

Configurable device discovery based on SNMP

Slavko Gajin
Belgrade University Computer Centre, Serbia
slavko.gajin@rcub.bg.ac.rs

Introduction

- » Motivation
 - » To avoid manual initial configuration and update
- » Network device discovery
 - » Populates database with all network infrastructure data
 - » Keeps it up to date with periodic data updates
 - » Maintains an accurate overview of the network elements to support efficient network operation and planning
- » Asset Inventory Management
 - » Accurate inventory of all the hardware and software assets in an organization
- » Core of network management system
- » “To Know What We Have, Where It Is and How It Is Used”

Network device discovery

- » Discover network devices by IP addresses
 - » Brut scan IP address range (ping, snmp)
- » Discover network devices, topology and IP address space
 - » Start with the seed router and go through the network topology hop-by-hop
 - » Use next-hop from routing table
 - » Scan sub-networks on each interface and find connected routers
 - » Use CDP or LLDP
 - » Discover L3 network topology
 - » Discover IP address space – subnets on each interface
- » Discover network devices by MAC addresses - per LAN/VLAN
 - » Inspect ARP table on each router interface
 - » Pair IP and MAC addresses
 - » Find switches on the LAN
 - » Analyze forwarding tables on the switches
 - » Be aware of DHCP pools in the network
 - » Discover L2 network topology (**forwarding tables, STP**)

Discover devices and its components

- » Detect device type
 - » router, switch, UPS, host (Linux, Windows...)
- » Detect device vendor
- » Detect device model
- » Detect device resources (attributes)
 - » System name, model, serial number
- » Detect device components and their resources
 - » Interfaces
 - » Physical entities - modules, cards, CPU, memory...
 - » Logical entities – storage partitions, virtual memory, routing tables, connected users, BGP peers, QoS policies etc.
 - » Software components – installed software, running processes...
- » Using SNMP
 - » from CLI
 - » from MIB browsers
 - » from program code using snmp libraries

Using SNMP - CLI

- » snmpwalk command

- » `snmpwalk -v 2c -c public 10.10.10.1`

```
snmpwalk -v 2c -c xxxxx 147.91.x.x | more

SNMPv2-MIB::sysDescr.0 = STRING: amres-core-J
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.2636.1.1.1.2.25
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (200792781) 23 days, 5:45:27.81
SNMPv2-MIB::sysContact.0 = STRING: helpdesk@rcub.bg.ac.rs
SNMPv2-MIB::sysName.0 = STRING: amres-core-J-re0
SNMPv2-MIB::sysLocation.0 = STRING: Racunarski centar Univerziteta u Beogradu
(AMRES)
SNMPv2-MIB::sysServices.0 = INTEGER: 4
IF-MIB::ifNumber.0 = INTEGER: 144
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
.....
```

- » lot of typing, lot of texts, impractical ☹

Using SNMP – MIB browsers

- ❖ Navigation through MIB tree
- ❖ Inspect OID
- ❖ Choose a device and community
- ❖ Show retrieved results as a list and table
- ❖ Example:
 - ❖ ICmyNet.MIB, module in ICmyNet framework (www.icmynet.com)

The screenshot shows the ICmyNet MIB browser interface. The top navigation bar includes tabs for MultiLog, MIB (which is selected), Flow, NMS, and Alarm. On the right, there's a user name 'Gajin, Slavko (gaja)' and a gear icon. The main window has a title bar 'ospfAreaAggregateTable < private < hrSystem < hrDeviceTable < hrStorageTable < liftable < system' with a 'Refresh' button. Below this is a table titled 'amres-core-L' with columns 'oid' and 'value'. The table contains several rows of system information. To the left of the table is a 'MIB Tree' sidebar with sections like Request, Search, and Favorites. Under 'Favorites', there's a 'Snmp reports' section with a 'Details' dropdown set to 'Identifier'. Below this are fields for Type (Identifier), Name (system), OID (.1.3.6.1.2.1.1), Status (current), and Description.

oid	value
sysDescr.0	Cisco IOS Software, s72033_rp Software (s72033_rp-ADVISORIESK9_WAN-M), Version 12.2(33)SXI5, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Sat 23-Oct-10 01:30 by pr
sysObjectID.0	.1.3.6.1.4.1.9.1.283
sysUpTime.0	23 days, 2:52:52.27
sysContact.0	helpdesk@rcub.bg.ac.rs
sysName.0	amres-core-L
sysLocation.0	Racunarski centar Univerziteta u Beogradu (AMRES)
sysServices.0	78
sysORLastChange.0	0:00:00.00

Standard MIBs

- » System (.1.3.6.1.2.1.1)
 - » Name, description, uptime

oid	value
sysDescr.0	Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SXI5, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Sat 23-Oct-10 01:30 by pr
sysObjectID.0	.1.3.6.1.4.1.9.1.283
sysUpTime.0	23 days, 2:52:27
sysContact.0	helpdesk@rcub.bg.ac.rs
sysName.0	amres-core-L
sysLocation.0	Racunarski centar Univerziteta u Beogradu (AMRES)
sysServices.0	78
sysORLastChange.0	0:00:00.00

Standard MIBs

» Interfaces (IF-MIB)

» IfTable (.1.3.6.1.2.1.2.2), IfXTable (.1.3.6.1.2.1.31.1)

index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts
.1	1	GigabitEthernet1/1	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d0	up(1)	up(1)	0:02:17.64	268398712	3626853429
.2	2	GigabitEthernet1/2	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d1	up(1)	up(1)	0:02:17.65	979263437	784822926
.3	3	GigabitEthernet1/3	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d2	up(1)	up(1)	0:02:17.65	2969258870	473057745
.4	4	GigabitEthernet1/4	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d3	up(1)	down(2)	0:02:14.58	0	0
.5	5	GigabitEthernet1/5	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	11 days, 15:52:23.96	33911862	188971807
.6	6	GigabitEthernet1/6	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d5	up(1)	up(1)	10 days, 2:41:55.62	4273989957	3087463275
.7	7	GigabitEthernet1/7	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d6	up(1)	up(1)	0:02:18.28	77756231	1951538053
.8	8	GigabitEthernet1/8	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	0:02:15.28	3978073848	1785799626
.9	9	GigabitEthernet1/9	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	2 days, 0:38:50.17	3303904794	4214720187
.10	10	GigabitEthernet1/10	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	2 days, 0:38:50.24	3038651397	3797176523

index	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifHCInUcastPkts	ifAlias
.1	Gi1/1	38120707	71355372	38742653	1996410	10226790777446	16512086470	Etherchannel, veza prva (1 Gbps, Trunk)
.2	Gi1/2	1380607	293544	19723159	34429025	396133179097	784839690	Poljoprivredni fakultet (1 Gbps, trunk)
.3	Gi1/3	4668644	6653273	19409364	34209167	217717706023	473057747	Nis (1 Gbps po SDH, trunk)
.4	Gi1/4	0	0	0	0	0	0	
.5	Gi1/5	11006412	1054404	37059	908486	64458837241	188974249	Bogoslovske fakultet (1 Gbps, routed)
.6	Gi1/6	4798257	85288	12990370	33716209	11554164229074	20268349668	Optika ka Velikoj Plani
.7	Gi1/7	3122770	26	16138071	34208780	1082514214642	1951642757	FON (1Gbps, Trunk)
.8	Gi1/8	254674	2	251409	4	1155114065664	1785869535	Narodna biblioteka Srbije
.9	Gi1/9	518076	1671	37053	6	16097221788428	17100341783	Etherchannel 1 prema amres-core-J
.10	Gi1/10	0	1	574757	1	15680226210699	16682769384	Etherchannel 2 prema amres-core-J

Standard MIBs

» Entity (ENTITY-MIB)

» Physical entity - entPhysicalTable (.1.3.6.1.2.1.47.1.1.1)

index	entPhysicalIndex	entPhysicalDescr	entPhysicalVendorType	entPhysicalContainedIn	entPhysicalClass	entPhysicalParentRelPos	entPhysicalName
.1		Cisco Systems Catalyst 6500 9-slot Chassis System	.1.3.6.1.4.1.9.12.3.1.3.144	0	chassis(3)	-1	WS-C6509
.2		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	1	Physical Slot 1
.3		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	2	Physical Slot 2
.4		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	3	Physical Slot 3
.5		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	4	Physical Slot 4
.6		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	5	Physical Slot 5
.7		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	6	Physical Slot 6
.8		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	7	Physical Slot 7
.9		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	8	Physical Slot 8
.10		Cisco Systems Catalyst 6500 9-slot Physical Slot	.1.3.6.1.4.1.9.12.3.1.5.1	1	container(5)	9	Physical Slot 9
.11		Cisco Systems Catalyst 6500 9-slot backplane	.1.3.6.1.4.1.9.12.3.1.4.14	1	backplane(4)	1	Backplane
.12		PS 1 Absent High Power Usage Sensor	.1.3.6.1.4.1.9.12.3.1.8.40	11	sensor(8)	3	PS 1 Absent High Power Usage Sensor
.13		fan-tray 1 fan-fail Sensor	.1.3.6.1.4.1.9.12.3.1.8.37	11	sensor(8)	4	fan-tray 1 fan-fail Sensor
.14		Container of Fan FRU	.1.3.6.1.4.1.9.12.3.1.5.139	1	container(5)	10	Container of Fan FRU 1
.15		Chassis fan-tray 1	.1.3.6.1.4.1.9.12.3.1.7.50	14	fan(7)	1	Fan-tray 1
.16		Container of Container of Power Supply	.1.3.6.1.4.1.9.12.3.1.5.140	1	container(5)	11	Container of Container of Power Supply
.17		Container of Power Supply 1	.1.3.6.1.4.1.9.12.3.1.5.141	16	container(5)	1	Container of Power Supply 1
.18		110/220v AC power supply, 2500 watt 1	.1.3.6.1.4.1.9.12.3.1.6.24	17	powerSupply(6)	1	PS 1 WS-CAC-2500W
.19		power-supply 1 fan-fail Sensor	.1.3.6.1.4.1.9.12.3.1.8.38	18	sensor(8)	1	power-supply 1 fan-fail Sensor
.20		power-supply 1 power-output-fail Sensor	.1.3.6.1.4.1.9.12.3.1.8.39	18	sensor(8)	2	power-supply 1 power-output-fail Sensor

» Logical entity - entLogicalTable (.1.3.6.1.2.1.47.1.2.1)

index	entLogicalIndex	entLogicalDescr	entLogicalType	entLogicalCommunity	entLogicalTAddress	entLogicalTDomain	entLogicalContextEngineID	entLogical
.1		vlan1	1.3.6.1.2.1.17		93:5b:00:70:00:a1	1.3.6.1.6.1.1	80:00:00:09:03:00:00:0e:84:da:13:d0	vlan-1
.2		vlan1800	1.3.6.1.2.1.17		93:5b:00:70:00:a1	1.3.6.1.6.1.1	80:00:00:09:03:00:00:0e:84:da:13:d0	vlan-1800
.3		vlan1801	1.3.6.1.2.1.17		93:5b:00:70:00:a1	1.3.6.1.6.1.1	80:00:00:09:03:00:00:0e:84:da:13:d0	vlan-1801
.4		vlan1806	1.3.6.1.2.1.17		93:5b:00:70:00:a1	1.3.6.1.6.1.1	80:00:00:09:03:00:00:0e:84:da:13:d0	vlan-1806
.5		vlan1807	1.3.6.1.2.1.17		93:5b:00:70:00:a1	1.3.6.1.6.1.1	80:00:00:09:03:00:00:0e:84:da:13:d0	vlan-1807

Standard MIBs

» IP (IP-MIB)

- » ipAddrTable (.1.3.6.1.2.1.4.20) – used IP addresses

index	ipAdEntAddr	ipAdEntIfIndex	ipAdEntNetMask	ipAdEntBcastAddr	ipAdEntReasmMaxSize
.91.187.146.17	91.187.146.17	123	255.255.255.248		18024
.91.187.146.65	91.187.146.65	401	255.255.255.240		18024
.91.187.158.1	91.187.158.1	354	255.255.254.0		18024
.91.187.158.6	91.187.158.6	354	255.255.254.0		18024
.127.0.0.51	127.0.0.51	88	255.0.0.0		18024

- » ipRouteTable (.1.3.6.1.2.1.4.21) – Routing table

index	ipRouteDest	ipRouteIfIndex	ipRouteMetric1	ipRouteMetric2	ipRouteMetric3	ipRouteMetric4	ipRouteNextHop	ipRouteType	ipRouteProto
.0.0.0.0	0.0.0.0	326	0	-1	-1	-1	147.91.6.90	indirect(4)	ospf(13)
.10.8.0.0	10.8.0.0	29	21	-1	-1	-1	147.91.6.81	indirect(4)	ospf(13)
.10.15.0.0	10.15.0.0	0	0	-1	-1	-1	147.91.7.79	indirect(4)	local(2)
.91.187.128.0	91.187.128.0	90	2	-1	-1	-1	147.91.7.106	indirect(4)	ospf(13)
.91.187.128.128	91.187.128.128	90	2	-1	-1	-1	147.91.7.106	indirect(4)	ospf(13)
.91.187.129.0	91.187.129.0	90	2	-1	-1	-1	147.91.7.106	indirect(4)	ospf(13)
.91.187.130.0	91.187.130.0	90	2	-1	-1	-1	147.91.7.107	indirect(4)	ospf(13)

- » ipNetToMediaTable (.1.3.6.1.2.1.4.21), atTable .1.3.6.1.2.1.3.1 (ARP)

index	ipNetToMediaIfIndex	ipNetToMediaPhysAddress	ipNetToMediaNetAddress	ipNetToMediaType
.5.147.91.220.1	5	00:0e:39:ed:1c:00	147.91.220.1	static(4)
.5.147.91.220.2	5	00:15:77:6a:20:00	147.91.220.2	dynamic(3)
.5.147.91.220.3	5	00:22:68:59:68:3e	147.91.220.3	dynamic(3)
.5.147.91.220.27	5	00:20:18:a0:5f:4c	147.91.220.27	dynamic(3)
5.147.91.220.27	5	00:20:18:a0:5f:4c	147.91.220.27	dynamic(3)

Standard MIBs

- » ICMP (IP-MIB)
 - » icmpStatsTable (.1.3.6.1.2.1.5.29) – statistics of ICMP packets
- » UDP (UDP-MIB)
 - » udpTable (.1.3.6.1.2.1.7.5)

oid	value
icmpInMsgs.0	15069277
icmpInErrors.0	3423
icmpInDestUnreachs.0	59449
icmpInTimeExcds.0	8748
icmpInParmProbs.0	0
icmpInSrcQuenches.0	3
icmpInRedirects.0	1015336
icmpInEchos.0	13977548
icmpInEchoReps.0	167
icmpInTimestamps.0	1
icmpInTimestampReps.0	1
icmpInAddrMasks.0	0
icmpInAddrMaskReps.0	1
icmpOutMsgs.0	37127346
icmpOutErrors.0	0
icmpOutDestUnreachs.0	20217369
icmpOutTimeExcds.0	2933256
icmpOutParmProbs.0	0
icmpOutSrcQuenches.0	0
icmpOutRedirects.0	140
icmpOutEchos.0	214
icmpOutEchoReps.0	13977549

oid	value
udpInDatagrams.0	5498291
udpNoPorts.0	1144158
udpInErrors.0	5
udpOutDatagrams.0	461894451

index	udpLocalAddress	udpLocalPort
.147.91.0.112.123	147.91.0.112	123
.147.91.0.112.161	147.91.0.112	161
.147.91.0.112.162	147.91.0.112	162
.147.91.0.112.1645	147.91.0.112	1645
.147.91.0.112.1646	147.91.0.112	1646
.147.91.0.112.1698	147.91.0.112	1698
.147.91.0.112.2228	147.91.0.112	2228
.147.91.0.112.52996	147.91.0.112	52996
.147.91.0.112.59527	147.91.0.112	59527
.147.91.0.112.64805	147.91.0.112	64805
.147.91.4.161.67	147.91.4.161	67
.147.91.7.65.58343	147.91.7.65	58343
.147.91.7.65.58464	147.91.7.65	58464
.147.91.7.65.64700	147.91.7.65	64700
.224.0.1.40.496	224.0.1.40	496

Standard MIBs

- » TCP (TCP-MIB)
 - » tcpConnTable (.1.3.6.1.2.1.6.13)

oid	value
tcpRtoAlgorithm.0	vani(4)
tcpRtoMin.0	300
tcpRtoMax.0	60000
tcpMaxConn.0	-1
tcpActiveOpens.0	648
tcpPassiveOpens.0	58
tcpAttemptFails.0	0
tcpEstabResets.0	35
tcpCurrEstab.0	3
tcpInSegs.0	10984811
tcpOutSegs.0	10236300
tcpRetransSegs.0	620

index	tcpConnState	tcpConnLocalAddress	tcpConnLocalPort	tcpConnRemAddress	tcpConnRemPort
.147.91.0.112.52387.147.91.0.127.639	established(5)	147.91.0.112	52387	147.91.0.127	639
.147.91.0.112.57067.147.91.201.228.639	established(5)	147.91.0.112	57067	147.91.201.228	639
.147.91.0.112.62776.147.91.0.124.639	established(5)	147.91.0.112	62776	147.91.0.124	639

Device type specific MIBs

- » How to recognize device type?
 - » Discovery test – retrieve values unique to the specific device type
- » Routers
 - » Discovery test - How to recognize a router?
 - » Routing table? Hosts also have a routing table...
 - » **sysServices** (.1.3.6.1.2.1.1.7)
 - » bit position indicates OSI/TCP layer
 - » Example: 6 (dec) = 0110 (bin) – **Layer 3** and Layer 2 (L3 switch)
 - » **ipForwarding** (.1.3.6.1.2.1.4.1) in IP-MIB
 - » forwarding(1) – for routing capable devices
 - » not-forwarding(2) – for all other devices



oid	value
ipForwarding.0	Forwarding(1)
ipDefaultTTL.0	255
ipInReceives.0	3429105075
ipInHdrErrors.0	3753432
ipInAddrErrors.0	10086063
ipForwDatagrams.0	1138136864
ipInUnknownProtos.0	0
ipInDiscards.0	0
ipInDelivers.0	48091139
ipOutRequests.0	521372392
ipOutDiscards.0	19525055
ipOutNoRoutes.0	681
ipReasmTimeout.0	30

Device type specific MIBs - Routers

- ❖ BGP protocol (BPG4-MIB)
 - ❖ `bgpPeerTable (.1.3.6.1.2.1.15.3)`

index	.0.0.0.0	.62.40.125.177	.82.117.193.109	.147.91.6.190	.147.91.6.214	.160.99.1.12	.195.111.106.254
bgpPeerIdentifier	195.111.97.66	62.40.97.1	89.216.7.253	147.91.0.139	78.28.128.1	160.99.1.12	195.111.97.66
bgpPeerState	established(6)	established(6)	established(6)	established(6)	established(6)	established(6)	established(6)
bgpPeerAdminStatus	start(2)	start(2)	start(2)	start(2)	start(2)	start(2)	start(2)
bgpPeerNegotiatedVersion	4	4	4	4	4	4	4
bgpPeerLocalAddr	0.0.0.0	62.40.125.178	82.117.193.110	147.91.6.189	147.91.6.213	147.91.0.127	195.111.106.253
bgpPeerLocalPort	49591	56647	179	59540	56115	56544	179
bgpPeerRemoteAddr	0.0.0.0	62.40.125.177	82.117.193.109	147.91.6.190	147.91.6.214	160.99.1.12	195.111.106.254
bgpPeerRemotePort	179	179	31912	179	179	179	52243
bgpPeerRemoteAs	1955	20965	31042	6701	43752	13303	1955
bgpPeerInUpdates	320582	1660325	387	206797	8	3	2451507
bgpPeerOutUpdates	4	28	15	28	34	9	24
bgpPeerInTotalMessages	375231	1694800	39704	271326	66428	66781	2453324
bgpPeerOutTotalMessages	73039	36089	42833	63644	72288	72615	73059
bgpPeerLastError	00:00	06:06	04:00	04:00	04:00	04:00	06:07
bgpPeerFsmEstablishedTransitions	1	382	3	3	8	3	1
bgpPeerFsmEstablishedTime	2015365	611221	1181526	1755202	394247	211749	2015370
bgpPeerConnectRetryInterval	32	32	32	32	32	32	32
bgpPeerHoldTime	90	90	90	90	90	90	90

Device type specific MIBs - Routers

↳ OSPF protocol (OSPF-MIB)

↳ ospfAreaTable (.1.3.6.1.2.1.14.2), ospfLsdbTabl (.1.3.6.1.2.1.14.4)

index	.0.0.0	.147.91.1.0	.147.91.3.0
ospfAreaId	0.0.0.0	147.91.1.0	147.91.3.0
ospfAuthType	0	0	0
ospfImportAsExtern	1	2	2
ospfSpfRuns	640	51	52
ospfAreaBdrRtrCount	28	1	1
ospfAsBdrRtrCount	12	0	0
ospfAreaLsaCount	291	2	2
ospfAreaLsaCksumSum	9836984	16543	26147
ospfAreaSummary	2	1	1
ospfAreaStatus	active(1)	active(1)	active(1)

index	.91.187.158.6.0	.147.91.0.57.0	.147.91.0.112.0
ospfIfIpAddress	91.187.158.6	147.91.0.57	147.91.0.112
ospfAddressLessIf	0	0	0
ospfIfAreaId	0.0.0.0	0.0.0.0	0.0.0.0
ospfIfType	1	3	3
ospfIfAdminStat	1	1	1
ospfIfRtrPriority	1	0	0
ospfIfTransitDelay	1	1	1
ospfIfRetransInterval	5	5	5
ospfIfHelloInterval	10	10	10
ospfIfRtrDeadInterval	40	40	40
ospfIfPollInterval	120	120	120
ospfIfState	5	2	2
ospfIfDesignatedRouter	91.187.158.6	0.0.0.0	0.0.0.0
ospfIfBackupDesignatedRouter	0.0.0.0	0.0.0.0	0.0.0.0
ospfIfEvents	2	1	1
ospfIfAuthKey			
ospfIfStatus	active(1)	active(1)	active(1)
ospfIfMulticastForwarding	1	1	1

Device type specific MIBs - Routers

- » MPLS (MPLS-LSR-MIB, MPLS-VPN-MIB)
 - » mplsInSegmentTable (.1.3.6.1.3.96.1.3)
 - » mplsOutSegmentTable (.1.3.6.1.3.96.1.6)

TEST PE						
index	.0.0	.0.1	.0.2	.0.3	.0.13	.0.17
mplsInSegmentIfIndex						
mplsInSegmentLabel						
mplsInSegmentNPop	1	1	1	1	1	1
mplsInSegmentAddrFamily	ipV4(1)	ipV4(1)	ipV4(1)	ipV4(1)	ipV4(1)	ipV4(1)
mplsInSegmentXCIIndex	1	513	1025	1537	6657	8705
mplsInSegmentOwner	other(1)	other(1)	other(1)	other(1)	other(1)	other(1)
mplsInSegmentTrafficParamPtr	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0
mplsInSegmentRowStatus	active(1)	active(1)	active(1)	active(1)	active(1)	active(1)
mplsInSegmentStorageType	volatile(2)	volatile(2)	volatile(2)	volatile(2)	volatile(2)	volatile(2)
mplsInSegmentAdminStatus	up(1)	up(1)	up(1)	up(1)	up(1)	up(1)
mplsInSegmentOperStatus	up(1)	up(1)	up(1)	up(1)	up(1)	up(1)

TEST PE						
index	.0.0	.0.1	.0.2	.0.3	.0.13	C
mplsInSegmentOctets	0	0	0	0	0	
mplsInSegmentPackets	0	0	0	0	0	
mplsInSegmentErrors	0	0	0	0	0	
mplsInSegmentDiscards	0	0	0	0	0	
mplsInSegmentHCOctets	0	0	0	0	0	
mplsInSegmentPerfDiscontinuityTime	0:00:00.00	0:00:00.00	0:00:00.00	0:00:00.00	0:00:00.00	C

mplsVpnVrfTable (.1.3.6.1.3.118.1.2.2)

BG-PE							Pivot	Refresh
index		mplsVpnVrfName	mplsVpnVrfDescription	mplsVpnVrfRouteDistinguisher	mplsVpnVrfCreationTime	mplsVpnVrfC		
	.5.83.65.51.84.51		SA3T3 - probni VRF		1:1		0:00:12.50	
	.7.83.65.51.84.51.95.65		SA3T3_A		13092:17		0:00:12.51	
	.7.86.80.78.45.66.73.79		VPN-BIO		10.130.24.240:32		0:00:12.51	
	.8.80.105.110.103.45.86.80.78		Ping-VPN		147.91.0.117:12321		0:00:12.50	
	.9.86.80.78.45.65.83.84.82.79		VPN-ASTRO		10.130.22.220:30		0:00:12.51	
	.10.102.111.114.119.97.114.100.105.110.103						0:00:12.51	

Device type specific MIBs - Switches

- » BRIDGE-MIB
- » Discovery test
 - » dot1dBaseBridgeAddress (.1.3.6.1.2.1.17.1.1)
- » dot1dBasePortTable (.1.3.6.1.2.1.17.1.4)
 - » pairing switching ports with interfaces (ifTable)

index	.1	.2	.3	.4	.6	.7	.12	.130	.131	.132	.134	.136	.137	.138	.140	.142	.143	.267	.276	.280	.282
dot1dBasePort	1	2	3	4	6	7	12	130	131	132	134	136	137	138	140	142	143	267	276	280	282
dot1dBasePortIfIndex	1	2	3	4	6	7	12	18	19	20	22	24	25	26	28	30	31	43	52	56	58
dot1dBasePortCircuit	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0	.0.0
dot1dBasePortDelayExceededDiscards	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
dot1dBasePortMtuExceededDiscards	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

- » dot1dTpFdbTable (.1.3.6.1.2.1.17.4.3)
 - » MAC switching table (CAM)

Device type specific MIBs - Switches

- dot1dStp (.1.3.6.1.2.1.17.2)

- STP info

- dot1dStpPortTable (.1.3.6.1.2.1.17.2.15)

- STP port status

oid	value
dot1dStpProtocolSpecification.0	unknown(1)
dot1dStpPriority.0	24577
dot1dStpTimeSinceTopologyChange.0	0:02:10.00
dot1dStpTopChanges.0	16384
dot1dStpDesignatedRoot.0	60:01:00:0e:39:ed:1c:00
dot1dStpRootCost.0	0
dot1dStpRootPort.0	0
dot1dStpMaxAge.0	2000
dot1dStpHelloTime.0	200
dot1dStpHoldTime.0	100
dot1dStpForwardDelay.0	1500
dot1dStpBridgeMaxAge.0	2000
dot1dStpBridgeHelloTime.0	200
dot1dStpBridgeForwardDelay.0	1500

index	.1	.2	.3	.4
dot1dStpPort	1	2	3	4
dot1dStpPortPriority	128	128	128	128
dot1dStpPortState	forwarding(5)	forwarding(5)	forwarding(5)	disabled(1)
dot1dStpPortEnable	enabled(1)	enabled(1)	enabled(1)	enabled(1)
dot1dStpPortPathCost	4	4	4	4
dot1dStpPortDesignatedRoot	60:01:00:0e:39:ed:1c:00	60:01:00:0e:39:ed:1c:00	60:01:00:0e:39:ed:1c:00	00:00:00:00:00:00:00:00
dot1dStpPortDesignatedCost	0	0	0	0
dot1dStpPortDesignatedBridge	60:01:00:0e:39:ed:1c:00	60:01:00:0e:39:ed:1c:00	60:01:00:0e:39:ed:1c:00	00:00:00:00:00:00:00:00
dot1dStpPortDesignatedPort	80:01	80:02	80:03	00:00
dot1dStpPortForwardTransitions	1	1	32	0

Device type specific MIBs - Hosts

- ❖ HOST-RESOURCES-MIB
- ❖ Discovery test
 - ❖ hrSystem (.1.3.6.1.2.1.25.1)
 - ❖ these (.1.3.6.1.2.1.25.1.1), hrSystemDate (.1.3.6.1.2.1.25.1.2)
- ❖ hrStorageTable (.1.3.6.1.2.1.25.2.3)

index	hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageAllocationFailures
.1	1	.1.3.6.1.2.1.25.2.1.2	Physical memory	1024	2073340	1880032	
.3	3	.1.3.6.1.2.1.25.2.1.3	Virtual memory	1024	4113552	1880156	
.6	6	.1.3.6.1.2.1.25.2.1.1	Memory buffers	1024	2073340	66268	
.7	7	.1.3.6.1.2.1.25.2.1.1	Cached memory	1024	1134492	1134492	
.10	10	.1.3.6.1.2.1.25.2.1.3	Swap space	1024	2040212	124	
.31	31	.1.3.6.1.2.1.25.2.1.4	/	4096	38933554	17421994	0
.35	35	.1.3.6.1.2.1.25.2.1.4	/boot	1024	101086	33859	0
.36	36	.1.3.6.1.2.1.25.2.1.4	/dev/shm	4096	259167	0	0
.37	37	.1.3.6.1.2.1.25.2.1.4	/home	4096	29971485	22323480	0

Device type specific MIBs - Hosts

» hrDeviceTable (.1.3.6.1.2.1.25.3.2)

index	hrDeviceIndex	hrDeviceType	hrDeviceDescr	hrDeviceID	hrDeviceStatus	hrDeviceErrors
.768	768	.1.3.6.1.2.1.25.3.1.3	GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	.0.0		
.769	769	.1.3.6.1.2.1.25.3.1.3	GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	.0.0		
.1025	1025	.1.3.6.1.2.1.25.3.1.4	network interface lo	.0.0	running(2)	0
.1026	1026	.1.3.6.1.2.1.25.3.1.4	network interface eth0	.0.0	running(2)	0
.1027	1027	.1.3.6.1.2.1.25.3.1.4	network interface eth1	.0.0	down(5)	0
.1028	1028	.1.3.6.1.2.1.25.3.1.4	network interface sit0	.0.0	down(5)	0
.1536	1536	.1.3.6.1.2.1.25.3.1.6	PHILIPS DVD-ROM SDR089	.0.0		
.3072	3072	.1.3.6.1.2.1.25.3.1.12	Guessing that there's a floating point co-processor	.0.0		

» hrProcessorTable (.1.3.6.1.2.1.25.3.3)

index	hrProcessorFwID	hrProcessorLoad
.768	.0.0	9
.769	.0.0	4

Vendors specific MIBs

- » private.enterprises (.1.3.6.1.4.1) subtree
 - » cisco (.1.3.6.1.4.1.9)
 - » apc (.1.3.6.1.4.1.318)
 - » microsoft (.1.3.6.1.4.1.311)
 - » juniperMIB (.1.3.6.1.4.1.2636)
 - » vmware (.1.3.6.1.4.1.6876)
 - » ...
- » Device model discovery
 - » Standard OID sysObjectID (.1.3.6.1.2.1.1.2)
 - » returns vendor specific OID which defines device model
 - » Example:
 - » sysObjectID = .1.3.6.1.4.1.9.1.283
 - » CISCO-PRODUCTS-MIB (.1.3.6.1.4.1.9.1)
 - » OID .1.3.6.1.4.1.9.1.283
 - » type: Identifier
 - » name: **Cat6509**
 - » returns no date

SNMP Report – Standard table

- » Standard table – Storage on the host
- » Problems:
 - » Size and Used space is given in special allocation unit (last column)
 - » Can be different – 1024, 4096
 - » How many MB we have?
 - » How many free space we have?
 - » in GB
 - » in %

index	hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageAllocationFailures
.1	1	.1.3.6.1.2.1.25.2.1.2	Physical memory	1024	2073340	1880032	
.3	3	.1.3.6.1.2.1.25.2.1.3	Virtual memory	1024	4113552	1880156	
.6	6	.1.3.6.1.2.1.25.2.1.1	Memory buffers	1024	2073340	66268	
.7	7	.1.3.6.1.2.1.25.2.1.1	Cached memory	1024	1134492	1134492	
.10	10	.1.3.6.1.2.1.25.2.1.3	Swap space	1024	2040212	124	
.31	31	.1.3.6.1.2.1.25.2.1.4	/	4096	38933554	17421994	0
.35	35	.1.3.6.1.2.1.25.2.1.4	/boot	1024	101086	33859	0
.36	36	.1.3.6.1.2.1.25.2.1.4	/dev/shm	4096	259167	0	0
.37	37	.1.3.6.1.2.1.25.2.1.4	/home	4096	29971485	22323480	0

SNMP Report - Composite column

- Choose only columns of interest
- Adding advanced composite column

The screenshot shows a list of SNMP objects on the left and a configuration panel on the right.

Left Panel (Available Columns):

- hrStorageDescr
- hrStorageAllocationUnits
- hrStorageSize
- hrStorageUsed
- hrStorageFree

Right Panel (Composite Column Configuration):

Name: hrStorageFree

hrStorageSize Choose -

hrStorageUsed Choose -

Buttons: + + 0

A yellow box highlights the "hrStorageFree" configuration area. A large blue arrow points from the configuration panel down to the resulting table below.

hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageFree
Swap space	1024	2040212	132	2040080
Physical memory	1024	2073340	2019196	54144
Virtual memory	1024	4113552	2019328	2094224
Memory buffers	1024	2073340	29244	2044096
Cached memory	1024	1253172	1253172	0
/	4096	38933554	17426377	21507177
/boot	1024	101086	33859	67227
/dev/shm	4096	259167	0	259167
/home	4096	29971485	22323567	7647918

SNMP Report - Composite column

- Free size in MB = (Size-Used)*AllocationUnit/1000000
- Free size in Perc =100*(Size-Used)/Size

Two composite column definitions are shown:

hrStorageFreeMB (Left):
Name: hrStorageFreeMB
(
hrStorageSize Choose -
- +
hrStorageUsed Choose -
+ - 0 + 0
)
* /
hrStorageAllocationUnits Choose -
/ +
1000000 Choose -

hrStorageFreePerc (Right):
Name: hrStorageFreePerc
100 Choose -
* /
(
hrStorageSize Choose -
- +
hrStorageUsed Choose -
+ - 0 + 0
)
/ /
hrStorageSize Choose -

hrStorageDescr	hrStorageFreeMB	hrStorageFreePerc
Swap space	2089	99.99
Physical memory	55	2.61
Virtual memory	2144	50.91
Memory buffers	2093	98.59
Cached memory	0	0.00
/	88093	55.24
/boot	69	66.50
/dev/shm	1062	100.00
/home	31326	25.52

24-25.4.20

SNMP Report – Multiple tables

- » To configure your own SNMP output
- » Choose only columns of interest
- » Combine data from different tables (example: ifTable, ifXTable)

index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts
.1	1	GigabitEthernet1/1	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d0	up(1)	up(1)	0:02:17.64	268398712	3626853429
.2	2	GigabitEthernet1/2	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d1	up(1)	up(1)	0:02:17.65	979263437	784822926
.3	3	GigabitEthernet1/3	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d2	up(1)	up(1)	0:02:17.65	2969258870	473057745
.4	4	GigabitEthernet1/4	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d3	up(1)	down(2)	0:02:14.58	0	0
.5	5	GigabitEthernet1/5	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	11 days, 15:52:23.96	33911862	188971807
.6	6	GigabitEthernet1/6	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d5	up(1)	up(1)	10 days, 2:41:55.62	4273989957	3087463275
.7	7	GigabitEthernet1/7	ethernet-csmacd(6)	1500	10000000000	00:0e:84:da:13:d6	up(1)	up(1)	0:02:18.28	77756231	1951538053
.0	0	GigabitEthernet1/0	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	0:02:15.20	3970070040	1705799020
.9	9	GigabitEthernet1/9	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	2 days, 0:38:50.17	3303904794	4214720187
.10	10	GigabitEthernet1/10	ethernet-csmacd(6)	1500	10000000000	00:0e:39:ed:1c:00	up(1)	up(1)	2 days, 0:38:50.24	3038651397	3797176523

index	ifName	ifInMulticastPkts	ifInBroadcastPkts	ifOutMulticastPkts	ifOutBroadcastPkts	ifHCInOctets	ifHCInUcastPkts	ifAlias
.1	Gi1/1	38120707	71355372	38742653	1996410	10226790777446	16512086470	Etherchannel, veza prva (1 Gbps, Trunk)
.2	Gi1/2	1380607	293544	19723159	34429025	396133179097	784839690	Poljoprivredni fakultet (1 Gbps, trunk)
.3	Gi1/3	4668644	6653273	19409364	34209167	217717706023	473057747	Nis (1 Gbps po SDH, trunk)
.4	Gi1/4	0	0	0	0	0	0	
.5	Gi1/5	11006412	1054404	37059	908486	64458837241	188974249	Bogoslovski fakultet (1 Gbps, routed)
.6	Gi1/6	4798257	85288	12990370	33716209	11554164229074	20268349668	Optika ka Velikoj Plani
.7	Gi1/7	3122770	26	16138071	34208780	1082514214642	1951642757	FON (1Gbps, Trunk)
.8	Gi1/8	254674	2	251409	4	1155114065664	1785869535	Narodna biblioteka Srbije
.9	Gi1/9	518076	1671	37053	6	16097221788428	17100341783	Etherchannel 1 prema amres-core-3
.10	Gi1/10	0	1	574757	1	15680226210699	16682769384	Etherchannel 2 prema amres-core-3

SNMP Report – Multiple tables

- » Solution: joining SNMP table - similar to SQL join
 - » specify source tables
 - » specify join conditions - columns from the tables which are equal
 - » select columns to be shown in output table (ordered)
- » Example - Joining ifTable and ifXTable

Source tables:

ifTable	Choose	-
ifXTable	Choose	- +

Join conditions:

Condition	-					
ifIndex	Choose	+	=	ifTable	Choose	+

Add new condition

ifName	ifXTable	Operations
ifAlias	ifXTable	Operations
ifDescr	ifTable	Operations
ifPhysAddress	ifTable	Operations
ifSpeed	ifTable	Operations

+ Add column **+ Add advanced column**

SNMP Report – Multiple tables

- Joining ifTable and ifXTable – Resulting table

ifName	ifAlias	ifDescr	ifPhysAddress	ifSpeed	ifMtu
VLAN-29		unrouted VLAN 29	00:0e:39:ed:1c:1d	0	1500
VLAN-400		unrouted VLAN 400	00:0e:39:ed:1d:90	0	1500
Vl60	Decija klinika Tirsova (1 Gbps)	Vlan60	00:0e:39:ed:1c:00	1000000000	1500
VLAN-776		unrouted VLAN 776	00:0e:39:ed:1f:08	0	1500
Vl61	Institut za onkologiju i radiologiju	Vlan61	00:0e:39:ed:1c:00	1000000000	1500
Vl300	eduroam-cisco5608-L	Vlan300	00:0e:39:ed:1c:00	1000000000	1500
Vl160	Nis – Gigabit over SDH	Vlan160	00:0e:39:ed:1c:00	1000000000	1500
VLAN-410		unrouted VLAN 410	00:0e:39:ed:1d:9a	0	1500
Vl172	Novi Sad - Gigabit	Vlan172	00:0e:39:ed:1c:00	1000000000	1500
VLAN-70		unrouted VLAN 70	00:0e:39:ed:1c:46	0	1500

SNMP Report – Multiple tables

Joining ifTable, ifXTable and ipAddrTable

Source tables:

ifTable	Choose	-
ifXTable	Choose	-
ipAddrTable	Choose	- +

Join conditions:

Condition

ifTable	Choose	+	=	ifXTable	Choose	+
---------	--------	---	---	----------	--------	---

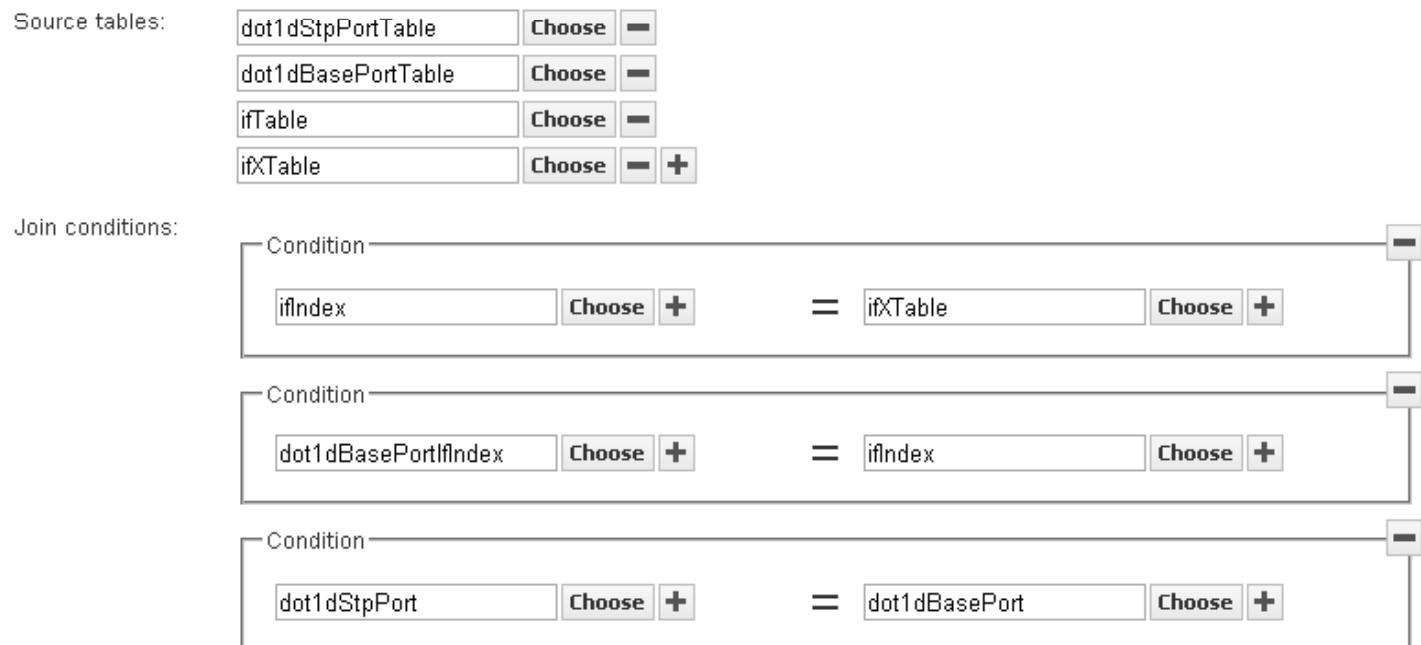
Condition

ifTable	Choose	+	=	ipAdEntIfIndex	Choose	+
---------	--------	---	---	----------------	--------	---

ifDescr	ifName	ipAdEntAddr	ipAdEntNetMask	ifPhysAddress
unrouted VLAN 29	VLAN-29	-	-	00:0e:39:ed:1c:1d
unrouted VLAN 400	VLAN-400	-	-	00:0e:39:ed:1d:90
Vlan60	VI60	147.91.126.1	255.255.255.0	00:0e:39:ed:1c:00
unrouted VLAN 776	VLAN-776	-	-	00:0e:39:ed:1f:08
Vlan61	VI61	147.91.198.7	255.255.255.128	00:0e:39:ed:1c:00
Vlan61	VI61	147.91.198.1	255.255.255.128	00:0e:39:ed:1c:00
Vlan300	VI300	91.187.168.1	255.255.254.0	00:0e:39:ed:1c:00
Vlan300	VI300	91.187.168.6	255.255.254.0	00:0e:39:ed:1c:00
Vlan160	VI160	147.91.6.253	255.255.255.252	00:0e:39:ed:1c:00
unrouted VLAN 410	VLAN-410	-	-	00:0e:39:ed:1d:9a
Vlan172	VI172	147.91.5.157	255.255.255.252	00:0e:39:ed:1c:00

SNMP Report – Multiple tables

- Joining 4 tables with different indexes
 - Interface and SPT information



ifName	ifAlias	ifAdminStatus	ifOperStatus	dot1dStpPortState	ifPhysAddress	ifSpeed
Fa3/20	cisco-wlc-L-service-port	1	2	1	00:01:63:d4:c5:ed	1000000000
Gi5/1	veza ka cisco5508-L kontroleru	1	1	5	00:0e:83:15:ed:50	1000000000
Gi1/12	Farmacija (1 Gbps, Trunk)	1	1	5	00:0e:84:da:13:db	1000000000
Fa3/24	Veza ka cisco2950-ucionica port TO-143	1	2	1	00:01:63:d4:c5:f1	1000000000
Fa3/26	cisco-wlc-R-service-port	1	2	1	00:01:63:d4:c5:f3	1000000000
Gi1/1	Etherchannel, veza prva (1 Gbps, Trunk)	1	1	5	00:0e:84:da:13:d0	1000000000
Gi1/2	Poljoprivredni fakultet (1 Gbps, trunk)	1	1	5	00:0e:84:da:13:d1	1000000000

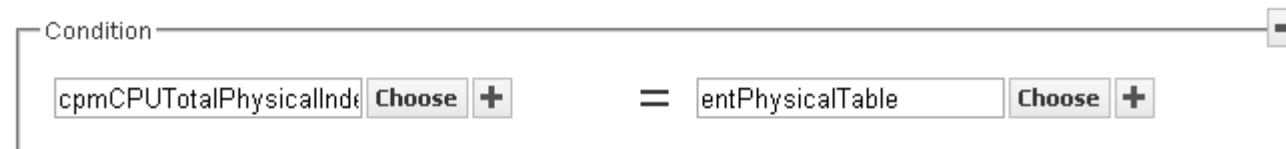
SNMP Report – Multiple tables

- Joining standard Entity table and Cisco specific table with CPU load information

Source tables:

cpmCPUTotalTable	Choose	-
entPhysicalTable	Choose	- +

Join conditions:



cpmCPUTotalPhysicalIndex	entPhysicalDescr	cpmCPUTotal5secRev	cpmCPUTotal1minRev	cpmCPUTotal5minRev
2017	CPU of Routing Processor 5	14	15	19
2001	CPU of Switching Processor 5	22	21	22
3001	CPU of Module 1	88	88	88
4001	CPU of Module 2	86	87	87

Device discovery

- » Discovery SNMP enabled devices
 - » by IP address - ping, SNMP, APR...
- » Discovery device type
 - » Router, Switch, Linux, Windows, UPS, Printer...
- » Discovery device resources – attributes
 - » Name, Description, MAC, Location, Uptime...
- » Discovery device vendor
 - » Cisco, Juniper, HP, IBM, Microsoft...
- » Discovery device model
- » Discovery device components – **sub-devices**
 - » Interfaces – general for all network devices
 - » per device type - Processors, Memory, Modules, Storage, BGP peers, Batteries...
- » How to discover all types of devices, sub-devices, attributes, vendors?

Device model

- » Configure device data model:
 - » Device types
 - » Device Resources
 - » Device Vendors
 - » Sub-device types
 - » Sub-device Resources
 - » Hierarchy and Inherency

Device model

- » Root of the Device model hierarchy
 - » “**Network Device**” – Generic SNMP enabled network device

All Types

- Network Device
- Interface

Device Type Name:	Network Device
Description:	A generic network device
SNMP Test Expression:	(OID(.1.3.6.1.2.1.1.1.0) exists)
Parent (optional):	

Save

Resources

#	Name	Category	OID	
1	Name	Name	.1.3.6.1.2.1.1.5.0	   

- » Discovery expression
 - » System OID
- » Resources
 - » Name

Device model

- ❖ Root of the Device model hierarchy

- ❖ “Interface” – Generic sub-device

All Types

Network Device

Interface

Subdevice Type Name:	Interface
Description:	Interface
Subdevice OID:	.1.3.6.1.2.1.2.2.1.1
Subdevice Category:	Interface

Save

Resources

#	Name	Category	OID
1	Name	Name	.1.3.6.1.2.1.31.1.1.1.1
2	Description	Interface description	.1.3.6.1.2.1.31.1.1.1.18

- ❖ Resources

- ❖ Name
 - ❖ Description

Device model

» New Device Type

» “Router”

» All Types

»  **Network Device**

»  **Interface**

»  **Router**

»  **BGP peers**

»  **Physical Entity**

Device Type Name:

Router

Description:

Router - Layer 3 device

SNMP Test Expression:

(OID(.1.3.6.1.2.1.4.1.0) string equals "1" AND OID(.1.3.6.1.2.1.1.7.0) bitmask "4")



Parent (optional):

Network Device

 **Save**

Resources

 **Add**

#	Name	Category	OID	
1	Name	Name	.1.3.6.1.2.1.1.5.0	   
2	Description	Description	.1.3.6.1.2.1.1.1.0	   

» Parent – *Network Device*

» Discovery expression

»  **Match All**   

OID	string equals	.1.3.6.1.2.1.4.1.0	1	X
OID	bitmask	.1.3.6.1.2.1.1.7.0	4	X

» Resources

» Name – Inherent from *Network Device*

» Description – Newly defined

Device model

» New Sub-device Type

» “BGP peers”

>All Types

Network Device

Interface

Router

BGP peers

Physical Entity

Subdevice Type Name: BGP peers

Description: BGP peers

Subdevice OID: .1.3.6.1.2.1.15.3.1.1

Subdevice Category: BGP peers

Save

Resources

+ Add

#	Name	Category	OID	
1	Peer name	Peer name	.1.3.6.1.2.1.15.3.1.1	   
2	State	State	.1.3.6.1.2.1.15.3.1.2	   
3	Admin status	Admin status	.1.3.6.1.2.1.15.3.1.3	   
4	Local IP	Local IP	.1.3.6.1.2.1.15.3.1.5	   

» Sub-device OID - Table

» Resources

» Specific OID from the sub-device table

Device model

» New Sub-device Type

» “Physical Entity”

« All Types

« Network Device

« Interface

« Router

« BGP peers

Physical Entity

Subdevice Type Name: Physical Entity

Description: Physical entity on the device

Subdevice OID: .1.3.6.1.2.1.47.1.1.1.1.2

Subdevice Category: Physical Entity

Save

Resources

+ Add

#	Name	Category	OID	
1	Name	Name	.1.3.6.1.2.1.47.1.1.1.1.7	   
2	Description	Description	.1.3.6.1.2.1.47.1.1.1.1.2	   
3	Class	Class	.1.3.6.1.2.1.47.1.1.1.1.5	   
4	Model	Model	.1.3.6.1.2.1.47.1.1.1.1.13	   
5	Serial number	Serial number	.1.3.6.1.2.1.47.1.1.1.1.11	   
6	Parent	Parent	.1.3.6.1.2.1.47.1.1.1.1.4	   
7	Position	Position	.1.3.6.1.2.1.47.1.1.1.1.6	   

» Sub-device OID - Table

» Resources

» Specific OID from the sub-device table

Device model

- » New Device Type
 - » “MPLS Router”

All Types

- » Network Device
- » Interface
- » Router
- » BGP peers
- » Physical Entity
- » **MPLS Router**
- » VRF

Device Type Name:

Description:

SNMP Test Expression: 

Parent (optional): 

Save

Resources

+ Add

#	Name	Category	OID	
1	Name	Name	.1.3.6.1.2.1.1.5.0	
2	Description	Description	.1.3.6.1.2.1.1.1.0	

- » Parent – *Network Device*
- » Discovery expression
- » Resources
 - » Name – Inherent from *Network Device*

Device model

» New Sub-device Type

» “VRF”

« All Types

« Network Device

« Interface

« Router

« BGP peers

« Physical Entity

« MPLS Router

« VRF

Subdevice Type Name: **VRF**

Description: **VRF**

Subdevice OID: **.1.3.6.1.3.118.1.2.2.1.2**

Subdevice Category: **VRF**

Save

Resources

Add

#	Name	Category	OID	
1	VRF description	VRF description	.1.3.6.1.3.118.1.2.2.1.2	
2	Route distinguisher	Route distinguisher	.1.3.6.1.3.118.1.2.2.1.3	
3	Route number	Route number	.1.3.6.1.3.118.1.3.1.1.3	

» Sub-device OID - Table

» Resources

» Specific OID from the sub-device table

Device model

❖ New Device Type

❖ “Computer”

▫ All Types

-  [Network Device](#)
-  [Interface](#)
-  [Router](#)
-  [BGP peers](#)
-  [Physical Entity](#)
-  [MPLS Router](#)
-  [VRF](#)
-  **Computer**
-  [Host Physical Entity](#)

Device Type Name:	Computer		
Description:	Host Computer		
SNMP Test Expression:	(OID(.1.3.6.1.2.1.25.1.1.0) exists)		
Parent (optional):	Network Device		
<input checked="" type="checkbox"/> Save			
Resources			
+ Add			
#	Name	Category	OID
1	Name	Name	.1.3.6.1.2.1.1.5.0

Device model

- ❖ New Sub-device Type
 - ❖ “Host Physical Entity”

All Types

- ❑ Network Device
 - ❑ Interface
- ❑ Router
 - ❑ BGP peers
 - ❑ Physical Entity
- ❑ MPLS Router
 - ❑ VRF
- ❑ Computer
 - ❑ Host Physical Entity

Subdevice Type Name:

Description:

Subdevice OID:

Subdevice Category:

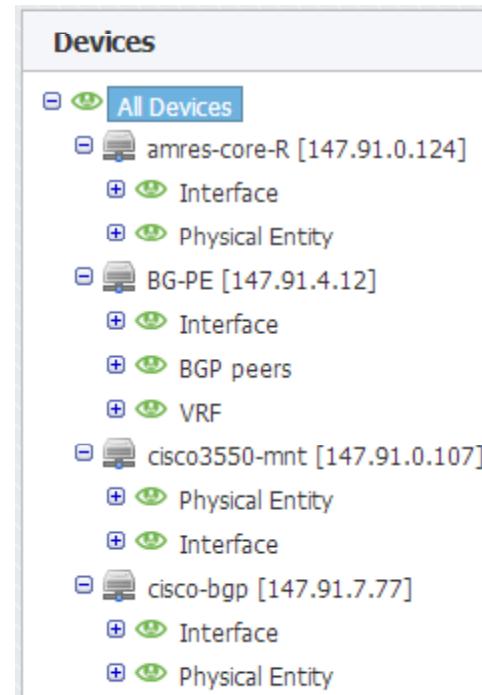
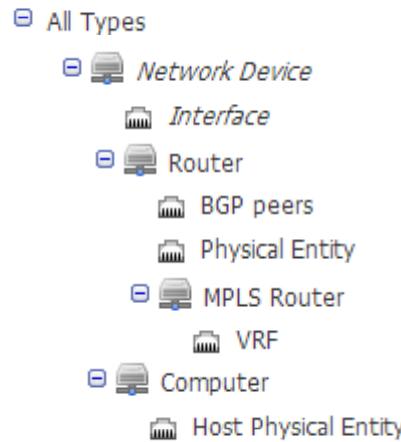
Save

Resources

#	Name	Category	OID	
1	Name	Name	.1.3.6.1.2.1.25.3.2.1.3	<input type="button" value="✎"/> <input type="button" value="─"/> <input type="button" value="▲"/> <input type="button" value="▼"/>
2	Status	Status	.1.3.6.1.2.1.25.3.2.1.3	<input type="button" value="✎"/> <input type="button" value="─"/> <input type="button" value="▲"/> <input type="button" value="▼"/>

Device model

Example



Example

Devices

- All Devices
- amres-core-R [147.91.0.124]**
 - Interface
 - Physical Entity
- BG-PE [147.91.4.12]
 - Interface
 - BGP peers
 - VRF
- cisco3550-mnt [147.91.0.107]
 - Physical Entity
 - Interface
- cisco-bgp [147.91.7.77]
 - Interface
 - Physical Entity
- Exporter_147.91.255.13 [147.91.255.13]
 - Interface

Name: amres-core-R
Address: 147.91.0.124
Types: Network Device, Router, MPLS Router
Description: Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SX15, RELEASE SOFTWARE (fc2) Tech Release Candidate (TAC) Software - 12.2(33)SX15

Interface

Name	Address	Description	Name	Interface description
Gi1/1	-	RCUB cisco2960-rek2	Gi1/1	RCUB cisco2960-rek2
Gi1/2	147.91.6.81/30	amres-core-L Routing	Gi1/2	amres-core-L Routing
Gi1/3	-	amres-core-J AMRES - deaktivirano	Gi1/3	amres-core-J AMRES - deaktivirano
Gi1/4	-	amres-core-J Trunk	Gi1/4	amres-core-J Trunk
Gi1/5	-	Etherchannel 1 prema amres-core-J	Gi1/5	Etherchannel 1 prema amres-core-J
Gi1/6	-	Etherchannel 2 prema amres-core-J	Gi1/6	Etherchannel 2 prema amres-core-J
Gi1/7	-	lancom WLC	Gi1/7	lancom WLC
Gi1/8	-	cisco5508-R	Gi1/8	cisco5508-R
Gi1/9	-	MCU Cusco 4510	Gi1/9	MCU Cusco 4510
Gi1/10	-	Cisco3560-hprek	Gi1/10	Cisco3560-hprek
Gi1/11	-	Veza ka cisco2950-rek7	Gi1/11	Veza ka cisco2950-rek7
Gi1/12	-	Etherchannel 1 prema amres-core-L	Gi1/12	Etherchannel 1 prema amres-core-L
Gi1/13	-	Etherchannel 2 prema amres-core-L	Gi1/13	Etherchannel 2 prema amres-core-L
Gi1/14	-		Gi1/14	
Gi1/15	-		Gi1/15	
Gi1/16	-		Gi1/16	
Gi1/17	-		Gi1/17	
Gi1/18	-	ACS Kontroler pristupa RCUB server sala	Gi1/18	ACS Kontroler pristupa RCUB server sala
Gi1/19	-	Cisco5508-L	Gi1/19	Cisco5508-L
Gi1/20	-		Gi1/20	
Gi1/21	-	Cat2960-skole	Gi1/21	Cat2960-skole
Gi1/22	-	Proba NAT za skole	Gi1/22	Proba NAT za skole
Gi1/23	-	Cat2960-skole	Gi1/23	Cat2960-skole
Gi1/24	-	ASR1002-skole	Gi1/24	ASR1002-skole
Gi1/25	-	C7201-mgmt	Gi1/25	C7201-mgmt
Gi1/26	-	Rek8	Gi1/26	Rek8
Gi1/27	-	JISP	Gi1/27	JISP
Gi1/28	-	JISP	Gi1/28	JISP

Example

Devices	Name	Description	Class	Model	Serial number	Position	Parent
>All Devices	WS-C6509-E	Cisco Systems Catalyst 6500 9-slot Chassis System	3	WS-C6509-E	SMG1114N6C6	-1	0
amres-core-R [147.91.0.124]	Physical Slot 1	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			1	1
Interface	Physical Slot 2	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			2	1
Physical Entity	Physical Slot 3	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			3	1
BG-PE [147.91.4.12]	Physical Slot 4	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			4	1
Interface	Physical Slot 5	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			5	1
BGP peers	Physical Slot 6	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			6	1
VRF	Physical Slot 7	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			7	1
cisco3550-mnt [147.91.0.107]	Physical Slot 8	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			8	1
Physical Entity	Physical Slot 9	Cisco Systems Catalyst 6500 9-slot Physical Slot	5			9	1
Interface	Backplane	Cisco Systems Catalyst 6500 9-slot backplane	4			1	1
cisco-bgp [147.91.7.77]	fan-tray 1 fan-fail Sensor	fan-tray 1 fan-fail Sensor	8			4	11
Interface	Container of Fan FRU 1	Container of Fan FRU	5			10	1
Physical Entity	WS-C6509-E-FAN 1	Enhanced 9-slot Fan Tray 1	7	WS-C6509-E-FAN	DCH11070299	1	13
Exporter_147.91.255.13 [147.91.255.13]	Container of Container of Power Supply	Container of Container of Power Supply	5			11	1
Physical Entity	Container of Power Supply 1	Container of Power Supply 1	5			1	15
PS 1 WS-CAC-3000W	AC power supply, 3000 watt 1	AC power supply, 3000 watt 1	6	WS-CAC-3000W	AZS10490KEW	1	16
power-supply 1 fan-fail Sensor	power-supply 1 fan-fail Sensor	power-supply 1 fan-fail Sensor	8			1	17
power-supply 1 power-output-fail Sensor	power-supply 1 power-output-fail Sensor	power-supply 1 power-output-fail Sensor	8			2	17
power-supply 1 power-output-mode Sensor	power-supply 1 power-output-mode Sensor	power-supply 1 power-output-mode Sensor	8			3	17
power-supply 1 incompatible with fan Sensor	power-supply 1 incompatible with fan Sensor	power-supply 1 incompatible with fan Sensor	8			4	17
power-supply 1 power-input Sensor	power-supply 1 power-input Sensor	power-supply 1 power-input Sensor	8			5	17
Container of Power Supply 2	Container of Power Supply 2	Container of Power Supply 2	5			2	15
PS 2 WS-CAC-3000W	AC power supply, 3000 watt 2	AC power supply, 3000 watt 2	6	WS-CAC-3000W	AZS10490KF7	1	27
power-supply 2 fan-fail Sensor	power-supply 2 fan-fail Sensor	power-supply 2 fan-fail Sensor	8			1	28
power-supply 2 power-output-fail Sensor	power-supply 2 power-output-fail Sensor	power-supply 2 power-output-fail Sensor	8			2	28
power-supply 2 power-output-mode Sensor	power-supply 2 power-output-mode Sensor	power-supply 2 power-output-mode Sensor	8			3	28
power-supply 2 incompatible with fan Sensor	power-supply 2 incompatible with fan Sensor	power-supply 2 incompatible with fan Sensor	8			4	28
power-supply 2 power-input Sensor	power-supply 2 power-input Sensor	power-supply 2 power-input Sensor	8			5	28
Sensor for counting number of OK VTTs	Sensor for counting number of OK VTTs	Sensor for counting number of OK VTTs	8			1	11
Sensor for counting number of OK Clocks	Sensor for counting number of OK Clocks	Sensor for counting number of OK Clocks	8			2	11
Sensor for counting number of OK Fans	Sensor for counting number of OK Fans	Sensor for counting number of OK Fans	8			1	11
Container of VTT 1	Container of VTT	Container of VTT	5			1	11
WS-C6K-VTT-E 1	VTT-E FRU 1	VTT-E FRU 1	9	WS-C6K-VTT-E	SMT1103P986	1	41
VTT 1 OK Sensor	VTT-E FRU 1 OK Sensor	VTT-E FRU 1 OK Sensor	8			1	42

Example

Devices

- ⊕ All Devices
- ⊕ amres-core-R [147.91.0.124]
 - ⊕ Interface
 - ⊕ Physical Entity
- ⊕ **BG-PE [147.91.4.12]**
 - ⊕ Physical Entity
 - ⊕ Interface
 - ⊕ BGP peers
 - ⊕ VRF
- ⊕ cisco3550-mnt [147.91.0.107]
 - ⊕ Physical Entity
 - ⊕ Interface
- ⊕ cisco-bgp [147.91.7.77]
 - ⊕ Interface
 - ⊕ Physical Entity
- ⊕ Exporter_147.91.255.13 [147.91.255.13]

Name: BG-PE
Address: 147.91.4.12
Types: Network Device, Router, MPLS Router
Description: Cisco IOS Software, 7200 Software (C7200P-ADVENTERPRISEK9-M), Version 15.2(4)M5, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2013 by Cisco Systems, Inc. Compiled Fri 13-Sep-13 19:12 by prod_rel_team

Physical Entity

Name	Description	Name	Description	Class	Model	Serial number	Position
Chassis	Cisco 7201, 1-slot chassis	Chassis	Cisco 7201, 1-slot chassis	3	CISCO7201	78011094	-1
PA Slot 1	PA Slot Container	PA Slot 1	PA Slot Container	5			1
c7201	Cisco 7201 Network Processing Engine	c7201	Cisco 7201 Network Processing Engine	9	CISCO7201	JAE14041SUE	1
SFP Port Container 0/0	SFP Port Container	SFP Port Container 0/0	SFP Port Container	5			1
Gi0/0	MV64460 Internal MAC RJ45	Gi0/0	MV64460 Internal MAC RJ45	10			1
SFP Port Container 0/1	SFP Port Container	SFP Port Container 0/1	SFP Port Container	5			2
Gi0/1	MV64460 Internal MAC RJ45	Gi0/1	MV64460 Internal MAC RJ45	10			2
SFP Port Container 0/2	SFP Port Container	SFP Port Container 0/2	SFP Port Container	5			3
module 0/2	1000BaseT	module 0/2	1000BaseT	9			1
GigabitEthernet0/2	MV64460 Internal MAC	GigabitEthernet0/2	MV64460 Internal MAC	10			1
FastEthernet0/0	i82546	FastEthernet0/0	i82546	10			4
SFP Port Container 0/3	SFP Port Container	SFP Port Container 0/3	SFP Port Container	5			4
Flash Card Slot Container CPU	Flash Card Slot Container CPU	Flash Card Slot Container CPU	Flash Card Slot Container CPU	5			4
disk0	256MB Compact Flash Disk for c7201	disk0	256MB Compact Flash Disk for c7201	9	MEM-7201-FLD256		1
usb 0	USB Port	usb 0	USB Port	10			5
PEM 0	Power Supply Container	PEM 0	Power Supply Container	5			2
PEM 1	Power Supply Container	PEM 1	Power Supply Container	5			3
Power Supply 1	Cisco 7201 AC Power Supply	Power Supply 1	Cisco 7201 AC Power Supply	6	PWR-7201-AC		1
Power Supply 2	Cisco 7201 AC Power Supply	Power Supply 2	Cisco 7201 AC Power Supply	6	PWR-7201-AC		1
NPE Inlet Temperature 0	NPE Inlet Temperature Sensor	NPE Inlet Temperature 0	NPE Inlet Temperature Sensor	8			1
NPE Outlet Temperature 0	NPE Outlet Temperature Sensor	NPE Outlet Temperature 0	NPE Outlet Temperature Sensor	8			2
CPU Die Temperature 0	CPU Die Temperature Sensor	CPU Die Temperature 0	CPU Die Temperature Sensor	8			3
+3.30 V Voltage 0	+3.30 V Voltage Sensor	+3.30 V Voltage 0	+3.30 V Voltage Sensor	8			4
+1.50 V Voltage 0	+1.50 V Voltage Sensor	+1.50 V Voltage 0	+1.50 V Voltage Sensor	8			5
+2.50 V Voltage 0	+2.50 V Voltage Sensor	+2.50 V Voltage 0	+2.50 V Voltage Sensor	8			6
+5.15 V Voltage 0	+5.15 V Voltage Sensor	+5.15 V Voltage 0	+5.15 V Voltage Sensor	8			7
+1.20 V Voltage 0	+1.20 V Voltage Sensor	+1.20 V Voltage 0	+1.20 V Voltage Sensor	8			8
VDD_CPU Voltage 0	VDD_CPU Voltage Sensor	VDD_CPU Voltage 0	VDD_CPU Voltage Sensor	8			9
-11.95 Voltage 0	-11.95 Voltage Sensor	-11.95 Voltage 0	-11.95 Voltage Sensor	8			10
VTT Voltage 0	VTT Voltage Sensor	VTT Voltage 0	VTT Voltage Sensor	8			11

Example

Devices	
<ul style="list-style-type: none"> <input type="checkbox"/> All Devices <input type="checkbox"/> amres-core-R [147.91.0.124] <ul style="list-style-type: none"> <input type="checkbox"/> Interface <input type="checkbox"/> Physical Entity <input checked="" type="checkbox"/> BG-PE [147.91.4.12] <ul style="list-style-type: none"> <input type="checkbox"/> Physical Entity <input type="checkbox"/> Interface <input type="checkbox"/> BGP peers <input type="checkbox"/> VRF <input type="checkbox"/> cisco3550-mnt [147.91.0.107] <ul style="list-style-type: none"> <input type="checkbox"/> Physical Entity <input type="checkbox"/> Interface <input type="checkbox"/> cisco-bgp [147.91.7.77] <ul style="list-style-type: none"> <input type="checkbox"/> Interface <input type="checkbox"/> Physical Entity <input type="checkbox"/> Exporter_147.91.255.13 [147.91.255.13] <ul style="list-style-type: none"> 	

Interface					
Name	Address	Description	Name	Interface description	
Fa0/0	-		Fa0/0		
Gi0/0	-		Gi0/0		
Gi0/1	10.10.0.2/30	Link ka CSC-CE	Gi0/1	Link ka CSC-CE	
Gi0/2	10.51.36.2/30		Gi0/2		
Gi0/3	-		Gi0/3		
Vo0	-		Vo0		
Nu0	-		Nu0		
Lo0	192.168.13.92		Lo0		
Lo1	192.168.17.1		Lo1		
Lo30	192.168.17.30		Lo30		
Lo32	192.168.17.32		Lo32		
Lo117	147.91.0.117		Lo117		
Gi0/0.2	10.10.0.5/30		Gi0/0.2		
Gi0/0.10	147.91.4.12/25		Gi0/0.10		
Gi0/0.450	10.48.0.1/24		Gi0/0.450		
GigabitEthernet0/1	-		GigabitEthernet0/1		
NV0	-		NV0		
Lo51	10.51.36.1		Lo51		
Lo33	192.168.17.34		Lo33		
Lo17	-		Lo17		

BGP peers						
Name	Description	Local IP	Peer name	Admin status	State	
0.0.0.0	-	0.0.0.0	0.0.0.0	1	1	
0.0.0.0	-	0.0.0.0	0.0.0.0	1	1	
0.0.0.0	-	0.0.0.0	0.0.0.0	2	1	
150.254.160.47	-	147.91.0.117	150.254.160.47	2	6	
192.168.13.93	-	192.168.13.92	192.168.13.93	2	6	

VRF					
Name	Description	VRF description	Route distinguisher	Route number	
	-		147.91.0.117:1	2	
SA3T3 - probni VRF	-	SA3T3 - probni VRF	1:1	0	
SA3T3_A	-	SA3T3_A	13092:17	1	
VPN-BIO	-	VPN-BIO	10.130.24.240:32	1	
Ping-VPN	-	Ping-VPN	147.91.0.117:12321	52	
VPN-ASTRO	-	VPN-ASTRO	10.130.22.220:30	1	

Example

Devices

- All Devices
 - afrodita.rcub.bg.ac.rs [147.91.1]**
 - Interface
 - Host Physical Entity
 - amres-core-R [147.91.0.124]
 - BG-PE [147.91.4.12]
 - cisco3550-mnt [147.91.0.107]
 - cisco-bgp [147.91.7.77]
 - Device_147.91.1.120 [147.91.1.120]
 - Exporter_147.91.255.13 [147.91.255.13]

Name: afrodita.rcub.bg.ac.rs
Address: 147.91.1.120
Types: Network Device, Computer
Description:

Interface

Name	Address	Description	Name	Interface description
lo	-		lo	
eth0	147.91.1.121/25		eth0	
eth1	-		eth1	
sit0	-		sit0	

Host Physical Entity

Name	Description	Name	Status
GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	-	GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	-
GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	-	GenuineIntel: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz	-
network interface lo	-	network interface lo	-
network interface eth0	-	network interface eth0	-
network interface eth1	-	network interface eth1	-
network interface sit0	-	network interface sit0	-
PHILIPS DVD-ROM SDR089	-	PHILIPS DVD-ROM SDR089	-
Guessing that there's a floating point co-processor	-	Guessing that there's a floating point co-processor	-

Further challenges

❖ Hierarchy of entries in SNMP table

Devices

- ⊕ All Devices
- ⊕ afroditा.rcub.bg.ac.rs [147.91.1]
 - ⊕ Interface
 - ⊕ Host Physical Entity
 - ⊕ amres-core-R [147.91.0.124]
 - ⊕ BG-PE [147.91.4.12]
 - ⊕ Physical Entity
 - Chassis [Cisco 7201, 1...
 - PA Slot 1 [PA Slot Con...
 - c7201 [Cisco 7201 Netw...
 - SFP Port Container 0/0...
 - Gi0/0 [MV64460 Interna...
 - SFP Port Container 0/1...
 - Gi0/1 [MV64460 Interna...
 - SFP Port Container 0/2...
 - module 0/2 [1000BaseT]
 - GigabitEthernet0/2 [MV...
 - FastEthernet0/0 [i82546]
 - SFP Port Container 0/3...
 - Flash Card Slot Contai...
 - disk0 [256MB Compact F...
 - usb 0 [USB Port]
 - PEM 0 [Power Supply Co...
 - PEM 1 [Power Supply Co...

Name	Description	Class	Model	Serial number	Position	Parent
Chassis	Cisco 7201, 1-slot chassis	3	CISCO7201	78011094	-1	0
PA Slot 1	PA Slot Container	5			1	1
c7201	Cisco 7201 Network Processing Engine	9	CISCO7201	JAE14041SUE	1	1
SFP Port Container 0/0	SFP Port Container	5			1	3
Gi0/0	MV64460 Internal MAC RJ45	10			1	3
SFP Port Container 0/1	SFP Port Container	5			2	3
Gi0/1	MV64460 Internal MAC RJ45	10			2	3
SFP Port Container 0/2	SFP Port Container	5			3	3
module 0/2	1000BaseT	9			1	8
GigabitEthernet0/2	MV64460 Internal MAC	10			1	9
FastEthernet0/0	i82546	10			4	3
SFP Port Container 0/3	SFP Port Container	5			4	3
Flash Card Slot Container CPU	Flash Card Slot Container CPU	5			4	3
disk0	256MB Compact Flash Disk for c7201	9	MEM-7201-FLD256		1	13
usb 0	USB Port	10			5	3
PEM 0	Power Supply Container	5			2	1
PEM 1	Power Supply Container	5			3	1
Power Supply 1	Cisco 7201 AC Power Supply	6	PWR-7201-AC		1	16
Power Supply 2	Cisco 7201 AC Power Supply	6	PWR-7201-AC		1	17
NPE Inlet Temperature 0	NPE Inlet Temperature Sensor	8			1	3
NPE Outlet Temperature 0	NPE Outlet Temperature Sensor	8			2	3
CPU Die Temperature 0	CPU Die Temperature Sensor	8			3	3
+3.30 V Voltage 0	+3.30 V Voltage Sensor	8			4	3
+1.50 V Voltage 0	+1.50 V Voltage Sensor	8			5	3
+2.50 V Voltage 0	+2.50 V Voltage Sensor	8			6	3
+5.15 V Voltage 0	+5.15 V Voltage Sensor	8			7	3
+1.20 V Voltage 0	+1.20 V Voltage Sensor	8			8	3
VDD_CPU Voltage 0	VDD_CPU Voltage Sensor	8			9	3
4.40 DC Voltage 0	4.40 DC Voltage Sensor	8			10	3

Further challenges

- » Hierarchy of entries from one SNMP table
- » Solution
 - » “Where” clause
 - » Inherent Index from the parent object
- » Populate all entries that match where clause criteria
- » Example:
 - » root entity:

```
select from entPhysicalTable  
      where entPhysicalContainedIn = 0
```
 - » sub-entity:

```
select from entPhysicalTable  
      where entPhysicalContainedIn = <parentIndex>
```

Further challenges

- » Hierarchy of entries from multiple SNMP tables
- » Solution
 - » “Where” clause
 - » Inherent Index from the parent object
 - » Support joining tables
- » Example: Cisco QoS policy

```
cisco#show policy-map
  Policy Map QOS-STUDY
    Class EMAIL
      bandwidth 128
    Class MUSIC
      bandwidth 32000
      shape average 100000 400 400
      queue-limit 100
      fair-queue
      fair-queue individual-limit 10000
    Class VOICE
      priority 256
      set dscp cs1
      police 500000 15625 15625 conform-action transmit exceed-action drop
```

Cisco QoS policy

Discover Policy on the Interface

cbQosServicePolicyTable

index	cbQosPolicyIndex	cbQosIfType	cbQosPolicyDirection	cbQosIfIndex
.256		mainInterface(1)	input(1)	16
.2		mainInterface(1)	input(1)	19
.3		mainInterface(1)	input(1)	20

ifTable

ifIndex	ifDescr
16	GigabitEthernet1/16
17	GigabitEthernet2/1
18	GigabitEthernet2/2
19	GigabitEthernet2/3
20	GigabitEthernet2/4

cbQosObjectsTable

index	cbQosObjectsIndex	cbQosConfigIndex	cbQosObjectType	cbQosParentObjectsIndex
.256	256	439856	policymap(1)	0
.256.1515683		7725555	police(7)	11021041
.256.4224289		6938753	classmap(2)	256
.256.4694866		8759218	matchStatement(3)	11021041
.256.9440051		9124931	police(7)	4224289
.256.9502753		1593	classmap(2)	256

“where”

cbQosPolicyMapCfgTable

index	cbQosPolicyMapName	cbQosPolicyMapDesc
.439856	dos	

Interface GigabitEthernet1/16
Policy dos (256)

Cisco QoS policy

- Discover Class-map on the Policy

Interface GigabitEthernet1/16
Policy dos (256)

“where”

cbQosObjectsTable

index	cbQosObjectsIndex	cbQosConfigIndex	cbQosObjectsType	cbQosParentObjectsIndex
.256.256		439856	policymap(1)	0
.256.1515683		7725555	police(7)	11021041
.256.4224289	6938753	8759218	classmap(2)	256
.256.4694866		9124931	matchStatement(3)	11021041
.256.9440051		1593	police(7)	4224289
.256.9502753			classmap(2)	256

cbQosCMCfgTable

index	cbQosCMName	cbQosCMDesc	cbQosCMInfo
.1593	class-default		matchAny(3)
.3479313	dos-icmp		matchAll(2)
.6938753	dos-tcpsyn		matchAll(2)

Interface GigabitEthernet1/16
Policy dos (256)

Class map dos-tcpsyn (4224289)
Class map class-default (9502753)

Cisco QoS policy

- Discover Match statement on the Class-map

Interface GigabitEthernet1/16

Policy dos (256)

Class map dos-tcpsyn (4224289)

Class map class-default (9502753)

cbQosObjectsTable

index	cbQosObjectsIndex	cbQosConfigIndex	cbQosObjectsName	cbQosParentObjectsIndex
.256.256		439856	policymap(1)	0
.256.1515683		7725555	police(7)	11021041
.256.4224289		6938753	classmap(2)	256
.256.4694866		8759218	matchStatement(3)	11021041
.256.9440051		9124931	police(7)	4224289
.256.9502753		1593	classmap(2)	256
.256.9510434		4031314	matchStatement(3)	4224289

“where”

cbQosMatchStmtCfgTable

index	cbQosMatchStatementName
.1594	any
.4031314	Match access-group name dos-tcpsyn
.8759218	Match access-group name dos-icmp

Interface GigabitEthernet1/16

Policy dos (256)

Class map dos-tcpsyn (4224289)

Match dos-tcpsyn

Class map class-default (9502753)

Cisco QoS policy

- Take statistics for the Class map

Interface GigabitEthernet1/16

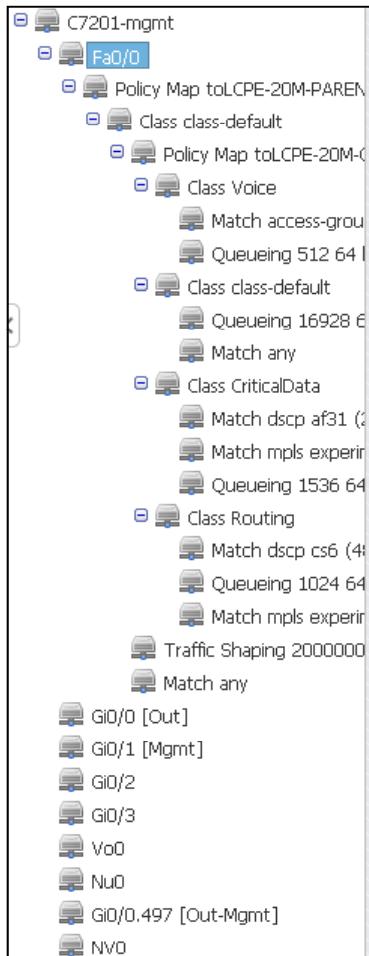
Policy dos (256)

Class map dos-tcpsyn (4224289)
Match dos-tcpsyn (9510434)
Class map class-default (9502753)

cbQosCMStatsTable

Index	cbQosCMPrePolicyByte	cbQosCMPrePolicyByte64	cbQosCMPrePolicyBitRate
.256.4224289	235200	235200	0
.256.9502753	963752	963752	40
.256.11021041	0	0	0
.304.1949569	2307232	2307232	136
.304.10002465	0	0	0

Cisco QoS policy



Name:	Fa0/0				
Description:					
ifSpeed:	100000000				
ifMacAddr:	88:43:e1:f7:99:18				
QoS Settings					
<table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Policy Map toLCPE-20M-PARENT output</td> <td>-</td> </tr> </tbody> </table>		Name	Description	Policy Map toLCPE-20M-PARENT output	-
Name	Description				
Policy Map toLCPE-20M-PARENT output	-				

Name:	Class Routing								
Description:									
cbQosCMInfo:	matchAny								
QoS Statements									
<table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Match dscp cs6 (48)</td> <td>-</td> </tr> <tr> <td>Queueing 1024 64 kbps false false 64 0 0 0 packets</td> <td>-</td> </tr> <tr> <td>Match mpls experimental topmost 6</td> <td>-</td> </tr> </tbody> </table>		Name	Description	Match dscp cs6 (48)	-	Queueing 1024 64 kbps false false 64 0 0 0 packets	-	Match mpls experimental topmost 6	-
Name	Description								
Match dscp cs6 (48)	-								
Queueing 1024 64 kbps false false 64 0 0 0 packets	-								
Match mpls experimental topmost 6	-								

Name:	Traffic Shaping 20000000 0 80000 80000 false 0 average bps 0 0
Description:	
cbQosTSCfgRate:	20000000
cbQosTSCfgExtBurstTime:	0
cbQosTSCfgBurstSize:	80000
cbQosTSCfgExtBurstSize:	80000
cbQosTSCfgAdaptiveEnabled:	false
cbQosTSCfgAdaptiveRate:	0
cbQosTSCfgLimitType:	average
cbQosTSCfgRateType:	bps
cbQosTSCfgPercentRateValue:	0
cbQosTSCfgBurstTime:	0

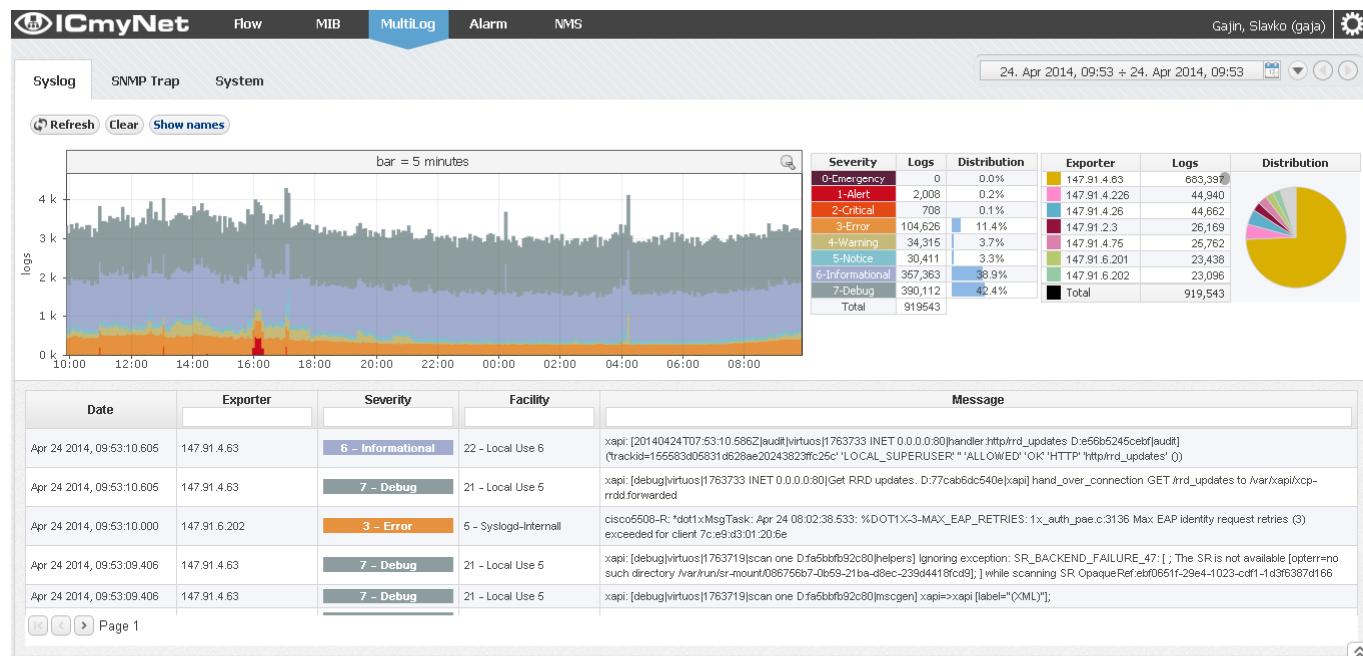
Further development

- » Provide hierarchy of entities
- » Provide joining with “where” clause
- » Extract individual index from composite index
- » Improve user interface (full object management)
- » Extend data model with performance monitoring elements
 - » Configure monitoring roles on devices and sub-devices
 - » Automatic populate monitoring system
- » The core of the new integrated NMS platform – ICmyNet.NMS
- » Integrated with the existing modules:
 - » ICmyNet.MIB, ICmyNet.Multilog, ICmyNet.Flow

Integrated monitoring solution

» ICmyNet.Multilog

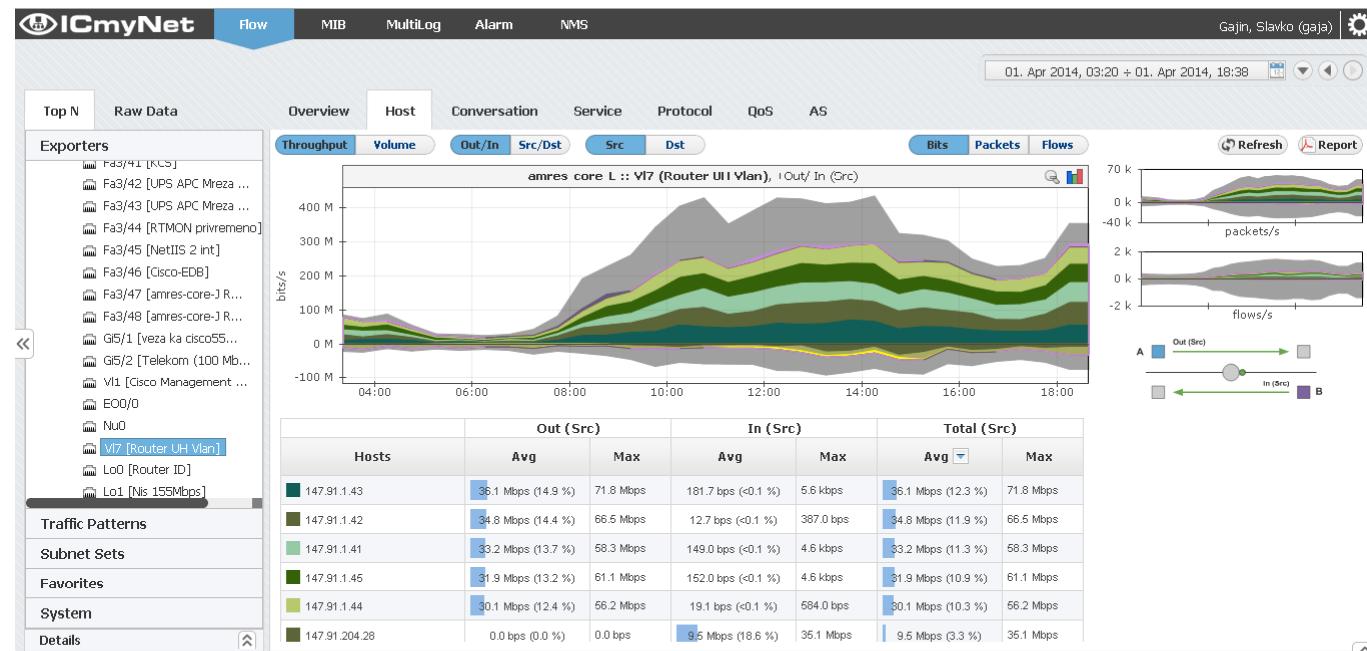
- » Syslog and SNMP trap collector and analyzer
- » Logs distribution per syslog severities and devices
- » Text filter message body
- » Show and analyze data from years to milliseconds



Integrated monitoring solution

» ICmyNet.Flow

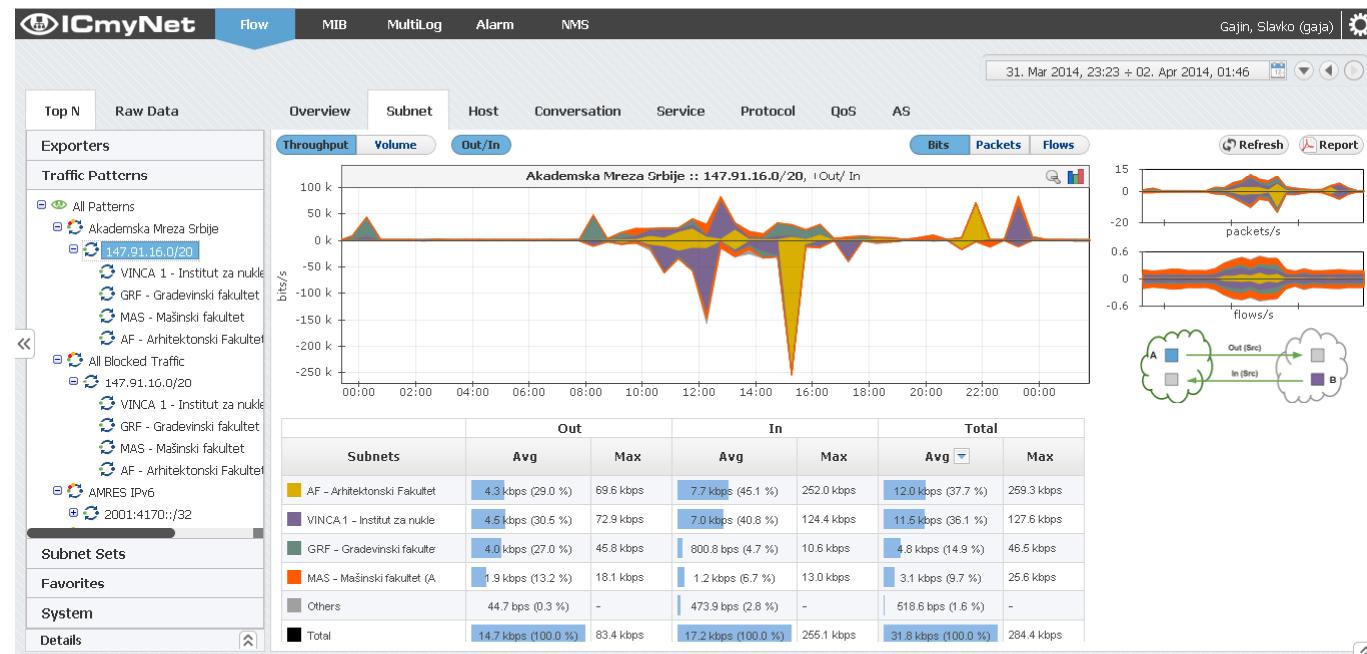
- » NetFlow/IPFIX collector and analyzer
- » Data aggregation per exporters, interfaces, traffic pattern, subnets
- » Hosts, Conversations, Services, Protocols, QOS, AS
- » Row data analysis
- » Alarms



Integrated monitoring solution

» ICmyNet.Flow

- » NetFlow/IPFIX collector and analyzer
- » Data aggregation per exporters, interfaces, traffic pattern, subnets
- » Hosts, Conversations, Services, Protocols, QoS, AS
- » Row data analysis
- » Alarms



Integrated monitoring solution

» ICmyNet.Flow

- » NetFlow/IPFIX collector and analyzer
- » Data aggregation per exporters, interfaces, traffic pattern, subnets
- » Hosts, Conversations, Services, Protocols, QOS, AS
- » Row data analysis
- » Alarms

The screenshot shows the ICmyNet.Flow application interface. At the top, there's a navigation bar with tabs: ICmyNet (selected), Flow, MIB, MultiLog, Alarm, and NMS. On the right side of the header, there's a user name 'Gajin, Slavko (gaja)' and a gear icon. Below the header, there are two main sections: 'Raw Files' on the left and a 'Flows' table on the right.

The 'Raw Files' section displays a tree view of log files by date. Under 'Mar - 2014', it shows '31. Mar' with sub-folders for '13h', '14h', '15h', '16h', '17h', '18h', '19h', '20h', '21h', '22h', and '23h'. Under 'Apr - 2014', it shows a single folder '31. Apr'. On the far left, there are navigation arrows for navigating through the log files.

The 'Flows' section contains a table with the following columns: Start Time, End Time, Duration, Src IP, Src Port, Dst IP, Dst Port, Protocol, and TOS. The table lists several network flow entries. For example, the first entry is from '31-03-2014 13:49:55.969' to '31-03-2014 13:49:56.97' with a duration of '0.128 sec'. The last entry is from '31-03-2014 13:49:55.968' to '31-03-2014 13:49:56.224' with a duration of '0.256 sec'. The 'Protocol' column shows mostly TCP, with one entry for HTTP and one for HTTP-Proxy.

Start Time	End Time	Duration	Src IP	Src Port	Dst IP	Dst Port	Protocol	TOS
31-03-2014 13:49:55.969	31-03-2014 13:49:56.97	0.128 sec	69.171.248.16	HTTPS	160.99.71.178	49571	TCP	0
31-03-2014 13:49:56.609	31-03-2014 13:49:56.609	0.0 sec	87.237.206.99	HTTP	147.91.173.31	33065	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.33	0.64 sec	31.13.64.7	HTTPS	147.91.244.8	39951	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:55.969	0.0 sec	147.91.244.8	39951	31.13.64.7	HTTPS	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.545	0.576 sec	147.91.1.44	HTTP-Proxy	147.91.36.2	51460	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.181	0.192 sec	147.91.1.44	HTTP-Proxy	147.91.36.2	51462	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.98	0.0 sec	160.99.71.178	49571	69.171.248.16	HTTPS	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.181	0.192 sec	147.91.173.31	52569	80.156.249.44	HTTP	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.545	0.576 sec	147.91.1.44	HTTP-Proxy	147.91.36.2	51465	TCP	0
31-03-2014 13:49:55.969	31-03-2014 13:49:56.545	0.576 sec	147.91.1.44	HTTP-Proxy	147.91.36.2	51463	TCP	0
31-03-2014 13:49:55.968	31-03-2014 13:49:55.968	0.0 sec	147.91.222.2	36382	91.222.6.74	HTTP	TCP	0
31-03-2014 13:49:55.968	31-03-2014 13:49:55.968	0.0 sec	91.222.6.74	HTTP	147.91.222.2	36382	TCP	0
31-03-2014 13:49:55.968	31-03-2014 13:49:56.160	0.192 sec	77.122.171.31	1221	160.99.41.208	11964	TCP	0
31-03-2014 13:49:56.608	31-03-2014 13:49:56.608	0.0 sec	147.91.1.44	HTTP-Proxy	91.187.144.127	36765	TCP	0
31-03-2014 13:49:56.608	31-03-2014 13:49:56.736	0.128 sec	147.91.244.8	50991	91.209.18.100	HTTP	TCP	0
31-03-2014 13:49:55.968	31-03-2014 13:49:56.288	0.320 sec	46.180.106.229	58857	160.99.41.208	3751	TCP	0
31-03-2014 13:49:55.968	31-03-2014 13:49:56.224	0.256 sec	147.91.173.31	52195	173.192.202.130	HTTP	TCP	0

Integrated monitoring solution

» ICmyNet.Flow

- » NetFlow/IPFIX collector and analyzer
- » Data aggregation per exporters, interfaces, traffic pattern, subnets
- » Hosts, Conversations, Services, Protocols, QOS, AS
- » Row data analysis
- » Alarms

The screenshot shows the ICmyNet Flow monitoring interface. At the top, there are tabs for Flow, MIB, MultiLog, Alarm (which is selected), and NMS. The status bar indicates "Gajin, Slavko (gaja)" and the date "03. Apr 2014, 00:00 + 04. Apr 2014, 23:59". Below the tabs is a search bar with "Auto refresh period: 5 min" and a refresh button. The main area displays a table of alarms with the following columns: #, Severity, Occurrences, Start, End, Duration, Module, Alarm, Source, Exporter, and Message. The table lists numerous "4-Warning" events from various interfaces and hosts, all reporting "Ovo je visok nivo paketa!". The table has 8 pages, with page 1 of 8 currently selected.

#	Severity	Occurrences	Start	End	Duration	Module	Alarm	Source	Exporter	Message
(1)	4-Warning		Apr 04, 23:55:00	Apr 05, 00:00:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(92.122.214.18)	147.91.4.151	Ovo je visok nivo paketa !
(7)	4-Warning		Apr 04, 18:05:00	Apr 05, 00:05:00	-	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 23:55:00	Apr 05, 00:05:00	00:10:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 22:00:00	Apr 04, 22:10:00	00:10:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 20:40:00	Apr 04, 20:46:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 20:10:00	Apr 04, 20:15:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 20:00:00	Apr 04, 20:05:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 18:50:00	Apr 04, 18:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
	4-Warning		Apr 04, 18:05:00	Apr 04, 18:15:00	00:10:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.12)	147.91.4.151	Ovo je visok nivo paketa !
(4)	4-Warning		Apr 04, 19:45:00	Apr 05, 00:00:00	-	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(93.225.13.232)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:55:00	Apr 05, 00:00:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(2.20.182.89)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:55:00	Apr 05, 00:00:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(2.20.182.112)	147.91.4.151	Ovo je visok nivo paketa !
(2)	4-Warning		Apr 04, 23:05:00	Apr 05, 00:00:00	-	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(67.237.206.99)	147.91.4.151	Ovo je visok nivo paketa !
(6)	4-Warning		Apr 04, 21:15:00	Apr 05, 00:00:00	-	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(31.13.84.49)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(81.187.168.106)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(94.212.141.205)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(83.137.171.192)	147.91.4.151	Ovo je visok nivo paketa !
(12)	4-Warning		Apr 04, 18:00:00	Apr 04, 23:55:00	-	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(64.15.113.77)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(82.125.49.151)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(24.21.123.150)	147.91.4.151	Ovo je visok nivo paketa !
(1)	4-Warning		Apr 04, 23:50:00	Apr 04, 23:55:00	00:05:00	Flow	High packet rate	INTERFACE(147.91.4.151-0)-HOST(92.53.6.38)	147.91.4.151	Ovo je visok nivo paketa !

» Free unlimited academic license - www.icmynet.com

24-25.4.2014, Prague, Campus network monitoring and security workshop, Slavko Gajin

Questions



slavko.gajin@rcub.bg.ac.rs