

@opennac

Network access control and management solution



Xavier González
xavi@opennac.org
Oct 2013

Summary

- Current situation
- What is openNAC?
- What does openNAC can do?
- openNAC architecture
- openNAC components
- openNAC services
- Contact us

openNAC solution

- 2 year+ of active development
- Opensource Network Access Control solution
- Enterprise support services available
- CentOS based

Current situation

- Corporate network access management is poorly controlled
- Mobile Workers. Users become more mobile
- More type of different devices like Smartphones, tablets,...
- This scenarios generate security and availability problems due to non controlled LAN access
- The security of the workstations is constantly threatened by new vulnerabilities
- Security, network management and monitoring tools of expensive and poorly integrated

What is openNAC?

- Network Access Control for corporate LAN / WAN environments
- Enables **authentication, authorization** and **audit** policy-based all access to network
- Multivendor solution
- Based on open source components and self-development
- Based on industry standards such as FreeRadius, 802.1x, ldap, ...
- Extensible, new features can be incorporated
- Easily integrated with existing systems
- It provides value added services such as configuration management, network, backup configurations, Network Discovery and Network Monitoring

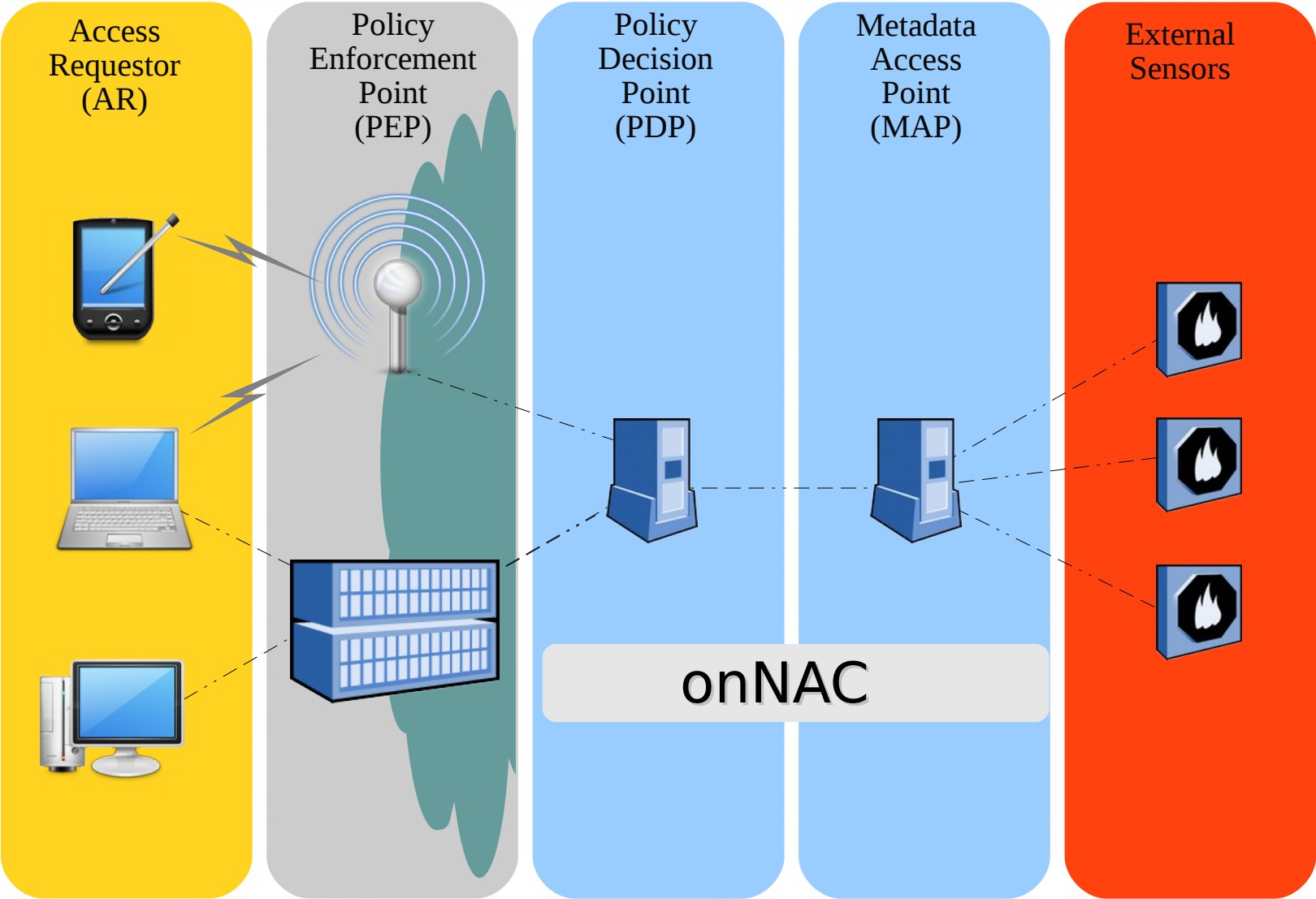
What does openNAC can do?

- Corporate network access based on a set of rules (access policy)
- The availability of Notifications or Quarantine to users regardless of the client device (via browser)
- Access accounting and audit
- Real time monitoring of users, allowing to instantly locate users, ip, mac, switch, port and physical location
- Value-added services such as monitoring, discovery and configuration of network infrastructure

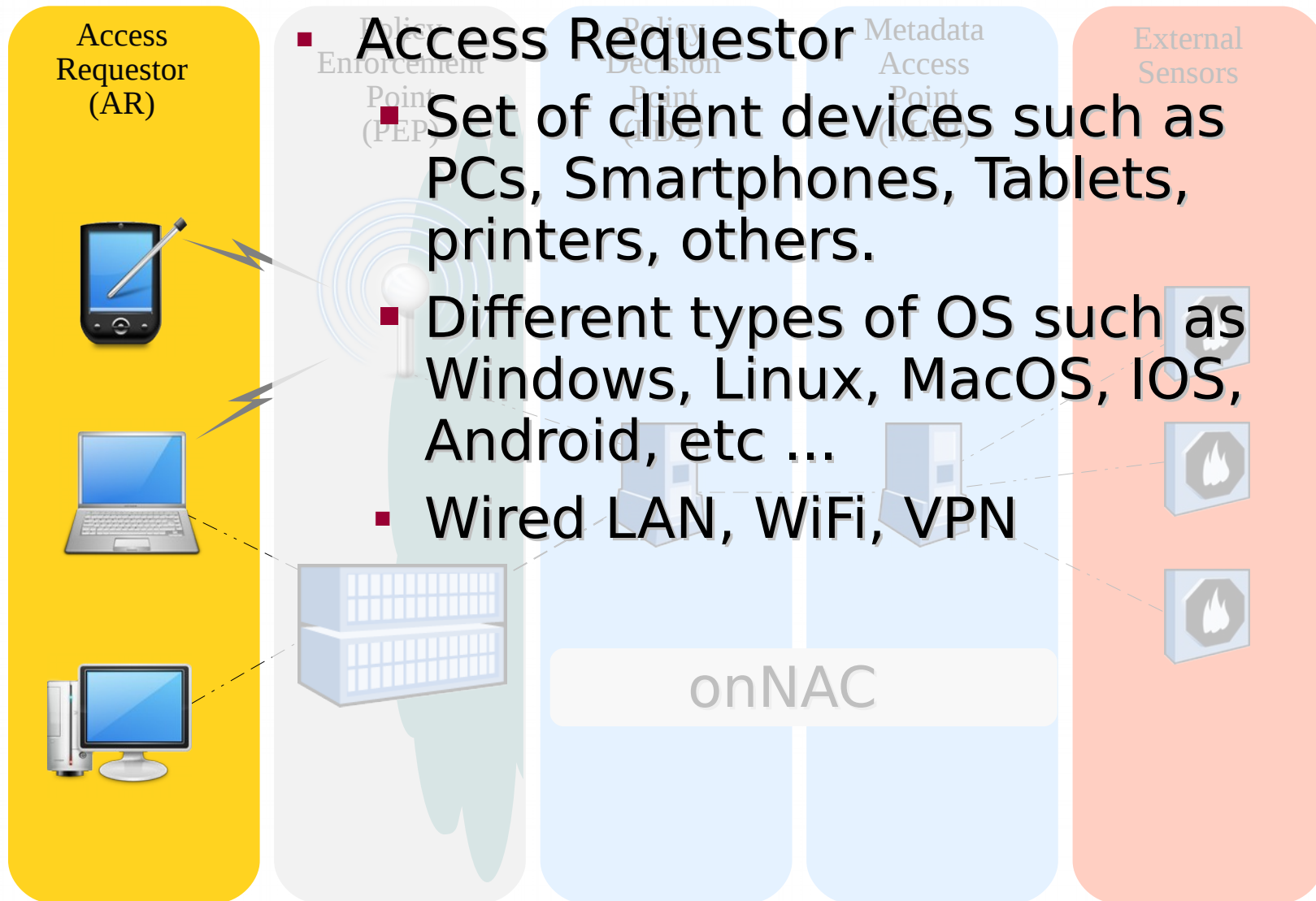
Features

- Authentication of 802.1x enable devices
- Authentication backend based on ldap or AD
- Support to detect rogue devices using 802.1x or SNMP traps
- Bulk configuration of network devices using module onNetConf
- Bulk backup of configuration of network devices using module onNetBackup
- Detection of os, antivirus, firewall and os updates of devices connected to enforce an access policy

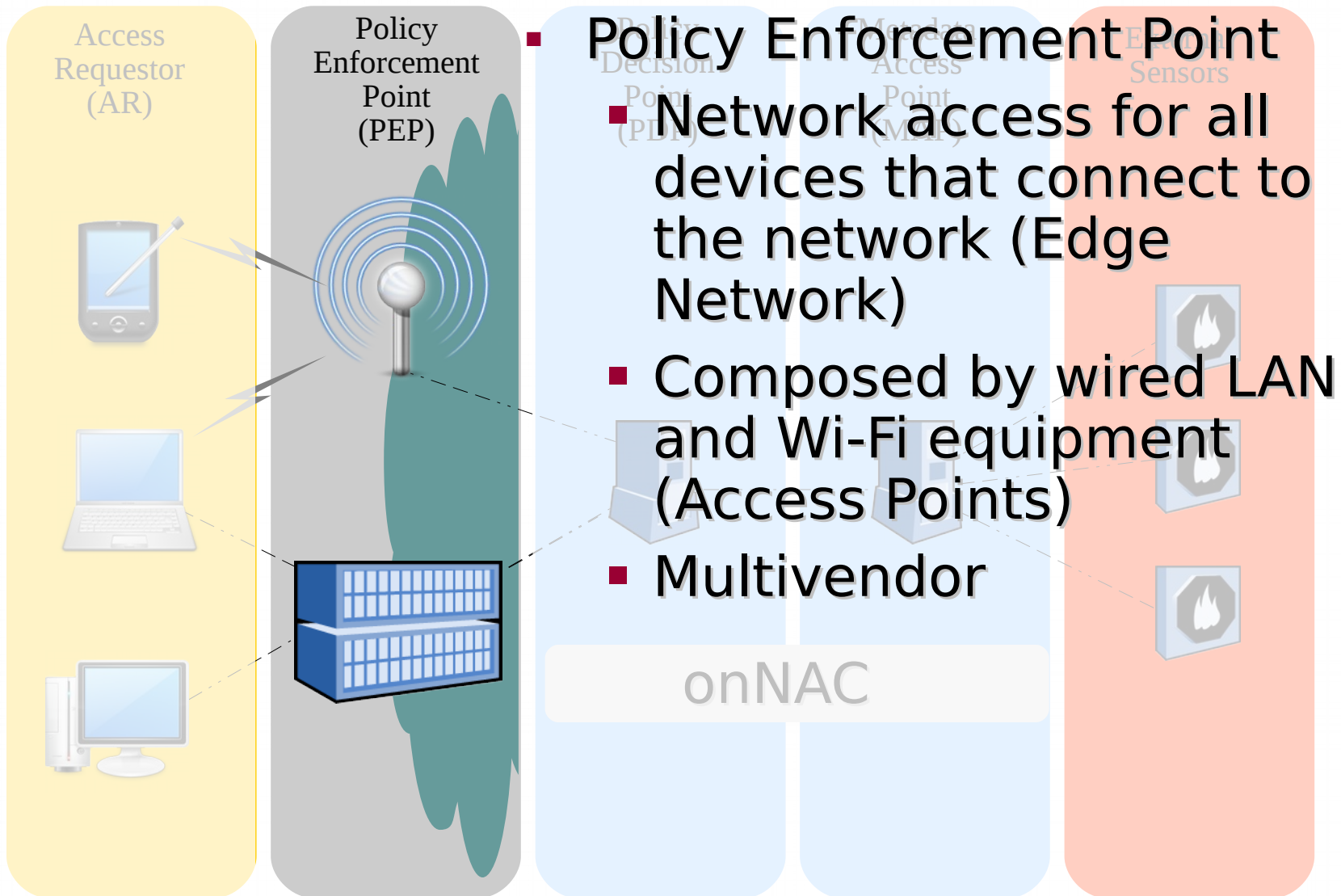
onNAC Architecture



onNAC Architecture



onNAC Architecture



onNAC Architecture

Policy Decision Point

- Service that allows system to take policy decisions that apply to each type of access based on identity, device, location, time, ...

Policy Decision Point (PDP)

Metadata Access Point (MAP)

External Sensors



onNAC

onNAC Architecture

Metadata Access Point

- Service that stores all data relating to incoming events
- All information is related to each other in order to maximize the utility
- Real time access to the information

Metadata Access Point (MAP)

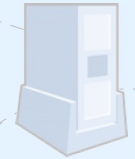
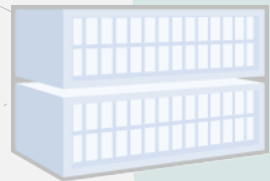
External Sensors

onNAC

onNAC Architecture

External Sensors

- Services such as IDS sensors or firewalls that can both provide new information to the platform as consulting onNAC information to make better decisions



onNAC

External Sensors



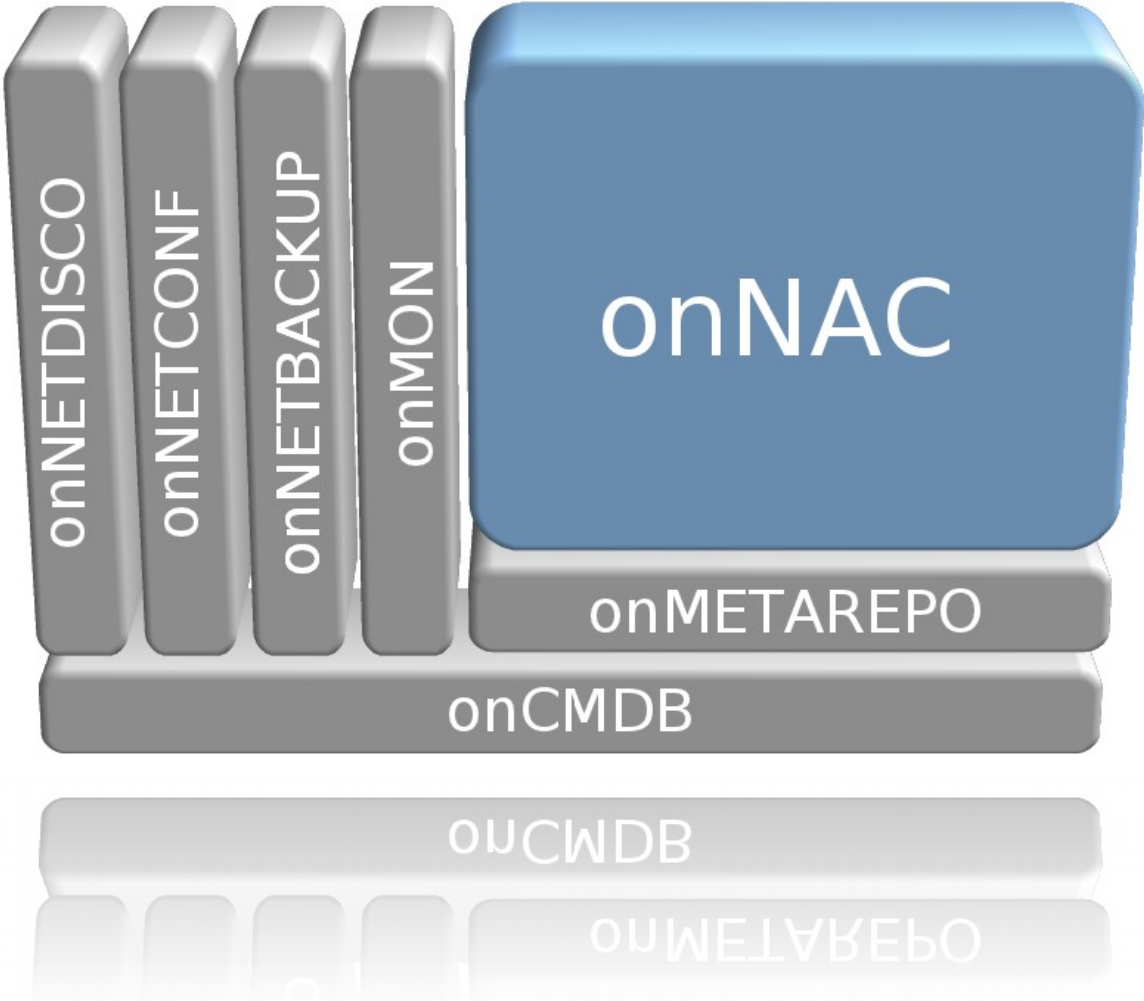
openNAC components



Modular architecture

- All information is stored in a CMDB
- Queue-based, allowing for greater scalability and traceability
- Very flexible identity backend, Idap, databases, etc ...
- Based in a REST APIs
- Frontend web based in DOJO
- Scripteable command line

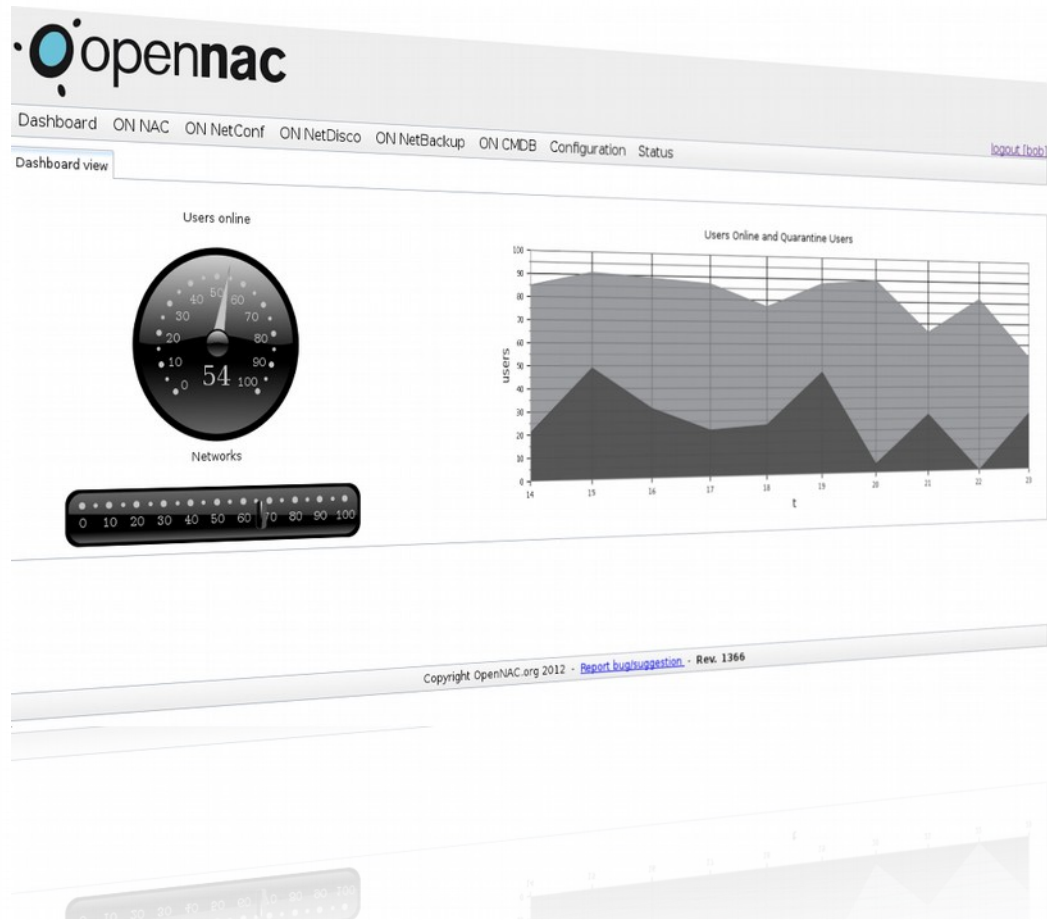
onNAC Component



onNAC description

- Is the main module, with the services of Authentication, Authorization and Audit Product
- Enables 802.1X authentication or captive web portal for all devices
- All security policy is defined and applied in this module
- Rogue devices detection

onNAC screenshots



Overall dashboard

onNAC screenshots

The screenshot displays the OpenNAC web interface. At the top, the OpenNAC logo is visible. Below it, a navigation bar contains links for Dashboard, ON NAC, ON NetConf, ON NetDisco, ON NetBackup, ON CVDB, Configuration, and Status. The user 'locut.lbb' is logged in. The main content area shows a table titled 'Dashboard view' with a 'Save filter' button. The table has columns for IP, MAC, User, Date, IP switch, Port switch, Wall socket, Type, and State. The data shows a list of users with their respective IP and MAC addresses, login dates, and switch information. The table is filtered to show 'No filter applied'.

IP	MAC	User	Date	IP switch	Port switch	Wall socket	Type	State
162.136.249.221	48:41:1:03:27:53	John	2012-05-29 11:13:57	172.16.1.33	37		SUPPLICANT	0
162.136.169.212	48:41:1:03:27:77	Martina	2012-05-29 11:13:57	172.16.1.42	13		SUPPLICANT	0
162.136.113.95	48:41:1:03:27:70	Maria	2012-05-29 11:13:57	172.16.1.41	4		SUPPLICANT	0
162.136.110.123	48:41:1:03:27:15	David	2012-05-29 11:13:57	172.16.1.35	29		SUPPLICANT	0
162.136.174.127	48:41:1:03:27:91	Albert	2012-05-29 11:13:57	172.16.1.49	7		SUPPLICANT	0
162.136.195.225	48:41:1:03:27:30	Oscar	2012-05-29 11:13:57	172.16.1.35	0		SUPPLICANT	0
162.136.76.259	48:41:1:03:27:30	Micuel	2012-05-29 11:13:57	172.16.1.44	26		SUPPLICANT	0
162.136.80.40	48:41:1:03:27:30	Ricerc	2012-05-29 11:13:57	172.16.1.32	16		SUPPLICANT	0
162.136.42.149	48:41:1:03:27:52	Xat	2012-05-29 11:13:57	172.16.1.33	8		SUPPLICANT	0
162.136.1164	48:41:1:03:27:38	Marc	2012-05-29 11:13:57	172.16.1.47	23		SUPPLICANT	0
162.136.228.153	48:41:1:03:27:48	John	2012-05-29 11:13:57	172.16.1.50	30		SUPPLICANT	0
162.136.245.78	48:41:1:03:27:39	bob	2012-05-29 11:13:57	172.16.1.33	15		SUPPLICANT	0

Copyright: OpenNAC.org 2012 Report bug/suggest: on Item: L3bb
Сopyright: OpenNAC.org 2012 Report bug/suggest: on Item: L3bb

State of users logged into the platform

onNAC screenshots - Policy

The screenshot displays the OpenNAC web interface. At the top, the OpenNAC logo is visible. Below it, a navigation bar includes links for Dashboard, ON NAC, ON NetConf, ON NetDisco, ON NetBackup, ON CMDB, Configuration, and Status. The current view is 'OnNAC Policy'. Action buttons include 'Add Rule', 'Edit Rule', 'Delete Rule', and 'Apply'. A 'Save filter' button is also present. The main content is a table with columns: Time, User/Identity, Switch, Vlan, Security Profile, and Comment. The table lists various policies, each with a checkbox and a red 'X' icon in the right margin.

<input type="checkbox"/>	Time	User/Identity	Switch	Vlan	Security Profile	Comment	
<input type="checkbox"/>	No filter applied						
<input type="checkbox"/>	Working hours	external consultant	ANY	Consultants	Internet	Connexion of external consultants	X
<input type="checkbox"/>	ANY	HR	ANY	HR	HR	HR group can access to HR services	X
<input type="checkbox"/>	ANY	Students	Training rooms,WIFI	Training	Training	Training facilities	X
<input type="checkbox"/>	ANY	System admin	ANY	System Admin	SysAdmin	System administrator access	X
<input type="checkbox"/>	ANY	Users	ANY	Users	Default	Default user profile	X
<input type="checkbox"/>	ANY	[no: auth]	ANY	external	Limited Internet	Default connexion for non authenticated users	X
<input type="checkbox"/>	ANY	[no: auth]	ANY	external	Limited Internet	Default connexion for non authenticated users	X
<input type="checkbox"/>	ANY	Users	ANY	Users	Default	Default user profile	X
<input type="checkbox"/>	ANY	System admin	ANY	System Admin	SysAdmin	System administrator access	X
<input type="checkbox"/>	ANY	Students	Training rooms,WIFI	Training	Training	Training facilities	X
<input type="checkbox"/>	ANY	HR	ANY	HR	HR	HR group can access to HR services	X
<input type="checkbox"/>	ANY	external consultant	ANY	Consultants	Internet	Connexion of external consultants	X

Comprehensive security policy to apply to all users

onNAC screenshots - Policy

Firefox Mozilla Firefox
http://192.168.104.253/admin/ 192.168.104.253/admin/ Google

OpenNAC

Dashboard ON NAC ON NetConf ON NetBackup ON CN

Dashboard view onNAC status OnNAC Policy

Add new Edit Delete Save order Discard order Refresh

Time	User/Identity	Device
00:00-01:00	albert.sole some Idap	test15000
03:00-04:00		
00:00-24:00	albert.sole some Idap	9C:E6:35
00:00-24:00	test2	quest user

Edit

Time: 0 item(s) selected

User/Identity: albert.sole

User group:

LDAP filter:

Device: ANY

Device group: test15000

*Vlan: SERVICE

VLANID: 330

Security Profile: ANY

Plugins: 0 item(s) selected

On error: 0 item(s) selected

Message: message

Comment: comment

Accept Cancel

Plugins	Log error	Alert cr
	0	1
	0	0
w7detect	0	0

logout [admin]

Copyright OpenNAC.org 2013 - > [Report bug/suggestion](#) - Rev. 2713M

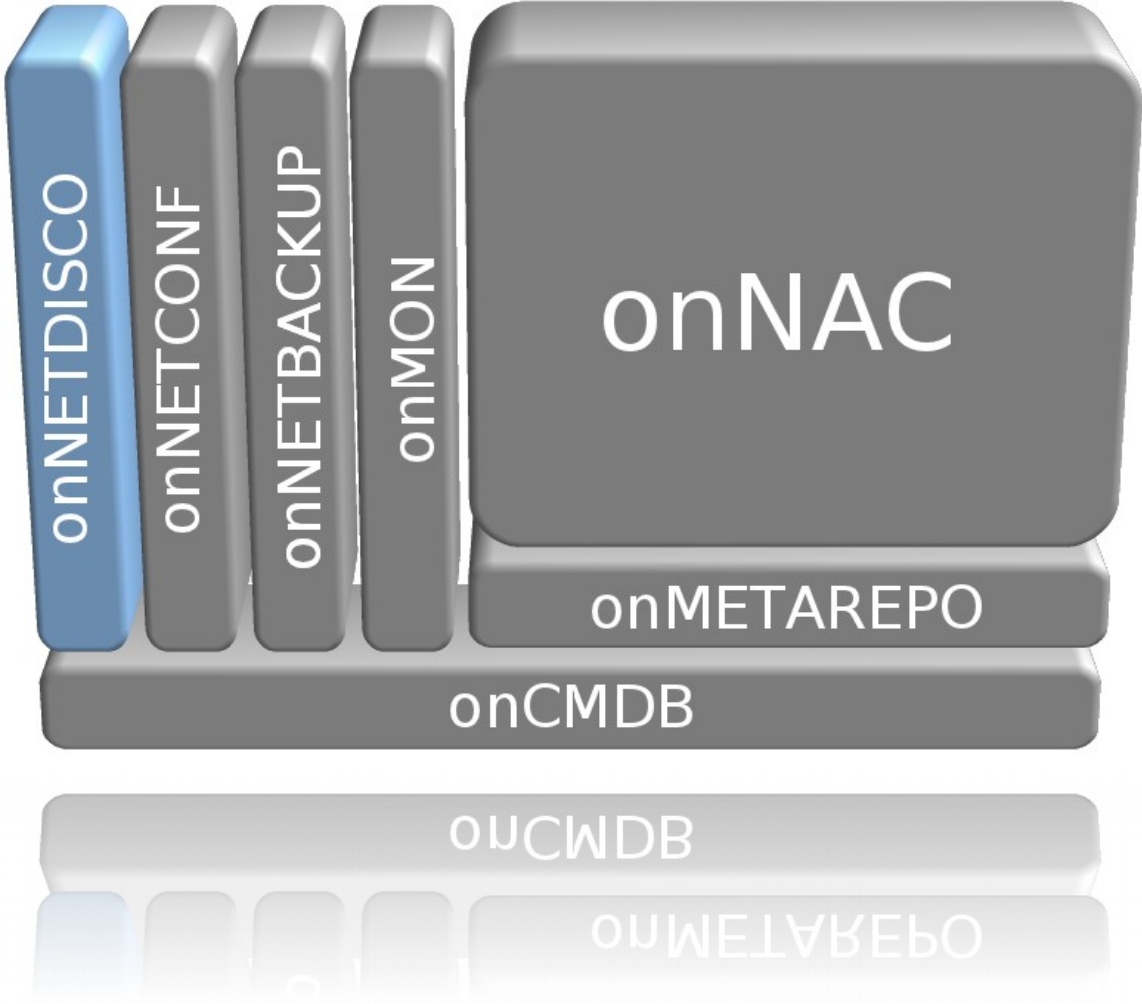
onNAC screenshots - CMDB

Dashboard view | onNAC status | OnNAC Policy | Network Devices

Add new Delete Save Discard Refresh Export data Import data Groups: -- none --

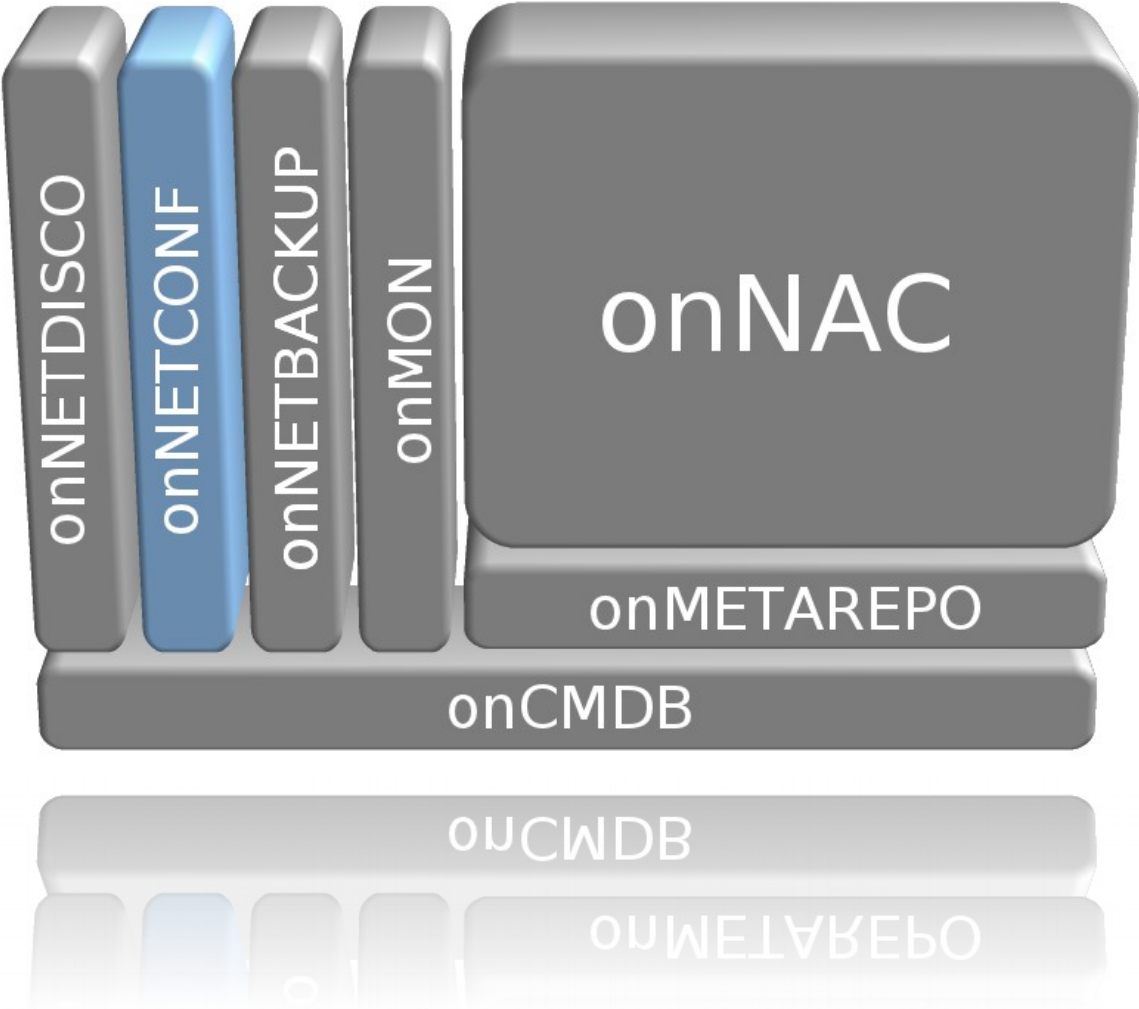
<input type="checkbox"/>	IP	Version	MAC Address	SNMP RO	SNMP RW	Purchase date	Purchase order	Warranty	Maintenance	EOL	Telnet user
<input type="checkbox"/>	192.168.108.44	1.19	00:AA:BB:CC:DD:EE	public	public	22/09/2012	1	12/02/2013	27/02/2013	22/09/2012	provas
<input type="checkbox"/>	192.168.108.50	1.19	00:AA:BB:CC:DD:EE	public	public	22/09/2012	1	27/02/2013	27/02/2013	22/09/2012	provas
<input type="checkbox"/>	192.168.108.51	1.19	00:AA:BB:CC:DD:EE	public	public	24/10/2013		24/10/2013	24/10/2013	24/10/2013	test

onNETDISCO component



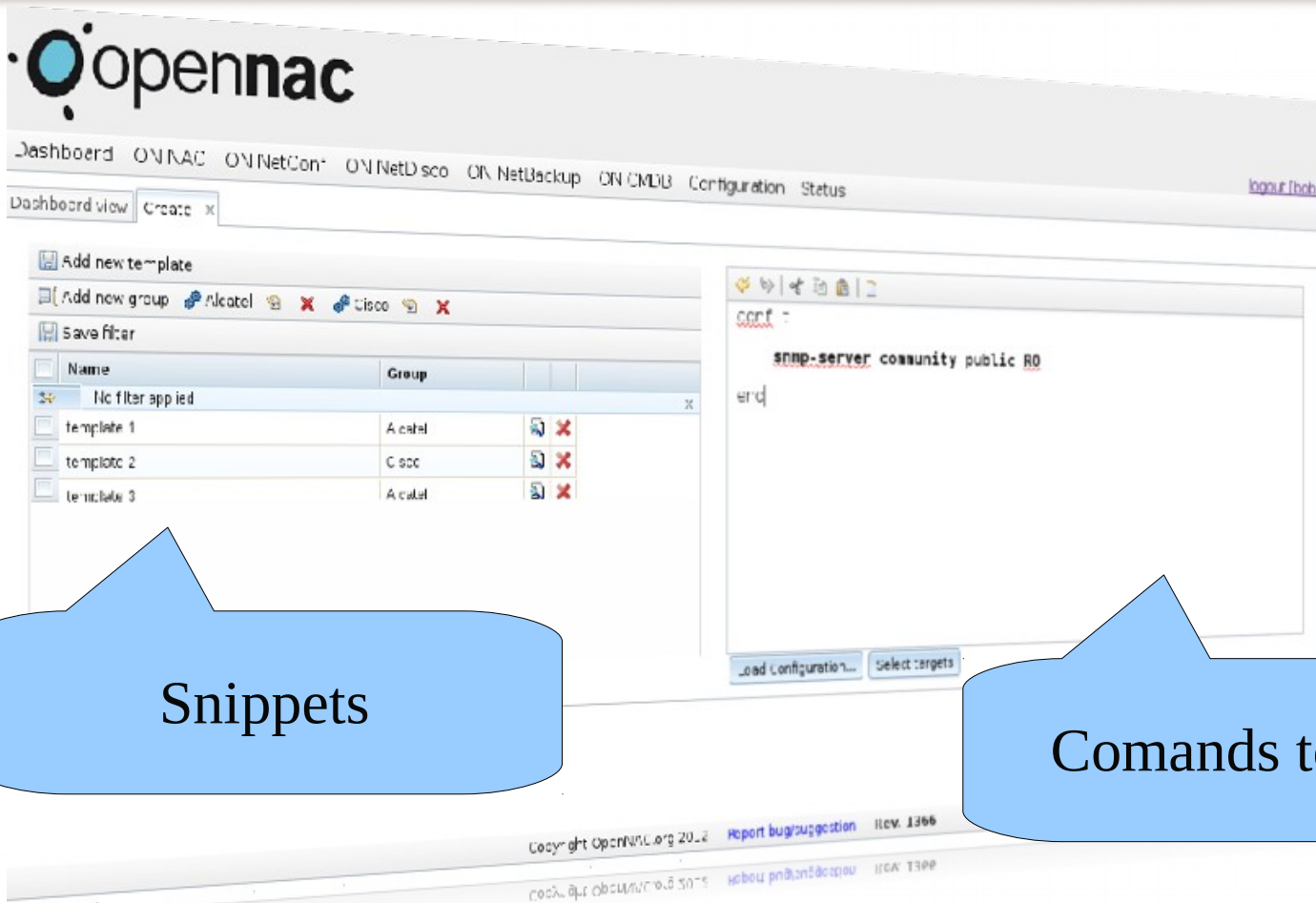
- Allows discovery of network devices
- Store discovered devices in the CMDB
- Maintains the inventory updated
- Discover the network topology, detecting devices without redundant links
- Allows periodic discovery tasks
- Queue-based
- Allows you to export the results to csv

onNETCONF component



- Network Equipment Configurator allows you to define configuration templates and apply them to sets of network equipment
- Frontend web or Web Service
- Based on a service queue to ensure traceability and integrity of any action
- Very useful for applying settings to large amount of network equipment
- Very useful to install and configure NAC service

onNETCONF Screenshots - Template



Snippets

Comands to send

Create a configuration template to send a group of network devices

onNETCONF Screenshots - Devices

The screenshot displays the OpenNAC web interface. At the top, the OpenNAC logo is visible. Below it, a navigation bar contains links for Dashboard, ON NAC, ON NetConf, ON NetDisco, ON NetBackup, ON CMDB, Configuration, and Status. A user profile for 'bob' is shown in the top right corner. The main content area is titled 'Targets' and 'Configuration'. It includes options for 'Add new group', 'Group 1', and 'Group 2'. A 'Save filter' button is also present. The central part of the interface is a table with the following data:

IP	Manufacturer	Family	Model
No filter applied			
<input type="checkbox"/> 10.128.60.250	ALCATEL	62244	OMNISTACK
<input type="checkbox"/> 10.128.60.249	ALCATEL	62244	OMNISTACK
<input type="checkbox"/> 10.128.60.250	ALCATEL	62244	OMNISTACK
<input type="checkbox"/> 10.128.60.249	ALCATEL	62244	OMNISTACK

At the bottom of the interface, there is a footer with copyright information: 'Copyright OpenNAC.org 2012 - Report bug/suggestion - Rev. 1367'.

Network device list

Equipment selection

onNETCONF Screenshots - Results

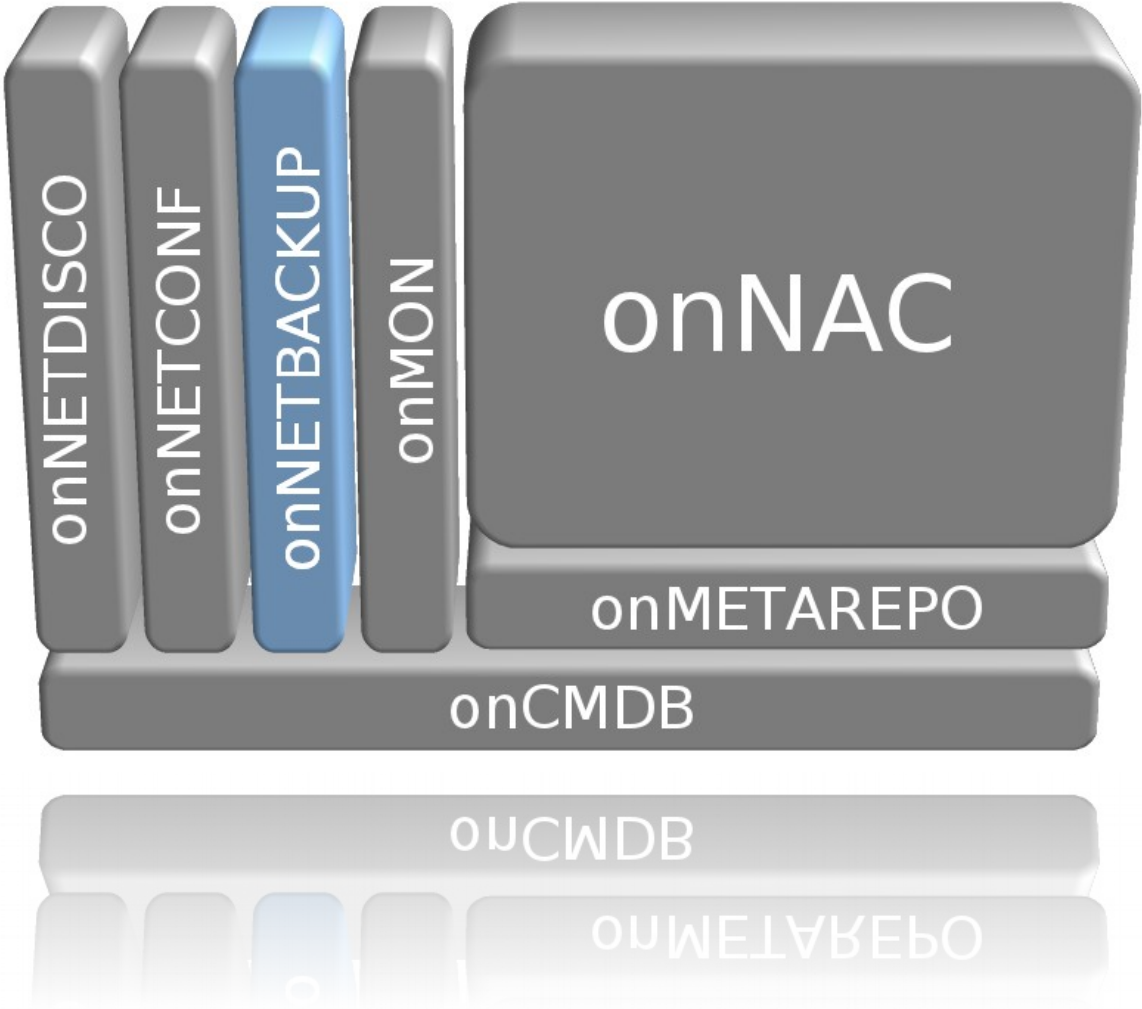
The screenshot displays the OpenNAC web interface. At the top left is the OpenNAC logo. The navigation bar includes links for Dashboard, ON NAC, ON NetConf, ON NetDisco, ON NetBackup, ON CMDB, Configuration, and Status. A user is logged in as 'bob'. The main content area shows a table of configuration tasks with columns for Subjob ID, Job ID, User ID, IP, Date, and State. The table contains four rows of data. Below the table, there is a footer with copyright information for OpenNAC.org 2012 and a link to report a bug/suggestion.

Subjob ID	Job ID	User ID	IP	Date	State
166561	1122	bob	10.128.60.250	2011-05-29 17:19:40	End Job
166560	1121	bob	10.128.60.249	2011-05-29 17:19:30	End Job
166559	1122	bob	10.128.60.250	2011-05-29 17:19:01	Create Job
166558	1121	bob	10.128.60.249	2011-05-29 17:18:01	Create Job

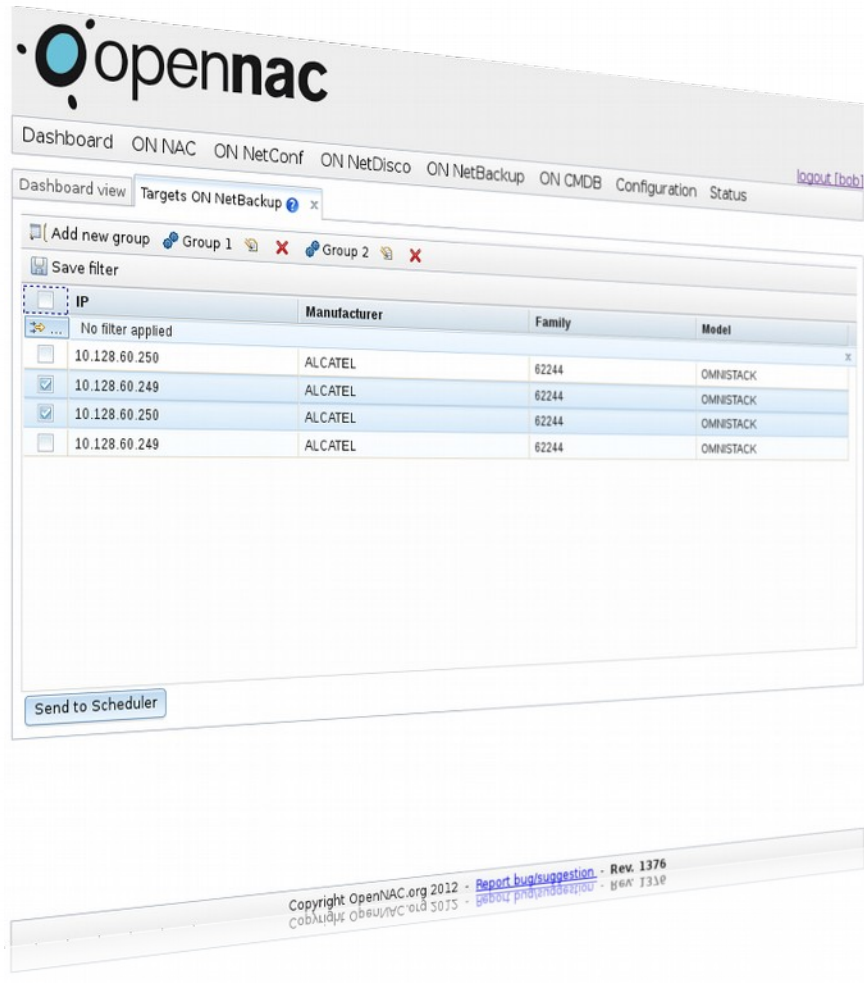
Copyright OpenNAC.org 2012 - [Report bug/suggestion](#) - Rev. 1367

Viewing the results of configuration tasks

onNETBACKUP component



- Make backups and automatic archiving of network devices configurations
- Allows programming device groups copies
- Allows define retention policy
- Based on a service queue to ensure traceability and integrity of any action



Selection of devices to perform backups

OpenNAC

Dashboard ON NAC ON NetConf ON NetDisco ON NetBackup ON CMDB Configuration Status [logout \(bob\)](#)

Dashboard view Targets ON NetBackup Scheduler ON NetBackup

Save filter

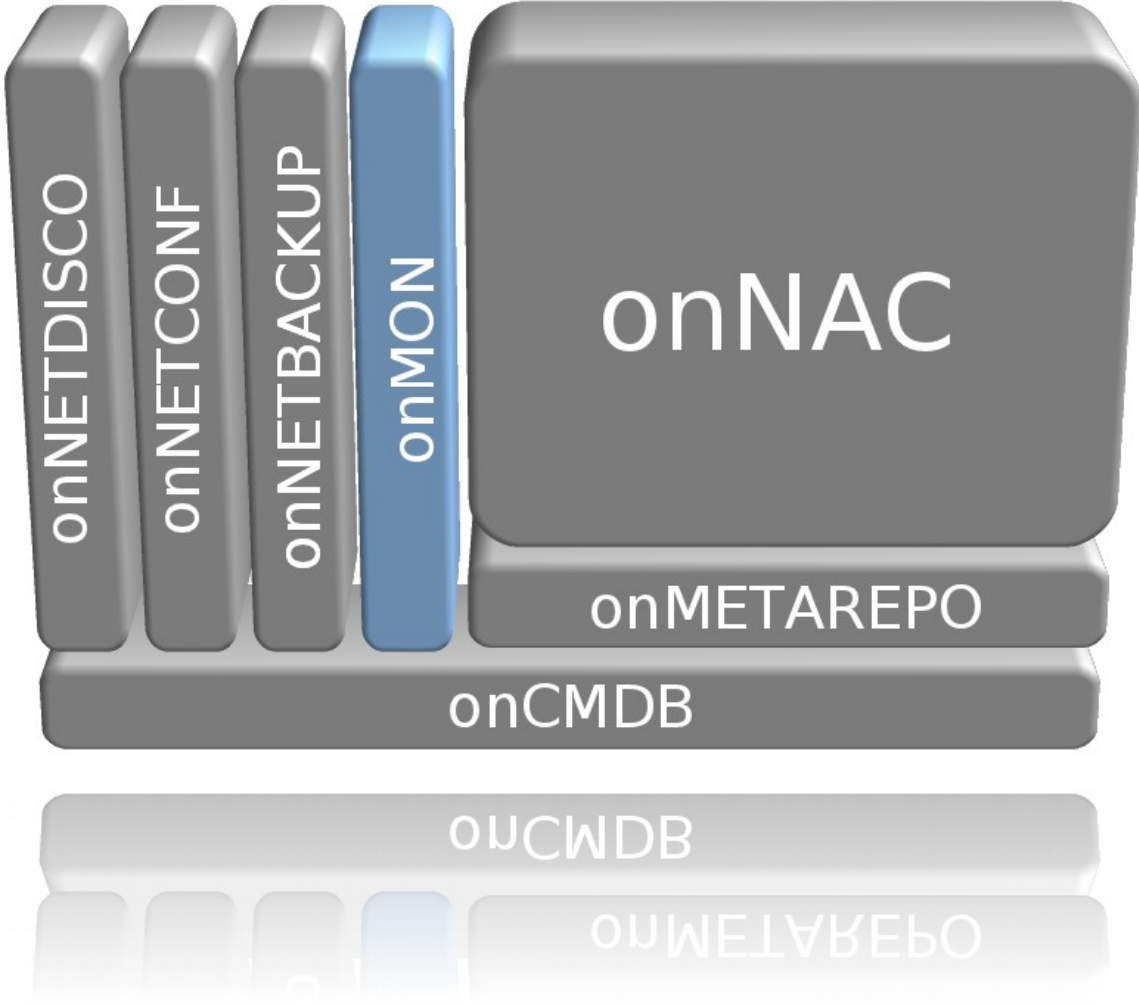
Minute	Hour	Day of Month	Month	Day of Week	Job	Status
59	23	*	2	*	Job 3	
45	13	*	6	1	Job 4	
00	8	1	12	*	Job 5	
10	15	*	*	*	Job 6	

Copyright OpenNAC.org 2012 - [Report bug/suggestion](#) - Rev. 1376

Copyright OpenNAC.org 2012 - [Report bug/suggestion](#) - Rev. 1376

Display planning backups

onMON component



- Monitoring is provisioned automatically from the CMDB
- Monitoring profiles available based on device type
- Real time network devices status
- Generates alerts if any of the parts of the network is not working properly



Navigation bar with menu items: STATUS, ALERTS, MODULES, HISTORY, CONFIGURATION, ADVANCED, SERVER, HELP. Server status: ● Configuration status: ● Logged in as admin Logout. Search input field with a magnifying glass icon.

Service Status > AGS > ES > JAVIER FERRERO > Network_JF > cisco-switch-12



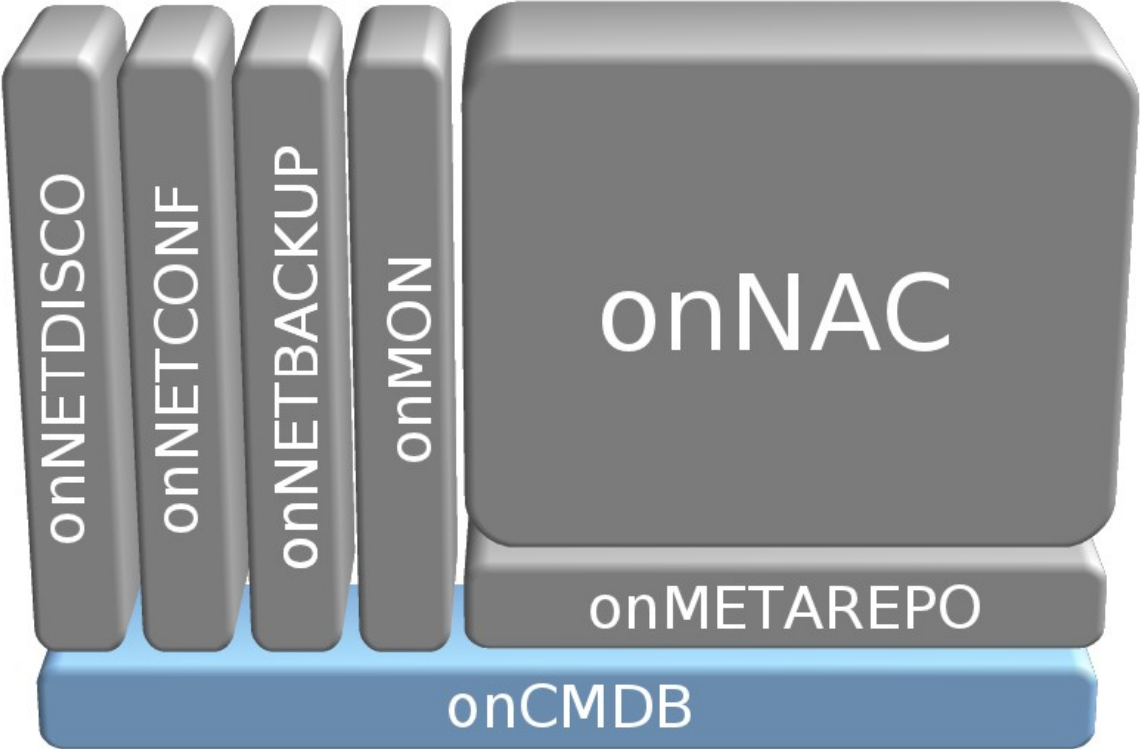
Host	Service	Status	Last Check	#	Status Information
cisco-switch-12	Cisco CPU load	OK	2012-05-12 16:58:12	1/3	Status is OK - CPU load average (5 min): 1 %, temperature normal
	Cisco memory utilisation	OK	2012-05-12 16:53:35	1/3	Status is OK - MEMORY: total: 36.78 MB, used: 17.27 MB (47%), free: 19.51 MB
Totals	2	2 OK			



Opsview Community Edition is supplied free of charge with no support, no maintenance and no warranty by Opsview or its Certified Partners. [Click here for support and enterprise modules](#)
© Opsview Limited 2012 All Rights Reserved

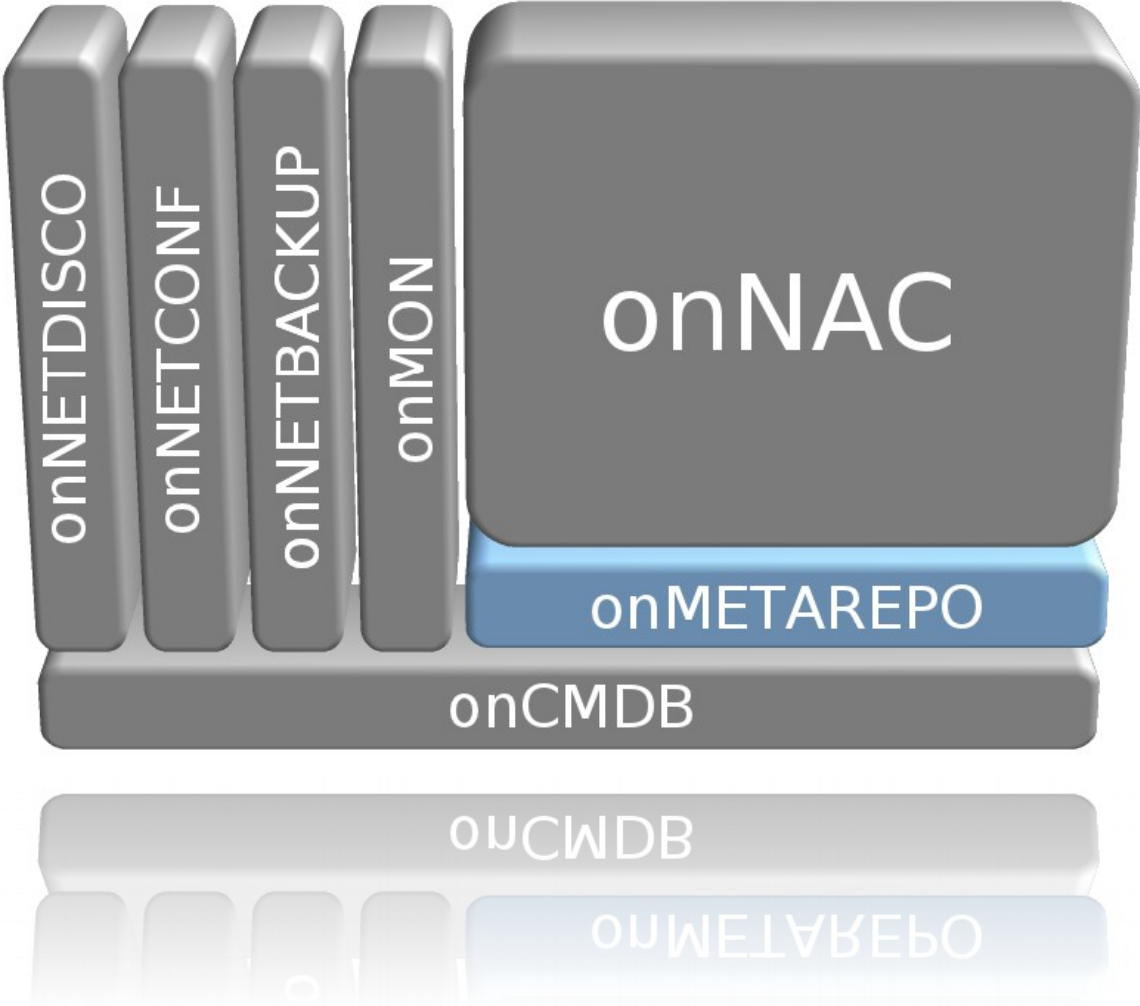
Viewing the status of a network computer

onCMDB component

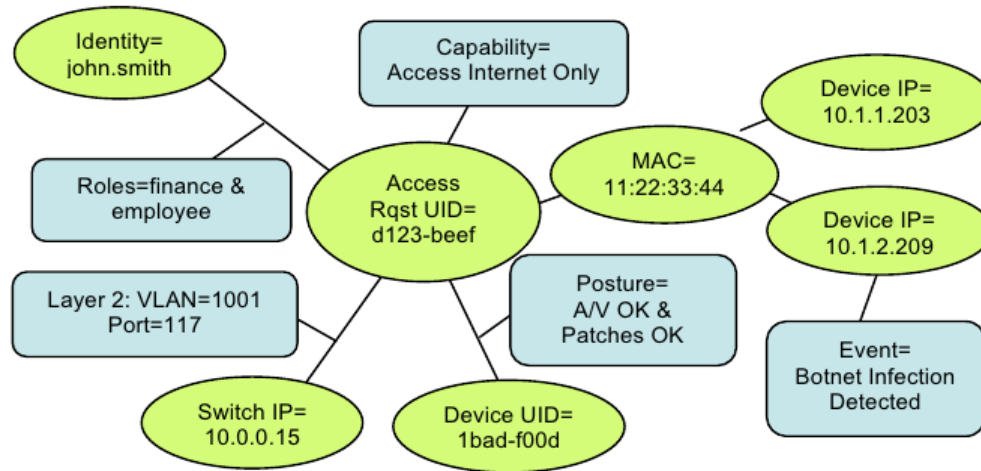


- The module CMDB is the repository of all information of the inventory
- Allows you to easily share information with other platforms
- It stores all the basic elements that use the platform as network devices, security rules, networks, groups, VLAN, ...

onMETAREPO component



- METADATA Access Point server module
- It uses protocol IF-MAP



openNAC services

- Security Consulting
 - Set architecture and methodology appropriate for a client to improve the security of access and authorization from your network
- Roll out
 - openNAC setups in companies and organizations
- Support
 - 7x24 support to openNAC installations
- Development and customization
 - Creating specific modules and functionality to customers
 - Support new infrastructure
- Integration
 - Integrating the solution with third tools

Contact

- <http://www.opennac.org>
- info@opennac.org
- Twitter: @opennac

·  opennac