

Cisco Services

Cisco Expo 2011

Helsinki

13.9.2011

Messukeskus

Cisco Smart Care

From reactive to proactive support services

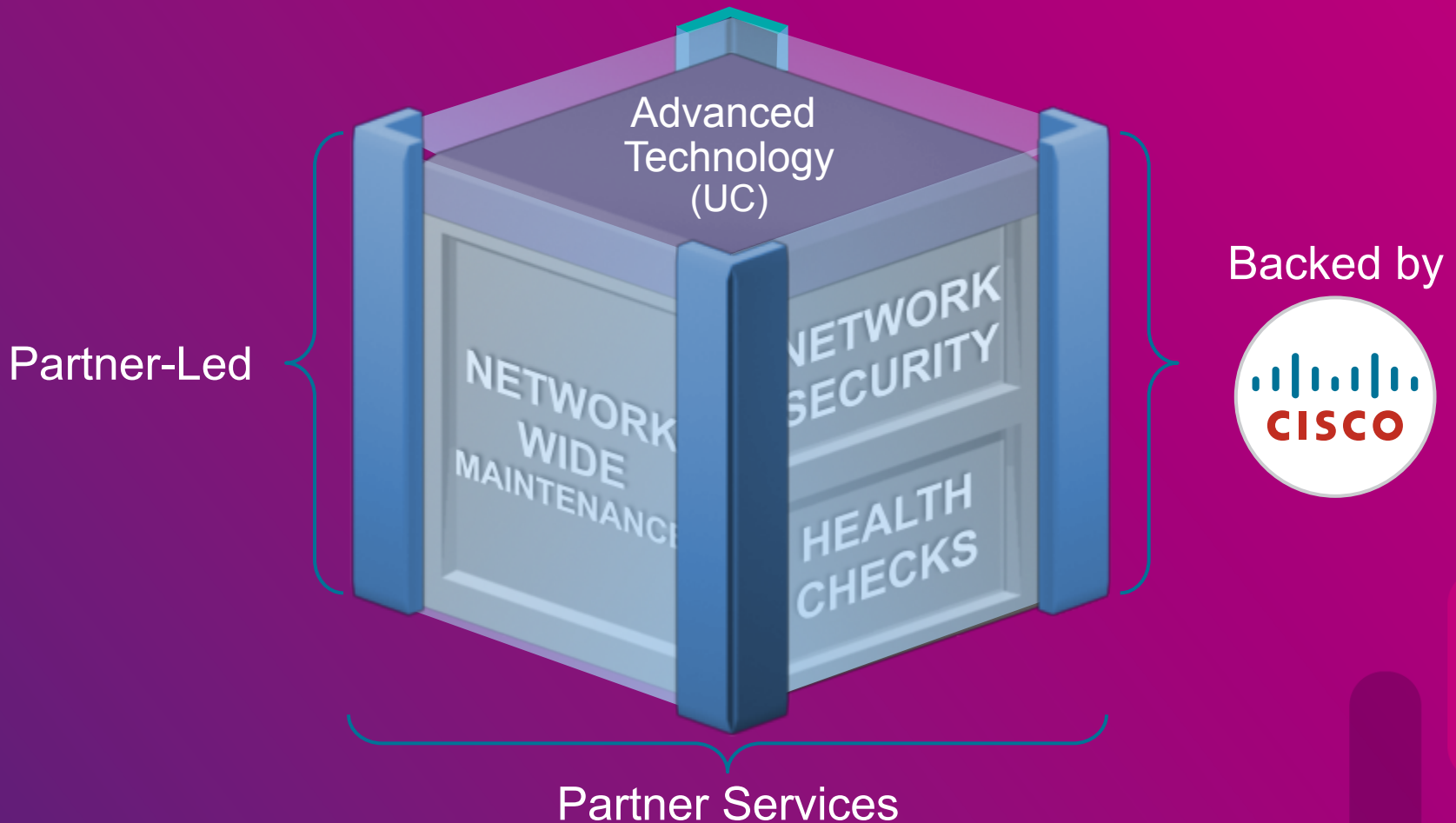
Samuli Kokki

Partner Services Development Manager

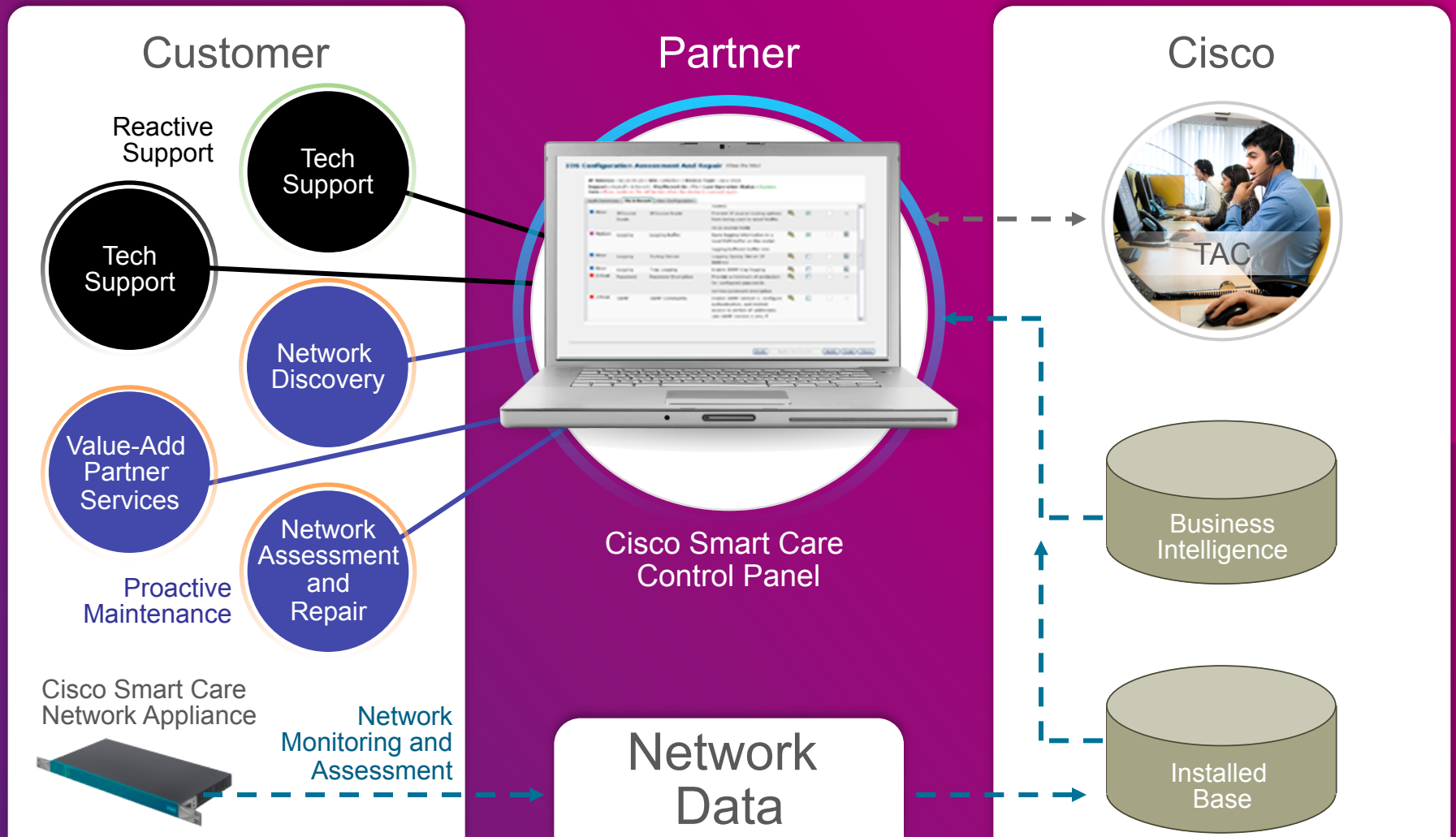
Cisco Smart Care

An innovative service that combines network-wide technical support with ongoing network monitoring and proactive maintenance to deliver a comprehensive approach to the care and continuous improvement of your network.

A Proactive Services Platform on Which Partners Can Build the Next Generation of Personalized Services



Network Discovery, Assessment, and Repair



Network Wide Maintenance

- 24x7 partner access to the TAC
- NBD hardware replacement with an option to upgrade individual devices to four hour coverage
- Cisco.com and Smart Care portal/tools access
- Cisco IOS® updates and upgrades
- Software application support updates

- Caveats and Call Outs:
 - Includes ESW for CallManager based networks
 - No On-Site Service SKUS



Smart Care Network Discovery

- First stage of Smart Care contract engagement
- All devices discovered within defined network – Cisco and non Cisco equipment
- Equipment initially identified via SNMP, with logins to retrieve inventory

Cisco Smart Care Service - Microsoft Internet Explorer

Basic Services - Discovery (Partner Initiated) (Step 1 of 3)

The Smart Care Discovery service uses Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) to find all network devices that can be discovered through IP. Select the discovery type, IP range, or subnet. Provide the IP address or subnet range and the community strings. For more information, click the Help icon.

Discovery Type: Medium - Cisco recommended
 IP Range - Cisco recommended

Starting IP Address:

Ending IP Address: Add

10.4.0.1-10.4.12.255 Delete
 10.2.0.5-10.2.12.254
 10.3.0.5-10.3.11.10
 10.4.0.5-10.4.12.100

SNMP Community: cisco Add
 cisco Delete

Possible Hosts: 3315

< Back Next > Suspend Session Terminate Session

Customers: [RAPID PERFORMANCE SYSTEMS](#) > Discovered Devices

Discovered Devices Items 1-26 of 26 | Rows per page: 50 | Go

Note: Phones will be discovered as part of Cisco Unified Call Manager/Cisco Unified Call Manager Express Inventory

Filter: All Match if: Contains Go Clear Filter | Display Unknown Devices

Select	Status	IP Address	Client Site	Source	Device Type	Device Classification
<input type="checkbox"/>	Ok	10.2.0.6	San Jose	Auto(Cisco)	Cisco 2621XM	Currently in inventory
<input type="checkbox"/>	Ok	10.2.0.10	San Jose	Auto(Cisco)	Cisco 2821	Currently in inventory
<input type="checkbox"/>	Ok	10.2.0.14	San Jose	Auto(Cisco)	Cisco 1811	Currently in inventory
<input type="checkbox"/>	Ok	10.2.0.18	San Jose	Auto(Cisco)	Cisco 827H	Currently in inventory
<input checked="" type="checkbox"/>	New	10.4.0.5	San Jose	Auto(Cisco)	Cisco 2851	New
<input checked="" type="checkbox"/>	New	10.4.0.6	San Jose	Auto(Cisco)	Cisco 2821	New
<input checked="" type="checkbox"/>	New	10.4.0.9	San Jose	Auto(Cisco)	Cisco 2851	New
<input checked="" type="checkbox"/>	New	10.4.0.10	San Jose	Auto(Cisco)	Cisco 2821	New
<input checked="" type="checkbox"/>	New	10.4.1.1	San Jose	Auto(Cisco)	Cisco 2821	New
<input type="checkbox"/>	Ok	10.4.1.3	San Jose	Auto(Cisco)	Catalyst 3560-24PS	Currently in inventory
<input checked="" type="checkbox"/>	New	10.4.2.1	San Jose	Auto(Cisco)	Cisco 2821	New
<input type="checkbox"/>	Ok	10.4.3.1	San Jose	Auto(Cisco)	Cisco 2821	Currently in inventory

Business Impact

Visibility and Optimization for Customers

Increased Visibility

82% Previously Uncovered

16% End of Sale

67% Vulnerabilities

Improve Service

-14% Support Cost Reduction

60% Alerts Which Avoided a Call

-32% Reduction in Downtime

“The visibility Smart Care provides is important, especially from the management side. We need to know what there is and how it’s working
Thys Coetzee, Director of IT, Zinpro Performance Minerals

Proactive Alerts and Integrated Intellishield Reports

- Highlights Field Notices, EoX notifications, PSIRTs and Intellishield alerts by devices
- Categorises errors

Customers: [RAPID PERFORMANCE SYSTEMS](#) > Proactive Notifications

Proactive Notifications Summary Items 1-5 of 5 | Rows

Filter: All Match if: Contains Go Clear Filter

Device Type	IP Address	Device Name	Installed-At Site	Total Alerts	Importance		
					Critical	Important	Informational
Cisco 3825	10.2.0.5	78.40.18.14	BALTIMORE_8679621_1	14 Open: 10 Ignored: 1 Resolved: 3	1	13	0
Catalyst 2970-24TS	10.2.10.3	T2-MO-SW2970	BALTIMORE_8679621_1	5 Ignored: 5	1	4	0
Cisco 2621XM	10.2.0.6	T2-B01-R2621	BALTIMORE_8679621_1	10 Open: 10	0	9	1
Catalyst 3750-24ME	10.2.11.3	T2-MO-SW3750	BALTIMORE_8679621_1	3 Open: 3	0	2	1
Catalyst 2960-24TT	10.2.12.3	T2-MO-SW2960	BALTIMORE_8679621_1	3 Open: 3	0	2	1

Page 1



Worldwide [c]

Search

Solutions Products & Services Ordering Support Training & Events Partn

HOME Security Intelligence Operations

ABOUT CISCO

SECURITY INTELLIGENCE OPERATIONS

Security Programs

IntelliShield Alert Manager

Cyber Risk Reports

Cisco IPS Active Update Bulletins

Technical Resources

Cisco Event Responses

Cisco IPS Signatures

Security Case Studies

Security Intelligence Operations Best Practices

Technical White Papers

Cisco Emergency Response

Security Intelligence Operations RSS Feeds

Cisco Applied Mitigation

Multiple SNMPv3 Implementations Hash-Based Message Authentication Code Manipulation Vulnerability

VULNERABILITY ALERT Powered by **IntelliShield**

Threat Type: **Unintended Weakness: Software Fault (Vul)**

IntelliShield ID: **16040**

Version: **15**

First Published: **June 10, 2008 02:18 PM EDT**

Last Published: **June 23, 2009 05:41 PM EDT**

Vector: **Network**

Authentication: **None**

Exploit: **Unproven**

Port: **161, 162**

CVE: **CVE-2008-0960**

BugTraq ID: **29623**

Urgency: **Unlikely Use**

Credibility: **Confirmed**

Severity: **Moderate Damage**

CVSS Base: **10.0** [CVSS Calculator](#)

CVSS Temporal: **7.4** [CVSS Version 2](#)

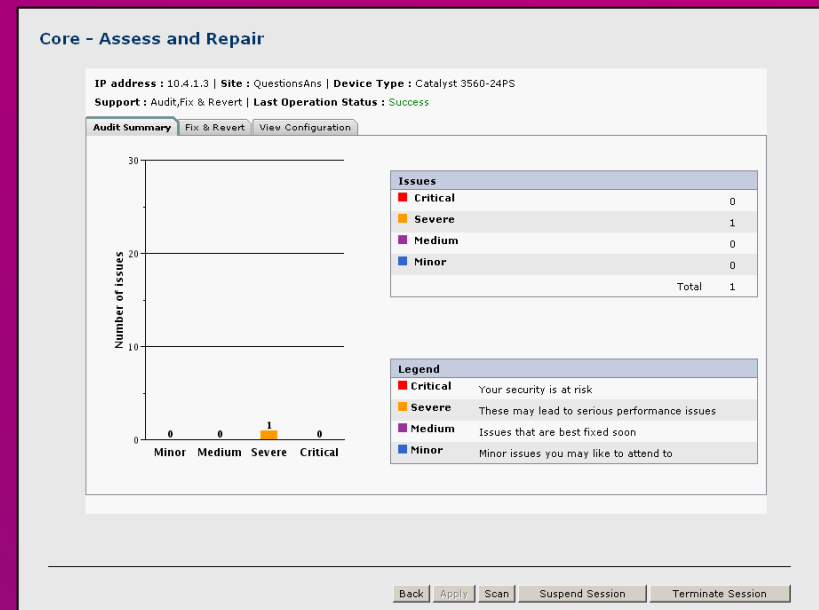
Proactive Notification per Device Items 1-8 of 8 | Rows per page: 10 | Go

Alert Status: Open Severity: All Type: All From: To: Go Clear

Device Type	IP Address	Device Name	Installed-At Site	Total Alerts	Based on Inventory	Chassis/Card	Alerts	Importance	Alert	Received	Alert Type	Action	Comments
Catalyst 37xx Stack	10.4.11.3	T4-MO-SW3750	SAN JOSE_3843893_1	8 (Open : 8)	09/08/2009 08:41:50	Chassis C3750	8	Critical	Security Notice [-] IntelliShield alerts Security alert 16040	07/31/2009 14:30:05	PSIRT	Open	-
								Important	Security Notice [-] IntelliShield alerts Security alert 15446	07/31/2009 14:30:05	PSIRT	Open	-
								Important	Security Notice [-] IntelliShield alerts Security alert 16638	07/31/2009 14:30:05	PSIRT	Open	-
								Important	Security Notice [-] IntelliShield alerts Security alert 16638	07/31/2009 14:30:05	PSIRT	Open	-
								Important	Security Notice [-] IntelliShield alerts Security alert 16638	07/31/2009 14:30:05	PSIRT	Open	-

Core Assessments

- Provide partners with analysis of primary configuration and operational parameters, including interface statistics and bandwidth analysis
- Run per device



- Issues categorised
- Click to fix
- Summary report available – “The Money Report”

Core - Assess and Repair

IP address : 10.4.1.3 | Site : QuestionsAns | Device Type : Catalyst 3560-24PS
Support : Audit,Fix & Revert | Last Operation Status : Success

Audit Summary | **Fix & Revert** | View Configuration

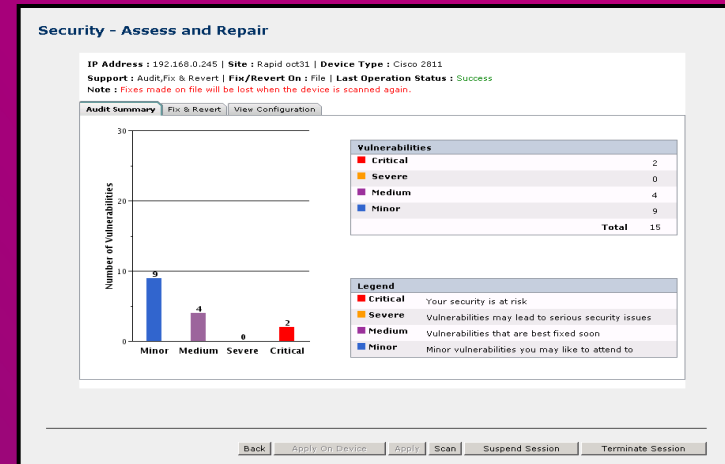
Severity	Issue	Sub Step	Description	CLI	Fix	Revert	Input
Severe	Buffer Misses	Very Big Buffer	Very Big Misses % refers to the percentage of vary big buffer misses. buffer verybig permanent 1771 big buffers have a buffer verybig min-free 442 buffer verybig max-free 2215 Bytes. Very Big Buffer tuning needs to be performed to reduce the ratio of misses to hits to less than 0.5%. Fixes made on the devices will not be effective immediately. Scanning the device immediately may still show the vulnerability as not fixed.		<input type="checkbox"/>	<input type="checkbox"/>	--

Write the running configuration to start up configuration

Back | Apply | Scan | Suspend Session | Terminate Session

Security Assessments

- Compares software configuration on each device with AS and NAS best practice
- Categorises errors
- Click to fix
- Option to review config changes and save to report format – “The Money Report”



Security - Assess and Repair

IP Address : 192.168.0.245 | Site : Rapid oct31 | Device Type : Cisco 2811
 Support : Audit,Fix & Revert | Fix/Revert On : File | Last Operation Status : Success
 Note : Fixes made on file will be lost when the device is scanned again.

Audit Summary | Fix & Revert | View Configuration

Severity	Vulnerability	Sub Step	Description	CLI	Fix	Revert	Input
Minor	Banner	Banner	Establish a warning banner to be displayed to users who try to log into the router. Use 'banner login in'		<input type="checkbox"/>	<input type="checkbox"/>	
Minor	CDP	CDP Global	Avoid releasing information about the router to directly-connected devices. Use 'no cdp enable' Disabling CDP may cause Voice outage.Fix this if necessary.		<input type="checkbox"/>	<input type="checkbox"/>	..
Medium	CDP	CDP Interface	Avoid releasing information about the router to directly-connected devices. Use 'no cdp running' Disabling CDP may cause Voice		<input type="checkbox"/>	<input type="checkbox"/>	..

Back | Apply On Device | Apply | Scan | Suspend Session | Terminate Session

Security - Assess and Repair

IP Address : 192.168.0.245 | Site : Rapid oct31 | Device Type : Cisco 2811
 Support : Audit,Fix & Revert | Fix/Revert On : File | Last Operation Status : Success
 Note : Fixes made on file will be lost when the device is scanned again.

Audit Summary | Fix & Revert | View Configuration

Original Configuration	Current Configuration
interface FastEthernet0/24 description B02_Data_192.168.22.0/24 encapsulation dot1Q 22 ip address 192.168.22.254 255.255.255.0	interface FastEthernet0/24 description B02_Data_192.168.22.0/24 encapsulation dot1Q 22 ip address 192.168.22.254 255.255.255.0 no cdp enable
interface FastEthernet0/0	interface FastEthernet0/0 no cdp enable
interface FastEthernet0/1	interface FastEthernet0/1 no cdp enable
interface FastEthernet0/2	interface FastEthernet0/2 no cdp enable
interface FastEthernet0/3	interface FastEthernet0/3 no cdp enable
interface Vlan1 no ip address	interface Vlan1 no ip address no cdp enable
router eigrp 1 network 10.1.1.0 0.0.0.255 network 192.168.0.240 0.0.0.7	router eigrp 1 network 10.1.1.0 0.0.0.255 network 192.168.0.240 0.0.0.7

Legend : Normal| Inserted Lines| Changed Lines| Deleted Lines

Back | Apply On Device | Apply | Scan | Suspend Session | Terminate Session

Voice Assessments and Monitoring

- **Presales:**
 - Allows partners to simulate voice traffic in a network over a period of time, monitor voice quality (MOS) and identify bottle necks
- **Post sales:**
 - Allow partners to continually monitor devices connected to Call Manager together with voice quality between segments

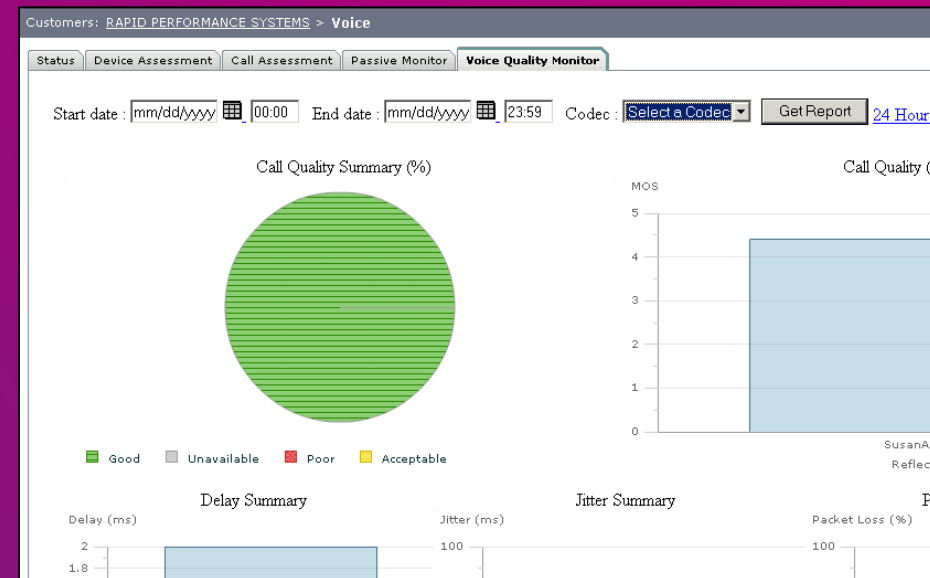
Customers: RAPID_PERFORMANCE_SYSTEMS > Voice

Status **Device Assessment** Call Assessment Passive Monitor Voice Quality Monitor

Device Assessment Items 1-2 of 2 | Rows per page: 10 | Go

Location ▲	Client Site	Device Type	IOS Version	QOS Enabled	Memory		Flash Memory		CPU Utilization
					Total	Free	Total	Free	
10.4.1.1	New Site	Cisco 2821	12.3(14)T7	✔ Yes	256	29%	61.25	24%	1%
10.4.3.1	New Site	Cisco 2821	E V 12.4(20060821:184334)	✔ Yes	256	44%	61.25	28%	-

Page 1 of 1



Configuration Backup Secure Remote Access and Restore

Partner also has access to:

- Backup configuration files locally
- Remote login (tunnel through the https connection) to devices on network. Can be used to restore configuration files
- Proactive monitoring using syslogs

Q & A

Samuli Kokki

samuli.kokki@cisco.com

+358 (0)40 7258 777