@opennac

Network access control and management solution

Xavier Gonzálẹz
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 differents 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

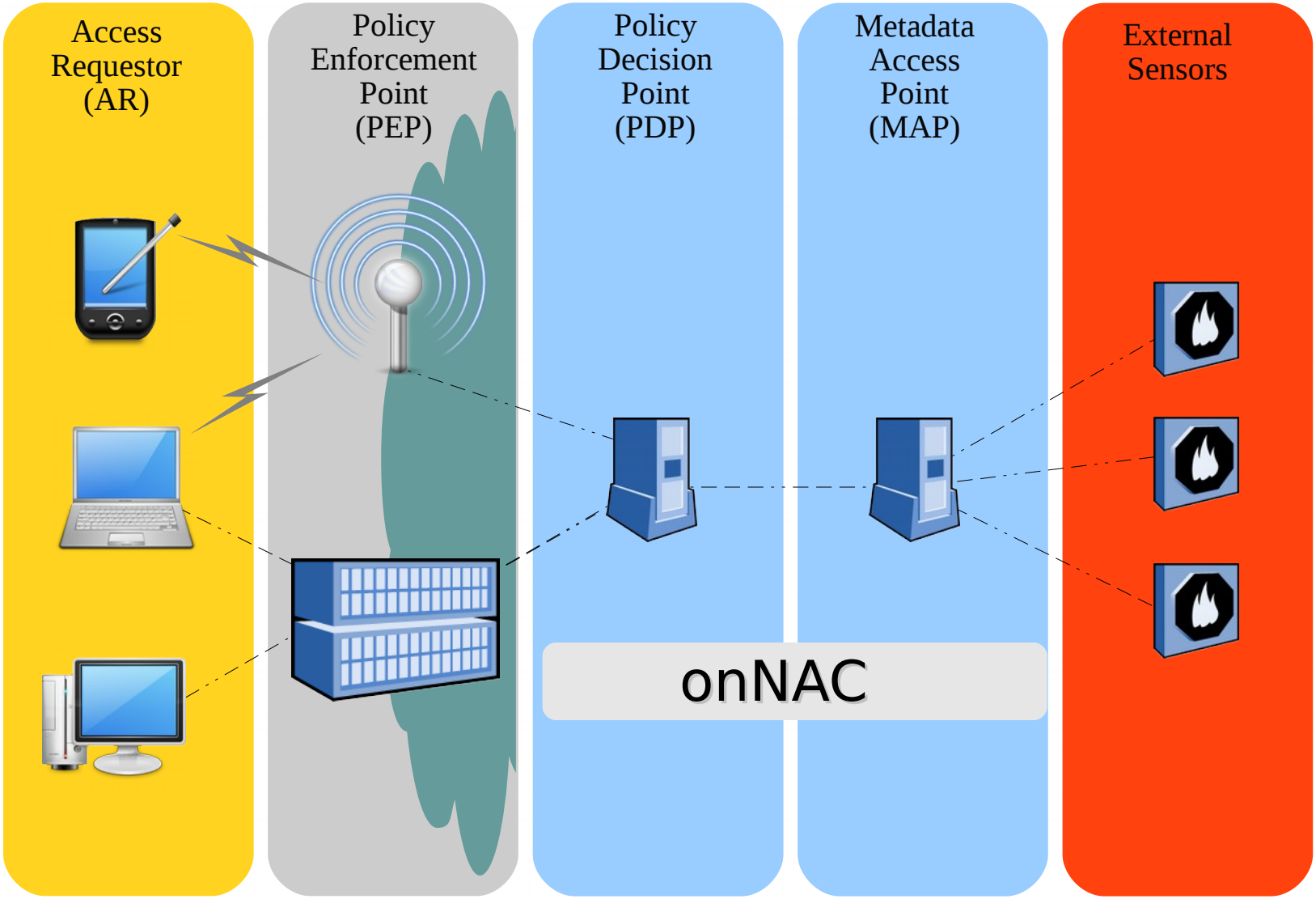
What does openNAC can do?

- 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

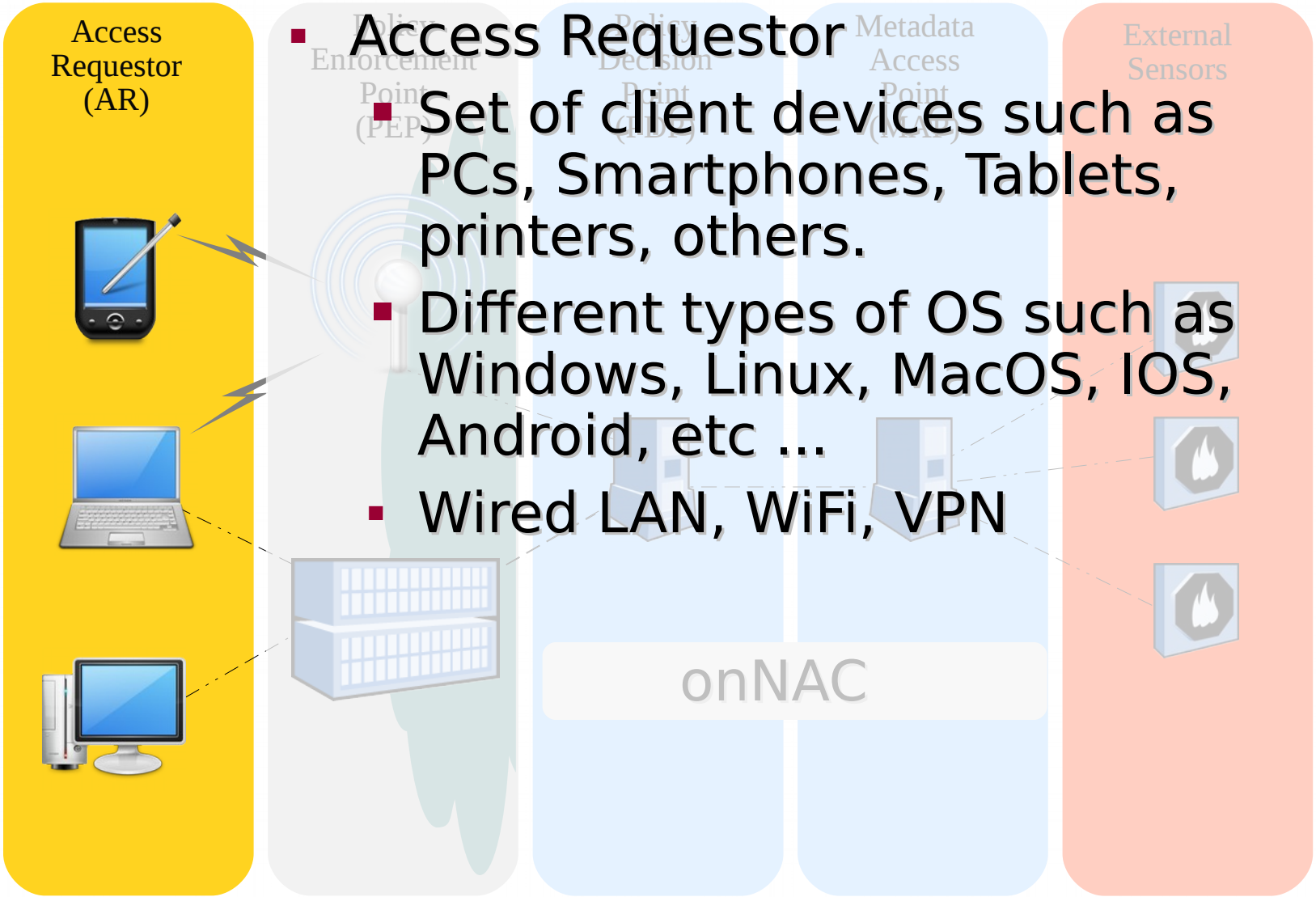
Features

- 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 conected to enforce an access policy

onNAC Architecture

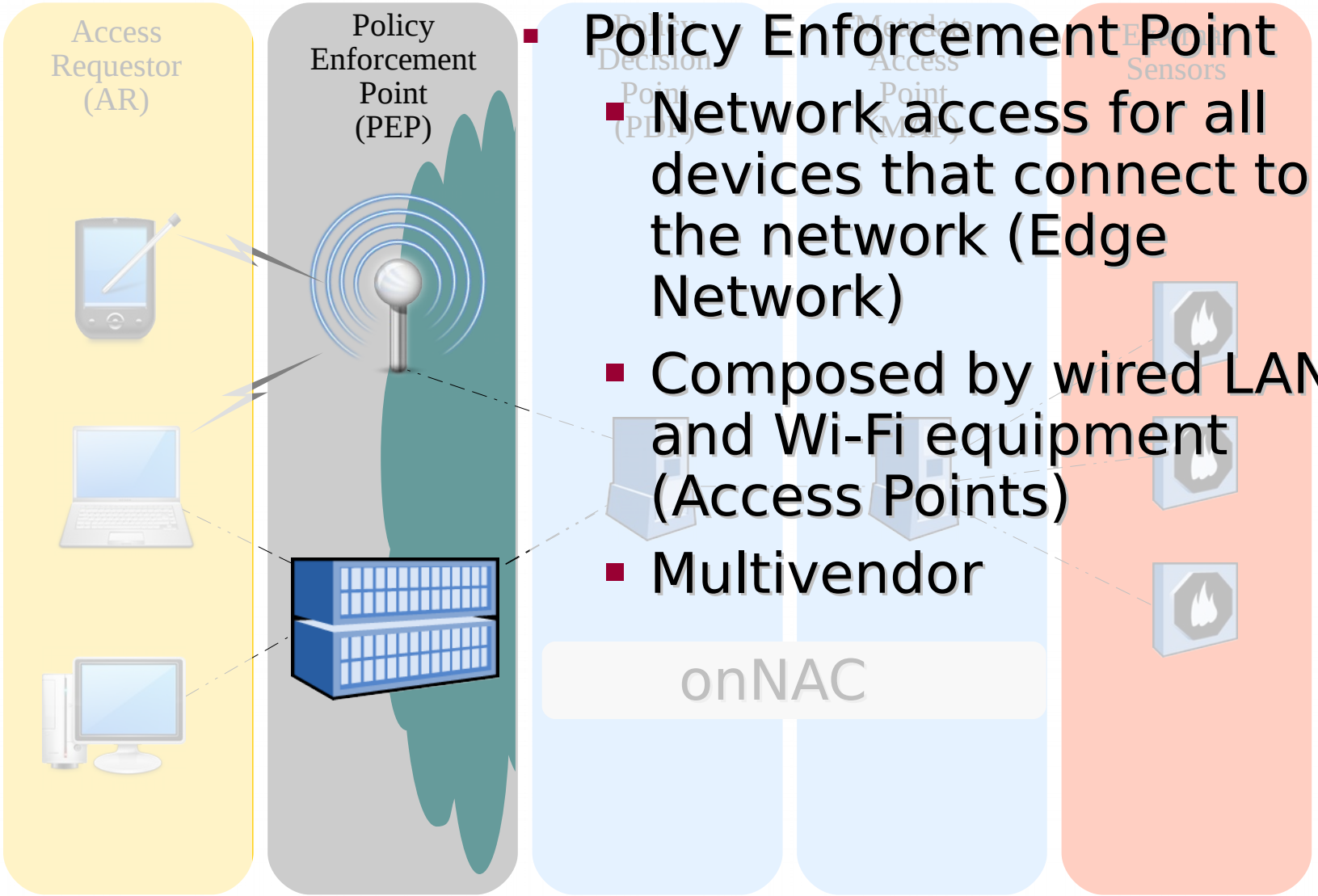


onNAC Architecture



- Access Requestor
  - Set of client devices such as PCs, Smartphones, Tablets, printers, others.
  - Different types of OS such as Windows, Linux, MacOS, IOS, Android, etc ...
  - Wired LAN, WiFi, VPN

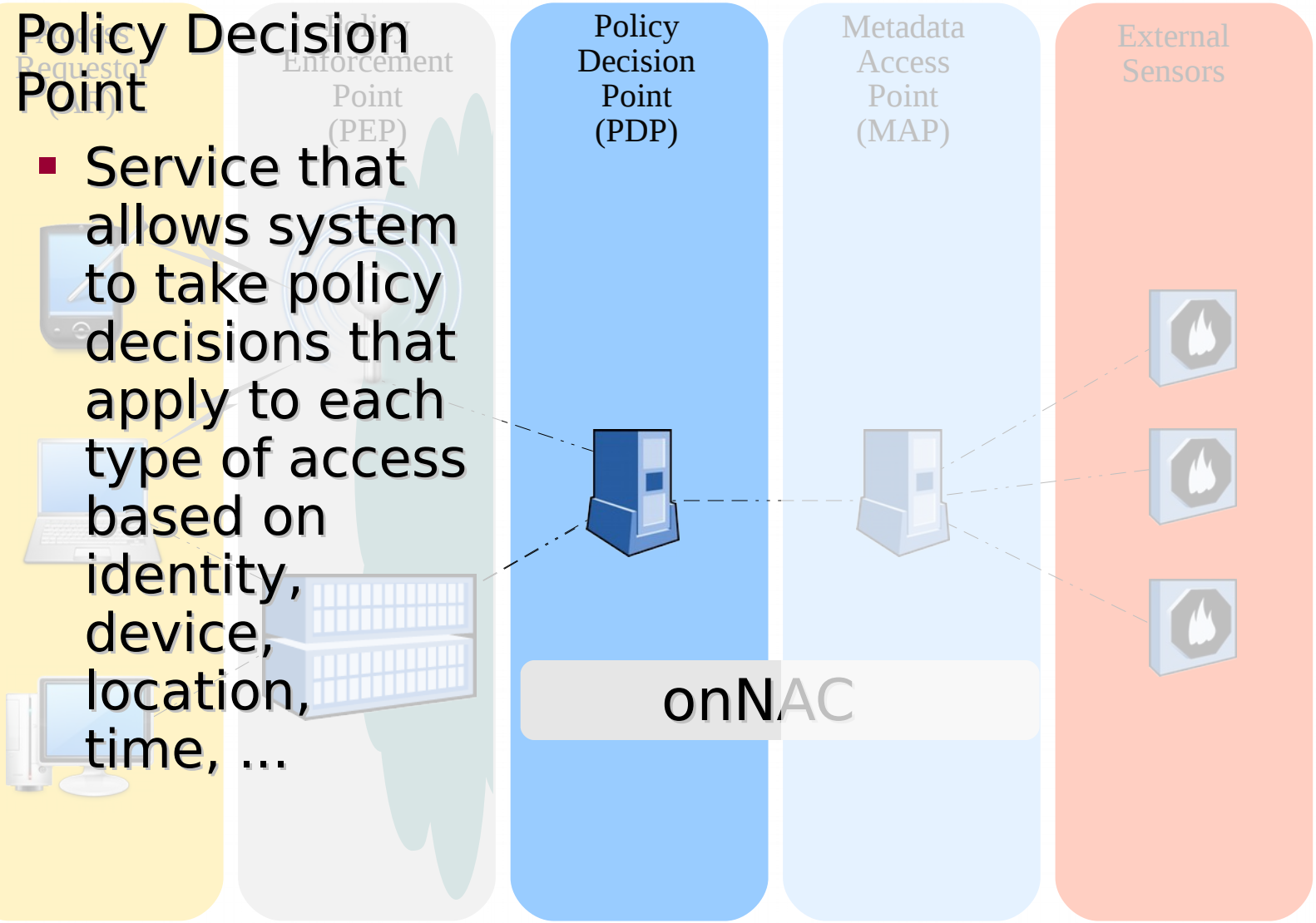
onNAC Architecture



- Policy Enforcement Point
  - Network access for all devices that connect to the network (Edge Network)
  - Composed by wired LAN and Wi-Fi equipment (Access Points)
  - Multivendor

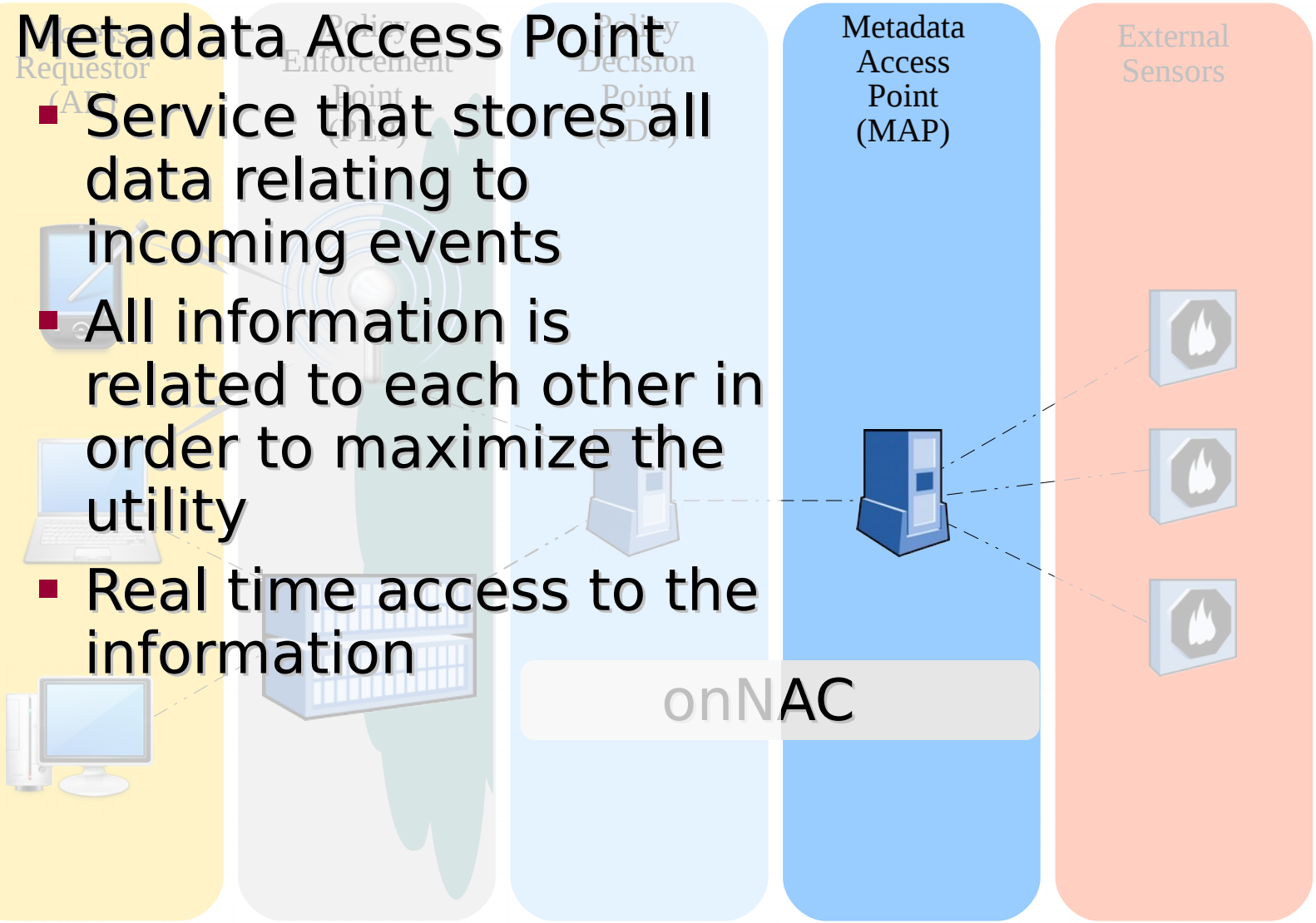
onNAC Architecture

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



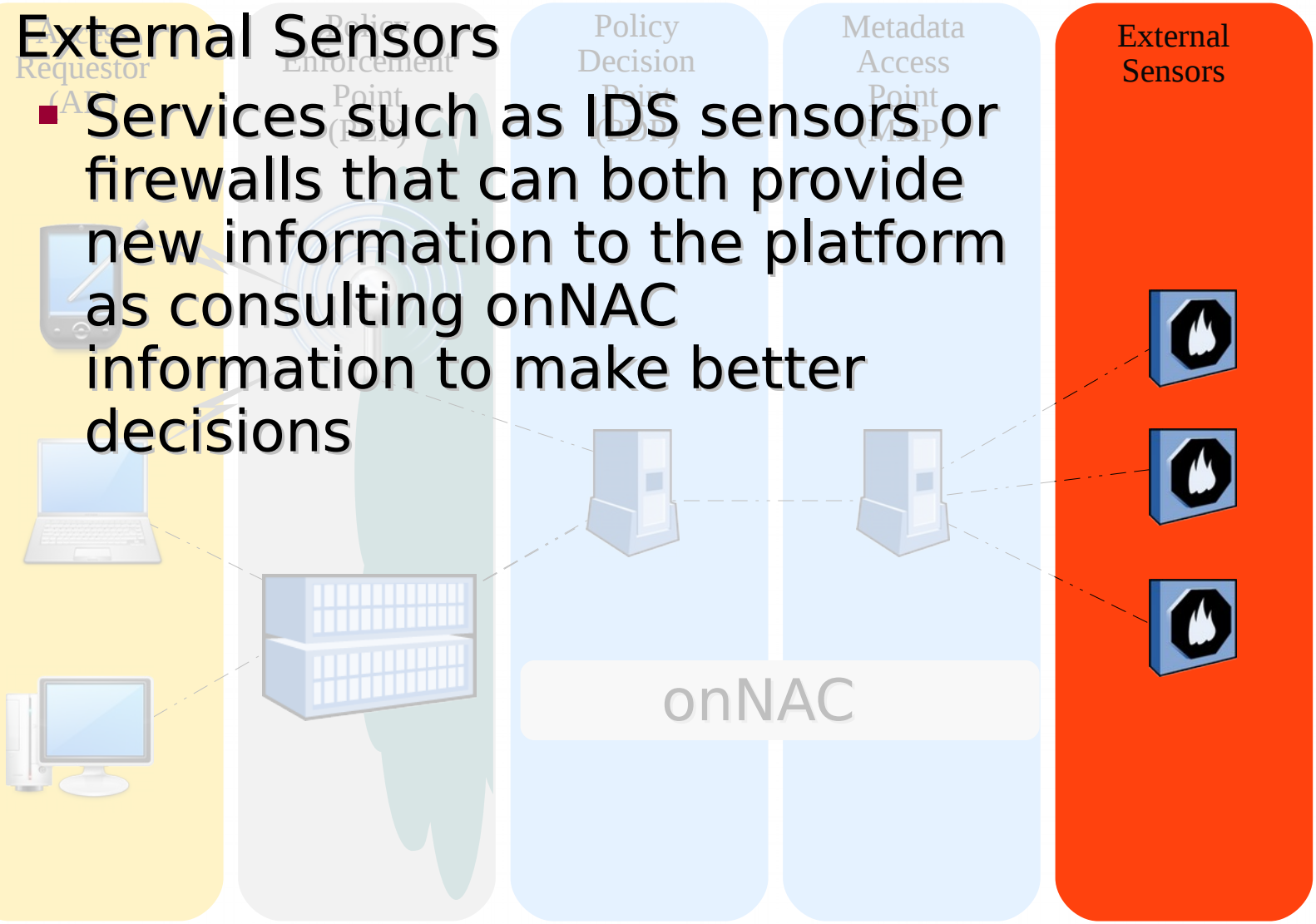
onNAC Architecture

- 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

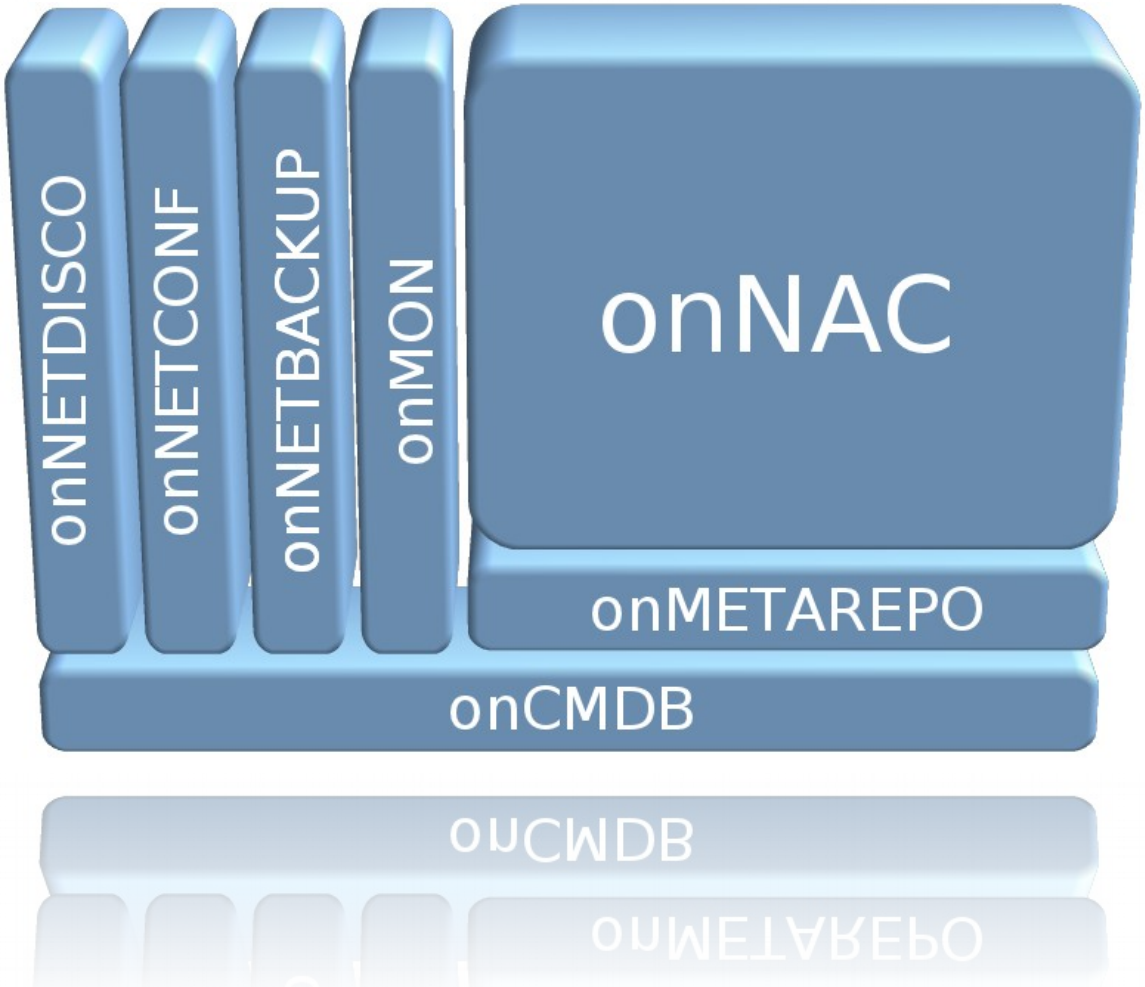


onNAC Architecture

- 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



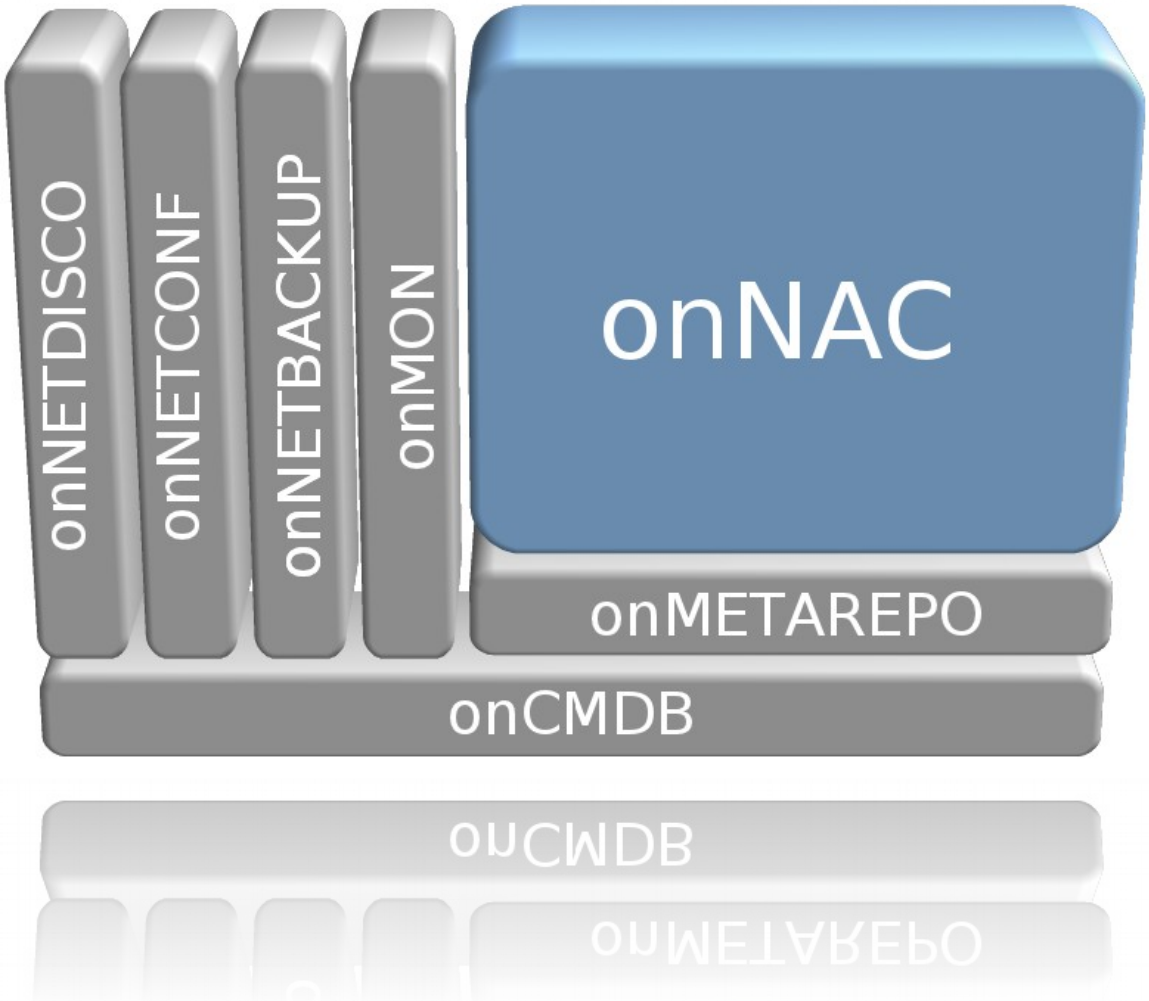
openNAC components



Modular architecture

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

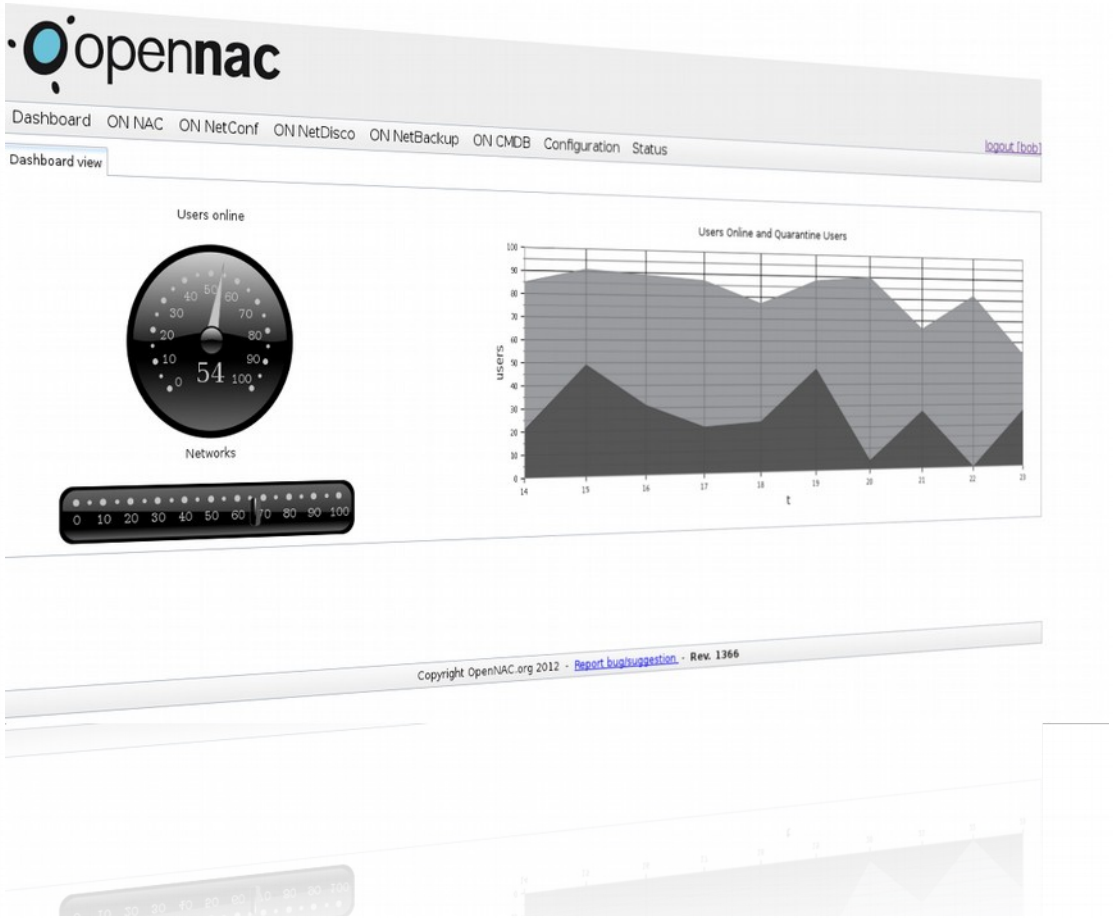
onNAC Component



onNAC description

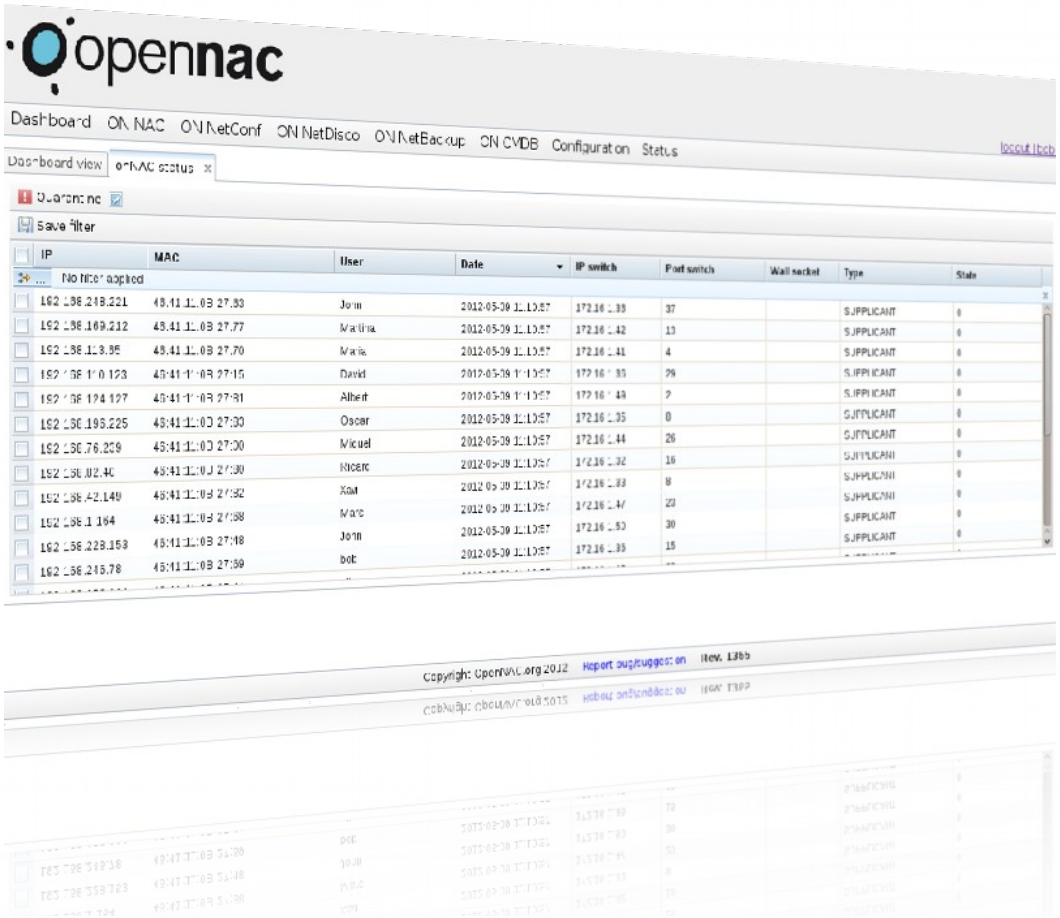
- Is the main module, with the services of Authentication, Authorization and Audit Product
- Enables 802.1X authentication or captive web portal for all devices
- All security policy is defined and applied in this module
- Rogue devices detection

onNAC screenshots



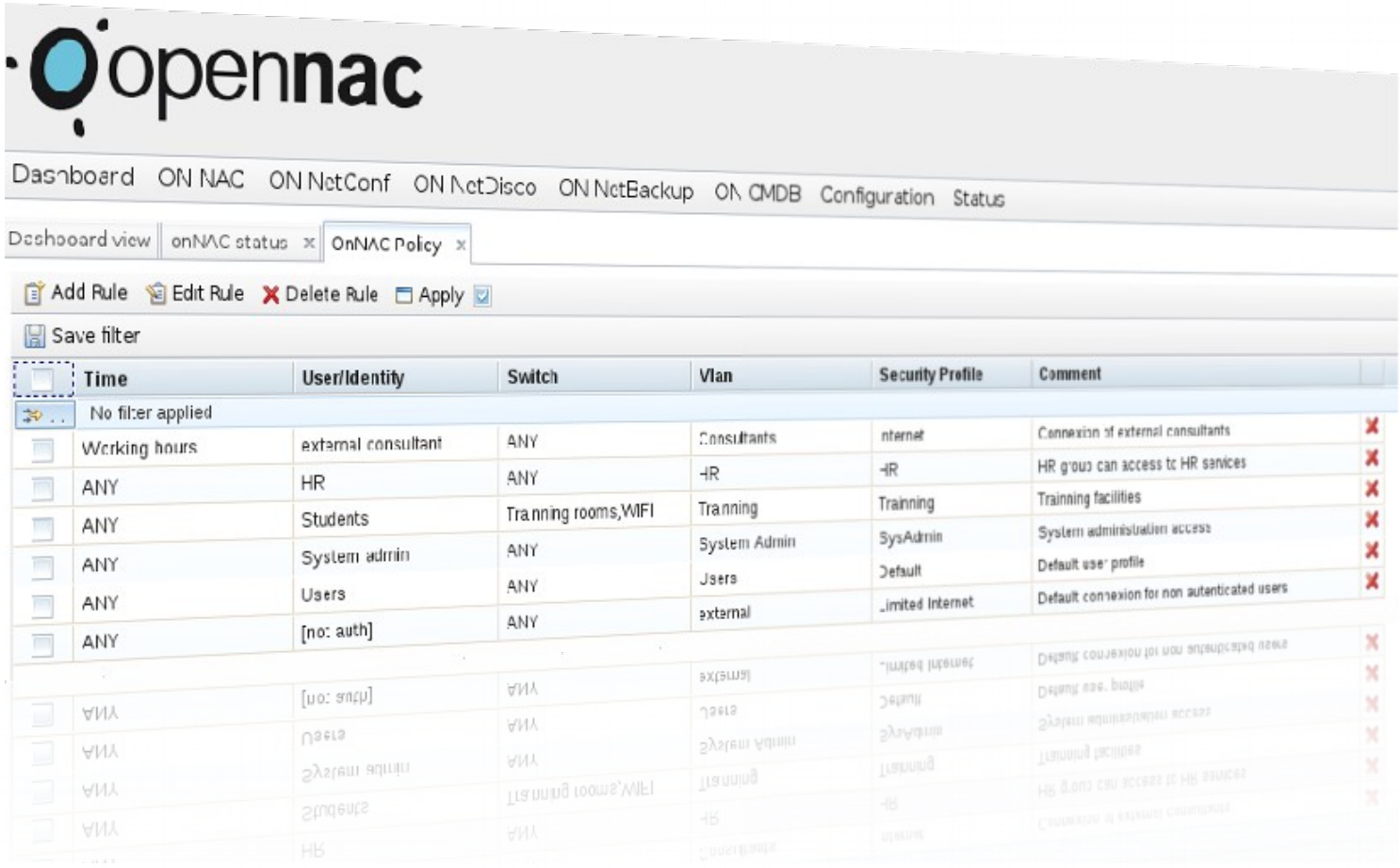
Overall dashboard

onNAC screenshots



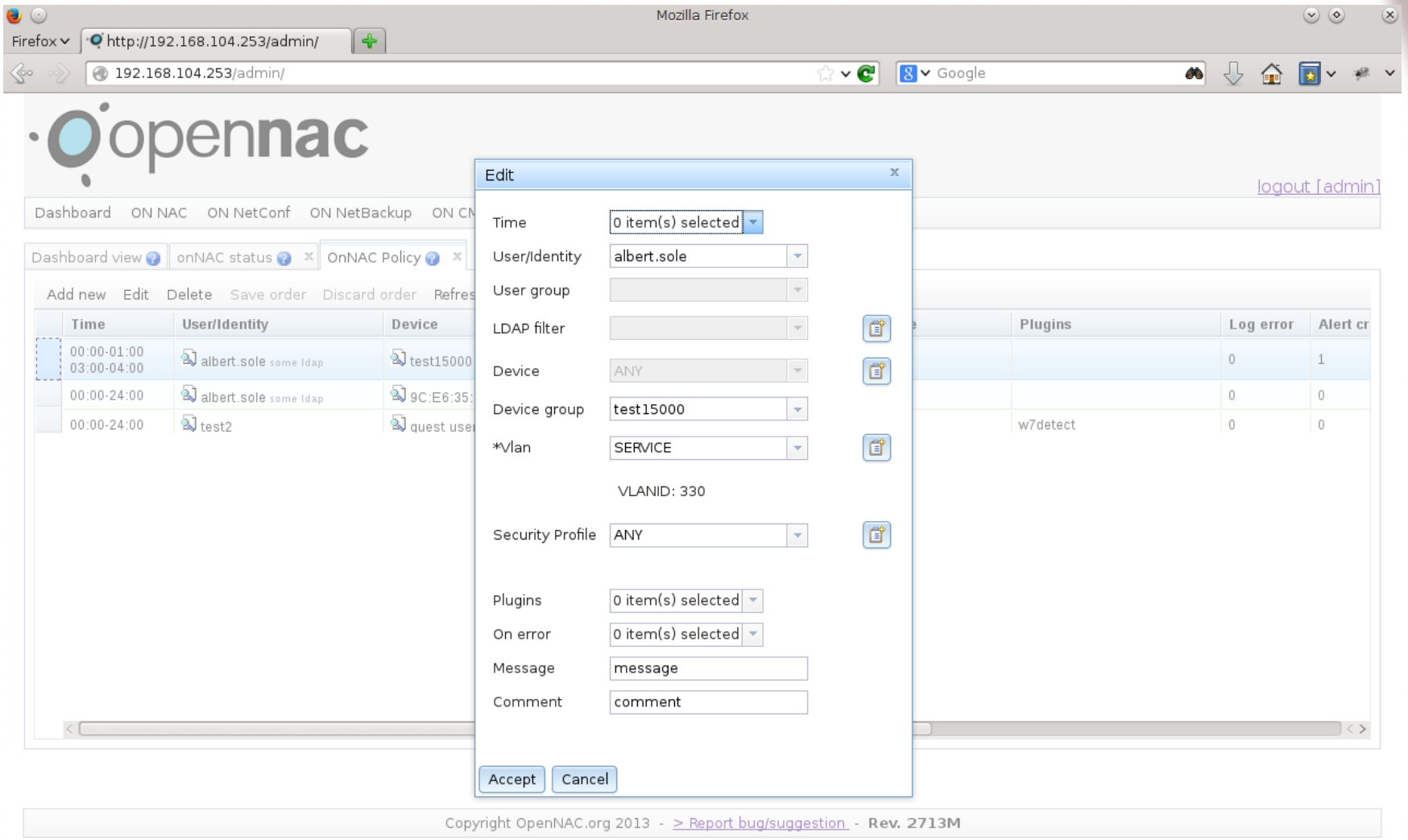
State of users logged into the platform

onNAC screenshots - Policy

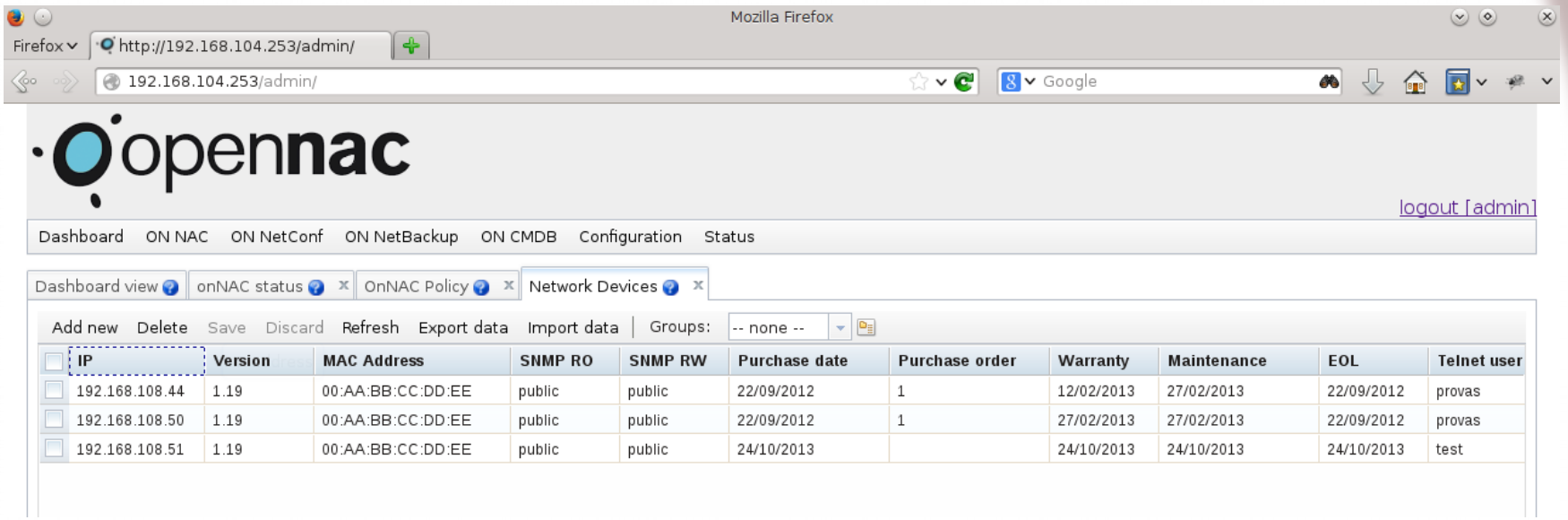


Comprehensive security policy to apply to all users

onNAC screenshots - Policy

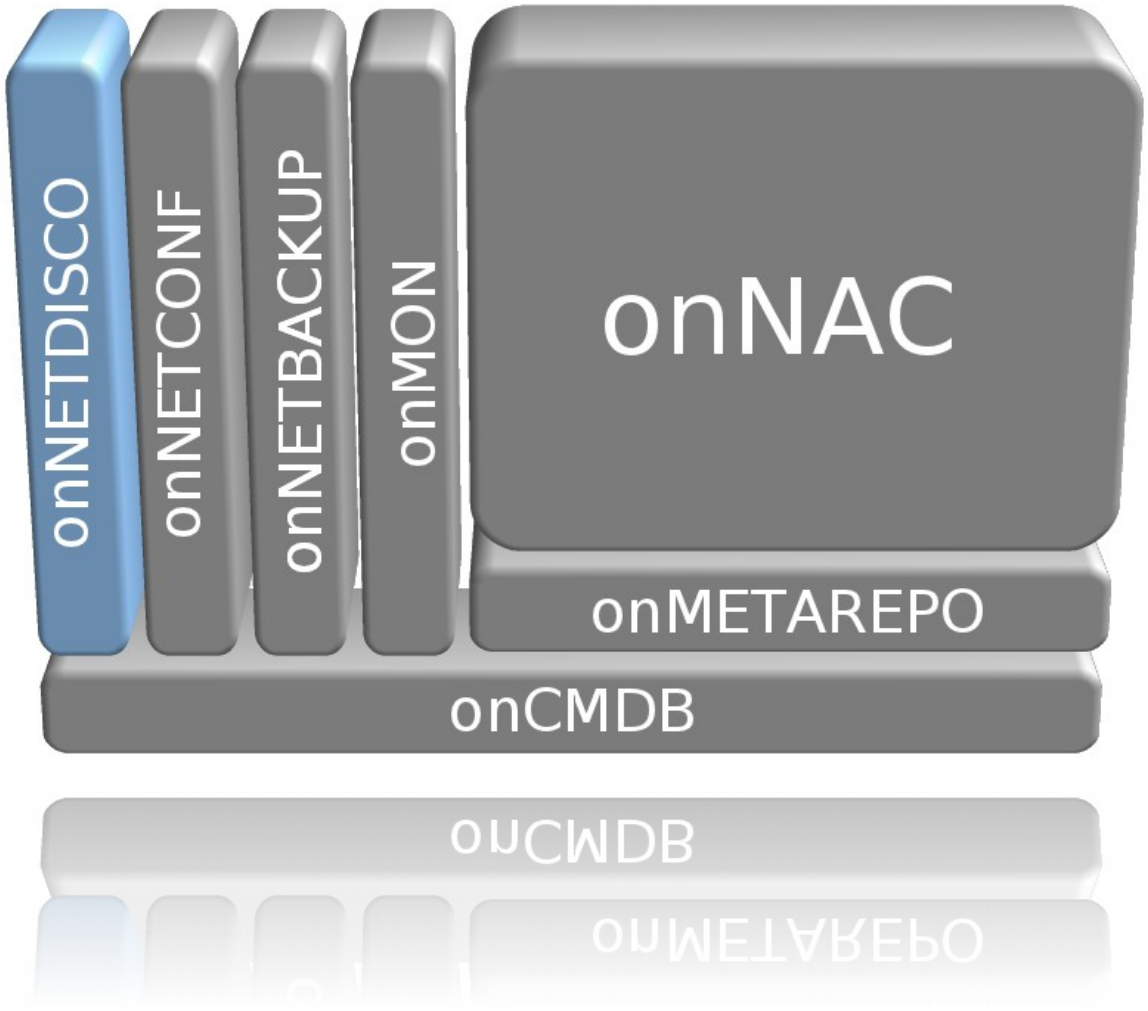


onNAC screenshots - CMDB



IP	Version	MAC Address	SNMP RO	SNMP RW	Purchase date	Purchase order	Warranty	Maintenance	EOL	Telnet user
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
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
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

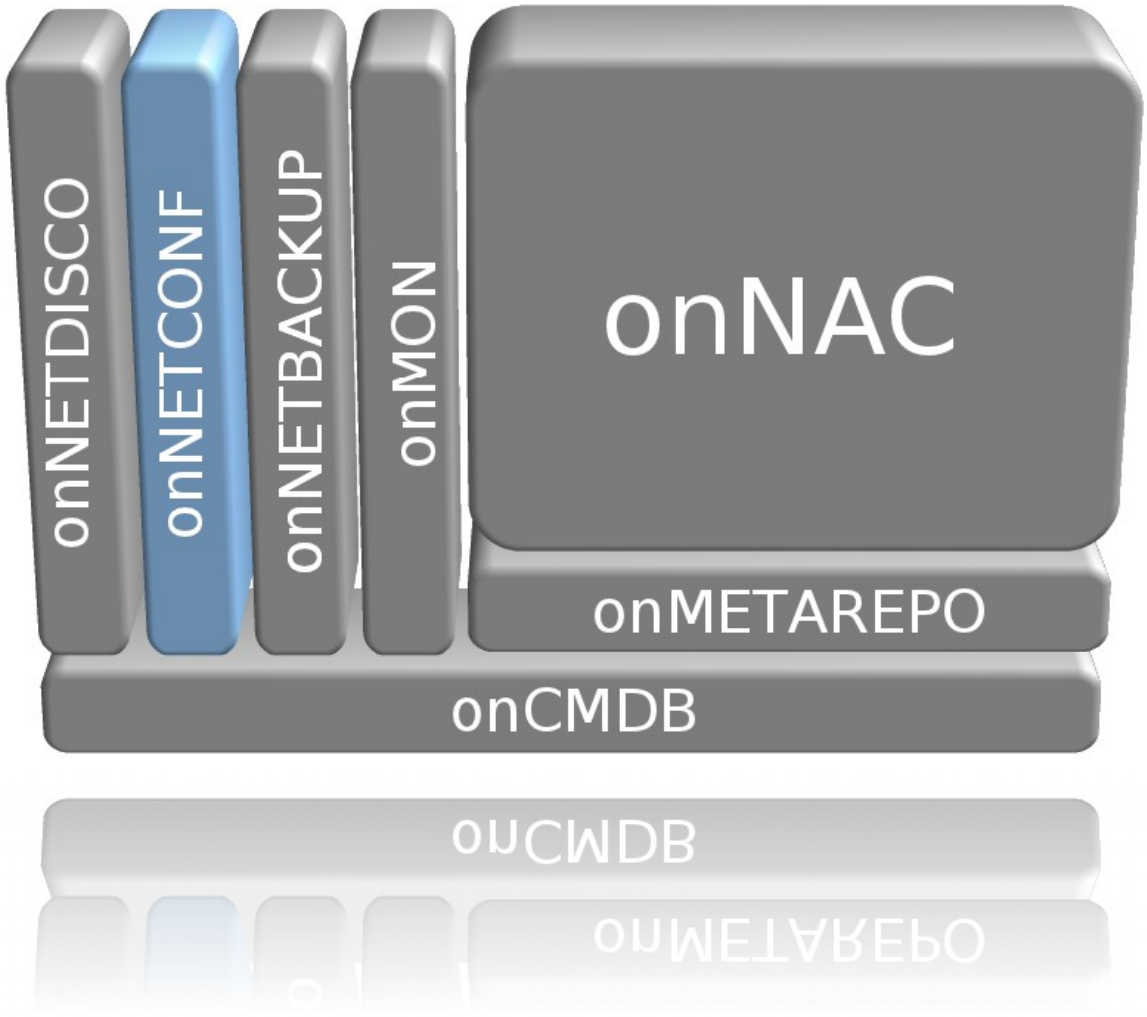
onNETDISCO component



onNETDISCO

- 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

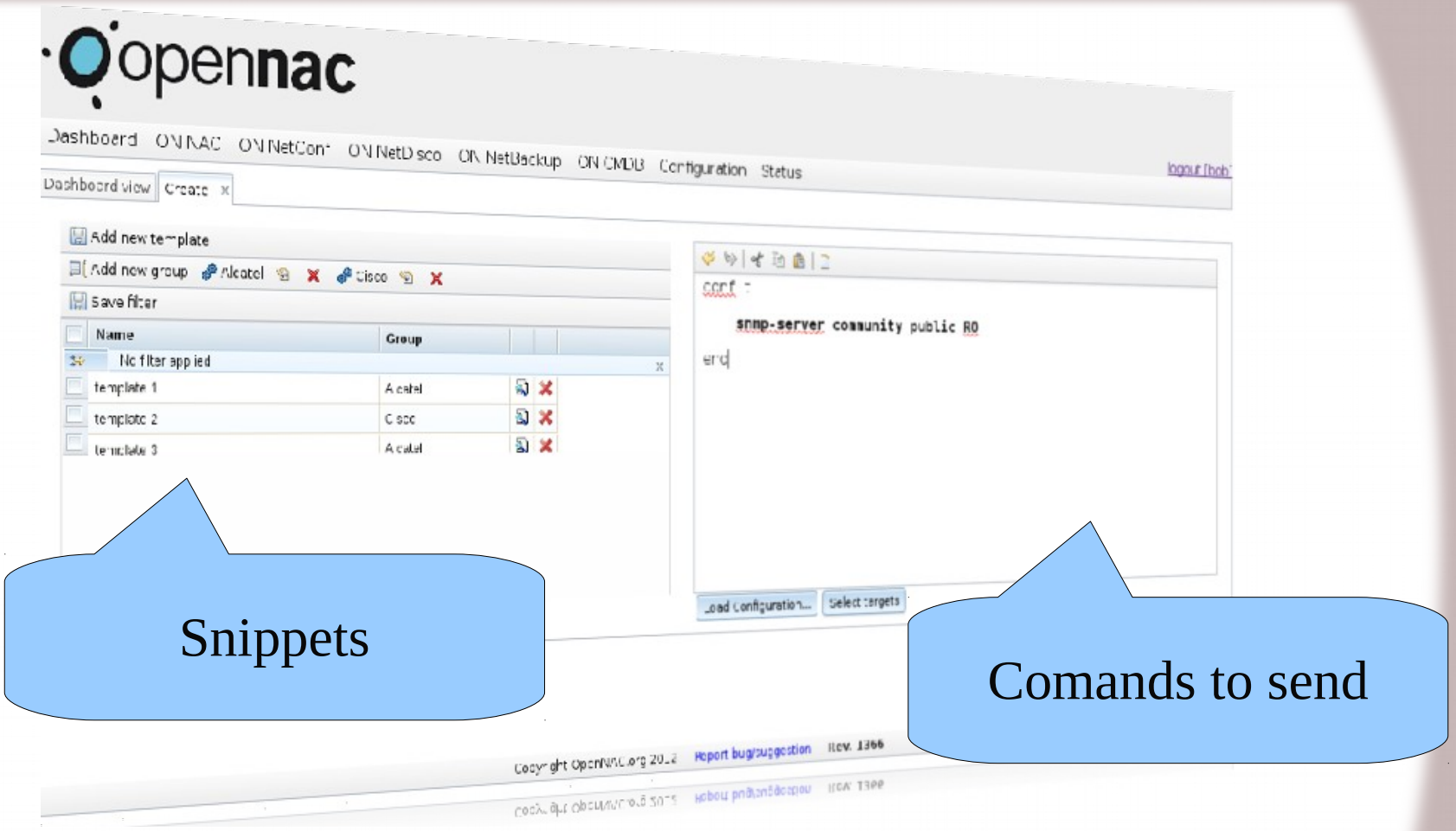
onNETCONF component



onNETCONF component

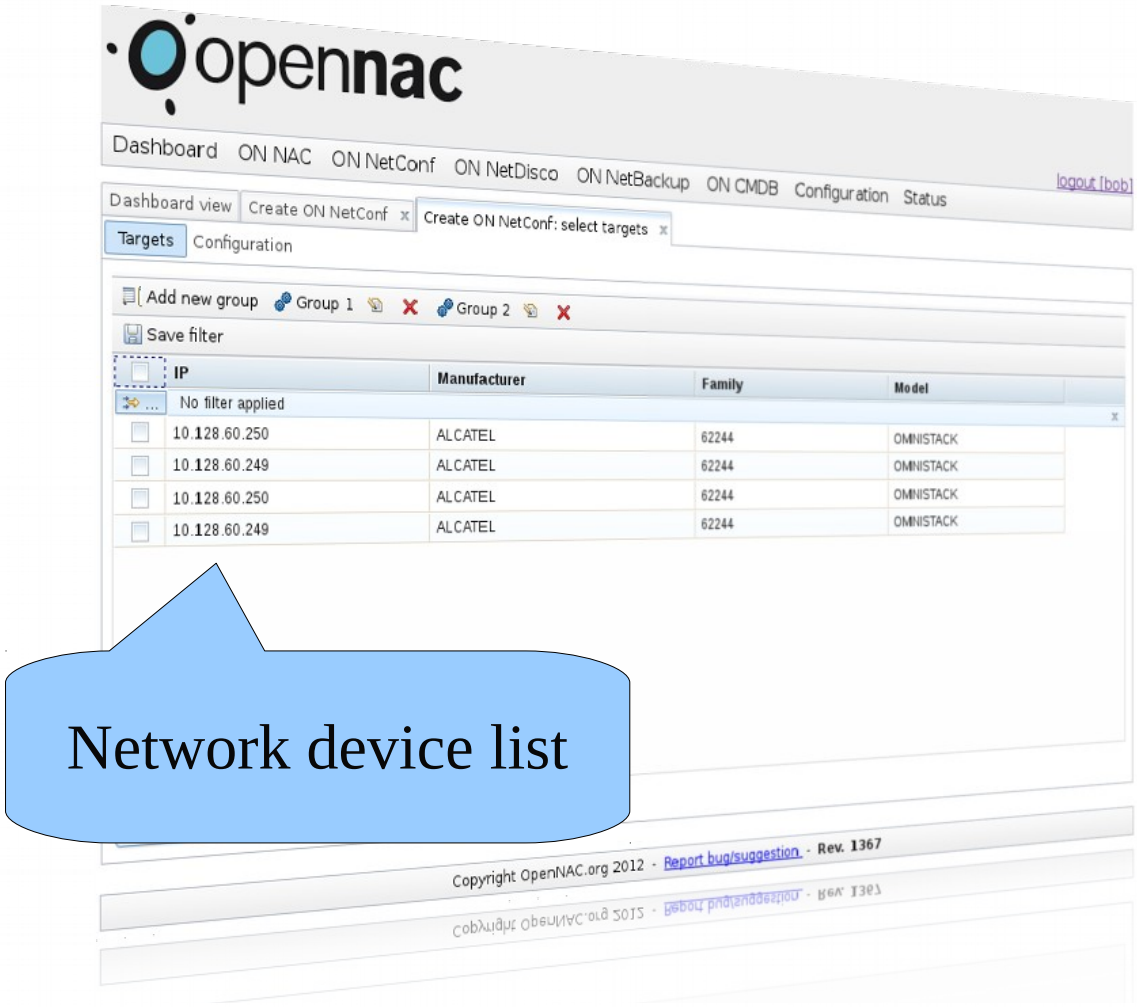
- Network Equipment Configurator allows you to define configuration templates and apply them to sets of network equipment
- Frontend web or Web Service
- Based on a service queue to ensure traceability and integrity of any action
- Very useful for applying settings to large amount of network equipment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

onNETCONF Screenshots - Template



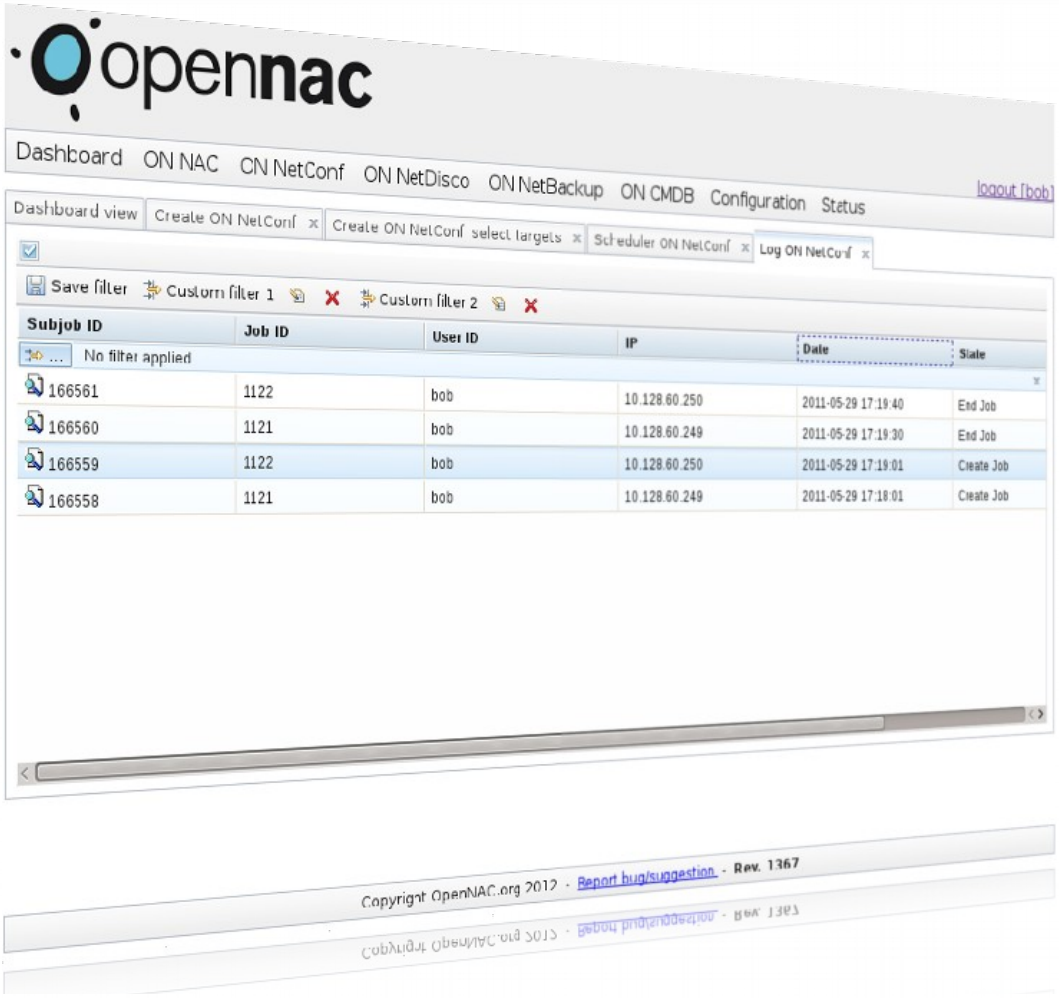
Create a configuration template to send a group of network devices

onNETCONF Screenshots - Devices



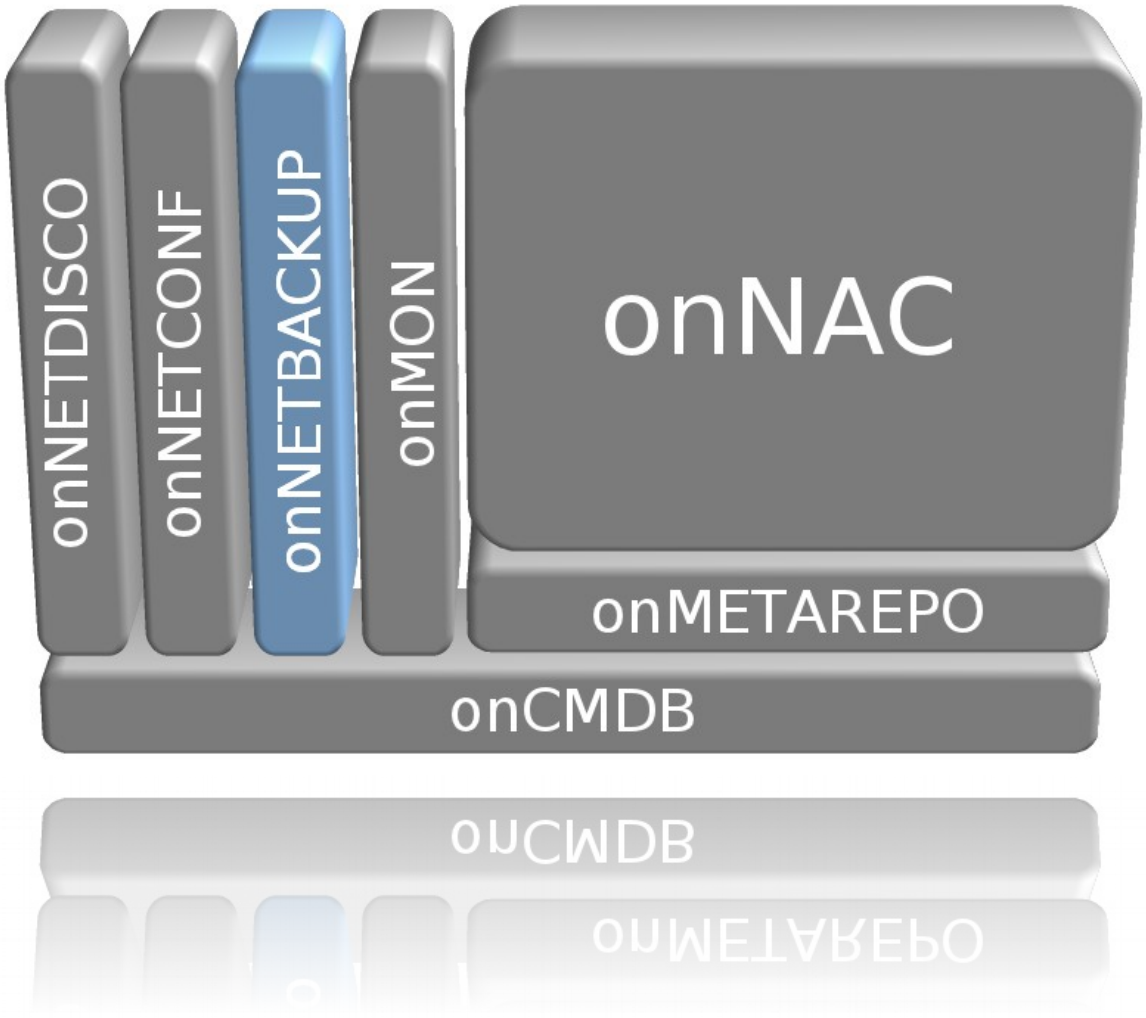
Equipment selection

onNETCONF Screenshots - Results



Viewing the results of configuration tasks

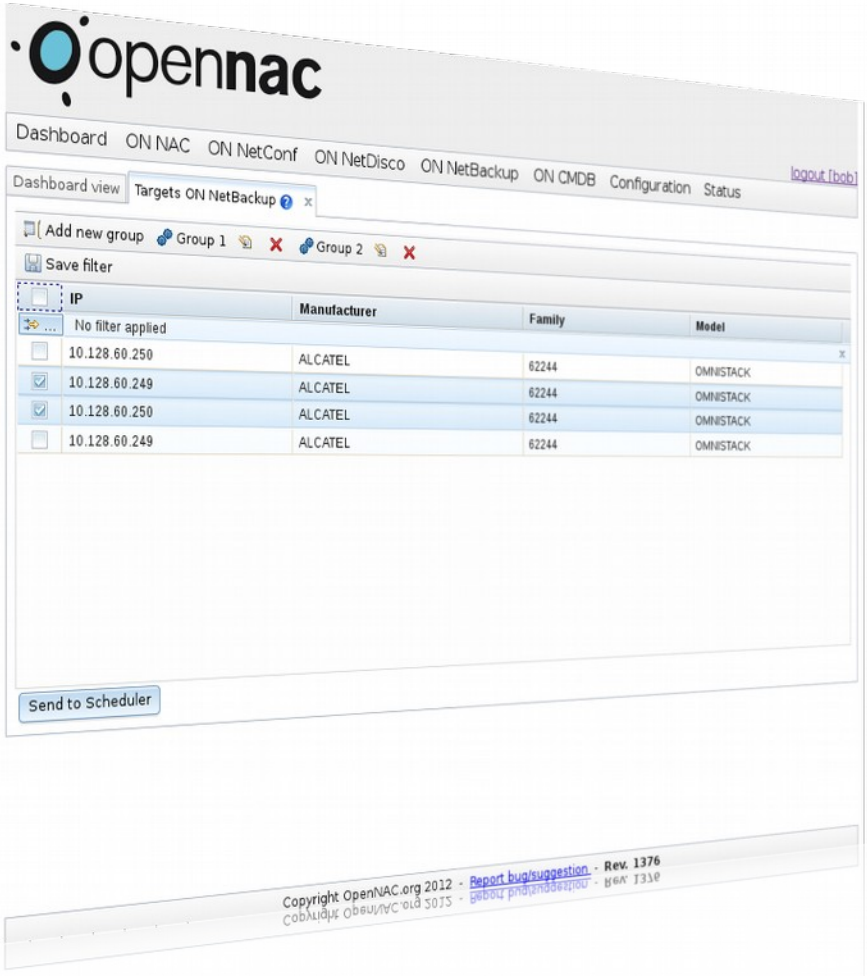
onNETBACKUP component



onNETBACKUP

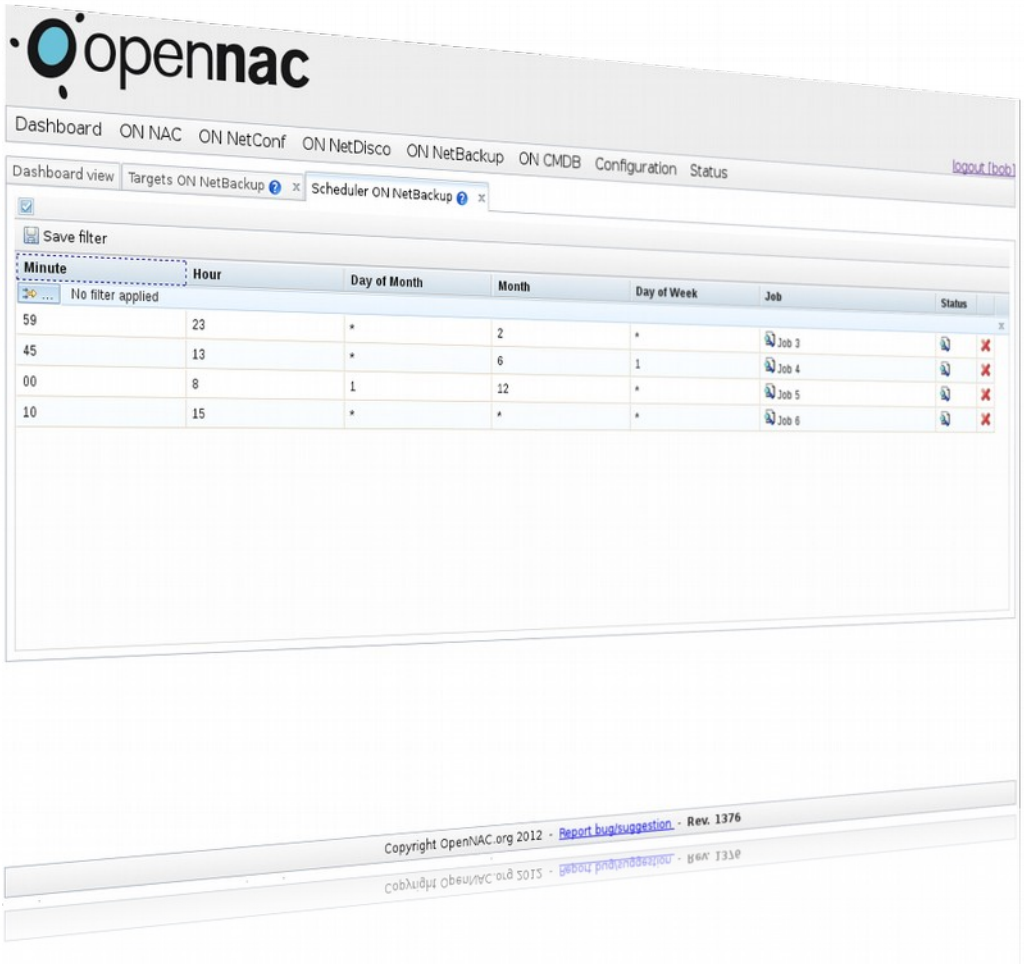
- Make backups and automatic archiving of network devices configurations
- Allows programming device groups copies
- Allows define retention policy
- Based on a service queue to ensure traceability and integrity of any action

onNETBACKUP



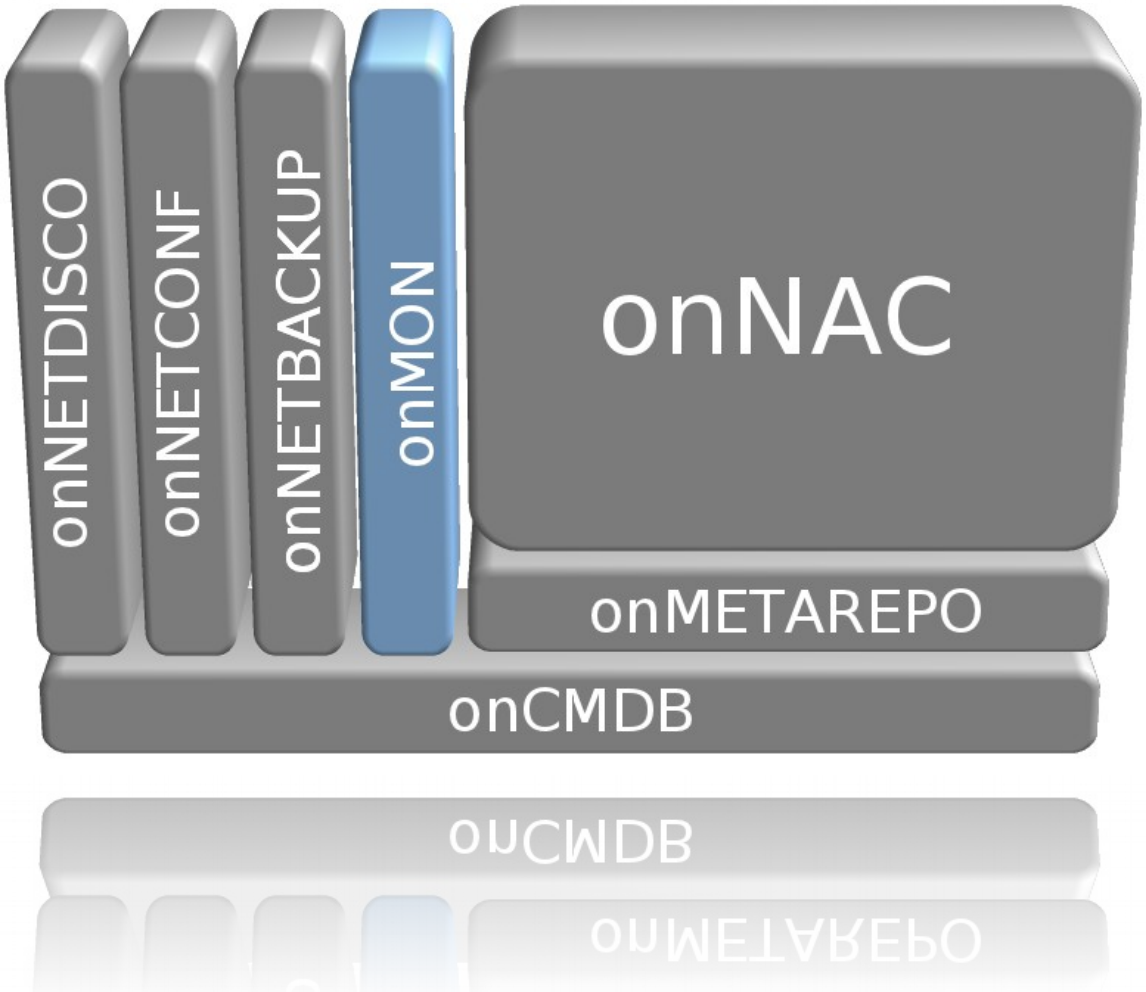
Selection of devices to perform backups

onNETBACKUP



Display planning backups

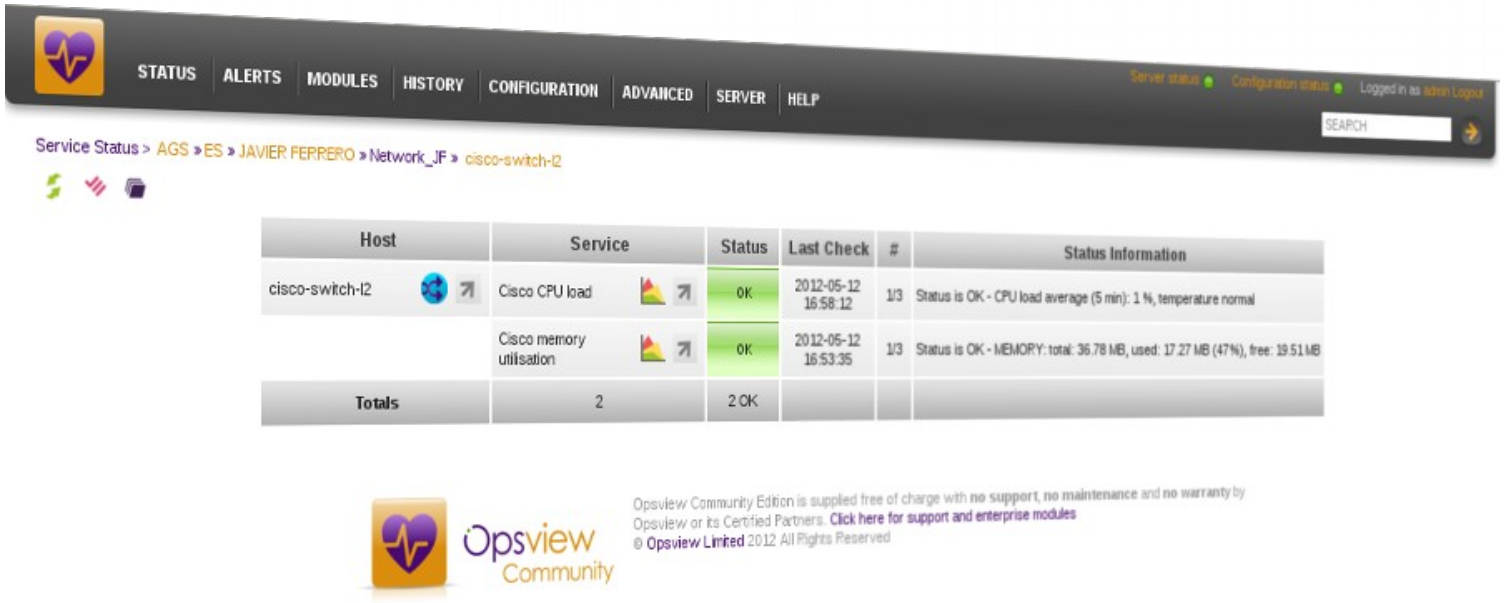
onMON component



onMON

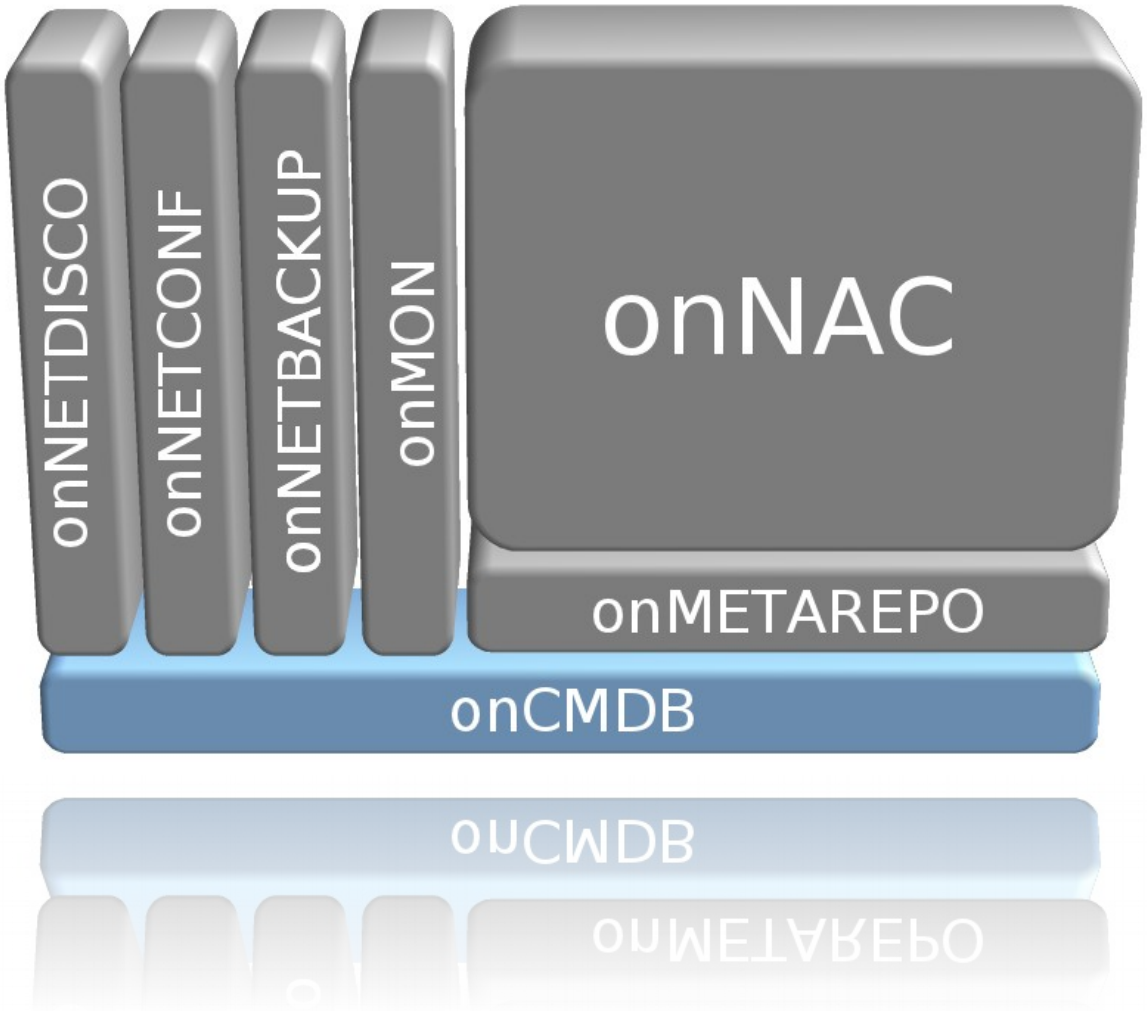
- Monitoring is provisioned automatically from the CMDB
- Monitoring profiles available based on device type
- Real time network devices status
- Generates alerts if any of the parts of the network is not working properly

onNETMON



Viewing the status of a network computer

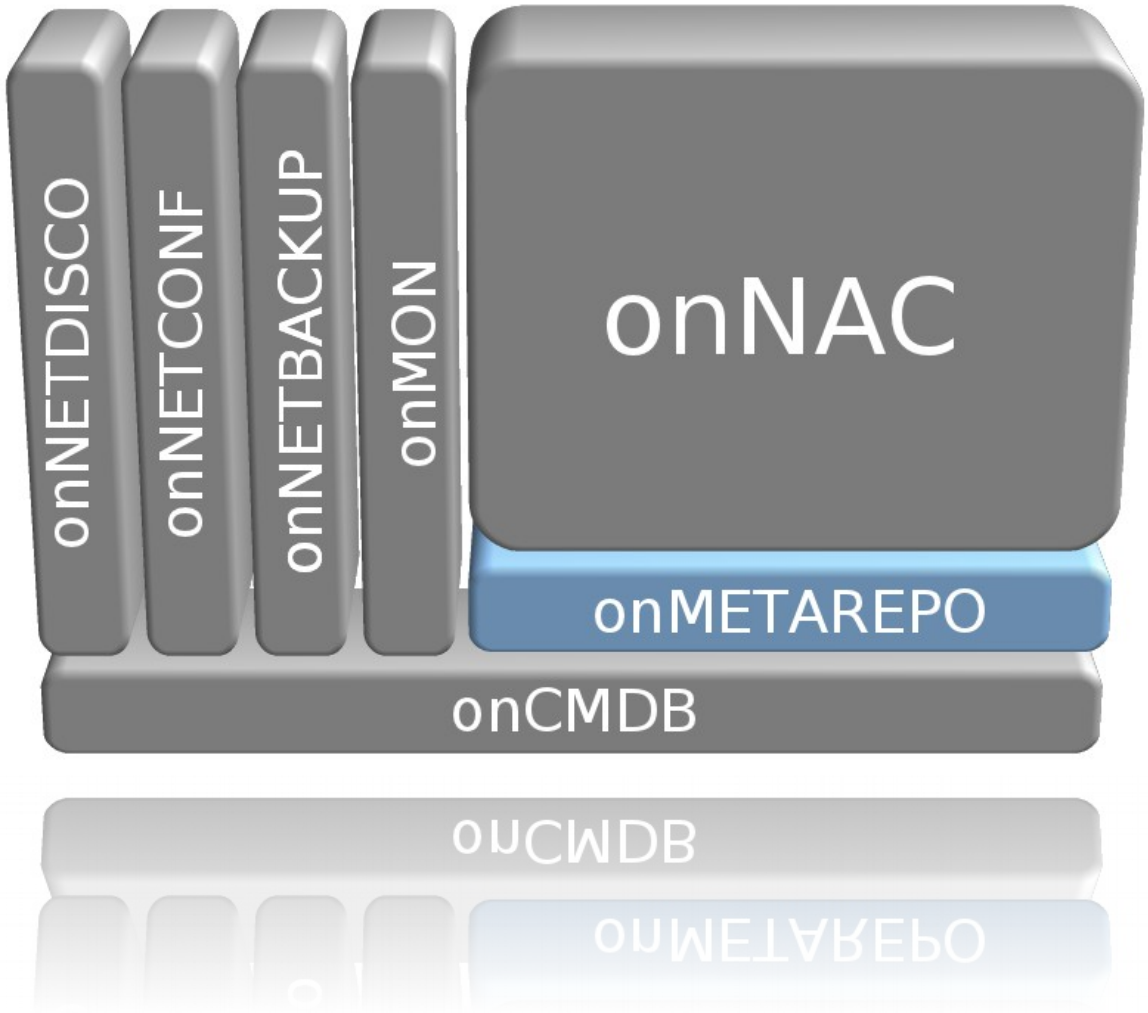
onCMDB component



onCMDB

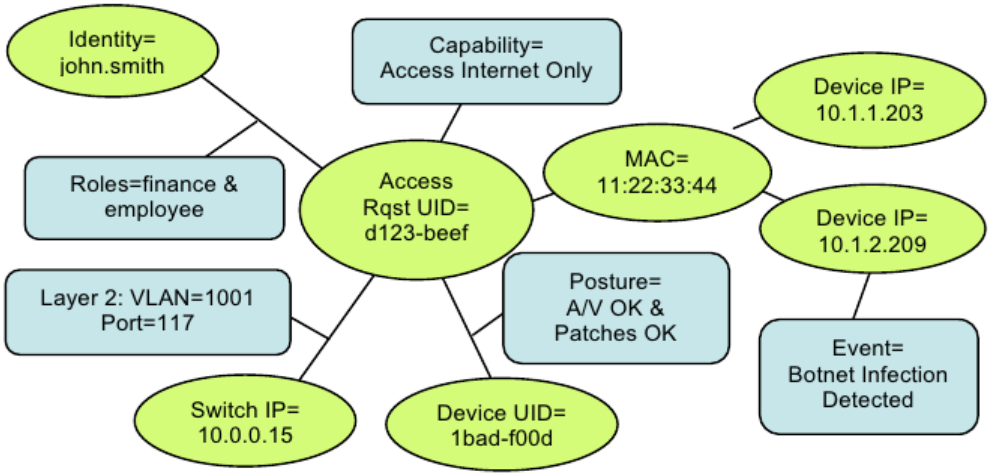
- The module CMDB is the repository of all information of the inventory
- Allows you to easily share information with other platforms
- It stores all the basic elements that use the platform as network devices, security rules, networks, groups, VLAN, ...

onMETAREPO component



onMETAREPO

- 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