StableNet® - WHITE PAPER

Managing End-to-End VoIP Networks

Document Ref: - SN_E2E_VoIP_WP_DP002_IV1

Author	David Poulton – COO Infosim (UK)
Document Reference	SN_E2E_VoIP_WP_DP002_IV1
Version Number	ISSUE 1
Issue Date	12th October 2013

Document Request – Contact: - sales@infosim.net

Contents

1 VoIP Management Overview

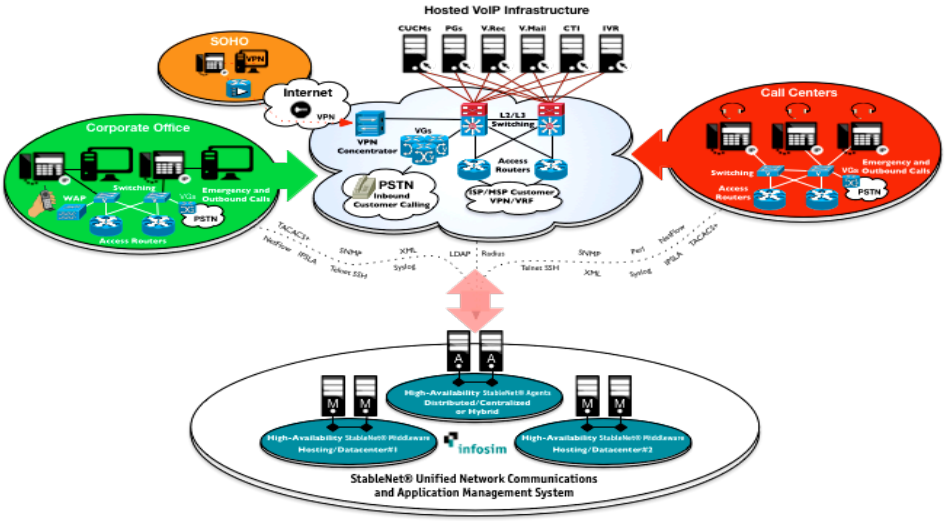
There are any number of VoIP management solutions available in today's market place. However, when you start to drill-down into the capabilities of these tools they tend to focus on the performance elements of your network infrastructure and associated VoIP metrics *(e.g. RTT, RTD\Latency, Packet Loss, Jitter, Moss, R-Factor etc.)* , assumptions are made on infrastructure and fault management being in place, so it is vitally important to assess the complete picture of your solution requirement before selecting the choice of tool to be deployed. VoIP monitoring lies central to this, as VoIP downtime and poor VoIP performance directly impacts such things as business performance, profitability and revenue. Achieving a consistent level of quality on VoIP calls requires multiple dependent components working properly, thus the importance of a monitoring system that correlates the infrastructure, performance, and fault management into an integrated End-to-End view is vital.

In order to manage a VoIP solution End-to-End you need to monitor the hosting environment, *(e.g. CUCMs, V.Rec, V.Mail, V.Gateways, SIP Trunks, etc.)* the WAN *(e.g. CE Access Routers, Core WAN if you're an ISP\MSP)*, and the end user locations. It is then vital that you on-board the identified components to best practice processes in order that you start to build up the End-to-End visibility of your VoIP managed service solution. Once the physical device component infrastructure has been on-boarded and tested *(e.g. SNMP trap, syslog collection, Netflow, etc.)*, for accuracy around the fault and event management, you can then build your performance measurements & reporting requirements based on Service Level Agreements *(SLAs)*, Key Point Indicators *(KPIs),* and threshold alarm management criteria for proactive management purposes.

Having End-to-End visibility of your VoIP solution is vital when troubleshooting issues and potential problem areas, as assuring a great customer experience can no longer be assessed simply by having green LEDs on a dashboard. StableNet® is a unified End-to-End Service Quality Management platform and therefore, takes a customer-centric approach to the service assurance monitoring infrastructure, performance, and fault management in a single solution. A unified management approach significantly cuts the time it takes to analyze complex issues in the managed environment. Best practice on-boarding reduces time to operate and assures rapid fault identification with root-cause-analysis (RCA), unique to the StableNet® architecture.

Infosim StableNet® is the only all-in-one unified End-to-End Service Quality Management tool capable of delivering and visualizing a complete End-to-End VoIP service solution monitoring system in a single product that has proven ROI *(Return-On-Investment)* in reducing capital *(CAPEX)* and operating *(OPEX)* expenditure, with conceivable savings in customer service credits thru reduced MTTR *(Mean-Time-To-Repair)*, and increased service availability.

Holistic VoIP End-to-End Management using StableNet®



2 Unified End-to-End VoIP Infrastructure Management

As mentioned in the previous section, many VoIP tools focus on performance metrics as being key to managing a great service experience but, its so much more than just performance that makes a service truly great. A complete End-to-End multi-functional management wrap that spans the entire service is what will provide your customers with a great proactive service experience. Remember… nobody is going to tell you that they are experiencing a great service! you only hear from customers when the service is poor.

There are many different vendor type technologies that have been introduced into the IP voice environment for example; if we look at the requirement for a VoIP Contact Center solution, or IPCC, there would be technology requirements for work force management, voice recording, voice mail systems, interactive voice response systems *(IVR)* etc. These technologies bring added complexities with them, proprietary management systems to manage the device or appliance that increase costs, operational workload, and more importantly introduces additional element management systems into an environment whereby support teams are already operating multi-platform technologies.

This of course ultimately becomes very costly to maintain and lacks holistic End-to-End visibility as you end up managing a solution whereby you are forever jumping between different management systems to isolate issues and problems, that in turn, increase your Mean-Time-To-Repair *(MTTR)* seriously affects contractual Service Level Agreements *(SLAs)*, tarnishes your customer experience that ultimately leads to loss of revenue and business opportunities.

The Infosim StableNet® unified management system delivers comprehensive End-to-End visibility and management across the entire customers VoIP domain. StableNet® is vendor agnostic and therefore supports multi-vendor converged technologies, including VoIP Unified Communications (UC) from Cisco, Avaya and Siemens with ongoing development for additional vendor products.

The StableNet® solution is a flexible service provisioning, and service assurance multifunctional platform that provides customers with a much broader range of capabilities that include:

- **Asset Management**: Inventory component management.
- **Configuration & Policy Management**: Component configuration backup\restoration, policy governance.
- **Fault & Event Management**: Correlated alarm management with Root-Cause-Analysis (RCA).
- **Performance & Capacity Management**: VoIP Performance, SLA, QOS, MOS, CDR management & reporting.
- **Visualization**: Service Topological and Weather map views.
- **Lifecycle Management**: Component End-of-Life *(EOL)*, End-of-Sale *(EOS)*, End-of-Service-Support *(EOSS)*.
- **Vulnerability Management**: Vendor vulnerability announcement management.

The Infosim StableNet® unified management solution provides a complete all-embracing multi-functional management wrap around your entire infrastructure enabling consistent End-to-End management, resulting in faster resolution *(MTTR)*, smarter operational management thru lower operating costs, seamless support, flexibility in scaling and provisioning a changing environment to meet new business products and developments, providing a great customer experience and service differentiation.

2.1 The VoIP Server\Appliance Hosting Environment

As mentioned in the previous section the VoIP IP Telephony *(IPT)*, and IP Contact Center *(IPCC)* hosting environment can have a variety of multi-vendor applications residing on server, or appliance server based hardware with varying operating systems *(e.g. Windows, Linux, Solaris)*. These devices, coupled with the LAN, WAN and security interconnectivity are on-boarded onto the management platform using best practice processes.

2.1.1 Server\Appliance Component Management

The VoIP hosting components will be a mixture of hardware server based technology that will typically be using a windows, or Linux, based operating systems that maybe customized in a particular way, or locked down to an appliance that will have the specific application(s) installed. Typically the VoIP hosting environment will be geographically resilient in order to maintain a high level of service availability.

The component types include:

- Call Manager Server Clusters *(e.g. Cisco UCM with Publisher & Subscriber CUCM Clusters, AVAYA CM R3, R5)*
- Voice Mail Servers *(e.g. Cisco Unity Voice Mail, AVAYA Audix R2, LX)*
- Peripheral Gateways *(e.g. PGs used for interfacing with other vendor systems e.g. Avaya)*
- CTI Servers
- Voice Recording Servers with SANs – *(e.g. Verint, Phobos)*
- Music-on-Hold (MOH)
- Work-Force-Management (WFM) – *(e.g. Aspect, Impact 360, AVAYA CMS)*
- Interactive-Voice-Response (IVR) – *(e.g. Genesys)*
- Wall Board Servers – *(e.g. Inova Wallboards)*
- IP Switchboards – *(e.g. Exony)*
- Voice & Media Gateways – *(e.g. Cisco VG248, Q.931, AVAYA G430-8300C, G350-8300C)*
- Other Server or Appliance Based Components

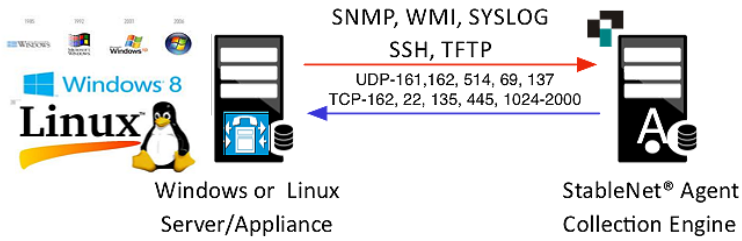
When on-boarding the server or appliance based components there will be a need to configure the network attributes that will include:

- SNMP *(Simple Network Management Protocol Version 2 or 3)*
  - SNMP Community String
  - SNMP Trap Types
  - SNMP Trap Destination addresses

- WMI *(Windows Management Instrumentation)*
  - Used on Windows O\S machines for monitoring key services\processes

The SNMP and WMI trap and event status data is then directed to the agent or collector as shown in the diagram below:

Server\Appliance to StableNet® Agent Management Data Flow



Once a server or appliance has been on-boarded a template for the monitoring criteria can be configured to your requirements. This is a one-off configuration process that can then be automatically repeated for the on-boarding of additional device components.

When a device has been on-boarded it is important that you verify you are receiving the trap data so as to ensure every attribute of the device is being monitored. Once you're receiving the trap data you should then look to configure agreed threshold alarm management metrics in order that the specific monitor can be proactively managed in a way whereby it generates an alarm when a threshold is breached, and automatically notifies support and service teams accordingly.

Examples of the types of standard server traps include:

- Availability
  - Server Network Availability Monitoring
  - Reachability Status
  - Response\Delay or IP Latency Status

- Environmental Monitoring
  - Operating Temperature
  - Power Usage\Consumption
  - Cooling Operation *(e.g. FAN & Temp operation)*

- Processors
  - CPU Utilization\Performance
  - CPU Status

- Memory
  - Available Memory
  - Total\Used\Free memory
  - Total\Used\Free swap space
  - Buffers & Cache

- Storage
  - Used\Free Disk Space
  - Used\Free Partition Space
  - Spin Speed
  - Buffered Disk read
  - Capacity

- Interfaces
  - Admin Status *(e.g. Up\Down)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound)*
  - VIP Support
  - Speed *(e.g. 10\100\1000\10000)*
  - Duplex *(e.g. Half\Full\Auto)*

In addition to the standard hardware and resource trap monitoring it is important to also monitor key and specific services which, are configured by enabling the specific trap types you require, and more specific to the Windows server o\s environment, ensuring that your WMI is configured to send the specific status information around key services that need monitoring.

Examples of Specific Key Service trap monitors include:

- WEB Services *(e.g. Apache Web Service Monitor)*

- HTTP Connect Time

- HTTPS Connect Time

- CUCM Key Services & Traps
  - CUCM CTI Manager Connect Time
  - CUCM Heartbeat Status
  - CUCM Registered\Unregistered CTI Devices
  - CUCM Registered\Unregistered Media Devices
  - CUCM Registered\Unregistered Phones
  - CUCM Registered\Unregistered Voice Mail Devices
  - CUCM Gateway States *(Active\Failed)*
  - CUCM Exhausted Media Resource Lists
  - CUCM QRT *(Quality Reporting Tool)*
  - CUCM Calls Attempted
  - CUCM Call Manager Heart-Beat
  - CUCM Calls Active

- CUCM Calls Completed
- CUCM Calls In Progress
- CUCM Initialization State
- CUCM Registered Hardware Phones
- CUCM Registered Phones *(SNMP Data source)*

- Syslog Status

It is essential to ensure that key service traps are enabled, are being monitored, and proactively managed via functional threshold alarm management.

When monitoring server or appliance device types it is always very important to understand the complete interconnectivity picture and touch-points of each device, for example: if a front-end web server with a back-end database suddenly lost connectivity the systems health may look OK to the support administrator however, the customer, or end user, would experience loss of service therefore, it is important to ensure your VoIP infrastructure interconnectivity is complete, and that all the required monitoring is wrapped around each component and its interconnected touch-point neighbor(s).

2.1.2 Key Features – VoIP hosting

This section highlights the key features of VoIP Hosting management using StableNet®: -

Feature ID	Feature Type	Feature Description	Feature Supported
#1	Server environmental monitoring.	Monitoring the server operating temperature, cooling and power consumption and applying threshold alarm management thru RAG (Red, Amber, Green) status & alarm notification management.	✓
#2	Server processor monitoring.	Monitoring the server processors utilization and reporting on performance, applying threshold alarm management thru RAG (Red, Amber, Green) status & alarm notification management.	✓
#3	Server memory monitoring.	Monitoring the server memory utilization and reporting on performance, applying threshold alarm management thru RAG (Red, Amber, Green) status & alarm notification management.	✓
#4	Server storage monitoring.	Monitoring the server storage, utilization, free space, spin speed etc. and reporting on performance, applying threshold alarm management thru RAG (Red, Amber, Green) status & alarm notification management.	✓
#5	Server network interface(s) monitoring.	Monitoring the server LAN network interfaces for utilization, errors, Duplex mismatches reporting on performance, applying threshold alarm management thru RAG (Red, Amber, Green) status & alarm notification management.	✓
#6	Key Application service monitoring.	Identification of key application services that are running on the server being monitored *(e.g. Apache Web Service)*, and monitor the running\stopped status of the key services and report status.	✓
#7	WMI (Windows) Support.	For severs running windows operating environments WMI support needs to be enabled for key service monitoring. A WMI StableNet® agent will monitor and report on the specific service status.	✓
#8	Asset inventory discovery.	When On-boarding of the server infrastructure commences it is important that every detail available from an asset viewpoint is collected as part of the asset discovery. StableNet® has full asset discovery functionality to collect this information and produce the appropriate reporting.	✓

#9	Server availability monitoring.	ICMP response monitoring for assurance that the server is still operational and responding to 'hello' requests.	✓
#10	Server network response and URL reachability & availability monitoring.	Measuring the response delay time of the server to ensure minimum delay thresholds are being achieved. URL reachability response & availability monitoring For WEB, and WEB based applications.	✓

2.1.3 Best Practice#1 – Server\Appliance Discovery Management

Understanding the current state and health of the server infrastructure is a fundamental requirement in any VoIP hosting infrastructure management environment. What you can't see you can't manage, or even understand, so it is paramount for VoIP infrastructure stability to have a tool that can constantly discover the state and health of the components in operation, and the full picture in terms of interconnectivity. Simply discovering the VoIP hosting environment once is not enough as the infrastructure is an ever change and evolving environment that needs the best practice processes and tools in place to auto-manage the change and evolution effectively and efficiently.

2.1.4 Best Practice#2 – Deployment Automation

Corporations today place a lot of emphasis on automation therefore, it is very important that when choosing a tool to operate your VoIP infrastructure environment, the tool can integrate seamlessly with you CRM system in order that auto-provisioning of new customer infrastructures, and the expansion of existing infrastructures, can be performed in a repeatable automated way. Having a consistent view of the infrastructure inventory and services will allow repeatable and consistent deployment of hardware and configuration in order to automate service fulfillment and deployment.

2.1.5 Best Practice#3 – Server\Appliance Patch Management

Tracking OS\Application feature types and versions in use across your entire VoIP infrastructure is a very important attribute for any VoIP monitoring tool capability. It is important to understand the feature sets and versions that are in use for a number of reasons: (1) Infrastructure best practice management design rules will stipulate approved OS\Application feature sets and versions authorized for use on the VoIP infrastructure. Scanning and correlating of the in-use OS\Application feature sets and versions will ensure design rule compliance. (2) Having full visibility of the OS\Application feature sets and versions in use will assist in the Vulnerability & lifecycle scanning process to highlight potential security risks and end-of-life, sale, and support of the feature sets and versions in use.

2.1.6 Best Practice#4 – VoIP Application Component Template Management

Prior to on-boarding a device\component it is imperative that you fully understand the devices management capabilities so as to then write\configure a template for the management of that device. Once written this template can then be used to on-board other\future devices of this type. StableNet® fully supports device template features and is an integral part of the StableNet® automated service provisioning functionality. Tools that support template on-boarding functionality ensure monitoring consistency throughout your VoIP infrastructure.

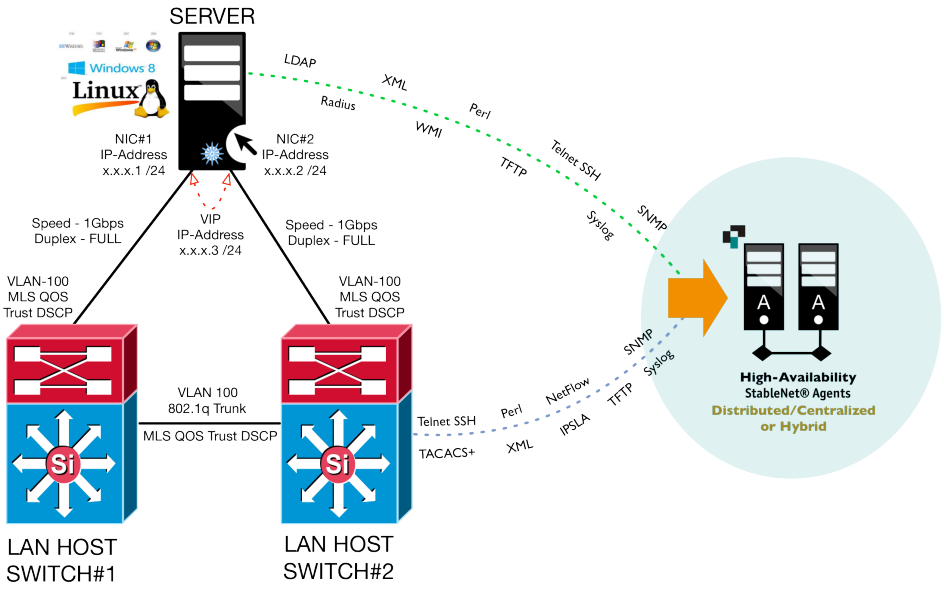
2.2 VoIP Hosting LAN Infrastructure Management

Once your entire VoIP server hosting environment has been on-boarded you can then start to map the interconnectivity from the server infrastructure to the LAN switching network *(e.g. Server → LAN Switching)*. This activity then starts the build out of the holistic End-to-End service visualization.

LAN switching is part of the backbone of your VoIP hosting infrastructure so any problems within this area will seriously affect your customers. Implementation of a management system that has a complete proactive monitoring solution will reduce the risk of potentially damaging service outages.

LAN component technology used to host the VoIP server\appliance infrastructure will typically be of a high specification with high-speed backplane and multi-gigabit network connectivity. On-boarding the LAN switching devices and port-mapping the server to switch-port connectivity will build the server to LAN switching layer2\3 topology relationships. Typically dual server network interface cards *(NICs)* are installed into the server\appliance devices for server to multi-switch connectivity that provides additional resiliency. Virtual IP addressing may also be employed for load-balancing and layer 3 routing purposes to assist in seamless failover scenarios.

Server → LAN Switching Connectivity with Agent Collector Flows



2.2.1 VoIP LAN Device Management

SNMP templates for on-boarding the LAN switching components will need to be setup in a way whereby all the identified SNMP trap types, Netflow, syslog, authentication, IPSLA, etc. have been enabled\configured, and the network management agents have connectivity to the LAN infrastructure for auto-discovery commencement.

Discovery of the LAN switching infrastructure will need to capture all of the asset inventory and configuration information of the switches, vendor, device type, card types, firmware, o\s version\feature sets, startup & running configuration etc. *(visit www.infosim.net\nccm for more details and to request the NCCM & VLM White Paper).*

Examples of the types of LAN Switching traps include:

- LAN Switch Availability
  - Switch Network Availability Monitoring
  - Reachability Status
  - Response\Delay or IP Latency Status

- LAN Switch Environmental Monitoring
  - Operating Temperature
  - Power Usage\Consumption
  - Cooling Operation *(e.g. FAN & Temp operation)*

- LAN Switch Processors
  - CPU Utilization\Performance
  - CPU Status

- LAN Switch Memory
  - Available Memory
  - Total\Used\Free memory
  - Total\Used\Free swap space
  - Buffers & Cache

- LAN Switch Storage\Flash
  - Used\Free Space
  - Capacity

- LAN Switch Port Interfaces
  - Status *(e.g. Up\Down)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound errors, CRCs, Drops, etc.)*
  - Speed *(e.g. 10\100\1000\10000)*
  - Duplex *(e.g. Half\Full\Auto)*

- LAN Switch VLAN Interfaces
  - Layer 2\3 VLAN IDs
  - Administrative Status *(e.g. Up\Down\Shutdown)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound errors, CRCs, Drops, etc.)*

The above is by no means an exhaustive list as vendors have many different trap types but it is essential that you identify the traps needed for assurance that every eventuality of failure and loss of service has been configured and monitored.

2.2.2 VoIP Hosting Management of SPAN & RSPAN Sessions

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer, or in a VoIP Call Center environment, voice recording device. SPAN copies *(or mirrors)* traffic received or sent *(or both)* on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

It is very important for corporations that voice recording is enabled and operating to consistently high levels in order to meet public regulatory guidelines and rules, for example FSA *(Financial Services Authority)*. Therefore all SPAN and RSPAN sessions should be identified and have the configuration elements backed up as part of the LAN device management wrap. The SPAN & RSPAN configurations should also be included within your config policies and governed in a way whereby the management system alarms you when a change to the configuration occurs. In addition to this you should also include the appropriate 'show SPAN\RSPAN monitor' command as part of the routine configuration backup job so as to police and report any inconsistencies on the status.

2.2.3 LAN QOS Monitoring

LAN Quality-of-Service will be configured with markings, trusts and policed as close to the traffic-sources as possible. Identification of the configuration of the DSCP COS markings and trusts within the layer 2 *(data-link-layer)* and layer 3 *(network layer)* switching LAN architecture will need to be known so as to ensure appropriate management and reporting. Best practices for policing of LAN quality of service configuration is through use of configuration policy & governance functionality. *(QOS performance monitoring and reporting is explained in further detail in section 2.5 – WAN QOS Management & Policing, section 2.5.3 – Netflow QOS, and section 3.6 – IP-SLA).*

2.2.4 Key Features – VoIP Hosting LAN Infrastructure

This section highlights the key features for VoIP Hosting LAN Infrastructure management using StableNet®: -

Feature ID	Feature Type	Feature Description	Feature Supported
#1	LAN asset management.	A comprehensive physical hardware discovery that includes model types, card types, card types with daughter cards e.g. Cat6500 Supervisor card with daughter MSFC card, chassis types etc.	✓
#2	LAN switching configuration management.	Configuration backup of LAN infrastructure layer 2 and 3 switching devices, with auto-backup scheduler, and auto-backup with config difference reporting on change.	✓
#3	Server → LAN switching topological\service mapping.	Graphical topology views of all discovered devices are a functional feature supporting both layer 2 and layer 3.	✓
#4	Availability monitoring.	Monitoring of all LAN switching devices for system, environmental and operational availability.	✓
#5	QOS monitoring.	Quality of Service monitoring via Netflow and configuration policy management to ensure QOS markings are being policed and reported.	✓
#6	Regulatory compliance management.	StableNet® can simplify the process for PCI, ISO27001, FCAPS, ITIL, SOX, HIPPA, or other business or regulatory standards.	✓
#7	SPAN\RSPAN monitoring.	SPAN\RSPAN configuration compliance policy management for SPAN\RSPAN session assurance.	✓
#8	IOS patch management.	IOS bulk or patch upgrade rollout is fully supported and can be configured to meet your specified process.	✓
#9	Lifecycle management.	Scanning of LAN vendor hardware infrastructure inventory for EOL\EOS\EOSS matches.	✓
#10	Vulnerability management.	Scanning of LAN vendor IOS Vulnerability announcements ensure that security and operational performance is being optimized.	✓

2.2.5 Best Practice#5 – Effective Network LAN Management

Effective LAN management is an integral part of the service delivery mechanism in any VoIP, or critical application, within a corporations infrastructure. The LAN network is the source-entry point from an Application Server and the end-delivery, or hand-off point to the user device\component. Therefore, it is not only necessary to ensure effective management of the LAN components, it is critical to know exactly how the LAN is performing and operating so as to assure and maintain consistent high levels of service availability. StableNet® provides you with the LAN performance, configuration and fault management functionality you need and, through the use of the customized dash-boarding and reporting, starts the build-out of the 'Single-Picture-Service-View' your operational and service teams require.

2.2.6 Best Practice#6 – Policy Assurance Operation

Governments and industry regulators require organizations to conform to standard best practices. In order to become compliant with these regulations such as PCI, ISO27001, FCAPS, ITIL, SOX, HIPPA, and others, device configuration should conform to these standards. These standards can range from a number of different requirements such as ensuring the presence, or absence, of certain strings, commands, or values. StableNet® assists greatly with this regulatory requirement automatically checking for compliance to the rules defined. Reports on policy compliance and violations are available out-of-the-box.

2.2.7 Best Practice#7 – VoIP Hosting LAN QOS Enablement

The LAN infrastructure that supports a VoIP hosting environment must have QOS trusts configured and tested to ensure marked VoIP packets are expedited through the LAN to the WAN handoff points. With a maximum acceptable VoIP round-trip time of 300ms and typical in-country round-trip times of 30-50ms it is imperative that the VoIP packets traversing the LAN infrastructure are accelerated using the vendor best practice QOS configuration trusts and policies. IT support organizations need to employ configuration policy and governance management to police the LAN QOS configuration policies and trusts that have been designed and tested so as to ensure no change or deviation of the performance is being compromised by rogue, or unauthorized changes. StableNet® NCCM and VLM fully supports this configuration requirement best practice. *(visit www.infosim.net\nccm for more details and to request the NCCM & VLM White Paper).*

2.2.8 Best Practice#8 – High Availability Monitoring

Traditionally legacy PBX voice networks were by design inherently reliable achieving high 99.99% - 99.999% service availability. In today's modern converged VoIP and Data network infrastructures achieving high levels of service is more difficult because of the additional complexities of convergence, a greater range of applications, and way more components to eliminate single point of failures are installed in order to achieve higher 99.999% service levels. However, achieving higher service levels requires much more than just a resilient\redundant network infrastructure. IT organizations need to significantly improve the range of tooling at their disposal, integrate the multiple functional tools to achieve a 'Single-Picture-Service-View' that includes functionalities such as performance, fault, configuration and service management. StableNet® is a unified multi-functional management system, it provides the complete management wrap enabling accurate proactive service assurance management.

2.3 Voice Gateway Management

Voice gateways can be hugely complex as there are a number of requirements that VoIP networks need in order to communicate with traditional PBX, PSTN, Internet *(e.g. Skype & Video)*, and Mobile networks. Voice gateways also need to support certain voice signaling and codec types in order to be effective within a VoIP infrastructure. So signaling types like SS7 *(Signaling System No. 7)*, H323, and protocols like SIP *(Session Initiation Protocol)* are common place within VoIP network infrastructures as are G.711, G.729 voice codec types.

Voice gateways are an integral part of any VoIP infrastructure solution as they connect the voice IP network to the Public Switch Telephony Network or PSTN. Voice gateways in general will be installed in most locations and will be used to provide interconnectivity for PSTN, corporation legacy PBX, Fax machines, emergency 911 outbound services, SIP Internet connectivity, legacy voice mail system etc. It is therefore fundamental, in terms of managing the End-to-End VoIP solution, that you identify and on-board all of the voice gateways located within the hosting and remote office locations.

Most voice gateways will support standard SNMP trap types that will include:

- VG Availability
  - Switch Network Availability Monitoring
  - Reachability Status
  - Response\Delay or IP Latency Status

- VG Environmental Monitoring
  - Operating Temperature
  - Power Usage\Consumption
  - Cooling Operation *(e.g. FAN & Temp operation)*

- VG Processors
  - CPU Utilization\Performance
  - CPU Status

- VG Memory
  - Available Memory
  - Total\Used\Free memory
  - Total\Used\Free swap space
  - Buffers & Cache

- VG Interfaces
  - Status *(e.g. Up\Down)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound errors, CRCs, Drops, etc.)*
  - Speed *(e.g. 10\100\1000\10000)*
  - Duplex *(e.g. Half\Full\Auto)*

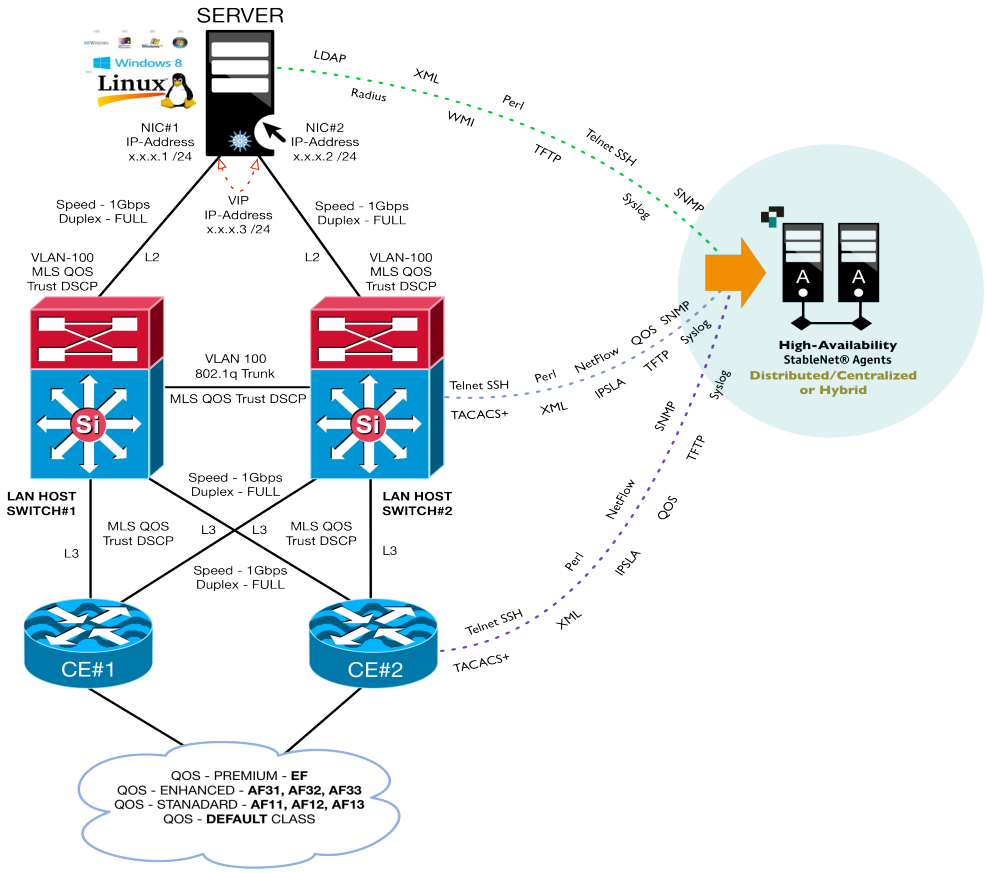
The above is by no means an exhaustive list as vendors have many different trap types but it is essential that you identify the traps needed for assurance that every eventuality of failure and loss of service has been configured and monitored. Most voice gateway vendors will also have specific SNMP MIBs available to perform more granular monitoring e.g. No of Channels available\used channels\channel utilization\ % of in-service channels current active, gateway status etc.

2.4 VoIP WAN Management

The Wide Area Network *(WAN)* is a key component in the VoIP delivery path as it's the WAN that ultimately delivers the call flow data from the VoIP Hosting environment to the remote locations. Because VoIP traffic is real-time it needs to be prioritized thru the WAN. Prioritization of VoIP packets is controlled via the queuing and Quality Of Service *(QOS)* configuration employed across the WAN. Typically class-based\low-latency queuing with specific QOS markings for VoIP *(e.g. EF, AF31, AF32 etc.)* will be configured for enhanced real-time critical services such as VoIP & Video. It is therefore extremely important that firstly, QOS\queuing and Marking Trusts are indeed employed and configured to a corporations best practice design rules and secondly, that the performance and management of the router components from the A-end thru to the Z-end of the WAN path are being monitored and reported in a consistent coherent way.

Typically ISP\MSP\Telco MPLS\MetroEthernet multi-customer core networks will either have trust QOS policies in place, or will police the QOS based upon the customer requirements. For managed service providers and Enterprise customers who manage their own VoIP solutions, but use a telecoms provider for the WAN element, it is imperative that you look to on-board the edge router, or CE router, devices. *(Most Telecoms providers will provide SNMP read-only, NetFlow, and syslog data feeds on request)*.

Server → LAN Switching → WAN Routing Connectivity with Agent Collector Flows



2.4.1 VoIP WAN Device Management

On-boarding of the WAN routers will enable the hosted LAN to WAN mapping interconnectivity from the VoIP hosting LAN switching network. This activity then continues the build out of the holistic End-to-End service visualization *(e.g. Server → LAN Switching → WAN Routing)*. As you continue the on-boarding and build-out of the infrastructure the holistic service picture starts to take shape.

When on-boarding the WAN devices you should employ a complete multi-functional management wrap around each device as it is important to capture, not just trap & syslog information, but also to engage technologies such as

Netflow, for real-time QOS statistics, and configuration capture for specific policy and governance policing. A full multi-functional management wrap with proactive threshold event and alarming will provide you with a complete service assurance management capability.

SNMP templates for on-boarding the WAN Router components will need to be setup in a way whereby all the identified SNMP trap types, Netflow, syslog, authentication, IPSLA, etc. have been enabled\configured, and the network management agents have connectivity to the WAN infrastructure for auto-discovery commencement.

Discovery of the WAN Router infrastructure will need to capture all of the asset inventory and configuration information of the switches, vendor, device type, card types, firmware, o\s version\feature sets, startup & running configuration etc. *(visit www.infosim.net for more details on the configuration management functionality modules available).*

Examples of the types of WAN Router traps include:

- WAN Router Availability
  - Switch Network Availability Monitoring
  - Reachability Status
  - Response\Delay or IP Latency Status

- WAN Router Environmental Monitoring
  - Operating Temperature
  - Power Usage\Consumption
  - Cooling Operation *(e.g. FAN & Temp operation)*

- WAN Router Processors
  - CPU Utilization\Performance
  - CPU Status

- WAN Router Memory
  - Available Memory
  - Total\Used\Free memory
  - Total\Used\Free swap space
  - Buffers & Cache

- WAN Router Storage\Flash
  - Used\Free Space
  - Capacity

- WAN Router Interfaces
  - Administrative Status *(e.g. Up\Down\Shutdown)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound errors, CRCs, Drops, etc.)*
  - Flapping Interface Avoidance Detection
  - Bandwidth Available

- WAN\Layer 3 VLAN Interfaces *(Typically used in MetroEthernet)*
  - Layer 3 VLAN IDs
  - Administrative Status *(e.g. Up\Down)*
  - Utilization *(e.g. inbound\outbound %util kbps, mbps etc.)*
  - Errors *(inbound & outbound errors, CRCs, Drops, etc.)*
  - Flapping Interface Avoidance Detection
  - Bandwidth Available

- QOS Queue Monitoring
  - Class-Based QOS or CBQOS
  - Throughput per class map reporting

The above is by no means an exhaustive list as vendors have many different trap types but it is essential that you identify the traps needed for assurance that every eventuality of failure and loss of service has been configured and monitored.

StableNet® is a unified multi-functional management system, it provides the complete management wrap enabling accurate proactive service assurance management.

2.5 WAN QOS Management & Policing

Quality of Service *(QOS)* is an essential requirement of any WAN network that's intention is to transport IP Telephony *(VoIP)* services. IP Telephony data is real-time, and therefore, needs minimum delay and latency thru the network so as to ensure rapid VoIP packet delivery, and provide coherent consistent audio quality.

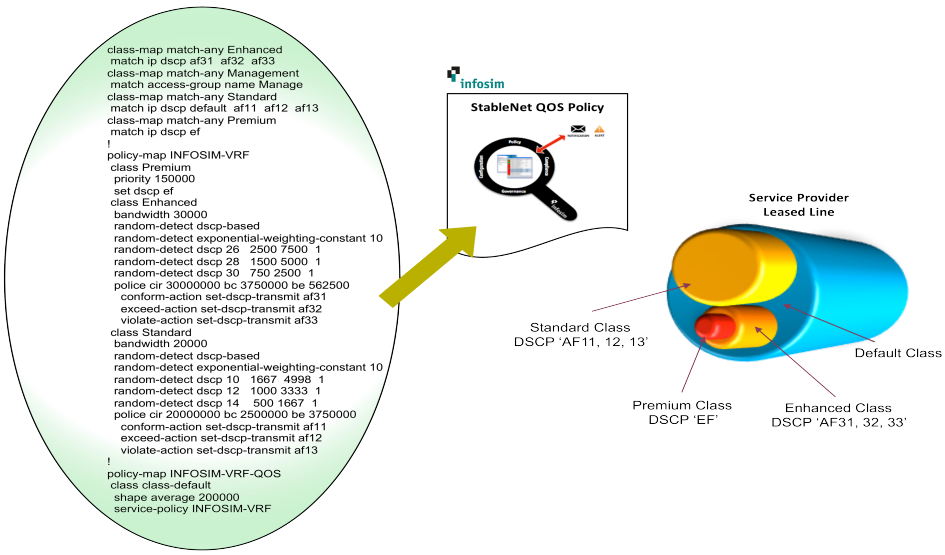
QoS can be used in any network environment in which bandwidth, latency, jitter, and data loss must be controlled, for example IP Telephony *(VoIP)*, or mission-critical applications for latency-sensitive software, or other multimedia applications. QoS also can be used to improve the throughput of traffic that crosses slower links, such as a DSL connectivity. All the network elements along the path that prioritized traffic takes must support and trust QoS markings. Such network elements include the sending and receiving hosts, Layer 2 *(Data Link layer)* network devices *(bridges and switches)*, and Layer 3 *(Network layer)* network devices *(routers)*, including routers used for wide area network *(WAN)* links. If a network device along this path does not support QoS, the traffic flow receives the standard first-come, first-served treatment on that network segment which will cause VoIP quality problems is undetected. Hence the need for having a fully integrated multi-functional management system that provides the necessary management wrap for a complete service assurance.

2.5.1 QOS Control

As mentioned in the previous section there is a need to employ QOS in order that you have control over the network environment in which bandwidth, latency, jitter, and data loss must be controlled, for example IP Telephony *(VoIP)*, or mission-critical applications for latency-sensitive software, or other multimedia applications. The role that QOS provides therefore allows control around bandwidth allocation to minimize and maximize bandwidth to network packets that are marked for prioritization purposes, policing and actioning priority based on these markings, changing the flow properties whereby, remarking of DSCP *(Differentiated services code point)* packets maybe necessary at the hosting edge of the LAN\WAN network, and shaping the traffic in order to reduce network bursts etc. where required.

You can see now why configuration management with policy and governance capability is a very important piece of the management wrap as you would want to absolutely ensure that your corporations QOS policies are being policed and governed in a way whereby change control is rigid and secure. Changes made to QOS policing needs to be undertaken in a controlled way so as to ensure no disruption or degradation to the service experience occurs.

QOS Configuration Policy Management

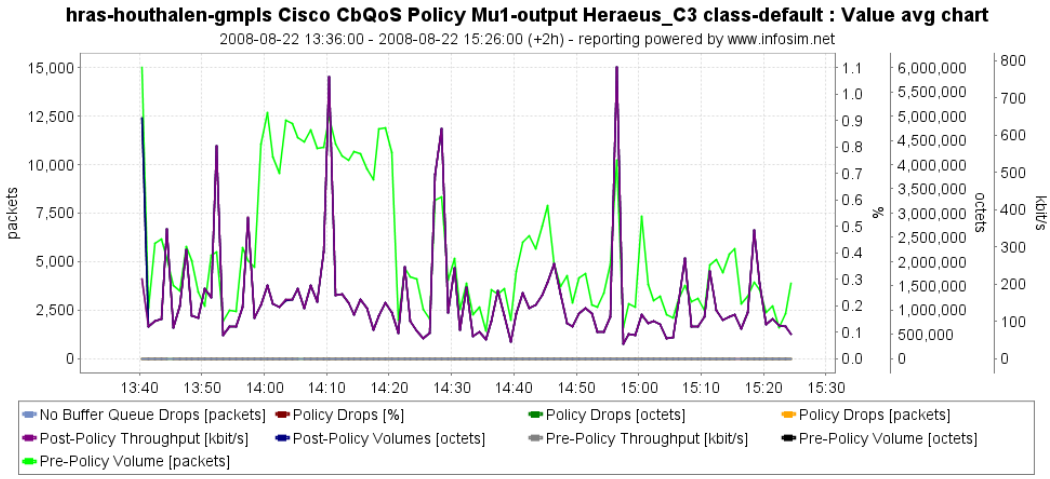


2.5.2 QOS Class Based Monitoring

Class-Based Policing allows you to control the maximum rate of traffic transmitted or received on an interface. Class-Based Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Class-Based Policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

It is therefore really important that comprehensive monitoring of the QOS class and policy configuration and performance is in place. Monitoring and reporting on the configured policy and class for utilization, packet loss, drops, queue depths etc. for pre and post policy comparison allows administrators to fine tune and ensure the VoIP traffic is optimized. Used additionally with Netflow provides even greater visibility and performance reporting capabilities.

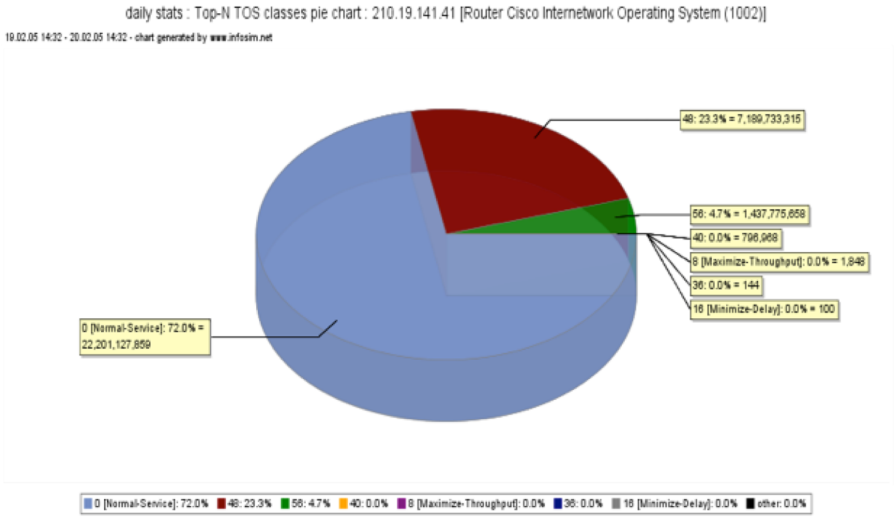
QOS Class Based Monitoring Example



2.5.3 Netflow QOS

Enabling Netflow on your network enables application visibility of usage flows traversing your network. Netflow also reports on Type of Service (ToS) and DSCP fields from traffic flows, that enable you to monitor and report on your bandwidth usage by application. Netflow will measure the effectiveness of your QoS policies, and report on QOS SLA thresholds. The StableNet® Netflow module is an integral part of the unified management system and is an essential functional element for VoIP management.

TOS – Type of Service Monitoring Example



2.5.4 Key Features – WAN & QOS Management

This section highlights the key features of the WAN & QOS management using StableNet®: -

Feature ID	Feature Type	Feature Description	Feature Supported
#1	WAN router availability monitoring.	Monitoring of all WAN Router devices for system, environmental and operational availability.	✓
#2	Configuration management.	Configuration backup of the entire WAN routing infrastructure devices, with auto-backup scheduler, and auto-backup with config-diff-view, reporting on change, BGP routing tables, QOS status etc.	✓
#3	Configuration policy and governance management.	Design rules and standards can be configured as a policy to then be checked for compliance against a specific element or service type.	✓
#4	QOS policy management.	The flexibility of the policy and compliance engine in StableNet® allows for complete customization and automation of your QOS services e.g. standard, enhanced and premium defined QOS service compliance.	✓
#5	QOS performance management.	Monitoring of configured queue groups, measuring queue bandwidth utilization, errors, drops, threshold queue alerting for sustained bandwidth peaks and excessive pack drops.	✓
#6	LAN→WAN topological and service visualization.	Graphical topological views of all discovered WAN devices and mapping them to the connected hand-off points for visualization of LAN interconnects and service views.	✓
#7	Netflow monitoring and reporting.	Netflow enables VoIP traffic analysis from your WAN routers. StableNet® supports Cisco CBQoS and VoIP IP-SLA providing the network and business impact visibility required. sFlow, jFlow, IPFIX, NetStream, and Netflow v5 – 9 supported.	✓
#8	Correlation management.	Unified management systems have built in cross-correlation between the multi-functional capabilities thus providing you with the ability to pin-point exactly what happened, when it occurred, the impact, and root cause in seconds which, is crucial to any real-time service such as VoIP.	✓
#9	Lifecycle management.	Scanning of WAN vendor hardware infrastructure inventory for EOL\EOS\EOSS matches.	✓
#10	Vulnerability management.	Scanning of WAN vendor IOS Vulnerability announcements ensure that security and operational performance is being optimized.	✓

2.5.5 Best Practice#9 – VoIP WAN Assessment

If you are a corporation that is just preparing for the deployment of VoIP across your existing WAN infrastructure, or you have had a partial VoIP deployment for sometime and your strategy has now changed whereby your business has made the decision to go for a fully converged VoIP solution. Apart from the obvious need to ensure the LAN and WAN components can support and control the real-time *(VoIP)* operation, it will be necessary to perform an extensive assessment of the network in order that an understanding of the baseline performance & capacity of the existing network can be understood and modeled for a VoIP solution. StableNet® VoIP assessment functionality can perform End-to-End VoIP testing over multiple locations in order to understand the behavior and performance of the network under stress conditions, and to be able to design the optimized configuration for QOS\queuing design rules required for VoIP deployment.

2.5.6 Best Practice#10 – VoIP WAN QOS Management

WAN bandwidth for most organizations is at a premium therefore, you need to be using it efficiently, and cost effectively. Deployment of VoIP is a real-time application that therefore, demands low-latency and expedited forwarding of VoIP packets. Even if you have high bandwidth available, you will still need to employ QOS, classify your VoIP traffic to use low-latency queuing, and ensure your entire WAN prioritizes anything with a VoIP marking. QOS best practices are to mark packets as close to the edge of the source as possible, classify and mark packets within the layer 2 and 3 elements of the network, and control the packet flows through use of access control and queuing techniques. Management of QOS is therefore an important function as you need to make sure your QOS policies are configured correctly, adhere to the QOS design rules, by using policy controls to police the rules, and that they are performing as designed, *(e.g. enough bandwidth has been allocated to each QOS policy)*, threshold alerting has been employed, and performance reporting is in place.

2.5.7 Best Practice#11 – WAN Management Readiness

Enabling the management of VoIP across a corporations enterprise network requires IT operational support services to avoid the all too common fragmented approach to network management of adopting legacy tools to address new problems. Your strategic VoIP solution must include a management system that is unified and capable of providing the performance, fault and configuration functionality required to managed an End-to-End VoIP solution. Your WAN assessment will provide you with the design rules and performance monitoring threshold KPIs *(Key-Point-Indicators)* needed for a successful VoIP deployment. StableNet® provide the unified management system for proactively managing your solution.

2.5.8 Best Practice#12 – WAN Netflow Enablement

Configuration of Netflow on your WAN routers is a best practice requirement in the deployment of VoIP. Netflow, and especially version 9 Netflow with flexible Netflow support, provides enhanced visibility of End-to-End flow visualization that provides an additional alternative unique and easy way to locate and pin-point troublesome areas of the WAN QOS flows. Reporting of TopN flows for application identification and awareness, details of Type of Services (TOS) and Differentiated Service Code Points (DSCP) flows and bandwidth usage an invaluable addition to your VoIP management solution. StableNet® version 6.5 Netflow performance module now supports version 9 Netflow.

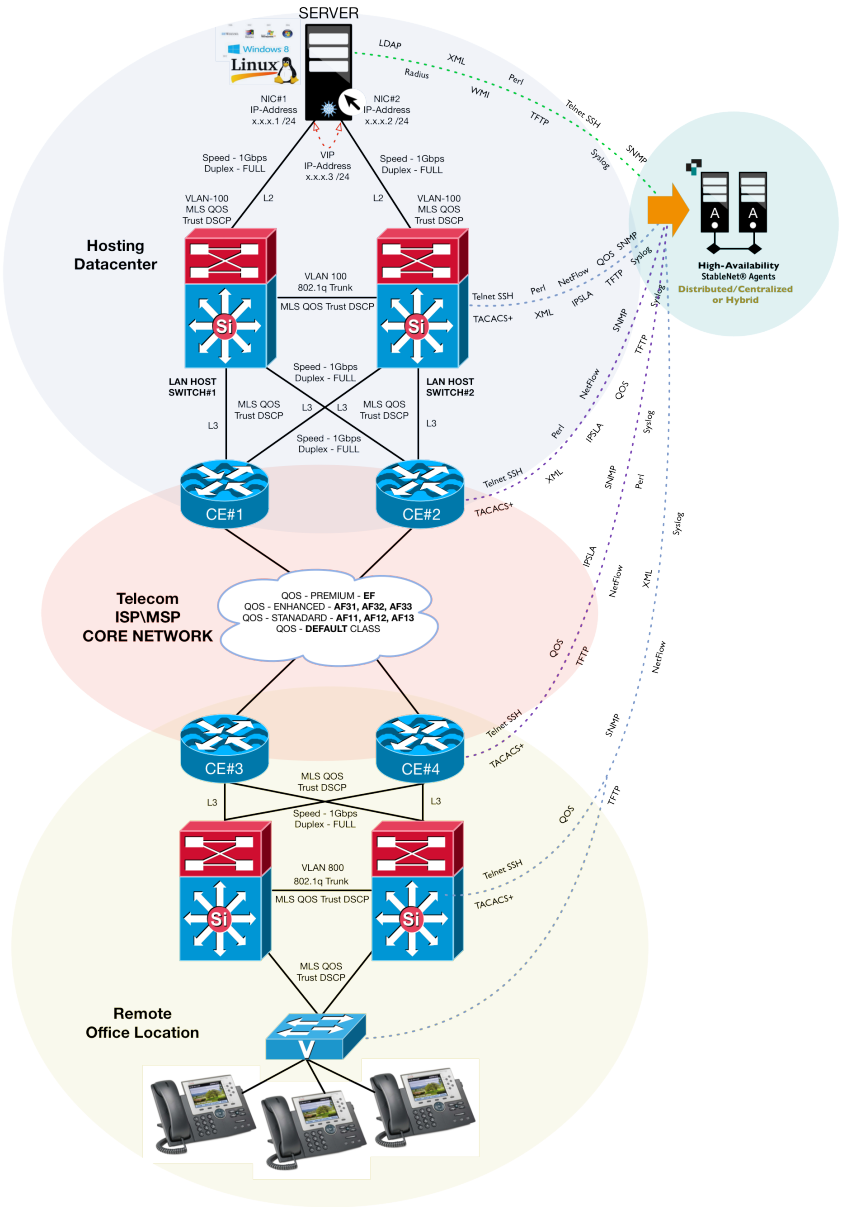
2.6 VoIP Remote Office or Call-Center Management

Completion of the End-to-End holistic picture requires the on-boarding of the far end remote office\call center locations LAN infrastructure. On-boarding of the remote office\call center locations LANs will enable the WAN to remote LAN mapping interconnectivity. This activity then completes the build out of the holistic End-to-End service visualization *(e.g. Server → LAN Switching → WAN Routing → Remote Office LAN)*.

Typically the WAN handoff to the remote office LAN is either resilient, or non-resilient, depending on the office location size, purpose, and criticality to the corporations business. A large corporations office location, or call center, would characteristically be designed with a resilient LAN infrastructure whereas, a smaller, or satellite office, locations will typically have a non-resilient small LAN infrastructure.

Remote location LAN infrastructures will most likely have additional server, voice and security devices that will need to be on-boarded for the holistic End-to-End picture to be complete. The following diagram details the types of remote location LAN infrastructure components you may need to identify for on-boarding monitoring and reporting purposes.

Server → LAN Switching → WAN Routing → Remote Office LAN Connectivity with Agent Collector Flows



2.6.1 Additional Remote Office VoIP Management Requirements

As seen in the diagram above some large remote office locations are not always straightforward from an on-boarding perspective. Many locations will have additional device types, *(e.g. Voice Recorders, Wall-Boards, Local Servers, Firewalls, Secured VoIP Areas etc.)* that will need to be identified and managed appropriately in order to ascertain the required accuracy for the holistic End-to-End visibility. Some of these additional requirements have been included within the sub-sections below.

2.6.1.1 Remote Office Secured Areas

Remote office locations may incorporate high-secured areas, or DMZs *(demilitarized zones)*, that need to be managed appropriately however, there is a BUT… the corporations business protection policies will not allow you to open the tcp\udp ports required for managing this environment. StableNet® has a solution for this eventuality whereby a low-cost remote agent may be installed within the DMZ area in order to collect and store the required monitoring and management information. A single port *(TCP-5100)* is the only port then required to be opened on the firewall for communication between the agent and the middleware system. An added security option is available for the encryption of this data flow between the agent and the middleware.

2.6.1.2 Remote Office Voice Recording

A corporations office\call center will almost certainly have some remote voice recording installed. The voice recorder servers will need to be on-boarded in the same way that you on-board the servers in the hosting environment, making sure that you identify all of the key services that need monitoring via SNMP or WMI depending on what operating system is being employed. Voice recording typically used SPAN & RSPAN session for voice VLAN\Port mirroring in order that the VoIP calls can be recorded. These should also be identified and managed *(see section 2.6.1.4)*.

2.6.1.3 Call Center Wall-Boards

Wall-boards installed within call centers have feeds that provide statistics to the call center management teams about numbers of inbound calls, missed call, aborted calls, calls answered within SLA, missed SLA etc. The wallboards are connected to the LAN infrastructure and are normally controlled via a local or remote server. Identifying these and bringing them under the same management best practices will ensure the appropriate management wrap and visibility of the service.

2.6.1.4 VoIP Remote Office Management of SPAN & RSPAN Sessions

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer, or in a VoIP Call Center environment, voice recording device. SPAN copies *(or mirrors)* traffic received or sent *(or both)* on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

It is very important for corporations that voice recording is enabled and operating to consistently high levels in order to meet public regulatory guidelines and rules, for example FSA *(Financial Services Authority)*. Therefore all SPAN and RSPAN sessions should be identified and have the configuration elements backed up as part of the LAN device management wrap. The SPAN & RSPAN configurations should also be included within your config policies and governed in a way whereby the management system alarms you when a change to the configuration occurs. In addition to this you should also include the appropriate 'show SPAN\RSPAN monitor' command as part of the routine configuration backup job so as to police and report any inconsistencies on the status.

2.6.1.5 VoIP Remote LAN QOS Monitoring

LAN Quality-of-Service will be configured with markings, trusts and policed as close to the traffic-sources as possible. In the case of remote office locations where VoIP handsets are deployed the LAN switch ports connecting the handsets will have IP-Phone DSCP trusts, or auto-trusts in place. Identification of the configuration of the DSCP COS markings and trusts within the layer 2 *(data-link-layer)* and layer 3 *(network layer)* switching LAN architecture will need to be known so as to ensure appropriate management and reporting. Best practices for policing of LAN quality of service configuration is through use of configuration policy & governance functionality. *(QOS performance monitoring and reporting is explained in further detail in section 2.5 – WAN QOS Management & Policing, section 2.5.3 – Netflow QOS, and section 3.6 – IP-SLA).*

2.6.1.6 VoIP Handset Management

The advancement of VoIP has allowed greater control around the management of the IP-Handset. This feature has so many benefits from an end-point management perspective. Firstly, the handset itself can be discovered as part of the overall asset management discovery process that then allows you to track handset movements around the network, perform lifecycle management, and for the first time to be able to accurate visualize an accurate number of handset in use. Secondly, there are a number of additional features available to collect from the handset: -

- Handset Monitoring
  - Availability – Handset Availability Monitoring
  - MOS – Last –Call Quality score
  - Jitter – Last Call Performance
  - Codec Type – Codec in use
  - Speed & Duplex
  - IP Address (handset)
  - Mac Address (handset)
  - Switch ID (Hostname of Connected Switch)
  - Switch Port\Interface (IP Handset Connected Interface\Port)

StableNet® fully supports VoIP handset management for handsets.

2.6.2 Key Features – VoIP Remote Office Management

This section highlights the key features of the VoIP Remote Office Management using StableNet®: -

Feature ID	Feature Type	Feature Description	Feature Supported
#1	Remote LAN→WAN e2e visualization.	Graphical topological views of all discovered remote LAN devices and mapping them to the connected hand-off WAN points for visualization of LAN interconnects and service views.	✓
#2	Configuration management.	Configuration backup of the entire remote LAN infrastructure devices, with auto-backup scheduler, and auto-backup with config-diff-view, reporting on change, VLAN trunking, routing tables, QOS status etc.	✓
#3	Lifecycle management.	Scanning of remote LAN vendor hardware infrastructure inventory for EOL\EOS\EOSS matches.	✓
#4	Vulnerability management.	Scanning of remote LAN vendor IOS Vulnerability announcements, ensure that security and operational performance is being optimized.	✓
#5	Voice recording management.	Monitoring of the voice recording LAN interconnects, SPAN\RSPAN sessions, Recorders, & key services.	✓
#6	Remote voice gateway management.	Monitoring of all remote voice gateways, LAN and PSTN\SIP interconnects & channels.	✓
#7	SPAN\RSPAN policy management.	Policy configuration template monitoring for all identified remote LAN SPAN\RSPAN sessions.	✓
#8	Secured VoIP monitoring.	Remote agent deployment for secured remote LAN\VLAN DMZ monitoring.	✓
#9	Call-Center wallboard management.	Call-Center wallboard management, switch-port monitoring, and control server monitoring.	✓
#10	VoIP Handset management.	Availability and statistical performance monitoring and reports for IP handset management.	✓

2.6.3 Best Practice#13 – Remote Office VoIP LAN Management

Remote office or call center LAN management is an integral part of the service delivery mechanism in any VoIP, or critical application, within a corporations infrastructure. The remote LAN network is the destination hand-off point for IP telephony *(e.g. VoIP Handsets, Softphone apps etc.)*, voice recording, wallboard systems and other peripheral LAN attached remote office device types. Therefore, it is not only necessary to ensure effective management of the remote LAN components, it is critical to know exactly how the remote LAN is performing and operating so as to assure and maintain consistent high levels of service availability. StableNet® provides you with the LAN performance, configuration and fault management functionality you need and, through the use of the customized dash-boarding and reporting, completes the build-out of the 'Single-Picture-Service-View' your operational and service teams require.

2.6.4 Best Practice#14 – Voice Recorder Management

Call centers, or IPCCs, and some remote office locations will have IP voice recording installed. Management of these voice recorders will need to be undertaken and monitored in the same way as any other server on the network. However, additional key service monitoring requirements will also need to be considered for example, number of active voice recording licenses in-use is a monitoring metric that is very important for corporation to keep a check on licensing used\allocated thus reducing the need for over-spending on recording licensing. Voice recorders connected to the LAN will normally have associated SPAN\RSPAN sessions configured to specific voice VLANs for voice recording capture. Effective configuration management as detailed in section 2.6.1.4 of the SPAN\RSPAN sessions is critical for ensuring that voice recording is operational. Voice recording for financial services is an FSA requirement and there assurance of regulatory compliance needs to be managed appropriately.

2.6.5 Best Practice#15 – VoIP Handset Management

One of the main advantages of a VoIP deployment is that the IP handset can now also be managed for effective asset inventory purposes, end of life analysis, and for operational monitoring around availability and call quality. Maintaining handset availability may seem a tedious non-business impact task but by enabling the management of IP handsets you are completing the End-to-End monitoring of your VoIP solution, qualifying the availability and operational readiness of the handsets within locations like call centers that could have impact on business revenues if the handsets or softphones have issues or intermittent errors. Therefore, consideration for IP handset monitoring should be seriously considered and is very cost effective when using StableNet® as you management platform.

3 VoIP Performance Monitoring

As mentioned in the VoIP management overview, section 1 of this document, a lot of VoIP monitoring tools tend to focus heavily on the performance management elements, and whilst this is an extremely integral part of any VoIP monitoring solution, it should also be viewed as one of a number of required functionalities needed to create a complete VoIP management solution.

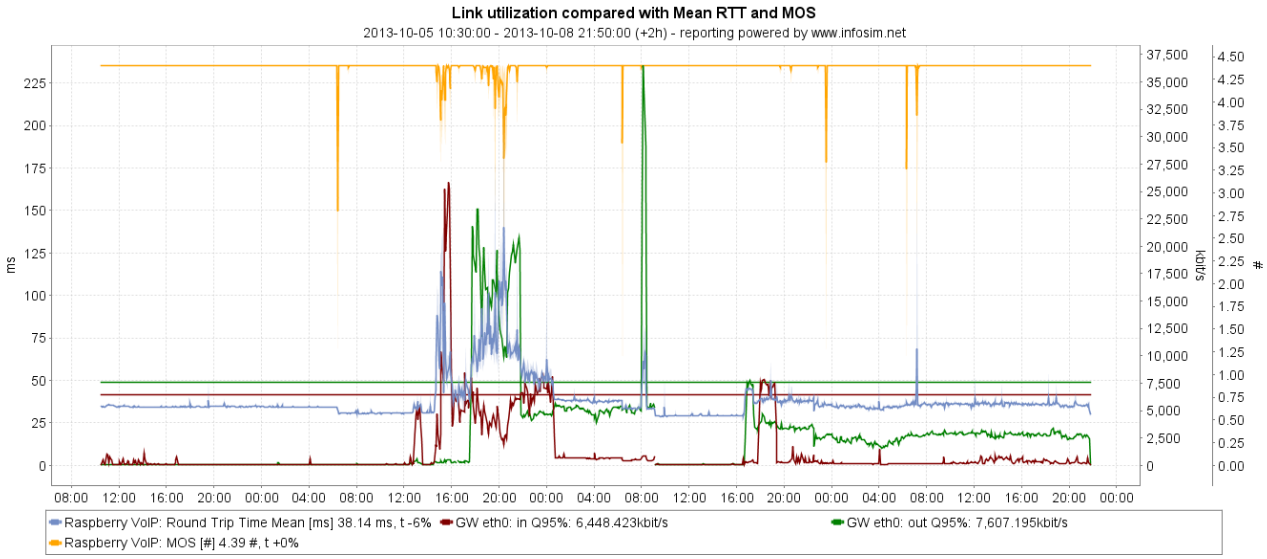
Voice over IP is a real-time application, it needs the packets of digitized speech to traverse the network path with minimum delay, and maximum speed. Each network device a VoIP packet traverses must be optimized appropriately for trusting, prioritizing and expediting the VoIP packets. Performance metrics for monitoring the quality of voice calls, the delivery of VoIP packets, and the performance and consistency of the network is principle in the prevention of service deterioration.

3.1 VoIP Performance Network Management

A network performance management tool needs to be capable of monitoring key VoIP metrics *(e.g. Latency, Jitter, Packet Loss, MOS, R-Factor)* from one end of the network to the other if real-time operational performance is to be successful. Management systems that provide a unified performance, fault, and configuration multi-functional capability are highly desirable and should be your preferred option. Having a multi-functional capability will not only provide you with the desired management wrap, it will maximize the management support effectiveness in dealing with service interruptions. For example; by cross-correlation of pin-pointing a performance problem, with an event or fault, that was caused by an unauthorized configuration change. Now, because you have the last known working configuration you can check the config-difference report, identify what has been changed, remediate the change back to the known working config thus fixing your performance problem that was first identified. Value-add management systems like StableNet® automate the cross-correlation of these types of problems and therefore help to free up valuable support resource and enable greater proactive monitoring.

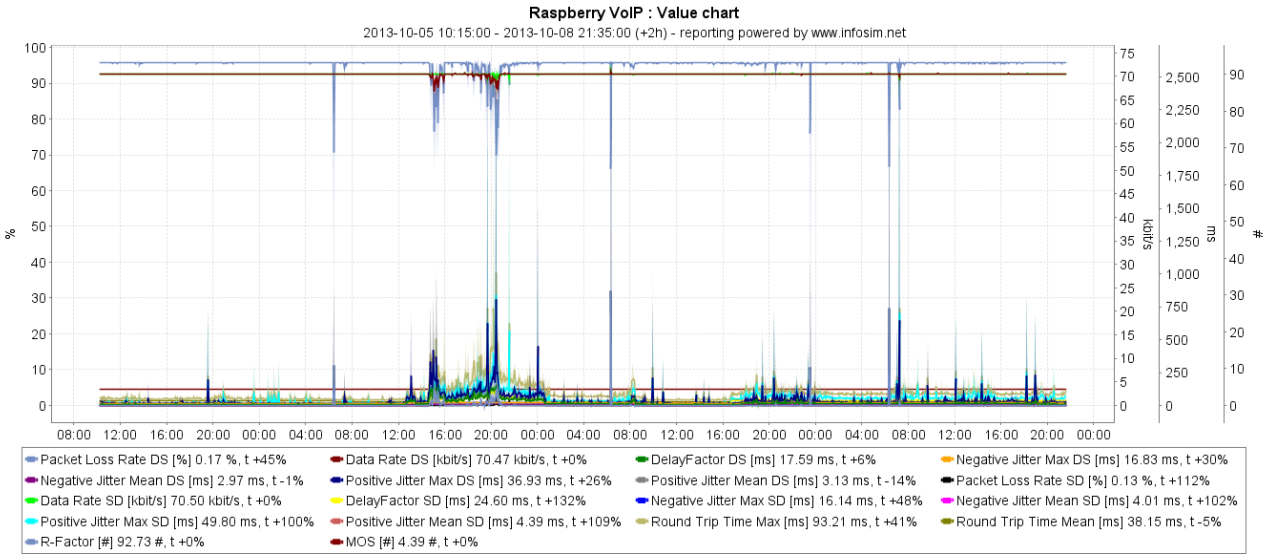
3.1.1 Latency Management & Reporting

RTD – Round-Trip-Delay, or Latency is the measure of time delay in packets of data traversing a network from the transmitting agent to the receiving agent. Because VoIP is a real-time application minimum Latency is a prerequisite. VoIP has a maximum Bidirectional tolerance of 150ms, round-trip of 300ms. This tolerance level is the extreme max and should not be exceeded. Typically in-country published round-trip latency figures are quoted anywhere between 20-100ms. Understanding the round-trip tolerances on a network you plan to deploy VoIP on is essential for threshold alarm & event management. You need to know when poor VoIP call quality has been reported, if it is latency induced, and by having thresholds configured around RAG (Red, Amber, Green) status you will be alerted prior to customers being affected in order that you can do something about the problem. Having a unified management system like StableNet® will greatly assist with pinpointing where latency issues reside as the correlation between the Alarm and Event system and the performance system is fully integrated within a single product.



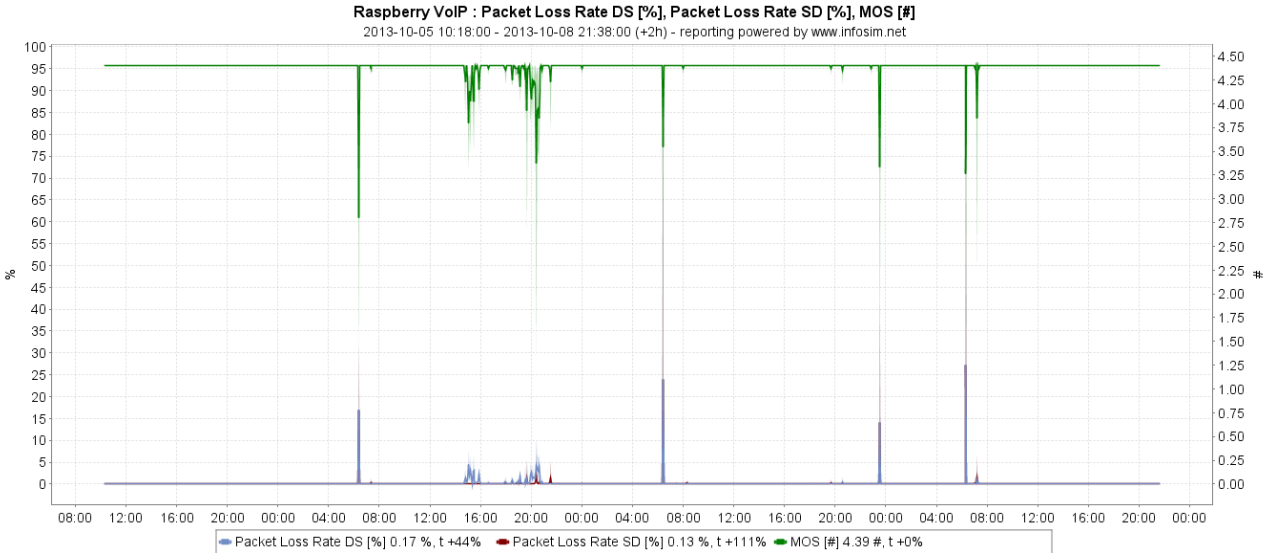
3.1.2 Jitter

Jitter is the variation of packet delay. The transient delay caused by network congestion, queuing, contention and re-routing effects the communication path through the network. Acceptable tolerance duration thresholds for jitter should not exceed 40ms as it is generally accepted that deterioration of the voice quality will be affected on sustained higher jitter delays.



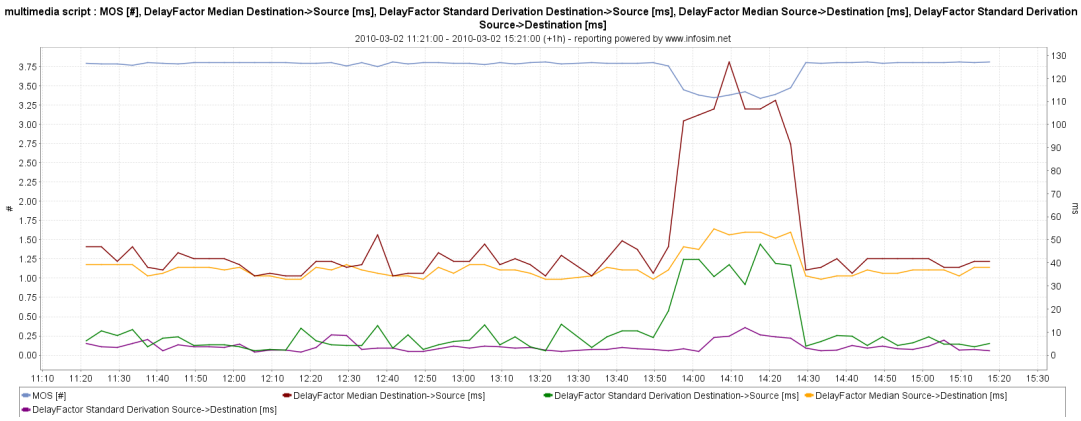
3.1.3 Packet Loss

Packet loss can cause serious problems in real-time applications like VoIP. Lost RTP packets are not retransmitted and in some cases the bursts of packet loss can cause serious issues like excessive call-clipping to occur. Allowable tolerance levels for packet loss is less than <1% for WANs and less than <0.05% for LANs. The implementation of QOS provides the control needed to ensure the consistent prioritization of VoIP packets reaching their destination thus minimizing the risk of packet loss. However; packet loss remains a key performance metric in the managing of VoIP due to the seriousness of the event.



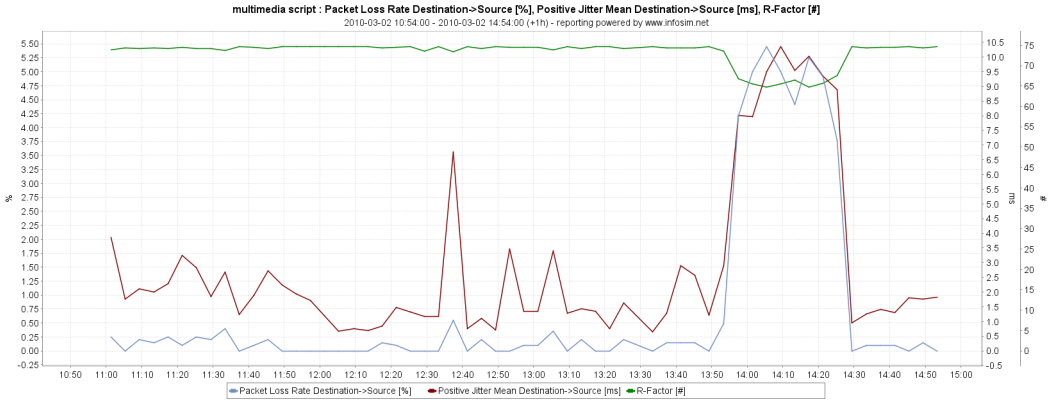
3.1.4 MOS

Mean-Opinion-Score is a test that has been used for decades in telephony networks to obtain the human user's view of the quality of the network. It is a subjective measurement of voice quality that provides a numerical indication expressed from 1 – 5 *(1-BAD, 2-Poor, 3-Fair, 4-Good, 5-Excellent)*. Tolerance thresholds for MOS are dependent on the type of voice codec you are using, for example, a G.711 Codec tolerance would be between 4.1 – 4.4 whereas a G.729 codec would be 3.9 – 4.0.



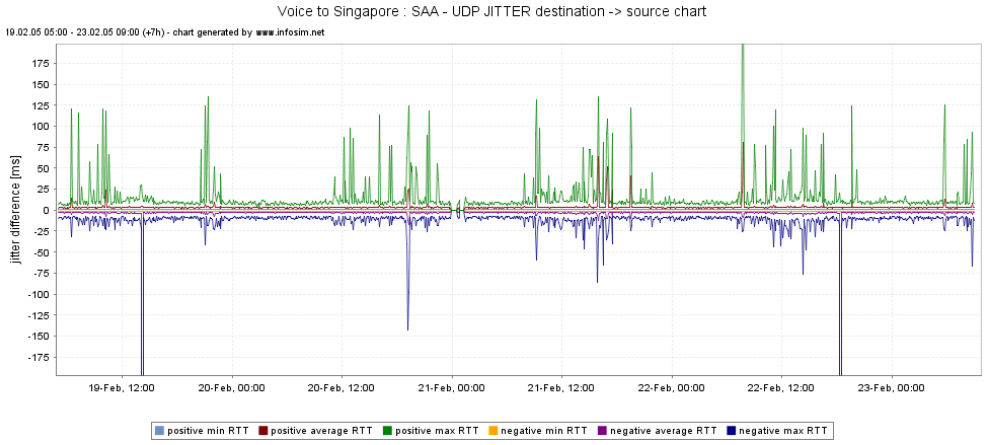
3.1.5 R-Factor

R-Factor is an alternative method of assessing call quality. Scaling from 0 to 120 as opposed to the limited scale of 1 to 5 makes R-Factor a somewhat more precise tool for measuring voice quality. R-Factor is calculated by evaluating user perceptions as well as the objective factors that affect the overall quality of a VoIP system, accounting for the Network R-factor and the User R-factor separately.



3.1.6 IP-SLA

IP SLA is a Cisco specific software module that enables Cisco devices to generate synthetic network traffic to monitor latency, packet loss, jitter, and mean opinion score (MOS) for VoIP networks. IP SLA can validate network performance, proactively identify network issues, and assist in simplifying the deployment of new IP services. IP-SLA can be used to set threshold monitors to alert and detect application degradation in the network, and notify you of issues before they start to impact your customer. StableNet® fully supports IP-SLA Measurements including: Latency, loss, jitter, and MOS.



3.1.7 Synthetic VoIP Performance Monitoring

Synthetic VoIP performance monitoring is essentially a series of spoof, or hoax VoIP calls and measurements sent between point-2-point, point-2-multipoint, or multipoint-2-multipoint locations within a network infrastructure. The test measurements can also include voice codec type (e.g. G.711, G.729 etc.) and will be configured to monitor and report VoIP performances metrics like MOS, R-Factor, Jitter, Packet Loss, and delay or latency for each call being tested to ascertain the performance of the call signaling and voice quality. Running synthetic testing should be part of your best practice strategy because it is very important to ascertain the performance of the network prior to any VoIP deployment and is therefore invaluable when it come to designing QOS and queuing policies etc.

3.1.8 Key Features – VoIP Performance Management

This section highlights the key features of the VoIP Performance Management using StableNet®: -

Feature ID	Feature Type	Feature Description	Feature Supported
#1	Latency performance & correlation management.	End-to-End Monitoring of delay\latency of the network with correlation of performance, fault, & configuration.	✓
#2	Jitter performance and threshold monitoring.	WAN Jitter performance monitoring with specified threshold alerting and notification management.	✓
#3	Packet loss control and monitoring.	End-to-End network Monitoring of packet loss with correlation of performance, fault, & configuration.	✓
#4	IP-SLA monitoring.	Cisco IP-SLA for synthetic VoIP performance reporting is fully supported by StableNet®.	✓
#5	MOS & R-Factor quality monitoring.	Call-Quality monitoring of VoIP networks.	✓
#6	Threshold alarm & automated alerting.	KPI Threshold settings for key VoIP performance management, with automated alerting on threshold breaches.	✓
#7	VoIP performance simulation.	StableNet® Agent-2-Agent synthetic VoIP performance simulation and KPI threshold tolerance management.	✓
#8	VoIP Optimization	Optimization\fine tuning of VoIP QOS and Threshold KPIs achieved through simulation testing results.	✓

3.1.9 Best Practice#15 – VoIP Packet Loss Management

Packet loss within a VoIP enabled network seriously affects voice quality. Because of the real-time nature of VoIP and the limitation on delay it is impossible to retransmit dropped packets. Allowable tolerance levels for packet loss is less than <1% for WANs and less than <0.05% for LANs so any consecutive stream of packet loss will result in degraded voice quality. Packet loss monitoring is one of the key VoIP impairment metrics and is therefore critical to monitor, report and alert when thresholds have been breached. The implementation of QOS and low-latency queuing will expedite VoIP packets through the network minimizing the risk of packet loss. StableNet® performance management

cross-correlates the monitoring of packet loss with the unified event and alarm system providing rapid problem identification and root cause of where the packet loss occurred.

3.1.10 Best Practice#16 – Jitter Management

Jitter means inter-packet delay variance. When multiple packets are sent consecutively from source to destination, for example, 10ms apart, and if the network is behaving ideally, the destination should be receiving them 10ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10ms. Using this example, a positive jitter value indicates that the packets arrived greater than 10ms apart. If the packets arrive 12 ms apart, then positive jitter is 2ms; if the packets arrive 8 ms apart, then negative jitter is 2ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal. Jitter is one of the key VoIP impairment metrics and is therefore critical to monitor, report and alert when thresholds have been breached. Through the use of IP-SLA comprehensive jitter management can be monitored to measure: Per-direction jitter *(source to destination and destination to source)*, Per-direction packet loss, Per-direction delay *(one-way delay)*, and Round-trip delay *(average round-trip time)*.

3.1.11 Best Practice#17 – Cisco IP-SLA Management

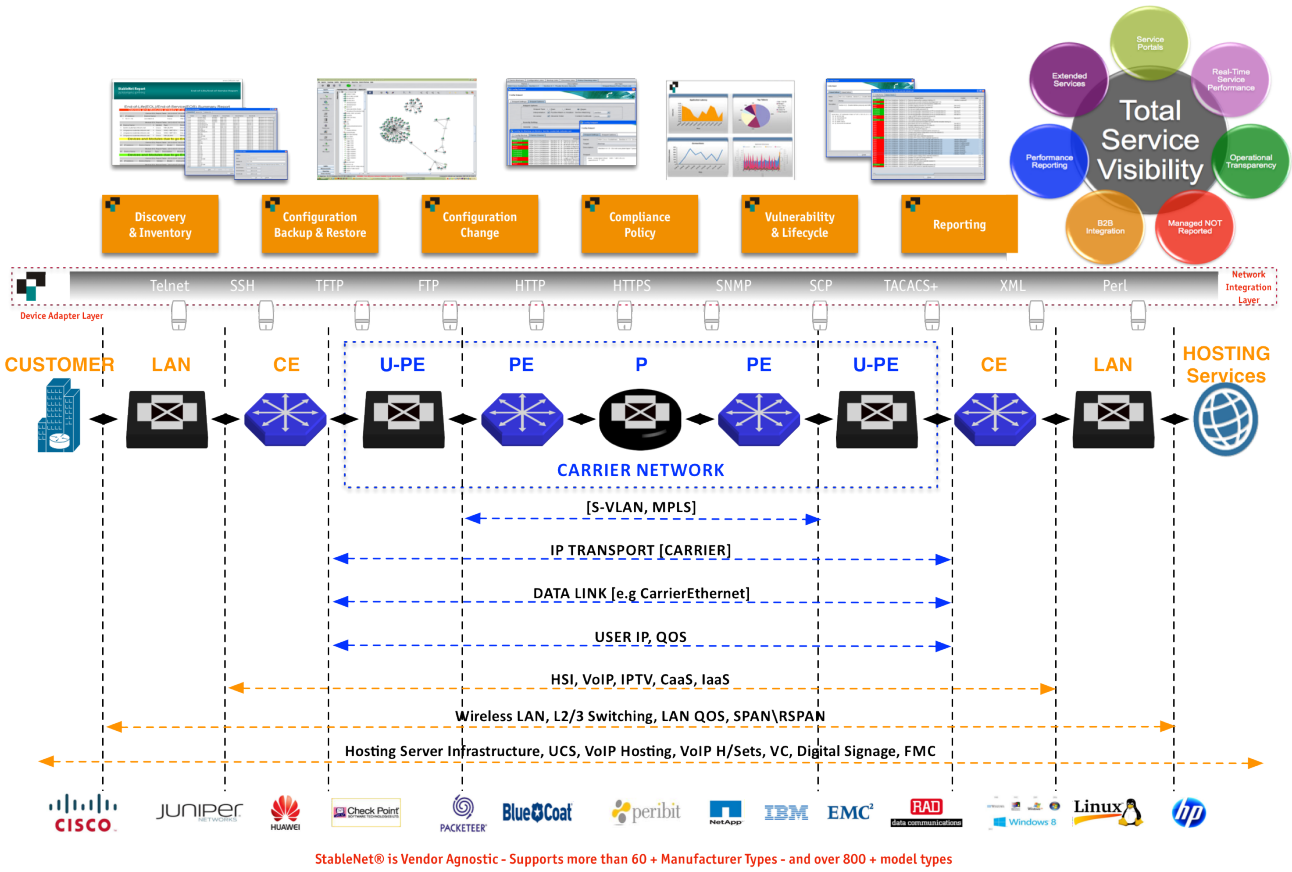
IP SLA is a Cisco specific software module that enables Cisco devices to generate synthetic network traffic to monitor latency, packet loss, jitter, and mean opinion score (MOS) for VoIP networks. If you are operating a Cisco based WAN then enabling IP-SLA traffic monitors for real-time simulation performance reporting is a best practice recommendation. StableNet® fully supports IP-SLA monitoring and reporting and can automatically configure the IP-SLA monitors via the configuration management deployment functionality.

3.1.12 Best Practice#18 – VoIP Simulation Performance Management

Running VoIP synthetic testing should be part of your best practice strategy because it is very important to ascertain the performance of the network prior to any VoIP deployment. It is also invaluable when it come to designing QOS and queuing policies etc. A great management performance attribute, or asset, is having a number of synthetic agents deployed around key parts of your network in order that you can stress the performance and measure the voice quality of the network so as to determine key thresholds, bandwidth scalability, and quality of service as your business growth demands. StableNet® VoIP assessment functionality can perform End-to-End VoIP testing over multiple locations in order to understand the behavior and performance of the network under stress conditions, and to be able to design the optimized configuration for QOS\queuing design rules required for VoIP deployment, scalability and growth.

4 The Holistic End-to-End Picture

Throughout this document I have spoken about the holistic End-to-End visualization, or the importance of the 'Single-Picture-Service-View' of your VoIP network. In order to be successful with the deployment of a VoIP solution you must deploy a multi-functional fully integrated management tool that has a comprehensive capability around performance, fault, event and configuration management, has seamless correlation in order to maximize the quality of both VoIP and Data services traversing your networks, improve and sustain high-levels of service availability, reduce MTTR, enhance your support teams productivity and proactivity by the facilitation of automated service provisioning and assurance.



'StableNet® is a unified multi-functional management system, it provides the complete management wrap enabling accurate proactive service assurance management'

5 Resources & Further Information

Follow the links below for further information about Infosim StableNet®.

1. Infosim Web Site: www.infosim.net
2. Infosim StableNet® Videos: http:\\www.infosim.net\resources\videos.html
3. Infosim StableNet® Case Studies: http:\\www.infosim.net\resources\case-studies.html
4. Infosim StableNet® Industry Reports: http:\\www.infosim.net\resources\industry-reports.html
5. Infosim StableNet® Product Sheets: http:\\www.infosim.net\resources\product-sheets.html
6. Infosim StableNet® Request Trial: http:\\www.infosim.net\support\trial.html

For any additional information, demonstrations or webinar requests: http:\\www.infosim.net\about\contact.html

EMA Radar – Report Summary & Infosim Profile

An external report by Enterprise Management Associates® (EMA™) Radar Report for Enterprise Network Management Systems (ENMS): Q4-2012. A report summary and Infosim profile produced and written by Tracey Corbo, and Jim Frey October 2012 is available using the following link below:

http:\\www.infosim.net\fileadmin\user_upload\resources\industry_reports\EMA-ENMS-Q4-2012_RadarSummary-Infosim.pdf

6 About this Document

This document provides details on the Infosim StableNet® unified management system and how it's multi-functional capabilities address a complete VoIP monitoring and reporting solution. Infosim StableNet® is the only all-in-one unified management tool capable of delivering and visualizing a complete End-to-End VoIP service solution monitoring system in a single product that has proven ROI *(Return-On-Investment)* in reducing capital *(CAPEX)* and operating *(OPEX)* expenditure, with conceivable savings in customer service credits thru reduced MTTR *(Mean-Time-To-Repair)*, and increased service availability.

6.1 About Infosim

Infosim is a leading manufacturer of automated Service Fulfillment and Service Assurance solutions for Telco's, ISP's, Managed Service Providers and Corporations. Infosim develops and markets StableNet®, the leading unified software solution for Fault, Performance and Configuration Management. StableNet® is available in two versions: Telco (for Telecom Operators and ISP's) and Enterprise (for IT and Managed Service Providers). StableNet® is a single platform unified management solution designed to address today´s many operational and technical challenges of managing distributed and mission critical IT infrastructures.

6.2 About Infosim StableNet® (Telco & Enterprise)

StableNet® Telco is a comprehensive unified management solution; offerings include: Quad-play, Mobile, High-speed Internet, VoIP (IPT, IPCC), IPTV across Carrier Ethernet, Metro Ethernet, MPLS, L2\L3 VPNs, Multi Customer VRFs, Cloud and FTTx environments. IPv4 and IPv6 are fully supported.

StableNet® Enterprise is an advanced, unified and scalable network management solution for true End-to-End management of medium to large scale mission-critical IT supported networks with enriched dashboards and detailed service-views focused on both Network & Application services.

StableNet® is a 3rd Generation highly automated Network Management System. The key differentiation of StableNet® to other legacy type Operational Support Systems (OSS) is that StableNet® is a Unified OSS system with three integrated functionalities that focus on Configuration, Fault and Performance Management, with Automated Root-Cause-Analysis (RCA). StableNet® can be deployed on a Multi-Tenant, Multi-Customer or Dedicated platform and can be operated in a highly dynamic flex-compute environment.

6.3 Infosim Total Quality Management

Infosim StableNet® is a Total Quality Management solution that enables End-to-End automated service fulfillment and assurance with flexible integration for service catalogue auto-provisioning. The Service-to-Provisioning-to-Customer process significantly reduces the Ready-for-Service *(RFS)* timescale and as a direct consequence enables Communication\Managed Service Providers *(CSPs\MSPs)* to reduce the time-to-bill on newly provisioned services thus maximizing revenues, whilst, provisioning a quality customer service experience.

7 Disclaimer

END OF DOCUMENT