# IL NAC alla SAPIENZA-NET

- Breve descrizione della rete
- Obiettivi
- Network Admission Control
  - Descrizione
  - Caratteristiche
  - Tecnologia

# SAPIENZA-NET

# Qualche numero

- 16 mila nodi
- 43 sedi

  (Roma+Latina+Civitavecchia+....)
- Il campus: ≈20 km di cavi a fibra ottica
- 110 punti di presenza negli edifici del campus

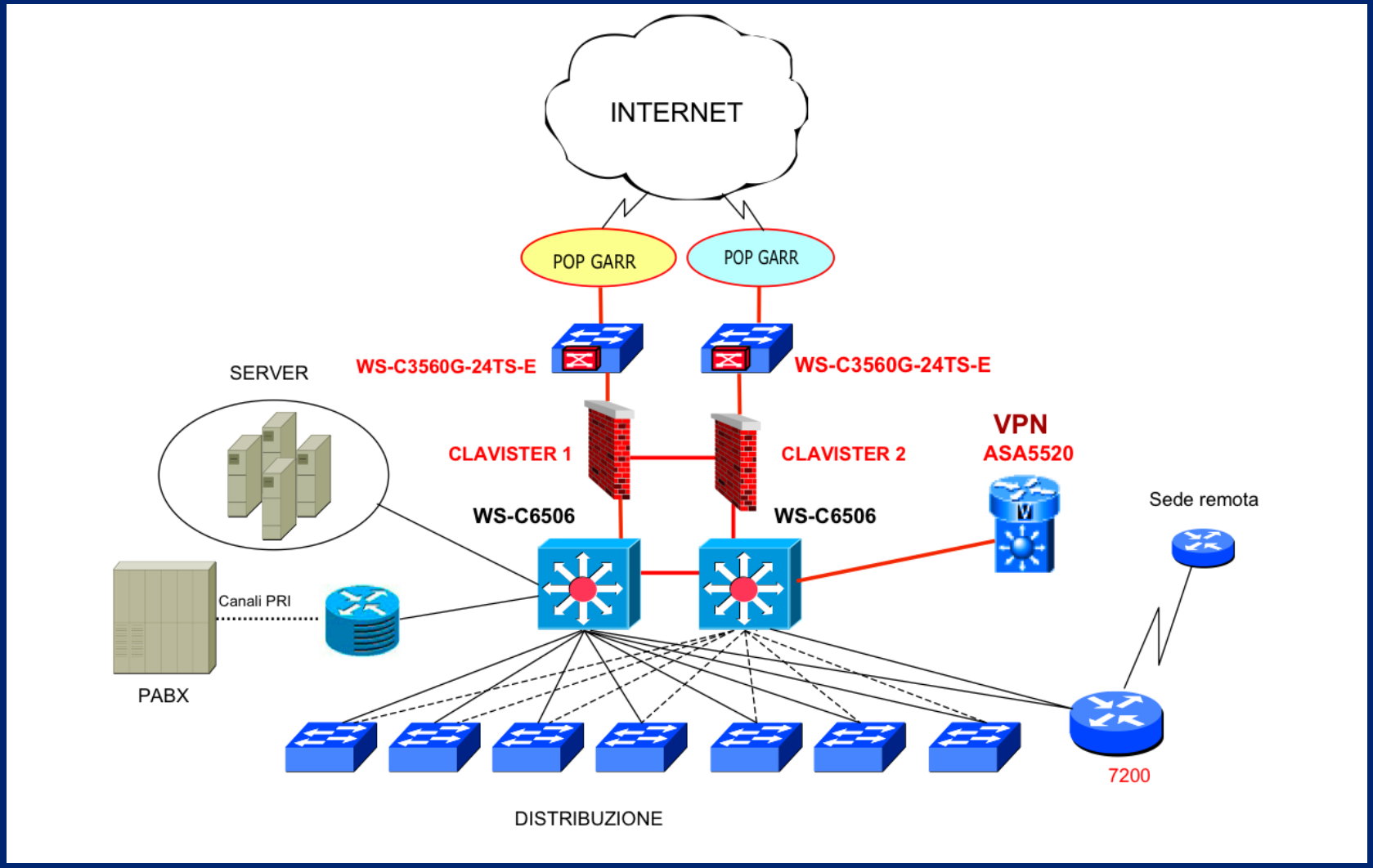


- Sapienza-wireless per gli studenti (~

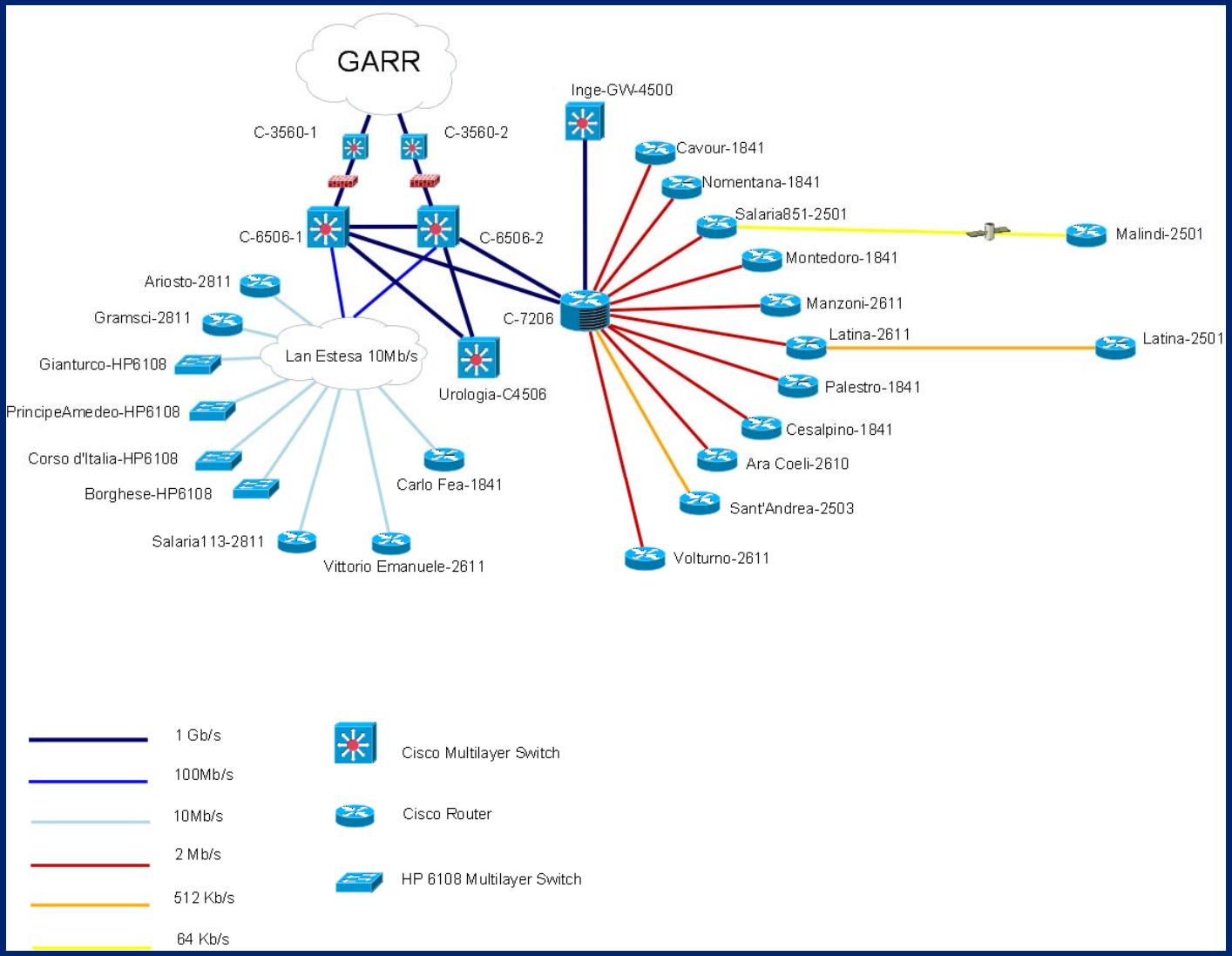
# Il campus


CISCO layer 3
HP 5300 layer 2
HP 2524
Via del Castro Laurenziano
Via A. Borelli
Viale Ippocrate
Regina
Elena
Viale
Piazza Sassari
Via G.M. Lancisi
Viale dell'Università
Via Cesare de Lollis
Viale del Policlinico
Piazzale Aldo Moro
Via dei Sardi

# La connessione al GARR



# La rete metropolitana



# Uso e abuso della rete

- Peer-2-peer
- Spam
- Spoofing
- Phishing
- Auto-assegnazione di indirizzo IP statico
- Installazione di switch e hub non dichiarati
- Installazione di wi-fi non autorizzati
- Installazione di NAT non autorizzati
- Installazione di DHCP non autorizzati

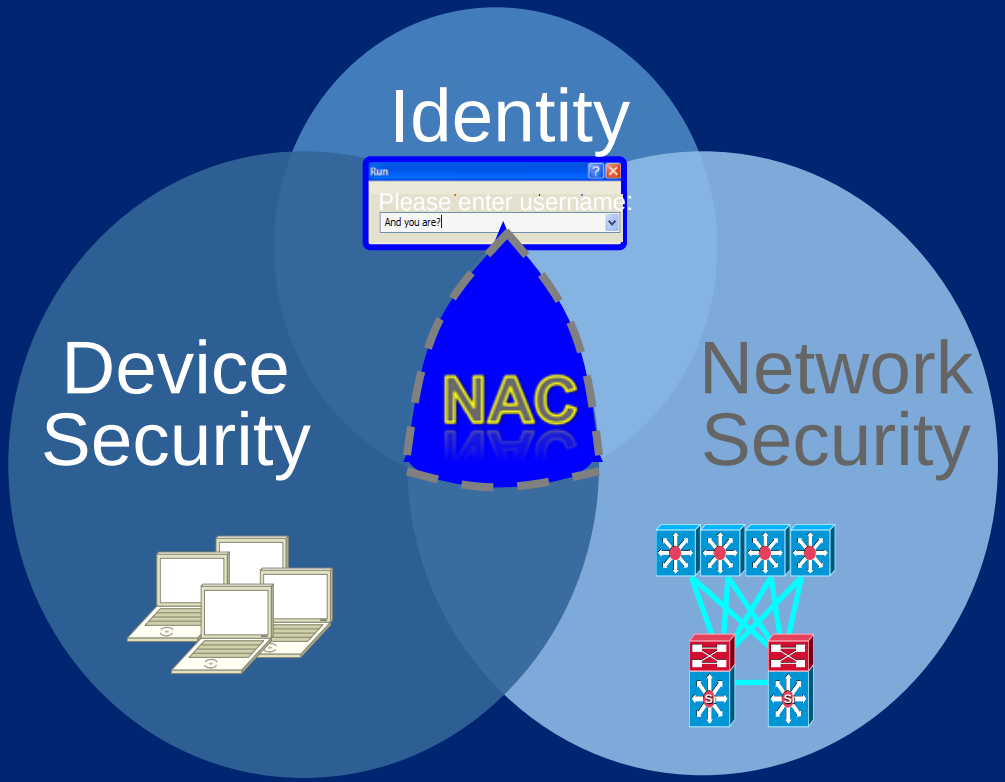
# NAC

# NAC Definition

Set of technologies, defined processes & controls tasked to control access to the Enterprise LAN allowing only authorized and compliant devices to access and operate on the network

# Network Admission Control: Overview

La soluzione NAC permette di delegare al network la verifica e il controllo della conformità alle policy di sicurezza per tutte le periferiche che cercano di accedere alla rete. L'accesso è permesso solamente a dispositivi conformi e affidabili mentre può essere negato a periferiche non conformi che in tal caso vengono reindirizzate ad un'area di quarantena ed eventuale remediation.



# Obiettivi

# Prerequisiti

- Non richiedere apparati di rete di un unico vendor
- Non richiedere cambiamenti significativi all'architettura di rete (ad es. DHCP)
- Non richiedere investimenti significativi all'infrastruttura di rete (ad es. 802.1x)
- Non richiedere agenti software da installare nei client
- Semplicità di implementazione
- Semplicità di uso
- Rilevazione di ogni elemento che entra in rete e sua locazione topologica

# Obiettivi


Il sistema deve essere in grado di rilevare tutti gli elementi connessi alla rete ( o in fase di connessione) ed identificarli

Il sistema deve generare una mappa topologica della rete sviluppata in tempo reale

Il sistema deve essere in grado di intercettare ogni nuovo elemento che si connette alla rete


Il sistema deve poter effettuare autenticazione dell'utente

**Network Admission Control**

# Selezione del NAC

- Requisiti principali del bando, oltre i prerequisiti
- Monitoraggio
  - Rilevare tutti gli elementi connessi
  - Generare inventario completo
  - Generare mappa della topologia fisica
  - La mappa deve essere navigabile
  - Localizzare l'elemento sulla mappa
- Controllo degli accessi
  - Intercettare ogni nuovo elemento
  - Effettuare autenticazione dell'utente
  - Blocco degli elementi sulla porta di accesso
  - Definizione delle politiche di accesso con più parametri
  - Consentire accesso ad area di quarantena
  - Autorizzazione manuale

# Selezione del NAC

- Hanno risposto 3 società offrendo
  - CISCO
  - HP
  - Insightix
- La valutazione tecnico-economica ha individuato Insightix come tecnologia, offerta da ASCOM Italia

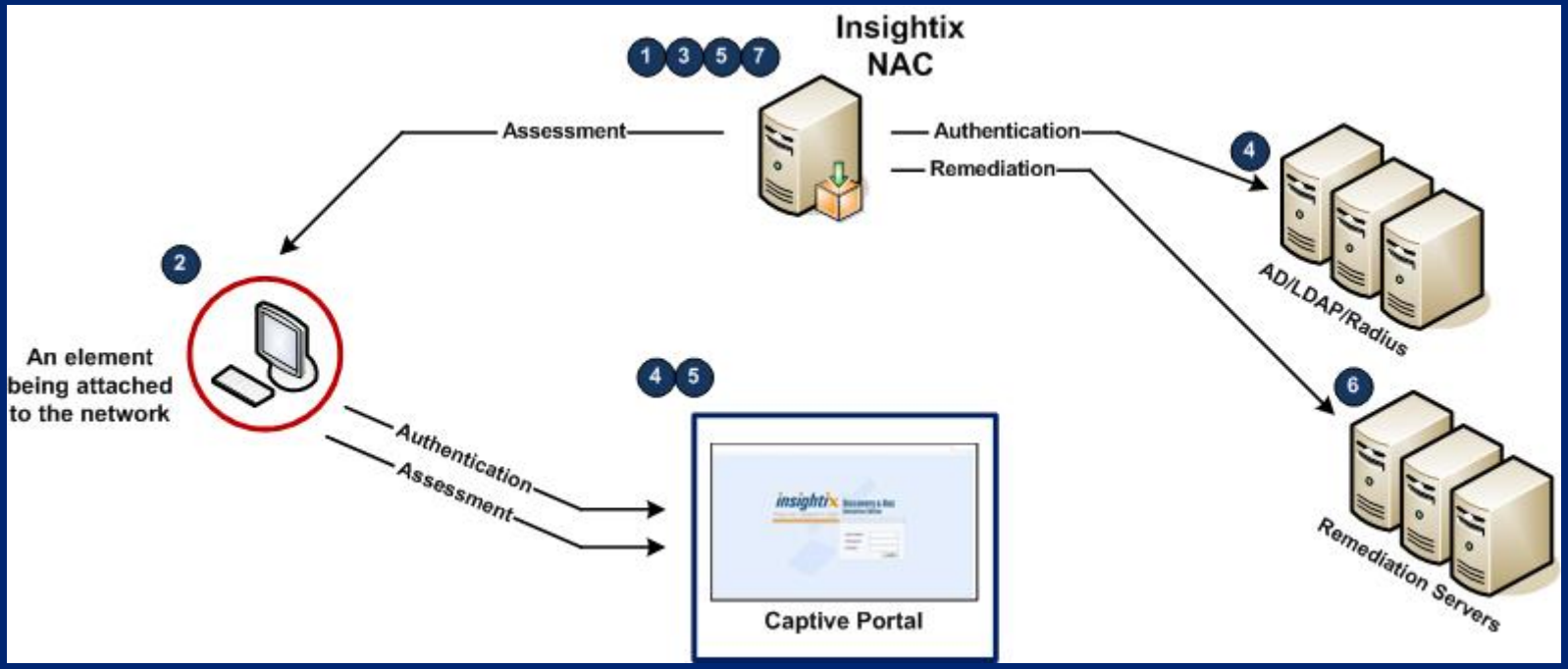
# Il NAC Insightix

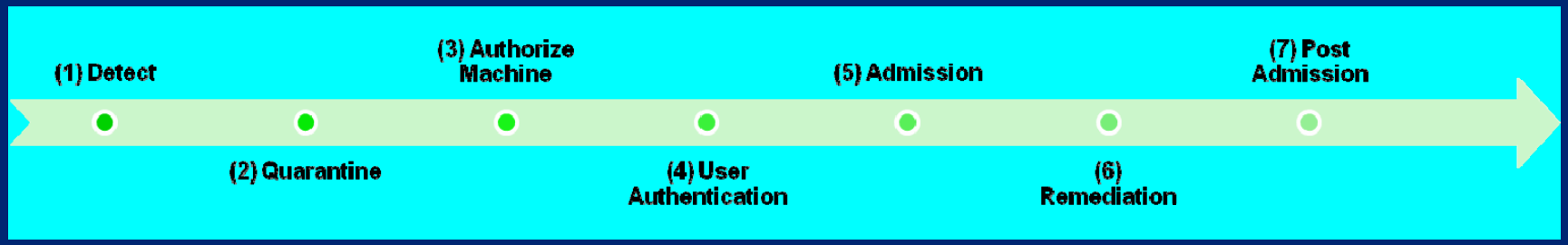
B. Borgia

# NAC Insightix

- NAC Insightix controlla constantemente la rete per fornire informazioni accurate dell'infrastruttura IT e per rilevare, in real-time, qualunque nuovo  elemento che si connette in rete
- A qualunque elemento, che non rispetta le regole di accesso in rete, è negata la connettività nel momento in cui tenta di entrare in rete.
- Qualunque cambiamento delle proprietà dell'elemento di rete è sotto controllo. Regole di "enforcement" possono essere legate a questi cambiamenti.

# Network Admission Control : Caratteristiche



# Network Admission Control
## Caratteristiche e Benefici

**Caratteristiche Insightix NAC**

- Real-Time Device Detection
- Network-wide Policy Enforcement
- Unique Blocking and Quarantine Techniques

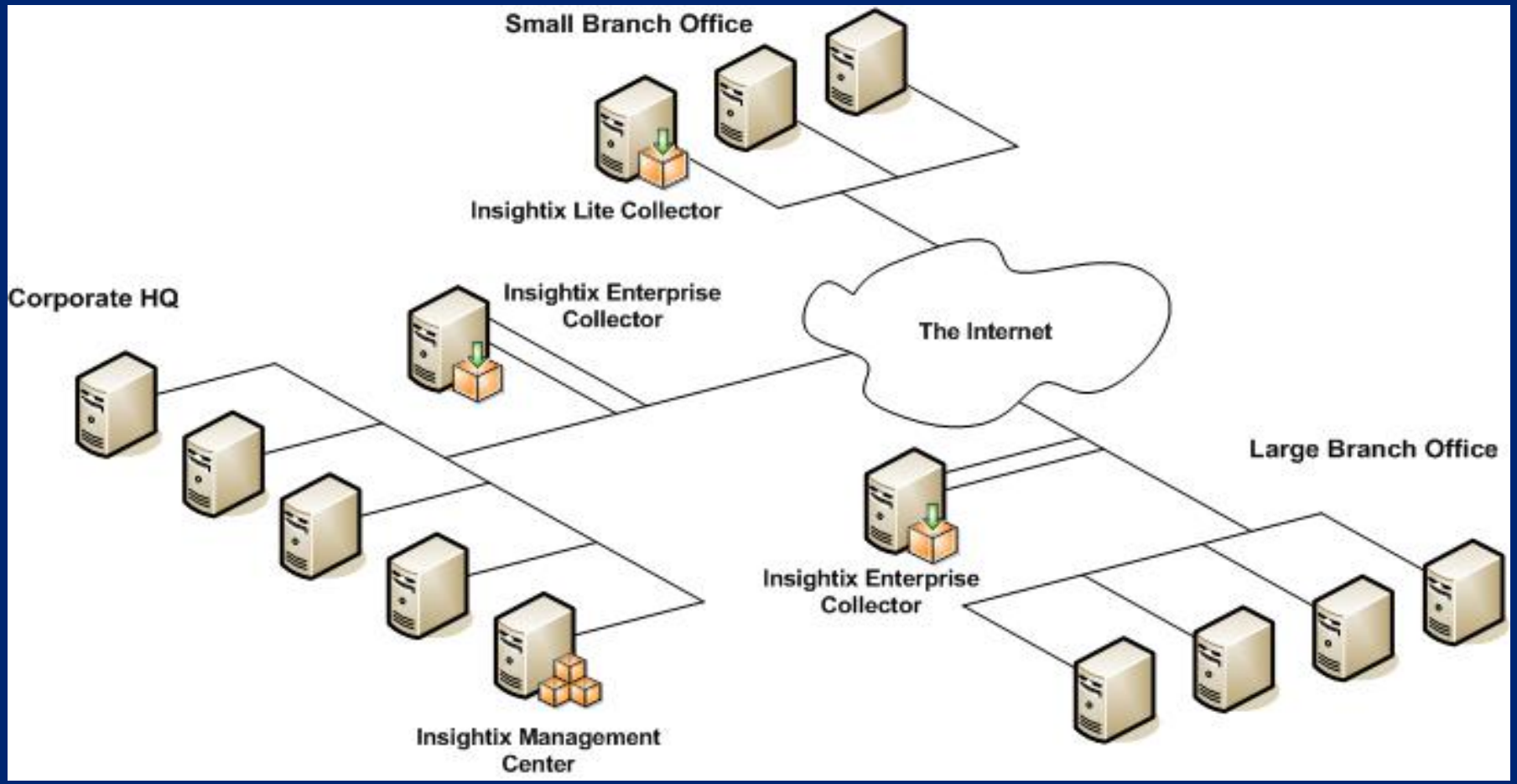
**Benefici Insightix NAC**

- Easy & Fast Implementation
- Full Network Coverage
- Low Total Cost-of-Ownership

# Insightix Architecture

- Insightix Management Center
- Insightix Enterprise Collector
  - Standalone / Parte di una installazione distribuita
  - Applicativo softyware su hardware dedicato con due interfacce di rete (NICs)
  - Agisce su VLAN multiple e domini di broadcast
- Insightix Lite Collector
  - Piccole sedi remote
  - Installato su macchine windows (non dedicate), richiede una sola NIC
  - Agisce su una singola VLAN / dominio di broadcast
- Modalità operativa
  - Alert
  - Enforced

# Architettura

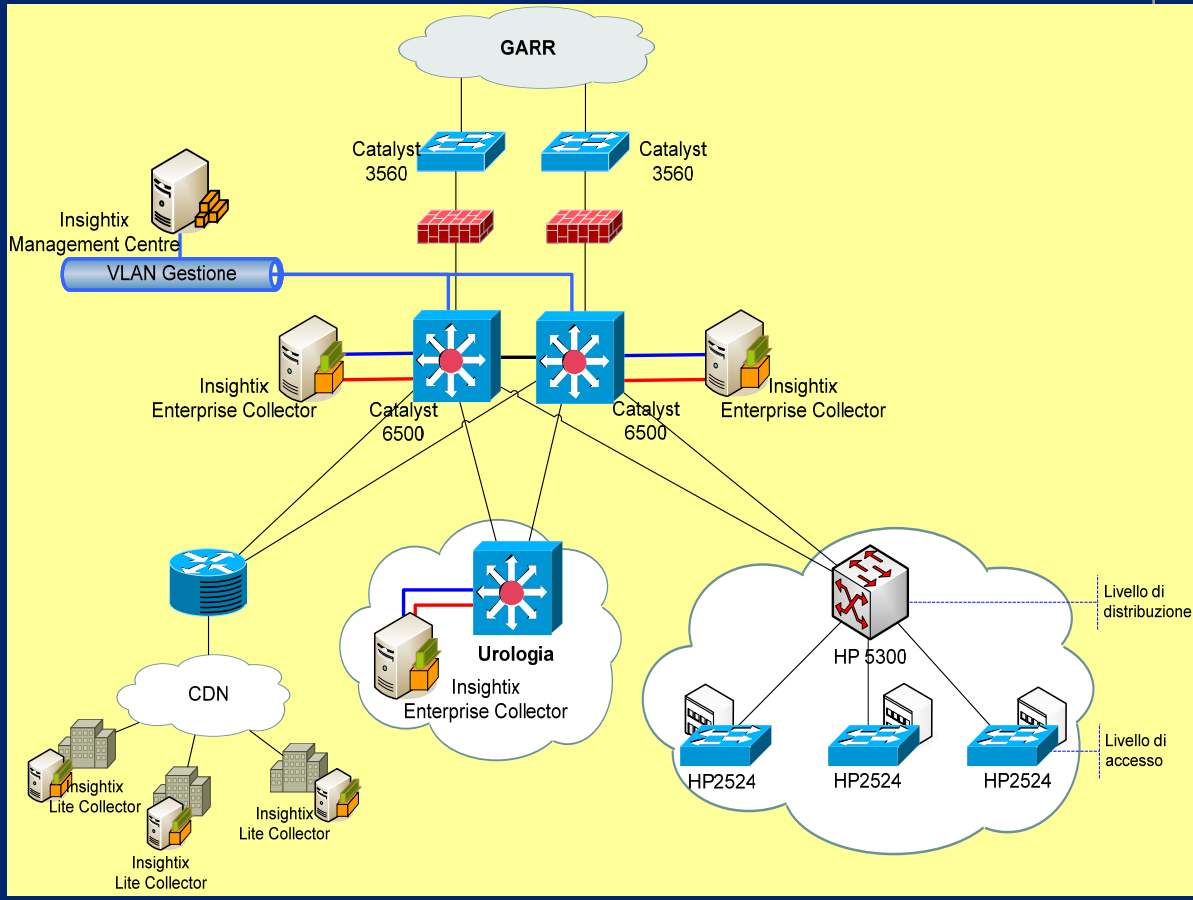


# Tecnologia Insightix

# Network Admission Control : Technology

## Insightix Technology

- **Tecnologia in attesa di brevetto**

Dashboard | Topology | Inventory | Performance | NAC | Alerts | Audit | Reports | Configuration

insightix

Log Out

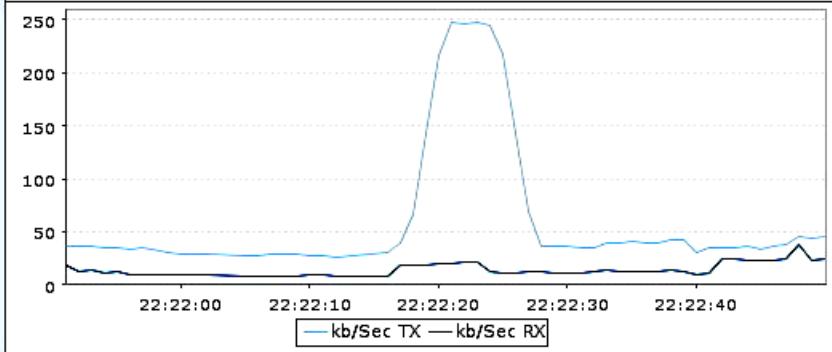
**System Summary**

| System Parameter | Information |
|---|---|
| System Uptime: | 1 days, 1 hours, 25 minutes, 42 seconds |
| System Version: | 2.5.211 |
| **Online Devices**: | 622 |
| Operating Systems Detected: | 615 |
| Operating Systems Not Detected: | 6 |
| Devices Without IPs: | 1 |
| **Offline Devices**: | 284 |
| **Total Devices**: | 906 |
| Frames Processed: | 93,748,086 |

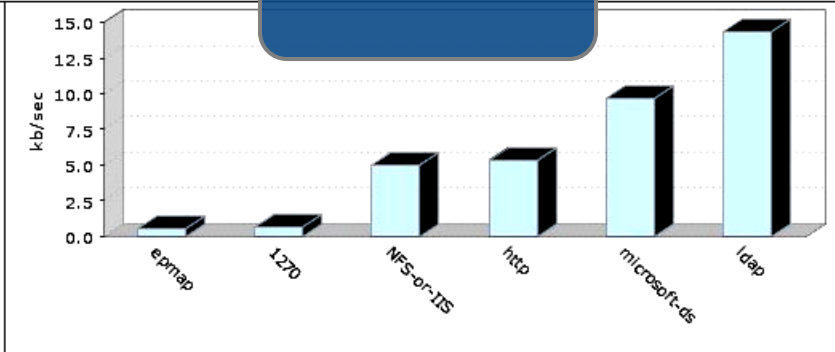
**OS Summary**

| OS Name | Number |
|---|---|
| Microsoft Windows 2000 | 187 |
| Microsoft Windows 2003 | 169 |
| Microsoft Windows XP SP2 | 151 |
| Microsoft Windows XP | 21 |
| Foundry IronWare Networking Device | 19 |
| Aten KVM Over IP Switch | 13 |
| Linux Kernel 2.4.5 - 2.4.18 | 13 |
| Linux Kernel 2.4.19 - 2.6.7 | 8 |
| HP Printer | 7 |

| # | Timestamp | Alert Message | Severity |
|---|---|---|---|
| 1 | 13-August-06 00:24:48 | IP Address 172.16. conflict detected between 00:d0:b7: and 00:0c:29: | ✖ |
| 2 | 13-August-06 00:24:48 | MAC Address 00:d0:b7: is associated with additional IP 172.16. | ⚠ |
| 3 | 13-August-06 00:20:09 | IP Address 172.16. conflict detected between 00:0c:29:2b:ec:27 and 00:0c:29: | ✖ |
| 4 | 13-August-06 00:20:09 | MAC Address 00:0c:29: is associated with additional IP 172.16. | ⚠ |
| 5 | 13-August-06 00:19:38 | MAC Address 00:50:56: is associated with additional IP 100.42. | ⚠ |



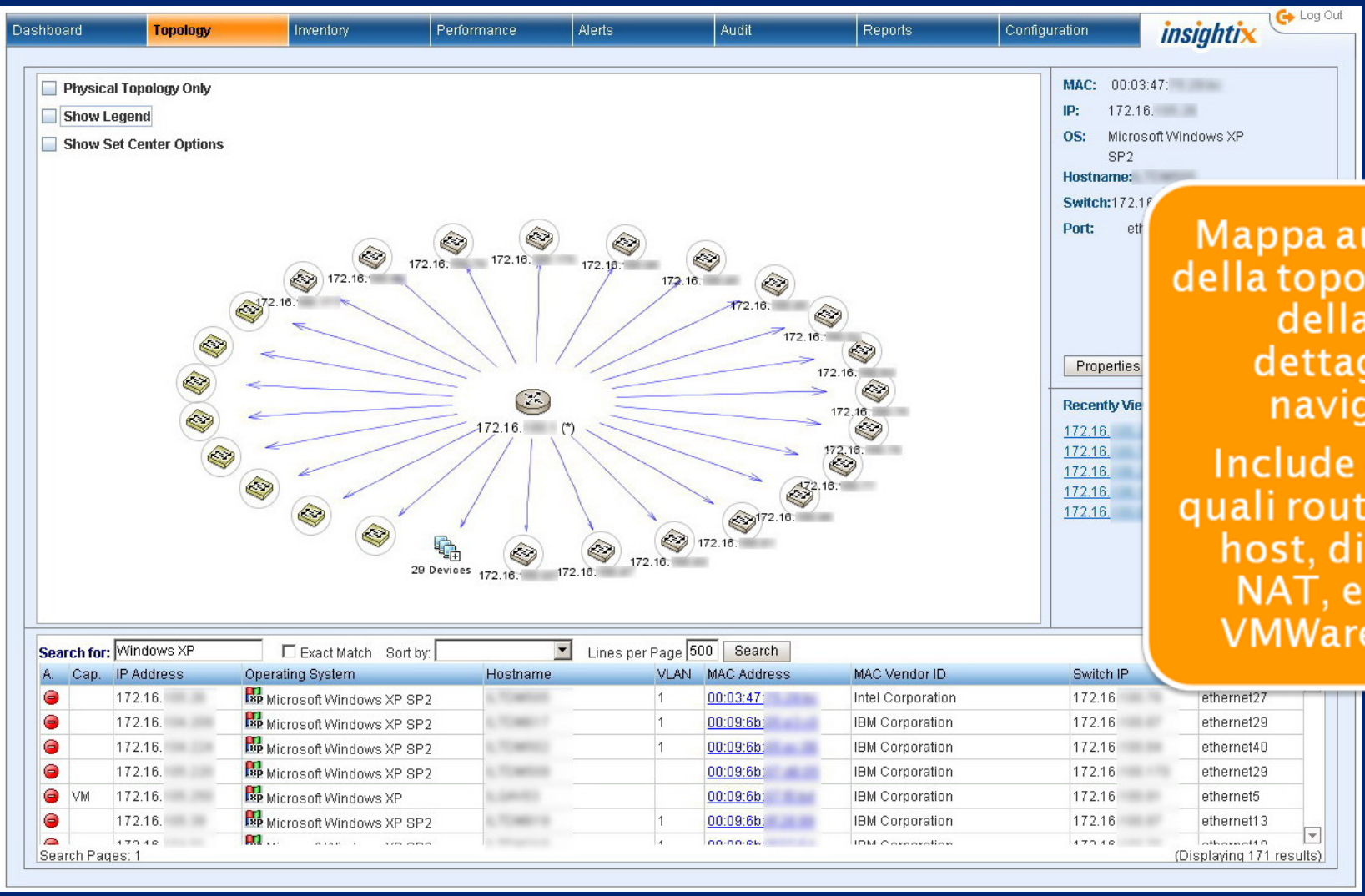

Bandwidth Utilization




Bandwidth Utilization (By Application)

Finestra iniziale

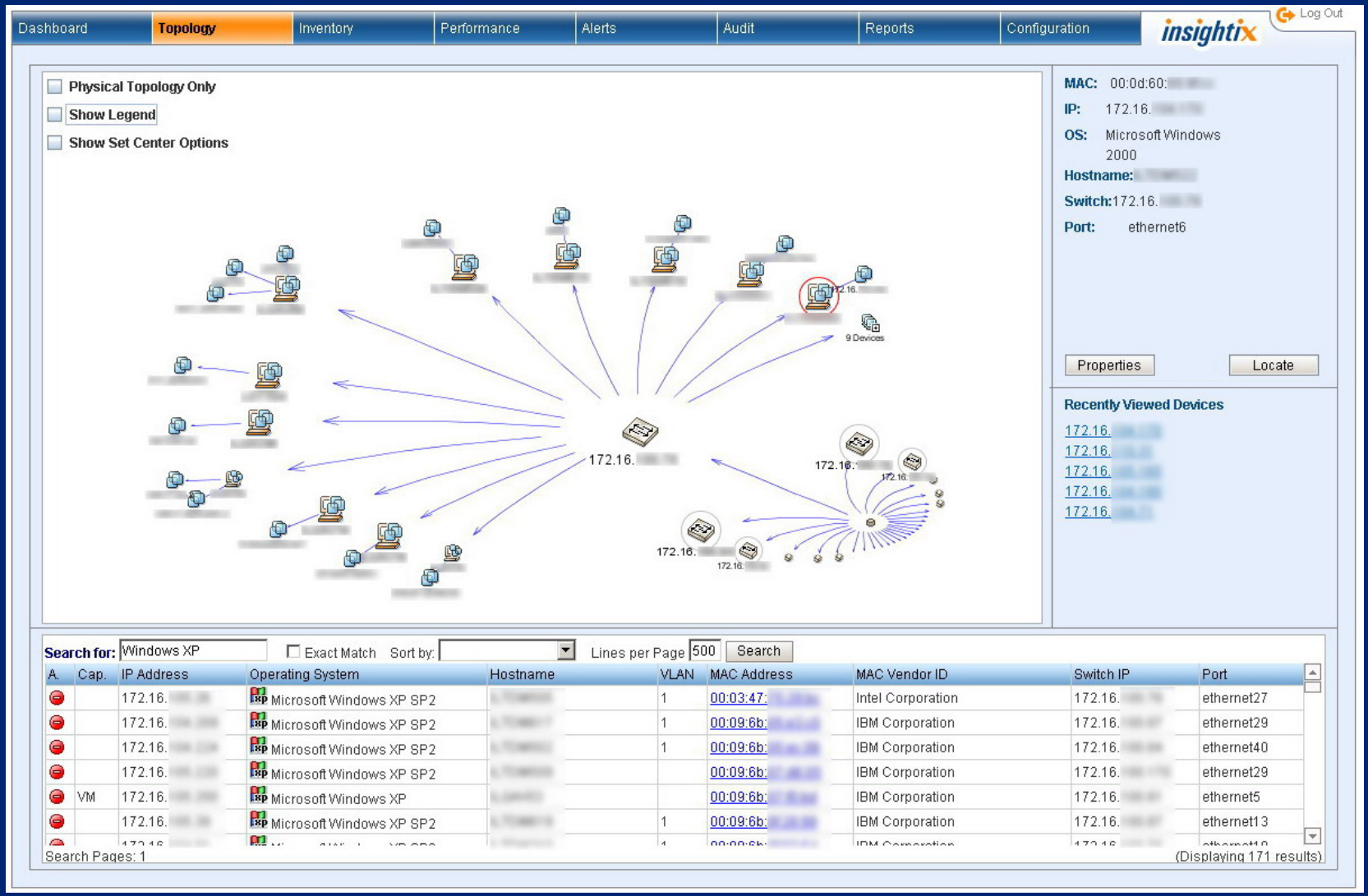
# Network Admission Control : Technology




Mappa automatica della topologia fisica della rete, dettagliata e navigabile.

Include elementi quali router, switch, host, dispositivi NAT, elementi VMWare e altro.

# Network Admission Control : Technology

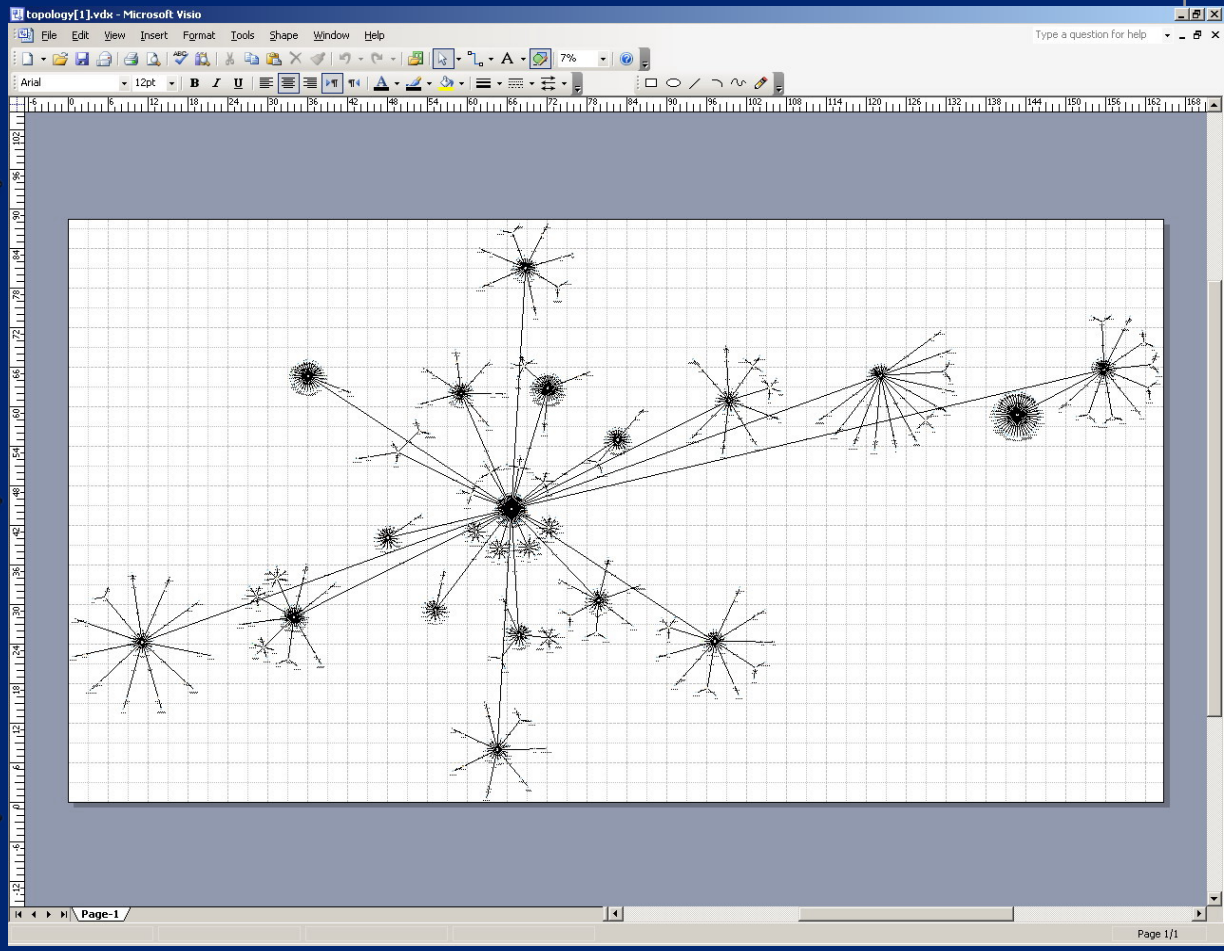


# Network Admission Control : Technology

La mappa può essere esportata in Ms Visio per essere utilizzata e modificata secondo le necessità

Esempio di esportazione (formato MS Visio). Cliccando sui vari rami e nodi costituenti il grafo, si possono dettagliare le proprietà dei componenti costituenti la mappa.

Il prodotto Insightix è in grado di esportarla anche in altri formati come CSV, PDF, HTML.



# Network Admission Control : Technology

- Inventario completo di tutti gli elementi di rete
- Indirizzo MAC
- Indirizzo IP
- Dominio
- Hostname
- Sistema operativo
- Servizi aperti
- Switch su cui è connesso
- Porte fisiche utilizzate
- Hotfix Microsoft
- ...e molto altro

| A. | Cap. | IP Address | Operating System | Name | Username | VLAN | MAC Address | MAC Vendor ID | Switch IP | Port |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 151.100.53.136 | Microsoft Windows XP | USER-RP256XZMCO | | 20 | 00:16:e6:85:58:a1 | GIGA-BYTE TECHNOLOGY CO.,LTD. | 172.16.128.19 | B3 |
| | | 151.100.53.147 | Microsoft Windows XP | PC-FE396AC1825B | | 5 | 00:1d:60:6d:e7:71 | ASUSTek COMPUTER INC. | 172.16.128.19 | B3 |
| | | 151.100.53.156 | UNKNOWN | labchif22 | | 20 | 00:0a:5e:3e:ac:23 | 3COM Corporation | 172.16.128.19 | B3 |
| | | 151.100.53.158 | Apple MAC OS 9.x | paperoga | | 20 | 00:05:02:2e:bc:4d | APPLE COMPUTER | 172.16.128.19 | B3 |
| | | 151.100.53.176 | UNKNOWN | mariapia | | 20 | 00:17:31:72:b0:55 | ASUSTek COMPUTER INC. | 172.16.128.19 | B3 |
| | | 151.100.53.179 | Microsoft Windows ME | LAB319 | | 20 | 00:50:fc:33:db:96 | EDIMAX TECHNOLOGY CO., LTD. | 172.16.128.19 | B3 |
| | | 151.100.53.190 | Microsoft Windows XP | PENTIUM | | 20 | 00:40:ca:5e:46:ef | FIRST INTERNAT'L COMPUTER, INC | 172.16.128.19 | B3 |
| | | 151.100.53.193 | UNKNOWN | scirocco | | | 00:0a:e4:45:15:49 | Wistron Corp. | | |
| | | 151.100.53.203 | Microsoft Windows Vista | PC-CLAUDIA | | 20 | 00:16:d3:1d:96:34 | Wistron Corporation | 172.16.128.19 | B3 |
| | | 151.100.53.210 | Microsoft Windows XP | LUPETTO | | 5 | 00:0f:1f:7e:0e:df | WW PCBA Test | 172.16.128.19 | B3 |
| | | 151.100.53.211 | Microsoft Windows XP | DDC-SXJ6XBHS8XL | | 5 | 00:18:f3:1a:e5:f0 | ASUSTek COMPUTER INC. | 172.16.128.19 | B3 |
| | | 151.100.53.214 | Microsoft Windows XP | STUDENTI | | 20 | 00:19:66:36:b5:77 | Asiarock Technology Limited | 172.16.128.19 | B3 |
| | | 151.100.53.215 | Microsoft Windows XP | keplero | | 20 | 00:c0:9f:22:96:86 | QUANTA COMPUTER, INC. | 172.16.128.19 | B3 |
| | | 151.100.53.219 | Linux Kernel 2.4.5 - 2.4.18 | pitagora1 | | | 00:e0:81:21:f4:fe | TYAN COMPUTER CORP. | | |
| | | 151.100.53.223 | Microsoft Windows XP | PC098 | | 5 | 00:30:48:81:04:4c | Supermicro Computer, Inc. | 172.16.128.19 | B3 |
| | | 151.100.53.247 | Microsoft Windows XP | UNIVERSI- | | 20 | 00:15:f2:39:ef:c3 | ASUSTek COMPUTER INC. | 172.16.128.19 | B3 |
| | | 151.100.53.251 | HP Service Processor | chagall | | | 00:00:48:95:db:37 | SEIKO EPSON CORPORATION | | |

Dashboard | Topology | Inventory | Performance | NAC | Alerts | Audit | Reports | Configuration | insightix | Log Out

**Properties** | Performance | Audit | Alerts | Event History

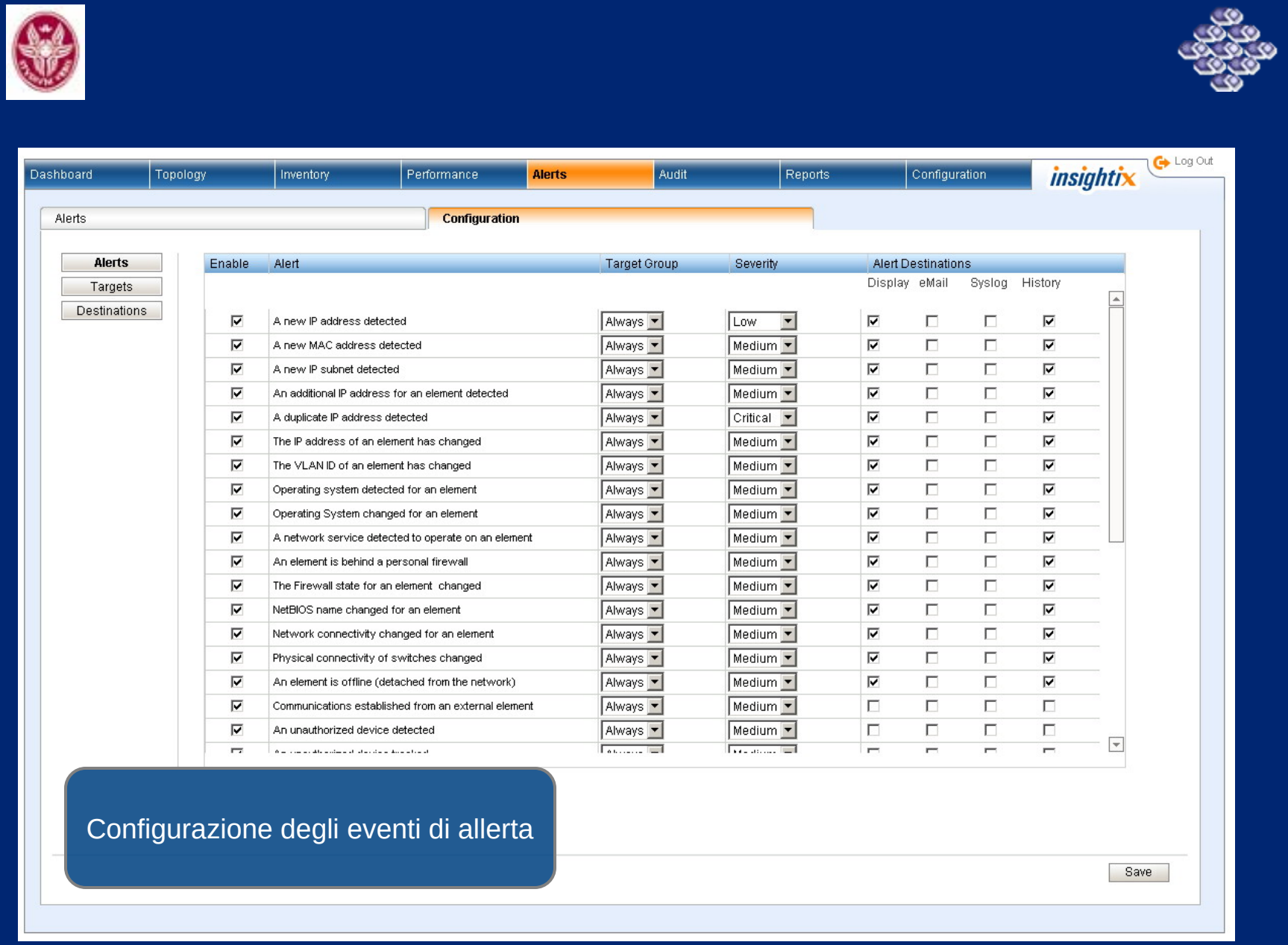
informazioni dettagliate, real-time per ogni elemento della rete

**Inventory Properties for 192.168.[redacted] (Online)**
**Active since: 03-August-06 16:46:28 (1 Week 2 Days 8 Hours 59 Minutes and 37 Seconds)**
**Last activity seen at: 13-August-06 01:46:01 (4 Seconds ago)**

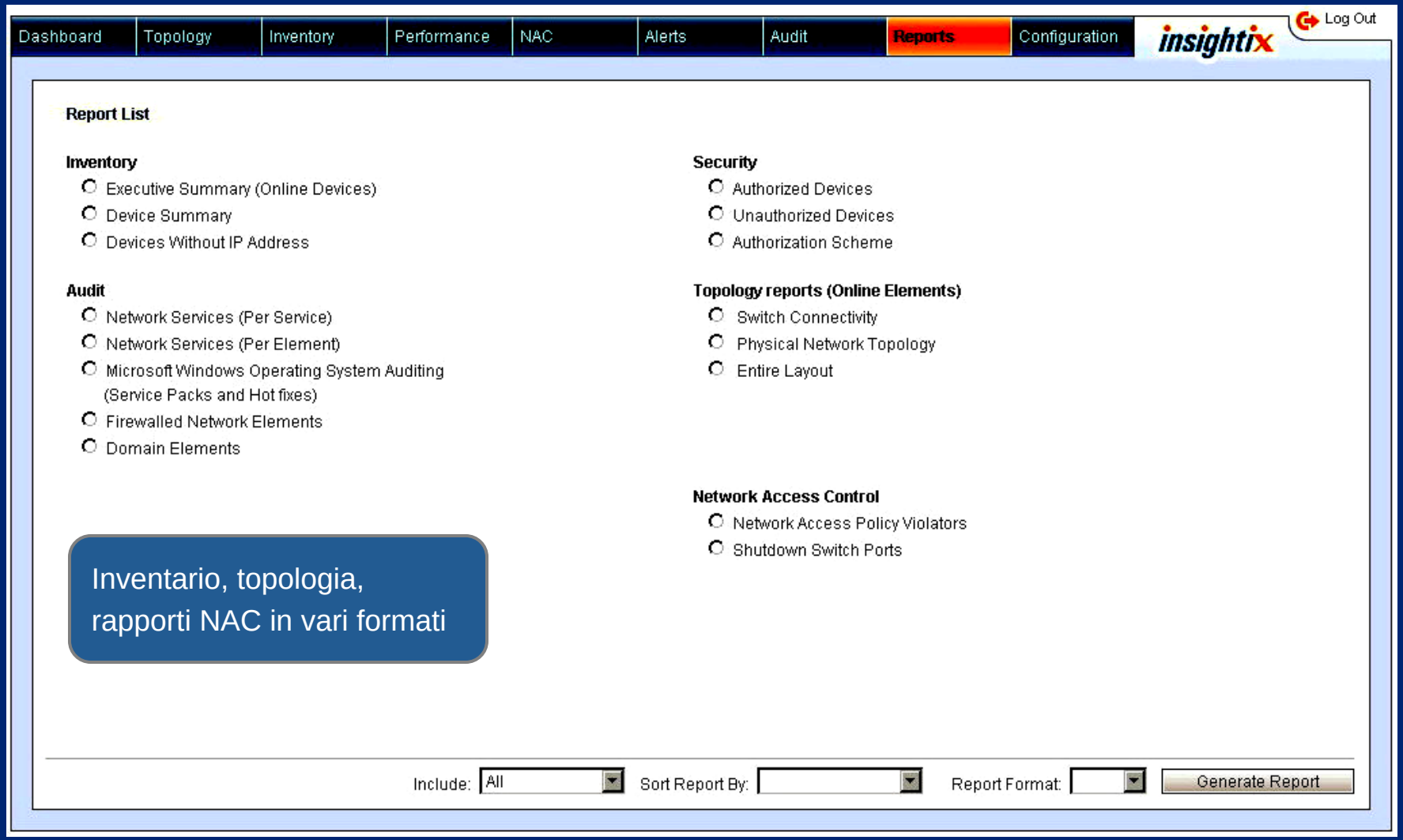
Inventory Main

| | | | | | |
|---|---|---|---|---|---|
| IP Address: | 192.168.[redacted] | OS: | Microsoft Windows 2003 SP1 | Switch IP: | 192.168.[redacted] |
| MAC Address: | 00:02:b3:[redacted] | Type | | Switch Port: | Fa0/1 |
| MAC Vendor ID: | Intel Corporation | Capability: | Domain Controller | Physical Location: | |
| VLAN ID: | 1 | | | | |
| Open Services: | TCP 21 (ftp)<br>TCP 25 (smtp)<br>TCP 53 (dns)<br>TCP 80 (http)<br>TCP 88 (kerberos) | DNS Name: | spiderman.[redacted] | Locate on Topology map | |
| | | NetBIOS Name: | SPIDERMAN | Firewalled: | no |
| | | Username (Windows): | administrator | Authorized: | yes |
| Hot Fixes: (Windows) | KB890046<br>KB893756<br>KB896358<br>KB896422<br>KB896424 | Domain: | [redacted] | | |
| | | Opened Sessions (Rx): | 0 | Opened Sessions (Tx): | 1 |
| | | Free Text: | | | |

Set as Offline | Save




Configurazione degli eventi di allerta




Inventario, topologia, rapporti NAC in vari formati

# Enforcement Methods

- Switch Integration
  - All switches are detected
  - Access to the switches is evaluated
  - The user is prompt if the information provided is not sufficient
- ARP Mitigation

# Implementazione alla SAPIENZA-NET

- Installazione del Manager Center
- Installazione di 5 collector
- Scoperta della rete (mappa)
- Implementazione del controllo accessi in Alert mode
  - Identificazione device ID
  - Autenticazione utente in fase di test

# Ringraziamenti

- ai colleghi del GARR
- al gruppo reti del CITICoRD
- ai presenti che pazientemente mi hanno seguito