



Report Pack for Cisco IP-SLA

Watch4Net Solutions
Corporate Headquarters:
4388, Saint-Denis street
Office 309, H2H 1Y2
Montréal, Canada

Index

Overview.....	3
Requirements.....	11
Installation.....	13
Snmp Collector setup.....	13
Data collection setup.....	14
Polling groups definitions.....	16
APG Web Portal setup.....	17
Guidelines to set up probes on Cisco devices.....	18
Guidelines to setup probes polled via their statistics tables.....	20
Guidelines to set up probes polled via their history operation table.....	20
About probe creation and management.....	21
Troubleshooting.....	22
Contact and Technical Support.....	24
Technical Support.....	24
Contact us.....	24
Legal Notices.....	25
Warranty.....	25
Copyright Notices.....	25
Trademark Notices.....	25

Overview

Watch4Net's report pack for Cisco IP-SLA is specifically designed to monitor most common IP-SLA probes running on Cisco IP-SLA enabled devices. Supported probe types include: Jitter, HTTP, IcmpEcho and several others. This report pack provides two ways of polling the Cisco IP-SLA enabled devices, which allow long term trend analysis or punctual troubleshooting when required.

The following reports are provided right after installing this report pack:

- IP-SLA Probe Inventory View (By device and probe type): list both running probes and device capabilities;
- IP-SLA Probe Performance View (By device): lists probes by device;
- IP-SLA Probe Performance View (By probe type): lists probes by probe type;
- Situations to Watch: Unsuccessful operations, Latency and Reachability problems, etc
- *History and Last Operation table based reports

Note: The “History and Last Operation table based reports” are disabled by default: this node must be enabled by editing it. Data collection for those reports is also disabled by default as it requires more bandwidth and resources.

The IP-SLA Probe Performance View (By Device or Probe type) includes detailed reports on the following probe types:

- TCP Connect operation;
- DHCP Operation;
- DNS Operation;
- ICMP Echo Operation;
- Jitter Operation;
- HTTP Operation;
- FTP Operation.

The following screenshots show those typical reports (APG 4.2 GUI shown).

Report root node

Report Packs / Cisco IP-SLA

mercredi 3 décembre 2008 16 h 14 GMT-05:00 >> jeudi 4 décembre 2008 16 h 14 GMT-05:00 | *Dernier Jour*

Cisco IOS IP SLAs measure performance by sending one or more packets to a destination IP device or a Cisco router. Cisco IOS IP SLAs use the timestamp information to calculate performance metrics such as jitter, latency, network and server response times, packet loss, and MOS voice quality scores (available when History and Last Operation table polling is enabled).

1. Inventory

⚡ Name	⚡
1. IP-SLA Probe List (By Device)	
2. IP-SLA Capability (By Device)	

2. IP-SLA Probe Performance View (By Device)

⚡ Device	⚡ IP Address	⚡ Probes
W4N-RTR2	10.128.0.2	12

3. IP-SLA Probe Performance View (By Probe Type)

⚡ Probe Type	⚡ Probes
Application Connection time (TCP Connect)	1
DHCP Address Request	1
DNS Lookup Time	1
Round Trip Delay (ICMP or UDP echo)	6
Round-trip delay, jitter, and packet loss	1
Round-trip time to get a Web page	1
Round-trip time to transfer a file (FTP)	1

4. Situations to watch

⚡ Name	⚡
1. Unsuccessful Application Connection time (TCP Connect)	
2. High latency Application Connection time (TCP Connect)	
3. Unsuccessful DHCP Address Request	
4. DNS performance	
5. DNS Availability	
6. Latency (ICMP or UDP echo)	
7. Reachability (ICMP or UDP echo)	
8. Jitter metrics, latency and packet loss	
9. Web pages accessibility	
10. FTP reachability	

Probe configuration report

1. IP-SLA Probe List (By Device) / W4N-RTR2

mercredi 3 décembre 2008 16 h 16 GMT-05:00 >> jeudi 4 décembre 2008 16 h 16 GMT-05:00 | *Dernier Jour*

This report shows the device's probes general configuration information. Further configuration information (if available) and probe completion metrics can be displayed by clicking on the probe itself.

Index	Owner	Tag	Type	Protocol	Source	Target	Freq.	Octets in use
110	eclipse	test678	tcpConnect	ipTcpConn	10.128.3.1	72.14.205.103	60	1 954
112	eclipse	test234	ftp	ftpAppl	10.128.3.1		240	1 954
111	eclipse	test123	dns	dnsAppl	0.0.0.0		240	2 130
117	eclipse	test678	dhcp	dhcpAppl	0.0.0.0	72.14.205.103	60	1 954
1	w4n	test	echo	iplcmpEcho	0.0.0.0	10.128.3.1	30	3 374
20	pmayer	20:test456	echo	iplcmpEcho	10.128.0.2	72.14.205.103	30	3 374
10	pmayer	10:test456	echo	iplcmpEcho	10.128.0.2	72.14.205.103	30	3 374
113	test345, eclipse	test345	http	httpAppl	10.128.3.1		240	1 814
21	pmayer	21:test456	echo	iplcmpEcho	10.128.0.2	72.14.205.103	30	3 374
116	eclipse	test567	jitter	jitterAppl	10.128.3.1	10.128.3.1	240	1 806
22	pmayer	22:test456	echo	iplcmpEcho	10.128.0.2	72.14.205.103	30	3 374
115	eclipse	test456	echo	iplcmpEcho	10.128.3.1	72.14.205.103	240	1 954

Device capabilities inventory

2. IP-SLA Capability (By Device) / W4N-RTR2

mercredi 3 décembre 2008 16 h 19 GMT-05:00 >> jeudi 4 décembre 2008 16 h 19 GMT-05:00 | **Dernier Jour**

This report displays the available protocols and probe types on the listed device.

Device	Ip	Location
W4N-RTR2	10.128.0.2	
Contact	Devdesc	
	Cisco Internetwork Operating System Software ..IOS (tm) C2600 Software (C2600-JK9O3S-M). Version 12.2(31). RELEASE SOFTWARE (fc2)..Technical Support: http://www.cisco.com/techsupport..Copyright (c) 1986-2005 by cisco Systems. Inc...Compiled Thu 11-Aug-0	

Available IP-SLA Probe Types		
Name	Supported (0: not supported, 1: supported)	
fileIO	0	✗
pathEcho	1	✓
dns	1	✓
http	1	✓
echo	1	✓
udpEcho	1	✓
tcpConnect	1	✓
script	0	✗
jitter	1	✓
dlsn	1	✓
dhcp	1	✓
ftp	1	✓

Available IP-SLA Protocols		
30 objets trouvés, affichage de 1 à 15. << < 1 2 > >> [Tout afficher]		
Name	Supported (0: not supported, 1: supported)	
isoClnsEchoAppl	0	✗
snaLU62EchoAppl	0	✗
vinesEcho	0	✗
netbiosEchoAppl	0	✗
apolloEcho	0	✗
apolloEchoAppl	0	✗
xnsEcho	0	✗
decNetEchoAppl	0	✗
notApplicable	0	✗
ipIcmpEcho	1	✓
ipxEchoAppl	0	✗
jitterAppl	1	✓
snaLU0EchoAppl	1	✓
dnsAppl	1	✓
ipUdpEchoAppl	1	✓
30 objets trouvés, affichage de 1 à 15. << < 1 2 > >> [Tout afficher]		

Probe performance view (by device)

2. IP-SLA Probe Performance View (By Device) / W4N-RTR2

mercredi 3 décembre 2008 16 h 20 GMT-05:00 >> jeudi 4 décembre 2008 16 h 20 GMT-05:00 | Dernier Jour

This report shows the device's probes general configuration information. Further configuration information (if available) and probe completion metrics can be displayed by clicking on the probe itself.
Thresholds are not set in this report as they differ from one probe type to another.

Index	Owner	Tag	Type	Protocol	Source	Target	Completion (ms)	Success (%)
117	eclipse	test678	dhcp	dhcpAppl	0.0.0.0	72.14.205.103		0,00
111	eclipse	test123	dns	dnsAppl	0.0.0.0		5	100,00
112	eclipse	test234	ftp	ftpAppl	10.128.3.1		1 558	
113	test345, eclipse	test345	http	httpAppl	10.128.3.1		69	100,00
1	w4n	test	echo	ipIcmpEcho	0.0.0.0	10.128.3.1	1	100,00
20	pmayer	20:test456	echo	ipIcmpEcho	10.128.0.2	72.14.205.103	49	100,00
10	pmayer	10:test456	echo	ipIcmpEcho	10.128.0.2	72.14.205.103	46	100,00
21	pmayer	21:test456	echo	ipIcmpEcho	10.128.0.2	72.14.205.103	49	100,00
22	pmayer	22:test456	echo	ipIcmpEcho	10.128.0.2	72.14.205.103	50	100,00
115	eclipse	test456	echo	ipIcmpEcho	10.128.3.1	72.14.205.103	47	100,00
116	eclipse	test567	jitter	jitterAppl	10.128.3.1	10.128.3.1	42	100,00
110	eclipse	test678	tcpConnect	ipTcpConn	10.128.3.1	72.14.205.103		

Typical probe performance graph

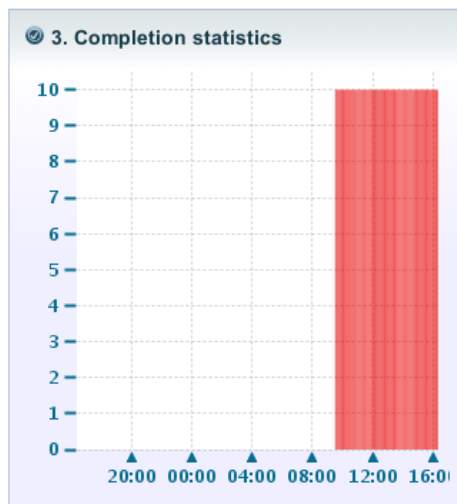
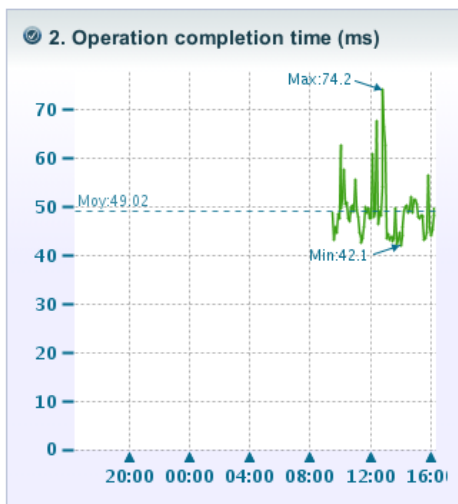
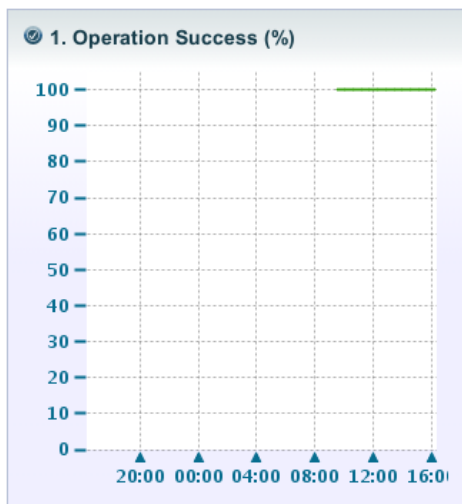
W4N-RTR2 / 20

mercredi 3 décembre 2008 16 h 21 GMT-05:00 >> jeudi 4 décembre 2008 16 h 21 GMT-05:00 | *Dernier Jour*

Owner
pmayer
Srcadr
10.128.0.2
Trgport
0

Tag
20:test456
Srcport
0

Protocol
iplcmpEcho
Trgadr
72.14.205.103

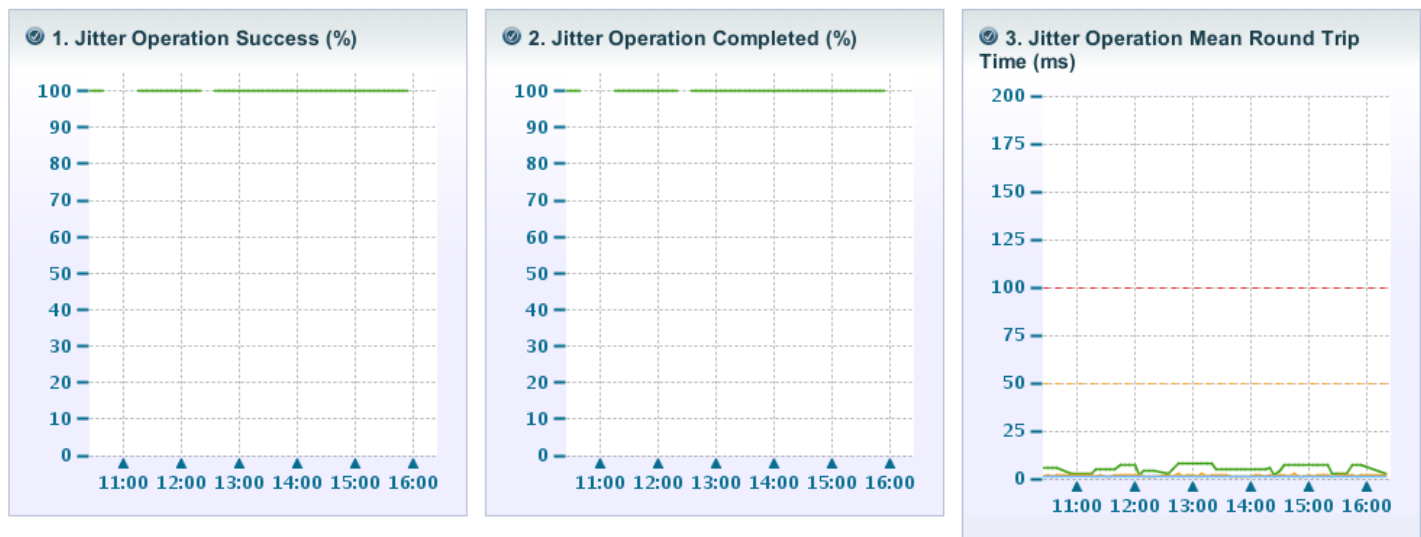


Jitter probe performance graph

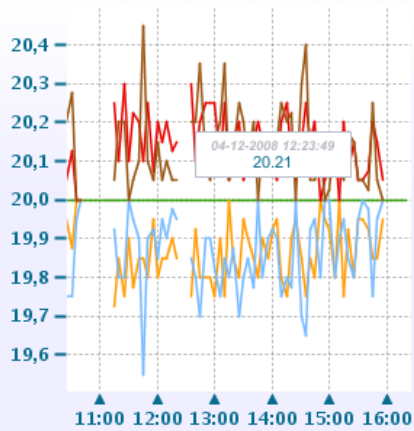
W4N-RTR2 / 116

jeudi 4 décembre 2008 10 h 25 GMT-05:00 >> jeudi 4 décembre 2008 16 h 25 GMT-05:00 | *Demier 6 Heures*

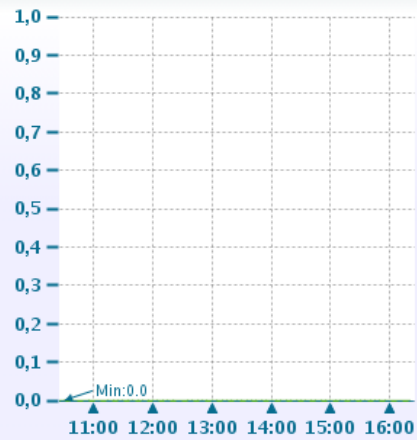
Owner	Tag	Protocol
eclipse	test567	jitterAppl
Srcadr	Srcport	Trgadr
10.128.3.1	0	10.128.3.1
Trgport		
17000		



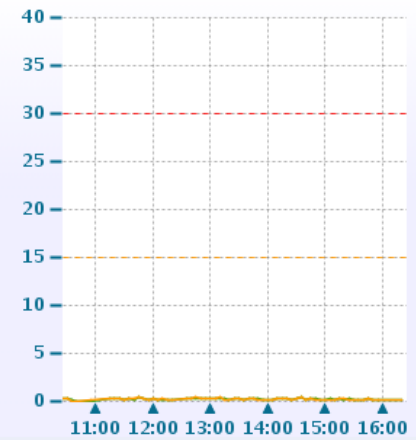
4. Jitter Relative to Packet Interval (ms)



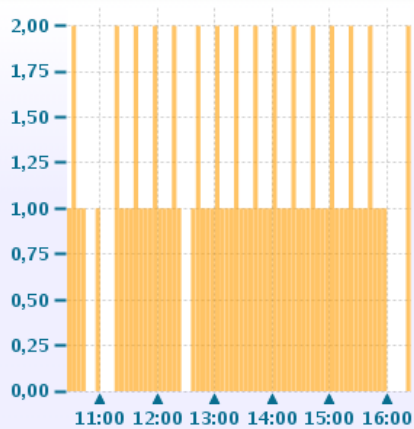
5. Jitter Packet Loss (%)



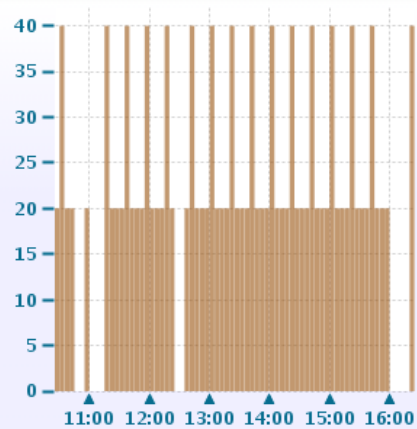
6. Maximum Jitter (Positive/Negative, ms)



7. Jitter Operations Detailed Statistics



8. Packet Metrics



Requirements

1. Watch4Net's APG Backend and Frontend must be installed. Versions higher than 4.2 are supported.
2. Cisco Routers are supported by this report pack. IOS version 11.2 and up are supported. IOS 12.0(5)T and higher is recommended.
3. Currently, officially supported probes are:
 1. IP/ICMP Echo
 2. SNA Echo
 3. TCP Connection
 4. UDP Echo
 5. Jitter/UDP Plus. VoIP UDP Jitter (MOS / ICPIF) also supported (last operation table polling only)
 6. HTTP
 7. FTP
 8. DHCP
 9. DNS

Probe support also depends upon the Cisco IOS version installed on the polled devices. Please note that certain metrics, such as MOS and ICPIF, may be obtained only from devices which support them (IOS 12.3(14)T or later provides these metrics).

IPSLA was introduced on IOS 12.3(14)T. It supercedes SAA (Service assurance agent). This report pack is compatible with both IPSLA and SAA, since both technologies are similar and use the same basic MIB.

SAA operation types were introduced gradually, starting from IOS 11.2:

dhcp: 12.0(5)T

dlsw: 12.0(5)T

dns: 12.0(5)T

echo (ipIcmpEcho, snaRUEcho, snaLUEchoAppl, snaLU2EchoAppl): 11.2

ftp: 12.1(1)T

http: 12.0(5)T

jitter: 12.0(5)T

tcpConnect: 12.0(3)T

udpEcho: 12.0(3)T

-
4. Supported probes shall be setup as explained in the last section of this document. Watch4Net also provides basic scripts and a GUI to manage and create the Cisco IP-SLA probes.

As a general guideline, leave the buckets-of-history-kept, distributions-of-statistics-kept, filter-for-history, hops-of-statistics-kept, hours-of-statistics-kept, lives-of-history-kept, paths-of-statistics-kept, samples-of-history-kept, statistics-distribution-interval and other parameters related to probe history/statistics to their **DEFAULT VALUE** when creating the probe on the Cisco device.

Installation

Normally, the Snmp Collector is deployed when installing APG 3.1 and higher. If that is not the case, please consult the Snmp Collector Installation and Administration Guide. One may determine if the Snmp Collector is already installed by examining the APG-Backend/conf/collecting.xml file and looking for:

```
<collector enabled="true" name="SnmpCollector" ..>
```

Snmp Collector setup

Starting with APG 4.1, the Snmp Collector is already set up and ready to use for IPSLA. No modification is required on the APG/APG-Backend/conf/collecting.xml file. The following is an excerpt for reference purposes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE config SYSTEM "collecting.dtd">
<config>
  <connectors>
    <connector name="Cache">
      <classname>com.watch4net.apg.v2.collector.plugins.CacheConnector</classname>
      <config-file>conf/cacheconnector.xml</config-file>
    </connector>
  </connectors>
  <filters>
    <filter enabled="true" name="CalculateSize" next="Cache">
      <classname>com.watch4net.apg.v2.collector.plugins.valueoffsetfilter.ValueOffsetFilter</classname>
      <config-file>conf/calculate-size.xml</config-file>
    </filter>
    <filter enabled="true" name="MapStoragePartType" next="CalculateSize">
      <classname>com.watch4net.apg.v2.collector.plugins.mappedpropertytagfilter.MappedPropertyTaggedFilter</cla
ssname>
      <config-file>conf/mapped-storage-parttype.xml</config-file>
    </filter>
    <filter enabled="true" name="HexToDecIPAdressConverter" next="MapStoragePartType">
      <classname>com.watch4net.apg.v2.collector.plugins.HexToDecIPAdressConverter</classname>
      <config-file>conf/hex-to-dec-ip-address-converter.xml</config-file>
    </filter>
    <filter enabled="true" name="IpSlaStatisticsTableFilter" next="HexToDecIPAdressConverter">
      <classname>com.watch4net.apg.v2.collector.plugins.ipslafilter.IpSlaStatisticsTableFilter</classname>
      <config-file>conf/ipsla-statistics-table-filter.xml</config-file>
    </filter>
    <filter enabled="true" name="SaaFilter2" next="IpSlaStatisticsTableFilter">
      <classname>com.watch4net.apg.v2.collector.plugins.SaaFilter</classname>
      <config-file>conf/saafilter2.xml</config-file>
    </filter>
  </filters>
</config>
```

```

    <filter enabled="true" name="SaaFilter1" next="SaaFilter2">
      <classname>com.watch4net.apg.v2.collector.plugins.filter.timestampsysuptime.TimestampSysuptimeMatching</c
lassname>
      <config-file>conf/ipsla-history-collection-filter.xml</config-file>
    </filter>
  </filters>
</collectors>
  <collector enabled="true" name="SnmpCollector" next="SaaFilter1">
    <classname>com.watch4net.apg.v2.collector.plugins.snmpCollector.SnmpCollectorSlave</classname>
    <config-file>conf/snmpcollector.xml</config-file>
  </collector>
  <collector enabled="false" name="SMDiscoveryCollector" next="OutageDetector">
    <classname>com.watch4net.apg.v2.collector.plugins.SmCollectorDiscovery</classname>
    <config-file>conf/sm-discovery.xml</config-file>
  </collector>
  <collector enabled="false" name="TextCollector" next="PropertyTaggingFilter">
    <classname>com.watch4net.apg.v2.collector.plugins.TextOutputCollector</classname>
    <config-file>conf/textoutputcollector.xml</config-file>
  </collector>
  <collector enabled="false" name="XMLCollector" next="OutageDetector">
    <classname>com.watch4net.apg.v2.collector.plugins.XMLCollector</classname>
    <config-file>conf/xmlcollector.xml</config-file>
  </collector>
  <collector enabled="false" name="IcmpCollector" next="OutageDetector">
    <classname>com.watch4net.apg.v2.collector.plugins.pingcollector.IcmpCollector</classname>
    <config-file>conf/icmp-collector.xml</config-file>
  </collector>
</collectors>
</config>

```

Data collection setup

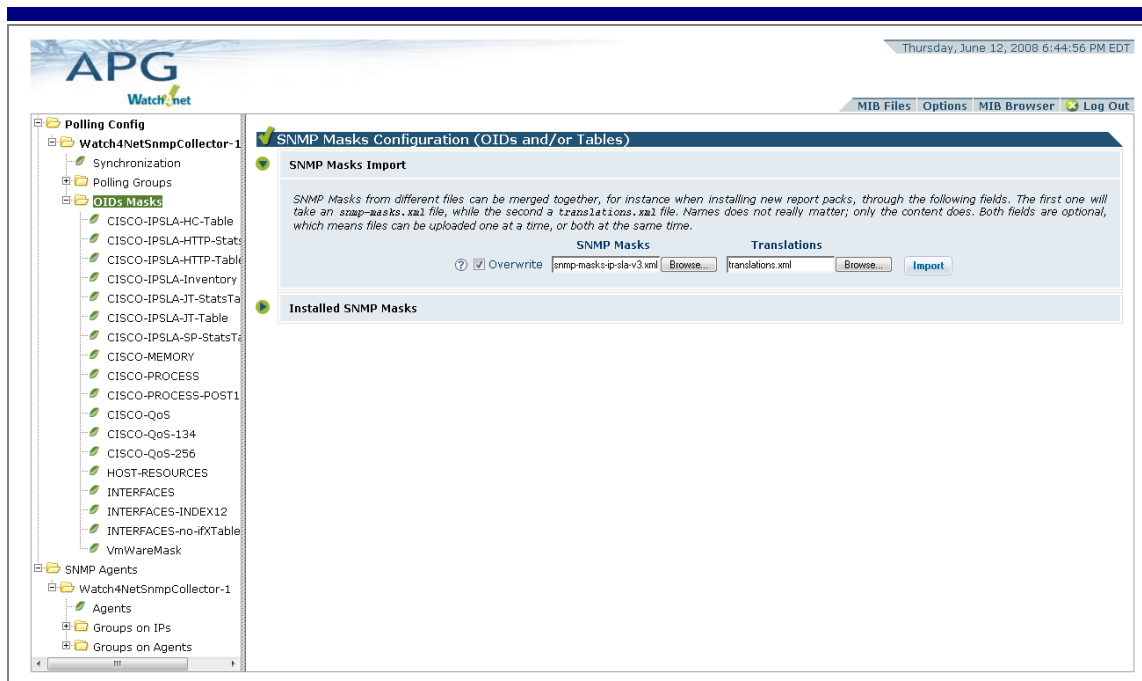
This should be done via the Snmp Poller configuration GUI. First, unzip the IPSLA configuration files that you have received from Watch4Net and keep the following files in an easy to find location:

- snmp-masks-ip-sla-v3.xml;
- translations.xml;
- slave-snmp-poller.xml.

Then upload these files to the Snmp Poller, using the Snmp Poller configuration GUI.

To do this:

- 1- Login to the mib browser (typically: <http://localhost:58080/mib-browser>)
- 2- Click the “Polling configuration” tab, then the “OIDs Masks” node:



Browse the snmp-masks-ip-sla-v3.xml (SNMP Masks) and translations.xml (Translations) and click the import button.

3- Click the “Polling Groups” node then the “Polling Groups Import” drop-down button. Browse the slave-snmppoller.xml file and import it.

4- Once you've imported the configuration files, populate the “Groups on Agents” named CISCO-IPSLA-STD with the snmp agents that you want to poll.

5- Upload the configuration to the running Snmp Poller and restart it via the Snmp Poller GUI. Data should start appearing in reports within the hour.

Note: To speed things up, wait 15 minutes after the collector was restarted, then:

1. telnet to the backendhost, on port 2001.
2. type: commitall
3. type: bye
4. wait 5 minutes and restart the APG Tomcat service.

Polling groups definitions

Polling Group Name	Polling Period	Agents Group	Snmp masks	Notes
PG_CISCO_IPSLA_INVENTORY	900 seconds. A 15 minute polling period allows quick probe discovery when they are set up.	IPSLA	CISCO-IPSLA-INVENTORY	This polling group is used to poll inventory data on the probes.
PG_CISCO_IPSLA_HISTORY	300 seconds.	IPSLA_HISTORY	CISCO-IPSLA-HISTORY	This polling group is used to poll the IPSLA History table (rttMonHistoryCollectionTable). This table contains data about the latest "n" operations for a probe. "n" being the number of statistics buckets configured for the probe. This group must be enabled manually to be used.
PG_CISCO_IPSLA	300 seconds	IPSLA	CISCO-IPSLA-STATSTABLE	Poll all probes, except Jitter, HTTP and IcmpPathEcho, using the statistics table.
PG_CISCO_IPSLA_JITTER	300 seconds	IPSLA	CISCO-IPSLA-JITTER-STATSTABLE	Polls the Jitter probes, using the statistics table.
PG_CISCO_IPSLA_HTTP	300 seconds	IPSLA	CISCO-IPSLA-HTTP-STATSTABLE	Polls the HTTP probes, using the statistics table.
PG_CISCO_IPSLA_LATEST_OPERATION	60 seconds. The polling period should be set to the shortest probe frequency in order to gather all data. Data point will be missing if polling occurs more slowly.	PG_CISCO_IPSLA_LATEST_OPERATION	CISCO-IPSLA-HTTP-LATEST, CISCO-IPSLA-JITTER-LATEST	Use this polling group to poll the latest operation tables for HTTP and Jitter probes. This group is OPTIONAL as it generates a lot of network traffic and cpu load on the device and collector.

NOTE about the POLLING PERIOD on the polling groups using the STATISTICS TABLES:

The polling period should be set to a value equal or higher than the slowest probe being queried. Otherwise, spurious values (with a zero value) may appear in the reports. This applies to the polling groups using the CISCO-IPSLA-XXX-STATSTABLE.

NOTE about the POLLING PERIOD on the polling groups using the LATEST-OPERATION tables:

The polling period should be set to a value smaller than the the probe with the smallest frequency. This shall be done to ensure that no data points are lost.

NOTE about the POLLING PERIOD on the polling groups using the HISTORY tables:

The polling group periods for those tables depend upon the probe configurations:

- The period may be set to 300 seconds when multiple history lives and buckets are used. For a typical application (a IcmpEcho probe, setup with a 60 seconds frequency, 15 buckets: 15 minutes retention time), a 300 seconds (10 minute) period could be used. However, it would also be possible to use 600 seconds (10 minutes) as it still falls within the probe's data retention time.
- The period must be set to a value smaller than the most frequently occurring probe if the probe buckets and lives are set to 1.

APG Web Portal setup

No setup is required for APG 4.1 as this report pack tree is included in the installation.

The report tree must be imported when using APG 4.2 as it is not included in the installation.

Guidelines to set up probes on Cisco devices

Probes may be set on the polled Cisco routers through the command line interface. However, certain guidelines apply to their creation in order to ensure polling result correctness.

As explained before in this document, there are two different ways to poll the IP-SLA probes on the Cisco devices. One can either choose to poll the statistics tables, located in the rttMonStats branch of the Cisco-RttMon-Mib mib or poll the last operation result tables, located in the rttMonHistory and rttMonLatestOper mib branches. Both ways offer pros and cons which are as follows:

	Statistics Tables	Latest Operation Tables (HTTP / Jitter)	History Operation Table (other probes)
Polling period	Long: 5 minutes or more is OK.	Short: Must be as short as the most frequently occurring probe on the polled devices, otherwise there will be missing data points.	Long: 5 minutes or more is OK if multiple history lives and buckets are setup for the probe. This increases memory usage on the polled device. Short: Must be as short as the most frequently occurring probe on the polled devices, otherwise there will be missing data points. This is the case when history buckets and lives are set to 1 to reduce memory usage on the polled device.
Data volume	Low, since the polling period is longer.	High, since the polling period is shorter.	High or Low, depending upon the case.
Collecting host CPU utilization	Low	High	High or Low, depending upon the case.
Polled device CPU utilization	Low, might have a slightly noticeable effect on the device	High, will have a visible effect on the device CPU utilization statistics.	High or Low, depending upon the case.

	CPU utilization statistics.		
Data granularity	Low: Averages are calculated on the polling period. Suitable for performance trending.	High. Suitable for troubleshooting specific problems, occurring at a precise time.	High. Suitable for troubleshooting specific problems, occurring at a precise time.

Guidelines to setup probes polled via their statistics tables

1. The owner should be set to a value. Any value is acceptable, as long as there is one. (i.e. John Smith, Sysadmin).
2. The tag should be set to a meaningful value. (IcmpEcho to www.google.com).
3. Leave the buckets-of-history-kept, distributions-of-statistics-kept, filter-for-history, hops-of-statistics-kept, hours-of-statistics-kept, lives-of-history-kept, paths-of-statistics-kept, samples-of-history-kept, statistics-distribution-interval and other parameters related to probe history/statistics to their **DEFAULT VALUE** when creating the probe on the Cisco device.
4. The probe frequency can be set to any number. However, keep in mind that this should be a reasonable value, such as 30, 60, 120, 240 or 300 seconds. Reports might seem a bit erratic if the probe frequency does not match the polling frequency: a “sawtooth” pattern may appear in the probe number of completed operations graph and packet metrics. This is normal but may be a bit alarming to a new user.
5. The probe's life should be set to “forever”, as they will be used for performance and trending purposes.

Guidelines to set up probes polled via their history operation table

1. These probes must have lives-of-history set to 1 or more (usually, 1 is enough).
2. These probes must have buckets-of-history-kept set to 1 or more (for a probe running every 30 seconds, on a device being polled every 5 minutes, this value should be greater than 10 to avoid losing any data).
3. These probes must have filter-for-history set to all (otherwise, no data will appear in the History table).

About probe creation and management

Since APG keeps historical data about every metric it receives, creating a new probe to replace a new one can be tricky as **probes are identified by their index number**. So, when a new probe is created in place of an old one, this new probe should be the same type as the one it replaces. To ensure this, probe management could be organized as follows:

Probe index range	Probe type
1 - 30	Jitter
30 - 60	HTTP
60 - 90	Other types, EXCEPT IpIcmpEcho, PathEcho, PathJitter
90 - 120	IpIcmpEcho
120 - 150	PathEcho (Not handed by this report pack).
150 - 180	PathJitter (Not handled by this report pack)

NOTE: Make sure the PathEcho and PathJitter (if used) probes are created at indexes higher than the last IpIcmpEcho probe. Doing otherwise will likely affect the polling of other probe types.

Troubleshooting

Symptom	Possible causes and solutions
No data is collected.	1. Make sure the snmp-agent is configured correctly (snmp version and community string). 2. Make sure the name attribute in snmp-polling-distribution.xml, <snmp-slave-poller> element, is the same as the one defined in slave-snmp-poller.xml file. 3. Make sure the polled agent supports CISCO SAA and that its probes are running.
Some probes are missing from the inventory reports in the Cisco IP-SLA: High Frequency Polling section.	Probes that are not setup to be polled via their latest operation table will not appear in this report. (their owner is not Watch4Net).
No data appears for Jitter probes; Inventory data is displayed correctly and is up to date.	The “ipsla monitor responder” or “rtr responder” may not be correctly set on the probe target device. This will cause the probe to fail. The rttMonJitterStatsError metric will increase in this case. No other data will be provided in the performance metrics, aside from error metrics. The probe configuration may be incorrect: check for discrepancies when setting the source interface, port, target address and port.
Information is not always up to date in the Probes Inventory.	This may be due to the fact that some data is too old to be displayed in the table. Increasing the “Time Threshold” value in Table -> Value -> Time Management might solve this problem.
Probes performance data is erratic.	The following symptoms may be due to a buggy IOS implementation. Known bugs include: rttMonJitterStatsCompletions: counter increases while the operation was not successful (rttMonJitterStatsNumOfRTT does not increase). This affects the Success% calculated metric.
Collector does not start after configuration files were edited.	Multiple causes are possible in this case. Check the logfiles, located in / APG-Backend/logs/collecting-*.log for details. The most common errors are made when manually editing the config

	files. Make sure they are formed properly, with end tags, and that elements are in the right place in the the structure.
--	--

Contact and Technical Support

Technical Support

WATCH4NET provides technical support by e-mail or phone during normal business hours (8:00 A.M-6:00 P.M. Eastern Time). In addition, WATCH4NET offers customers an access to a personalized web page to view, modify, or create help/trouble/support tickets. To access the service, point your browser to:

<http://www.watch4net.com/support>

E-Mail: support@watch4net.com

Phone: +1-866-840-9966

Contact us

You may also contact WATCH4NET at:

	CANADA MONTREAL HEADQUARTERS	CANADA TORONTO
ADDRESS	WATCH4NET 4388 Saint-Denis Street Office 309 Montreal, Quebec H2J 2L1 Canada	WATCH4NET 7030 Woodbine Avenue Suite 500 Markham, Ontario L3R 6G2 Canada
PHONE FAX	+1 514.842.6767 +1 514.842.3989	+1 905.843.4951 +1 905.846.8971

For sales inquiries, contact WATCH4NET Sales at:

sales@watch4net.com

WATCH4NET is on the World Wide Web at:

<http://www.watch4net.com>

Legal Notices

Warranty

Watch4Net makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Watch4Net shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material. A copy of the specific warranty terms applicable to the APG product can be obtained from Watch4Net Solutions.

Copyright Notices

© Copyright 2007-2009 Watch4Net Solutions. No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Watch4Net Solutions. The information contained in this material is subject to change without notice.

Trademark Notices

Watch4Net Solutions; and the Watch4Net logo are registered trademarks or trademarks of Watch4Net. All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.