describes the basic deployment scenarios one is likely to encounter when using Sparrow[IQ] to monitor their network. It focuses on getting the system up and running as quickly and easily as possible. Once initial setup is performed and analyses of results are presented, the system configuration can be refined as necessary to tailor the system to the client's network. Not covered in this document are the acquisition and installation of the Sparrow[IQ] installer or reflector agent software. For more detailed information, please consult the Sparrow[IQ] User's Guide.

2 Sparrow[IQ] Deployment

In order for Sparrow[IQ] to monitor and analyze network traffic, theSparrow[IQ] host must be connected to the network such that it has visibility of said traffic. This is accomplished in one of two ways, known as SPAN or TAP modes, depending on available network hardware and the number of network interfaces within the Sparrow[IQ] host. SPAN mode is the simpler of the two, utilizing a single host network interface and a single free port on a supported switch or router; TAP mode requires 2 (or more) network interfaces on the Sparrow[IQ] host and a network tap.

2.1 SPAN Mode

As mentioned above, SPAN mode requires that the Sparrow[IQ] host contains a single network interface connected to a switch or router that supports port mirroring. That switch, or router, must be configured to forward all traffic from its *uplink, or WAN, port* to that connected to the Sparrow[IQ] host. This essentially copies all incoming and outgoing network traffic to Sparrow[IQ] for analysis. Alternatively, if monitoring of a particular port on the switch or router is required, it can be mirrored

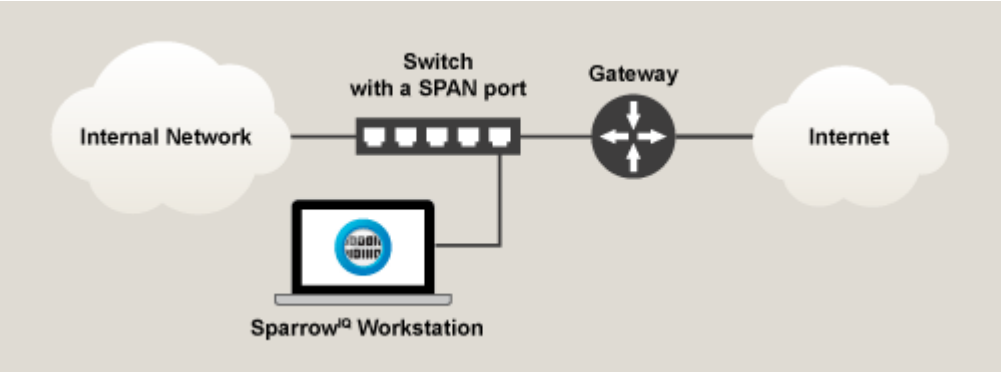

Figure 1- SPAN Mode Deployment

instead of the uplink port.Figure 1illustrates connecting Sparrow[IQ] to the network using SPAN mode.

The *port mirroring* feature is commonly found on many switches and routers, from those used in homes to those used in data centers. It may also be known as *SPAN* (used mostly by Cisco) or *RAP* (used mostly by 3Com). Many popular vendors support this, including Cisco, DLink, Dell, HP, Linksys, and Netgear.

Once properly connected to the network, Sparrow[IQ] must be configured to monitor the correct network interface on its host. This is accomplished via the *Probe* tab of the *Settings* page on the Sparrow[IQ] web console, as shown in Figure 2.

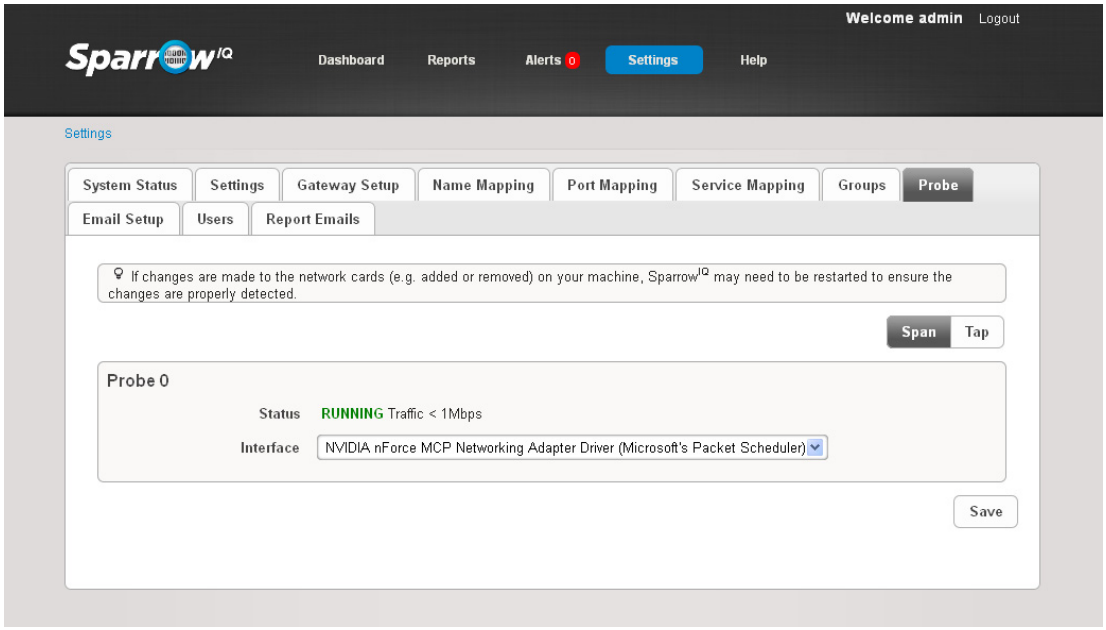

Figure 2 - Network Interface Selection (SPAN)

This page allows one to select between SPAN and TAP modes and to select the network interfaces on which to listen. SPAN mode is chosen by default. Network interface names, addresses, and estimated data rates are displayed to assist with proper selection. The current state of the probe monitoring an interface can be seen once that interface has been selected and saved. If any changes are made to the network interfaces on the host, such as enabling or disabling an interface through the operating system, Sparrow[IQ] must be restarted before those changes are reflected.

At this point, the Sparrow[IQ] host should be connected to a mirrored port and its network interface should be selected via the web console. After two or three minutes of collection, network traffic analysis should start to appear on the dashboard.

2.2 TAP Mode

Unlike SPAN mode, TAP mode requires the use of an additional piece of equipment, known as a *network tap*. This device contains two ports that pass all data between them, allowing the tap to be placed anywhere in the network without affecting traffic. For example, placed between the uplink port of a router and a WAN connection, the tap would capture all incoming and outgoing traffic. Placed elsewhere in the network, the tap would capture only that traffic which passes through it. Taps also have one or two monitor ports to which traffic is copied. Those taps that have only one monitor port, known as *aggregator* taps, have all traffic mirrored to that port; those with two ports mirror the IN and OUT traffic directions onto separate ports. These mirror port(s) must be connected to the Sparrow[IQ] host. One would choose this deployment scenario in cases where either the switch or

router does not support port mirroring or it would be inconvenient or impossible to configure the network as described for SPAN mode.Figure 3illustrates this scenario.

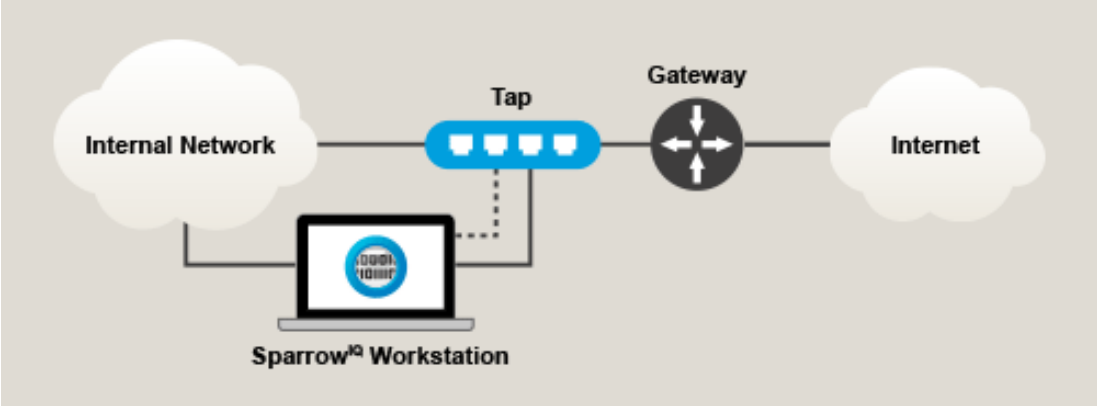

Figure 3 - TAP Mode Deployment

As shown above, the Sparrow^{IQ} host requires one or two connections to the network tap, depending on its number of monitor ports. Also, because monitor ports cannot be used as convention network connections, a separate connection is required if the Sparrow^{IQ} host requires network connectivity. Network taps from several vendors have been tested and used in practice, including Barracuda, VSS Systems, and NetOptics.

Once properly connected to the network, Sparrow^{IQ} must be configured to monitor the correct network interfaces on its host. This is accomplished via the *Probe* tab of the *Settings* page on the Sparrow^{IQ} web console, as shown in Figure 4.

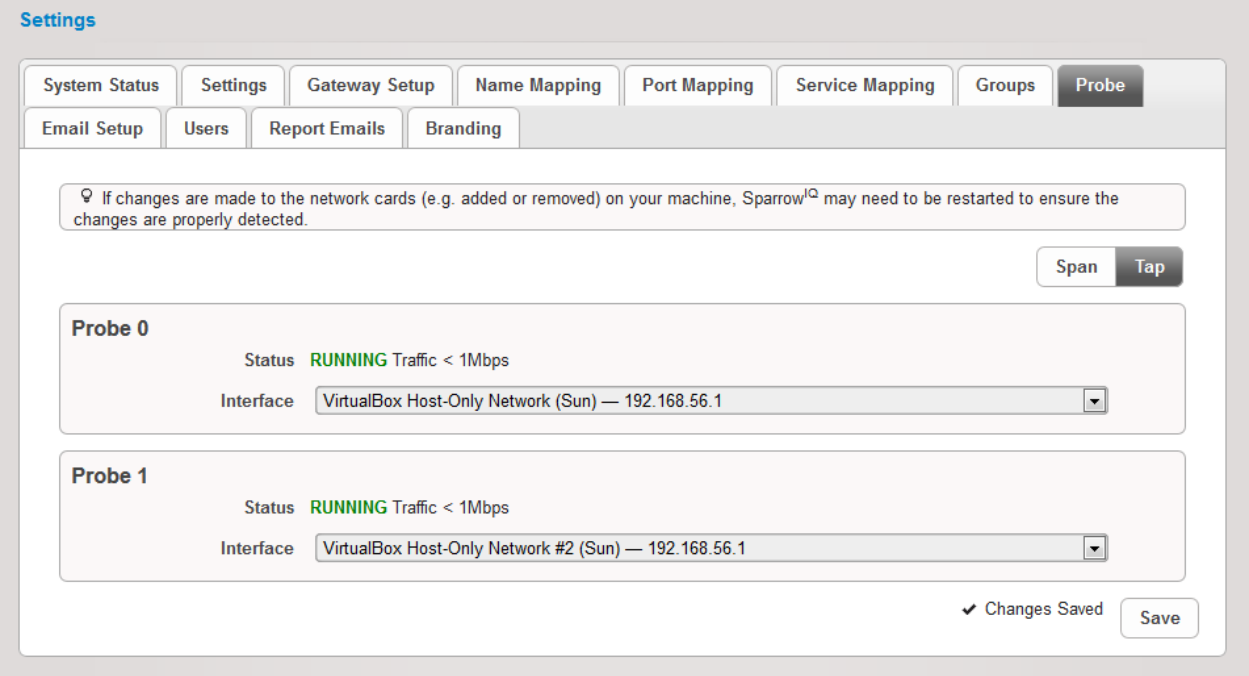

Figure 4 - Network Interface Selection (TAP)

This page allows one to select between SPAN and TAP modes and to select the network interfaces on which to listen. SPAN mode is chosen by default. Network interface names, addresses, and estimated data rates are displayed to assist with proper selection. The current state of the probe monitoring an interface can be seen once that interface has been selected and saved. If any changes are made to the network interfaces on the host, such as enabling or disabling an interface through the operating system, Sparrow^{IQ} must be restarted before those changes are reflected.

In this scenario, the choice between SPAN and TAP modes for the probe depends on the number of monitor ports on the tap. Aggregate taps that have only one monitor port can be treated as SPAN ports in that only one network interface is required. For taps that have two monitor ports, TAP mode must be selected on this page and two network interfaces must be selected, one for each traffic direction. Selections must be saved in order to take effect.

At this point, the Sparrow^{IQ} host should be connected to one or two monitor ports of a tap spliced into the network, and necessary network interfaces should be selected via the web console. After two or three minutes of collection, network traffic analysis should start to appear on the dashboard.

3 Path QoS

The *Path QoS* feature is used to monitor and analyze the quality of a network connection between the Sparrow^{IQ} host and another host, either on a local network or global Internet. This information is useful to diagnose problems with real-time communications, such as VoIP, video conferencing, or streaming. Assuming that Sparrow^{IQ} is already deployed and running, all features of the Path QoS feature are available through the widget on the primary dashboard, as seen in Figure 5.

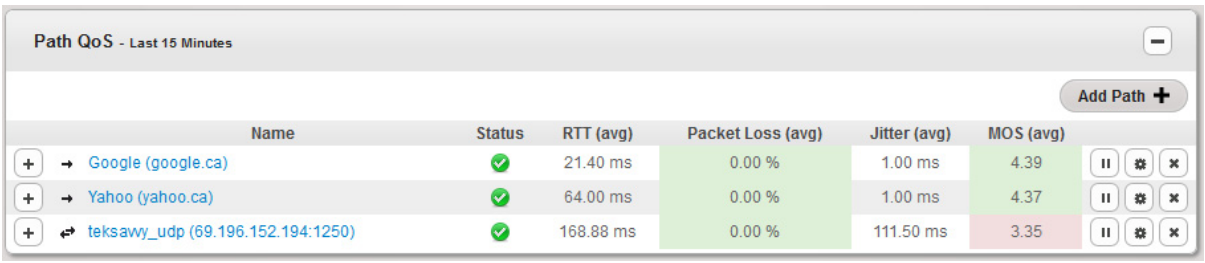

Figure 5 - Path QoS Widget

This widget allows one to configure up to 10 paths, depending the purchased version of Sparrow[IQ]. Each path analyzes the route from the Sparrow[IQ] host to the configured target by sending streams of test data to the target and analyzing the timing characteristics of the responses. By default, two ICMP paths, one to google.ca and one to yahoo.ca, come pre-configured. This section describes the configuration of additional paths and interpreting the results.

3.1 Path Configuration

Configuration of a path specifies the target and characteristics of test data generated to analyze the route from the Sparrow[IQ] host to that target. Characteristics of the test data should be defined such that they mirror actual real-time communications as closely as possible. For example, VoIP can be modeled by a high number of packets-per-minute (PPM) and a relatively low packet size, whereas video streaming tends to have a lower PPM and higher packet size. To configure a path, click the "Add Path" button within the Path QoS gadget on the dashboard, resulting in a form as shown in Figure 6.

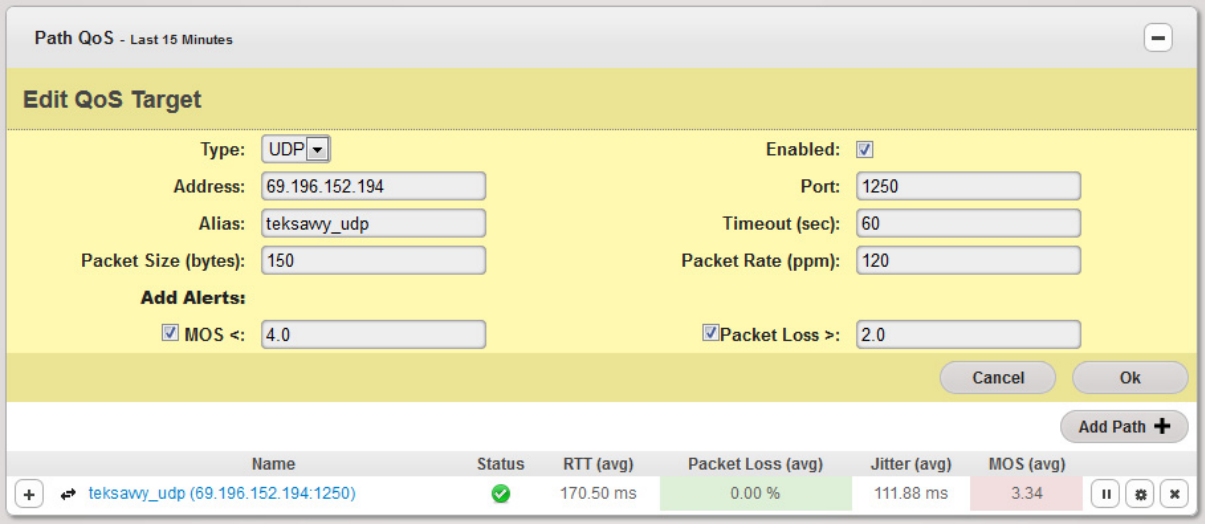

Figure 6 - Add / Edit QoS Path

The fields of this form include:

- **Type** – Selected protocol of test data, either ICMP or UDP. See sections 3.1.1 and 3.1.2 for more information on these protocols.
- **Enabled** – Whether or not this path is currently active.
- **Address** – The IPv4 address or resolvable name of the target host. This must be a host to which the Sparrow[IQ] host can communicate in order for testing to be successful.
- **Port** – Valid only for UDP, this specifies the port on which a reflector agent listens. See section 3.2for more detail on the reflector agent.
- **Alias** – A friendly name used to represent this path.
- **Timeout** – The length of time, in seconds, before a connection is determined to be lost.
- **Packet Size** – The size, in bytes, of each packet sent during the test. The valid range is 0 – 1000 bytes.
- **Packet Rate** – The rate, in packets-per-minute, that test packets are created and sent to the target host. The valid range is 1 – 600 PPM.
- **MOS Alert** – Simple alert based on the MOS value of the path falling below the given threshold.
- **Packet Loss Alert** – Simple alert based on packet loss percentage above the given threshold.

Of these parameters, only the address and, if using the UDP protocol, port number are required; defaults can be used for the rest. Alerts are disabled by default. All path parameters can be edited at any time using the edit icon.

3.1.1 ICMP Protocol

Similar to the *ping* command, paths configured for ICMP transmit echo requests to the target host, which replies with echo responses. This results in a *one-way* trace, as only the path from Sparrow[IQ] to the target host is analyzed. As expected, ICMP paths can be used for hosts to which one can successfully contact with the ping command; no additional hardware or software is required.

3.1.2 UDP Protocol

Unlike ICMP, the UDP protocol requires additional software on the target host to reflect test datagrams back to the Sparrow[IQ] host. For this, the Sparrow[IQ] Reflector Agent can be used, as described in section 3.2. Because reflected datagrams can be routed back to Sparrow[IQ] over a different path than they were originally sent, this results in a *two-way* trace, analyzing both the outgoing and incoming paths at the same time.

3.2 Sparrow[IQ] Reflector Agent

The Sparrow[IQ] Reflector Agent (SRA) is a software package that must be installed on target hosts for QoS path analysis with the UDP protocol. Its purpose is to simply reflect the UDP traffic generated by Sparrow[iQ] during testing. The installation package contains two pieces: an administrative console and a reflector service. The former presents the user with a means with which to configure the reflector service, while the latter simply runs in the background and responds to appropriate UDP traffic. For more information on obtaining and installing the SRA, please consult the Sparrow[IQ] User Guide.

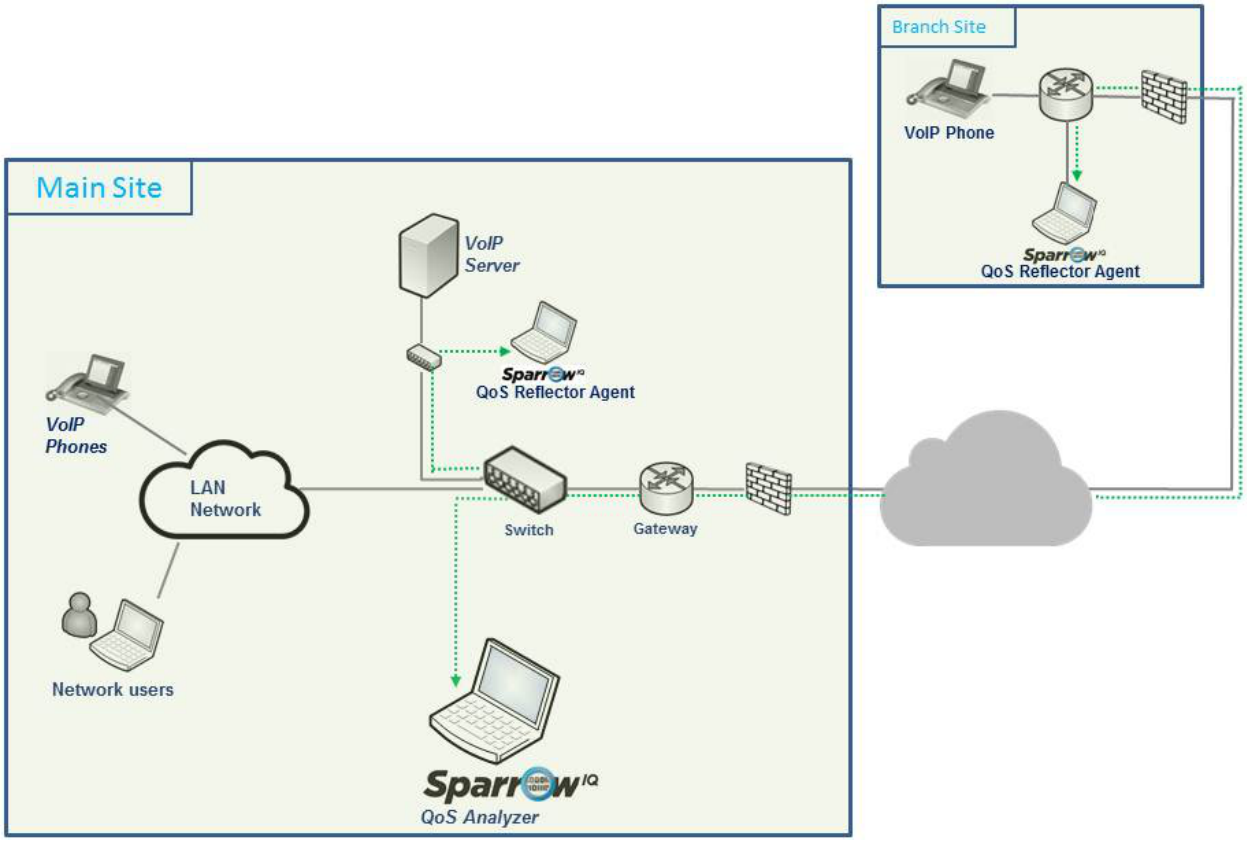

Figure 7 - Multi-site SRA Deployment

As seen in Figure 7, several SRAs can be deployed at strategic locations on the network in order to test different paths from the Sparrow[IQ] host. This diagram shows two reflectors, one near the VoIP server at the "Main Site", and another at a "Branch Site". A configuration such as this would be useful for

determining the connection quality to both the local VoIP server and, through firewalls and a public WAN, the remote VoIP phone. Each reflector would require its own path configuration in Sparrow[IQ] as streams of UDP traffic would be sent to each, independently.

3.2.1 Configuration

As suggested by Figure 8, only a few settings are required to configure the SRA.

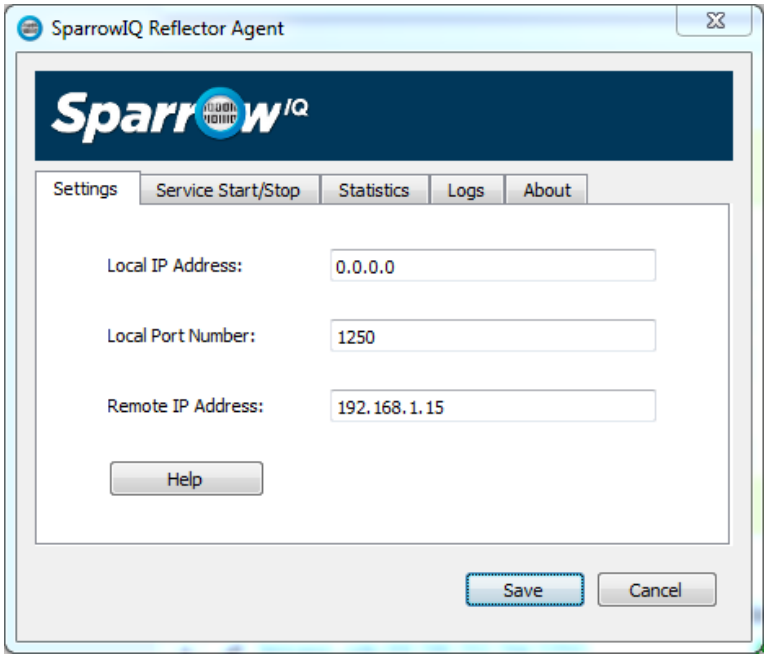

Figure 8 - SRA Settings

The local address and port parameters define how the SRA listens for incoming UDP traffic. By default, ports are bound to all network interfaces, signified by the use of the address 0.0.0.0 or a blank address. Alternatively, the IP address of a specific network interface can be entered to restrict the service to responding only to that interface. An incorrect value for local address can cause the service not to respond to any traffic, so care must be taken when setting to a non-default value. The port is simply the UDP port on which the SRA listens for incoming traffic. It must be the same as that configured in the Sparrow[IQ] Path QoS gadget for this target.

The "Remote IP Address" is used to filter out all traffic received by the SRA from hosts other than that specified. This is an optional setting that, if configured, should be set to the IP address of the Sparrow[IQ] host.

3.2.2 Controlling the Service

The SRA can be started and stopped manually, or it can be configured to run automatically when the computer on which it is installed is booted. Figure 9 illustrates the controls available for this configuration.

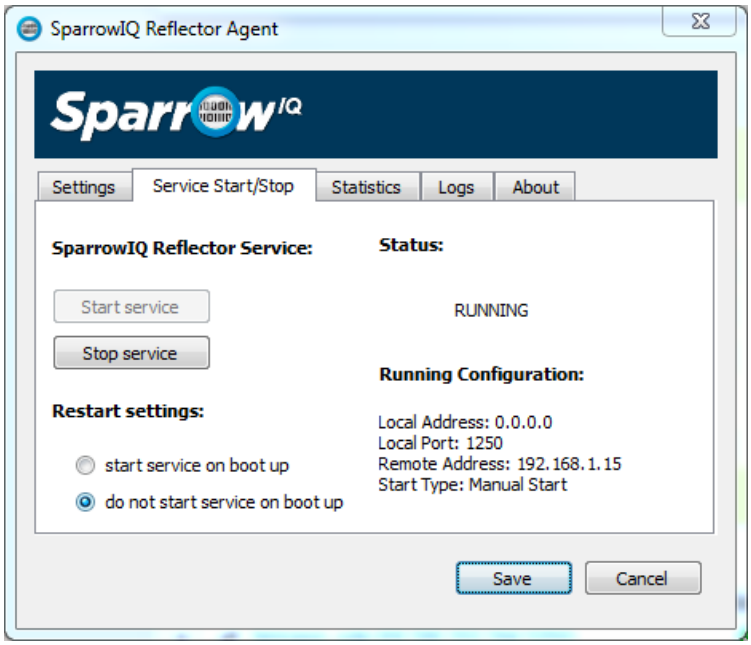

Figure 9 - SRA Starting & Stopping

On the left of the panel, the "Start Service" and "Stop Service" buttons are used to manually start and stop the reflector service. Below that, one can choose whether or not to start the service automatically at boot time. The right-hand-side of the tab shows the current state and run-time configuration of the service.

3.3 Interpreting Results

Several parameters are measured and calculated for each configured path. Summary information is displayed in the table, with more detailed analysis available by clicking the [+] icon to show a sub-table, or by clicking the path name to show a drilldown for the path. QoS results are calculated over the same timeframe as the dashboard as a whole, which can be selected using the duration selector above the QoS widget. Figure 10 shows the summary information and open sub-table.

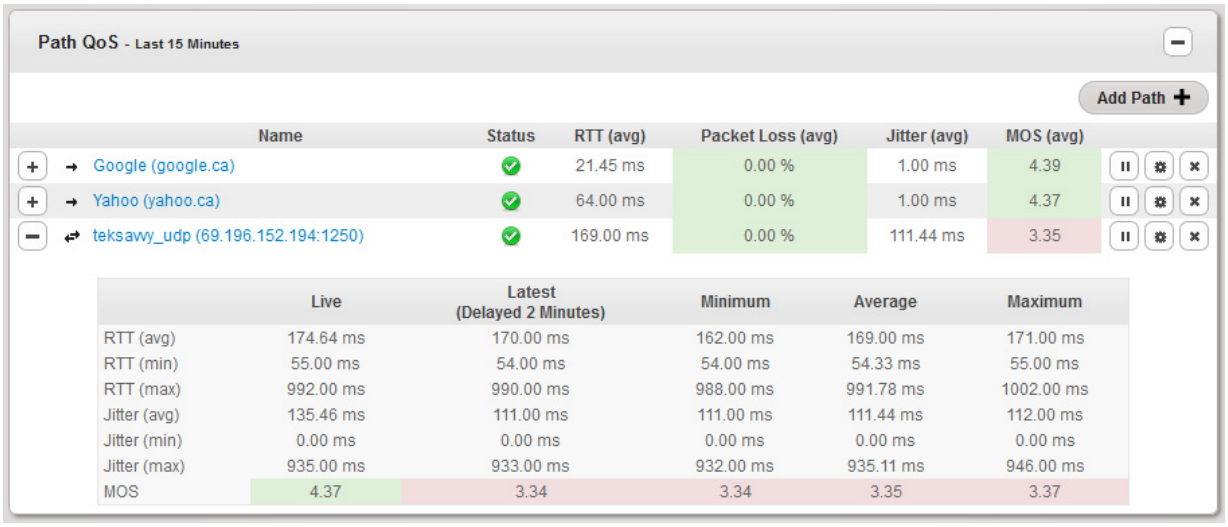

Figure 10 - Summary and Detailed Results

Summary information for a path includes:

- **Status** – icons representing one of OK, PAUSED, POOR, and LOST. POOR indicates that one or more consecutive packets have been lost, while LOST indicates that all packets have been lost for longer than the configurable timeout.
- **RTT (avg)** – the average Round Trip Time (RTT) in milliseconds between Sparrow^{IQ} and the target host. Low RTT provides for a better experience for low-latency communications.
- **Packet Loss (avg)** – the average packet loss percentage for the selected duration.
- **Jitter (avg)** – reported in milliseconds, jitter is a measure of variation in RTT. Real-time communications depend on a consistent connection between endpoints, as represented by a low average jitter.
- **MOS (avg)** – *Mean Opinion Score* (MOS) is an industry standard measure of quality incorporating RTT, loss, and jitter into a single representative score ranging from 1 to 5. One would expect a good experience over paths with a score greater than 4, whereas poor experiences can be expected for those with a score lower than 3.

A breakdown of RTT, jitter, and MOS is presented in the sub-table for each path. Results are stored with a granularity of one minute. For each one minute period, the MOS, and the minimum, average, and maximum values for RTT and jitter are recorded. Each column in the sub-table presents calculations based on these recorded values:

- **Live** – shows real-time data currently collected by the QoS engine, before it has been summarized into the one minute periods mentioned above.
- **Latest** – presents the most recent one-minute period contained within the selected dashboard timeframe.
- **Minimum** – the minimum values for the associated metric over the selected timeframe.
- **Average** – the average values for the associated metric over the selected timeframe.
- **Maximum** – the maximum values for the associated metric over the selected timeframe.

3.4 Configuration Example

This section walks the user through the basic configuration of path QoS analysis using both the ICMP and UDP protocols. Figure 11 illustrates an example network comprising a main site with a Sparrow^{IQ} host at 192.168.1.190, a VoIP server at 192.168.1.30, and a Sparrow^{IQ} Reflector Agent with address 10.0.0.100 at a branch site. The goal of this example is to configure two paths:

1. ICMP path between Sparrow^{IQ} and the VoIP server, and
2. UDP path between Sparrow^{IQ} and the reflector agent at the branch site.

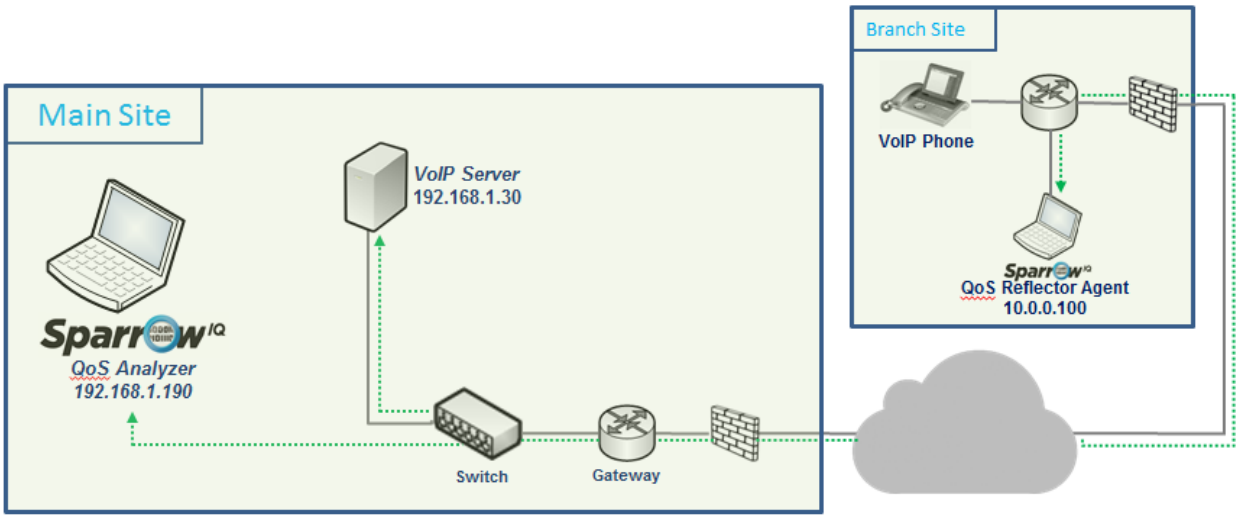

Figure 11 - Example Deployment Scenario

For this example, we assume that Sparrow^{IQ} and the Reflector Agent have been previously installed on their respective hosts.

3.4.1 Configuring ICMP Path to VoIP Server

Assuming that Sparrow^{IQ} is already installed and running on 192.168.1.190, the goal is to create an ICMP path to test the VoIP server at 192.168.1.30. This is accomplished as follows:

1. Navigate to the main dashboard.
2. Click the "Add Path" button in the *Path QoS* widget. A form, as seen in Figure 6, will be displayed.
3. Enter "192.168.1.30" in the *address* field, leaving all other parameters as their defaults.
4. Click the "OK" button. The form should vanish and an entry for the new path should appear in the list.
5. After a few moments, the status for the path should appear as OK, and live results should be visible by clicking the [+] icon on the left of the path's row. A table, as shown in Figure 10, appears, containing a summary of analysis.
6. After 2 to 3 minutes of gathering data, the rest of the table will be populated.

If live results fail to appear after a few moments, the following may help to resolve the problem:

1. Use the standard *ping* command on the Sparrow[IQ] host to verify communications with the VoIP Server. If this does not work, the VoIP server may be configured to block incoming ICMP traffic.
2. Verify that the correct address has been used for path configuration and that the path is enabled.
3. Use a packet sniffer, such as Wireshark, to verify that ICMP echo request packets are generated and responses received on the Sparrow[IQ] host.

3.4.2 Configuring UDP Path to Branch Site

Assuming that Sparrow[IQ] is already installed and running on 192.168.1.190 and the SRA installed on 10.0.0.100, the goal is to create a UDP path to test the route between them. This is accomplished as follows:

1. On the SRA, right-click the task-tray icon and open the configuration window, as seen in Figure 8.
2. Enter "30000" for the port and leave the other fields blank. This will configure the SRA to echo UDP traffic from any address on this port. Click Save.
3. Navigate to the Start/Stop tab, as seen in Figure 9. Click "Start Service." The status should show that the SRA is indeed running.
4. On the Sparrow[IQ] host, navigate to the main dashboard.
5. Click the "Add Path" button in the *Path QoS* widget. A form, as seen in Figure 6, will be displayed.
6. Select the "UDP" type.
7. Enter "192.168.1.30" in the *address* field and "30000" in the *port* field, leaving all other parameters as their defaults.
8. Click the "OK" button. The form should vanish and an entry for the new path should appear in the list.
9. After a few moments, the status for the path should appear as **OK**, and live results should be visible by clicking the [+] icon on the left of the path's row. A table, as shown in Figure 10, appears, containing a summary of analysis.
10. After 2 to 3 minutes of gathering data, the rest of the table will be populated.

If live results fail to appear after a few moments, the following may help to resolve the problem:

1. Use the standard *ping* command on the Sparrow[IQ] host to verify communications with the SRA. If this does not work, the SRA may be configured to block incoming ICMP traffic.
2. Verify that the correct address has been used for path configuration and that the path is enabled.
3. Use a packet sniffer, such as Wireshark, to verify that UDP echo request packets are generated and responses received on the Sparrow[IQ] host and SRA host.
4. If UDP traffic is not visible on either host, it may be blocked by the windows firewall. This can be tested by temporarily disabling that firewall on both hosts. *This is not a good long-term solution, but can be used to help isolate communication issues.*