WORKSHOP GARR 2023

NET MAKERS

Automatizzare la configurazione e l’accesso sicuro alla rete cablata con il software libero

Daniele Albrizio

Università di Trieste

Rete Università di Trieste (UniTS)

- *gran parte di una /16 IPv4 e una /48 IPv6*
- *circa 10k indirizzi registrati*
- *594 subnet*
- *324 vlan*
- *2 domini di vlan separati*
  - *UniTS*
  - *Lightnet (rete regionale gestita dallo stesso settore)*

Gestione della rete

- *Tecnici e referenti di struttura decentrati non dipendenti dal reparto IT*
- *Nuovi tecnici dipendenti dal reparto IT*

Aspetti positivi IPAM

- *Cosa abbiamo migliorato usando un IPAM e integrandolo con la rete*

Aspetti positivi IPAM

- *Facile inventory dei dispositivi e attrezzature utente collegati*
- *Delega assegnazione degli indirizzi in maniera aderente all'organizzazione interna*
- *Aiuto nell'introduzione di 802.1x*
  - *Migior accountability del traffico (GARR AUP)*

Aspetti positivi IPAM

- *Gestione visuale delle assegnazioni*
  - *DHCP fisse (reservation)*
  - *registrazioni a DNS (diretti e reverse)*
- *Gestione del ciclo di vita di IP, reti e dispositivi*
- *Gestione delle VLAN da assegnare*
- *Supporto alla nomadicità dei dispositivi*

Gestione precedente

Gestione precedente

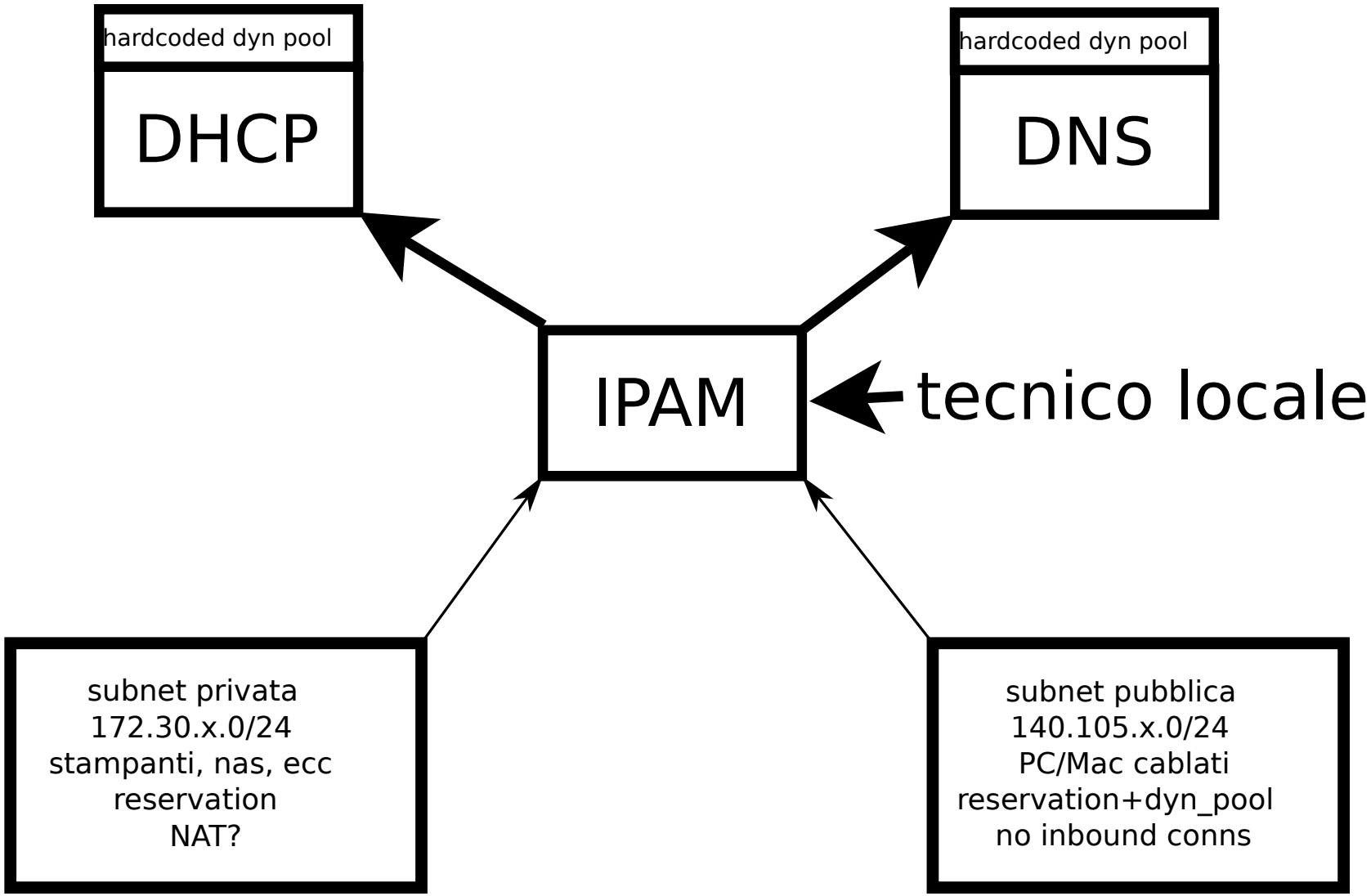
- *Foglio di calcolo per le vlan*
- *File di testo per le subnet*
- *Configurazione manuale del DNS a valle di un ticket di utenti o referenti delegati*
- *Reservation manuali su DHCP*
  - *In parte direttamente editate dai tecnici di Dipartimento con ssh e vim*
- *mac address bypass (MAB) manuale su file di configurazione radius*

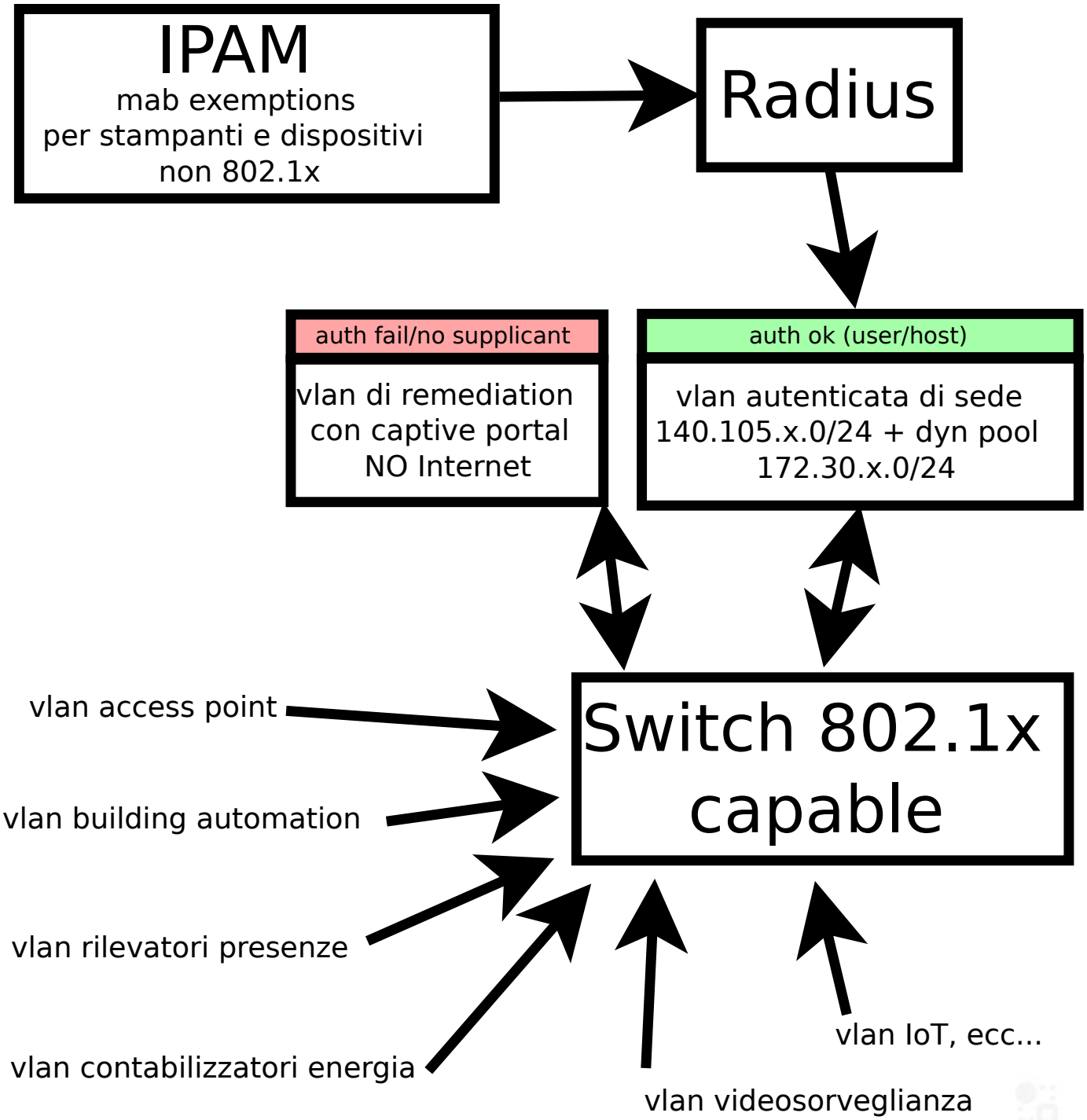
Nuovo modello

Nuovo modello

- *802.1x e Mac Address Bypass (MAB) ubiqui*
- *Servizi speciali su porte untagged*
- *Subnet geografiche idealmente per edificio/dominio amministrativo, ma:*
  - *Terminali biblioteche e VDI*
  - *Telefoni VoIP (LLDP-MED + MAB)*
  - *Diversi dipartimenti nello stesso edificio*
  - *Rete per la didattica frontale e convegni sulle cattedre*

Schema sedi NUOVE



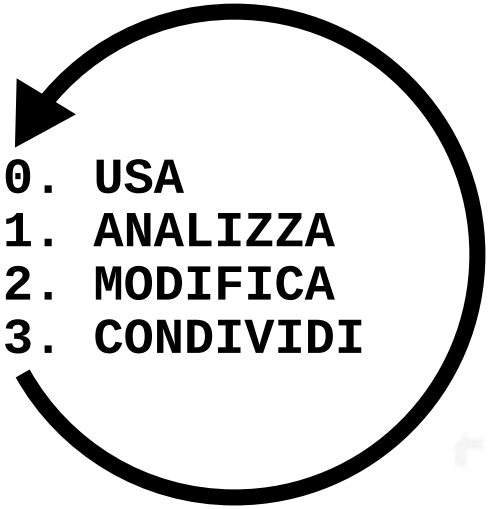

IPAM
mab exemptions
per stampanti e dispositivi
non 802.1x
Radius
auth fail/no supplicant
vlan di remediation
con captive portal
NO Internet
auth ok (user/host)
vlan autenticata di sede
140.105.x.0/24 + dyn pool
172.30.x.0/24
vlan access point
vlan building automation
vlan rilevatori presenze
vlan contabilizzatori energia
Switch 802.1x
capable
vlan videosorveglianza
vlan IoT, ecc...

Software

Soluzioni commerciali

- *Fanno spesso molto più di quanto serve (a noi)*
- *Non rispondono completamente alle esigenze, necessità di personalizzazioni talvolta spinte*
- *Licenze per IP lievitano rapidamente vista la dimensione della rete*

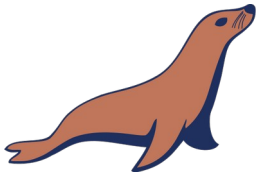
Soluzioni con Software Libero



- *Non integrate (ma integrabili)*
- *Reinventano l'acqua calda, ma alla fine:*
  - *fanno esattamente quel che mi serve*
  - *sono facilmente personalizzabili*
  - *sono velocemente "riparabili" in caso di problemi*

Software

- *DHCP (ISC)*
- *DNS (BIND)*
- *Radius (FREEradius)*
- *IPAM (phpIPAM)*
  - *REST API*
  - *Database*
  - *Script bash a cron (5 min per DNS e 1 min per DHCP)*

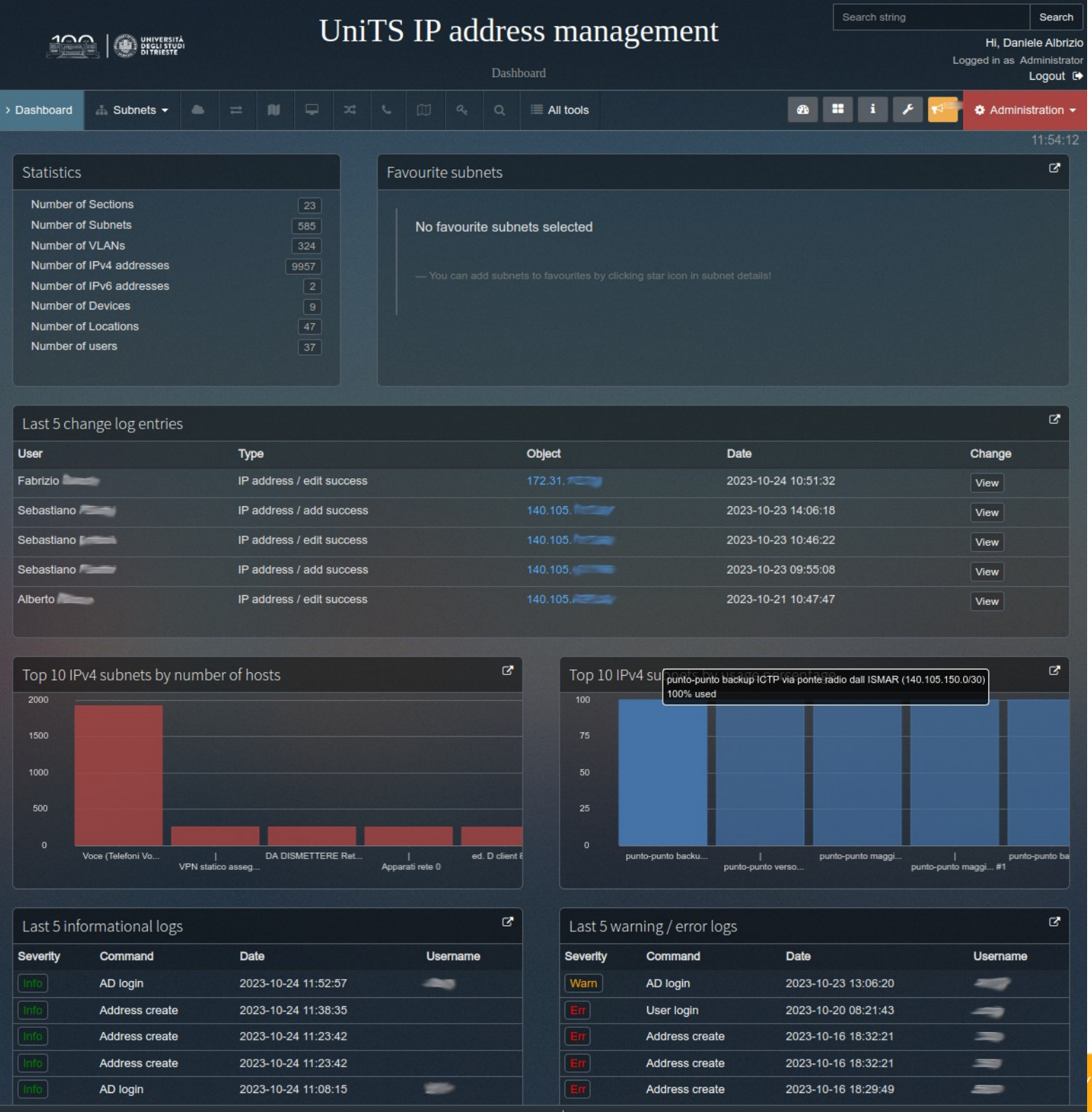


Requisiti e rischi

Requisiti

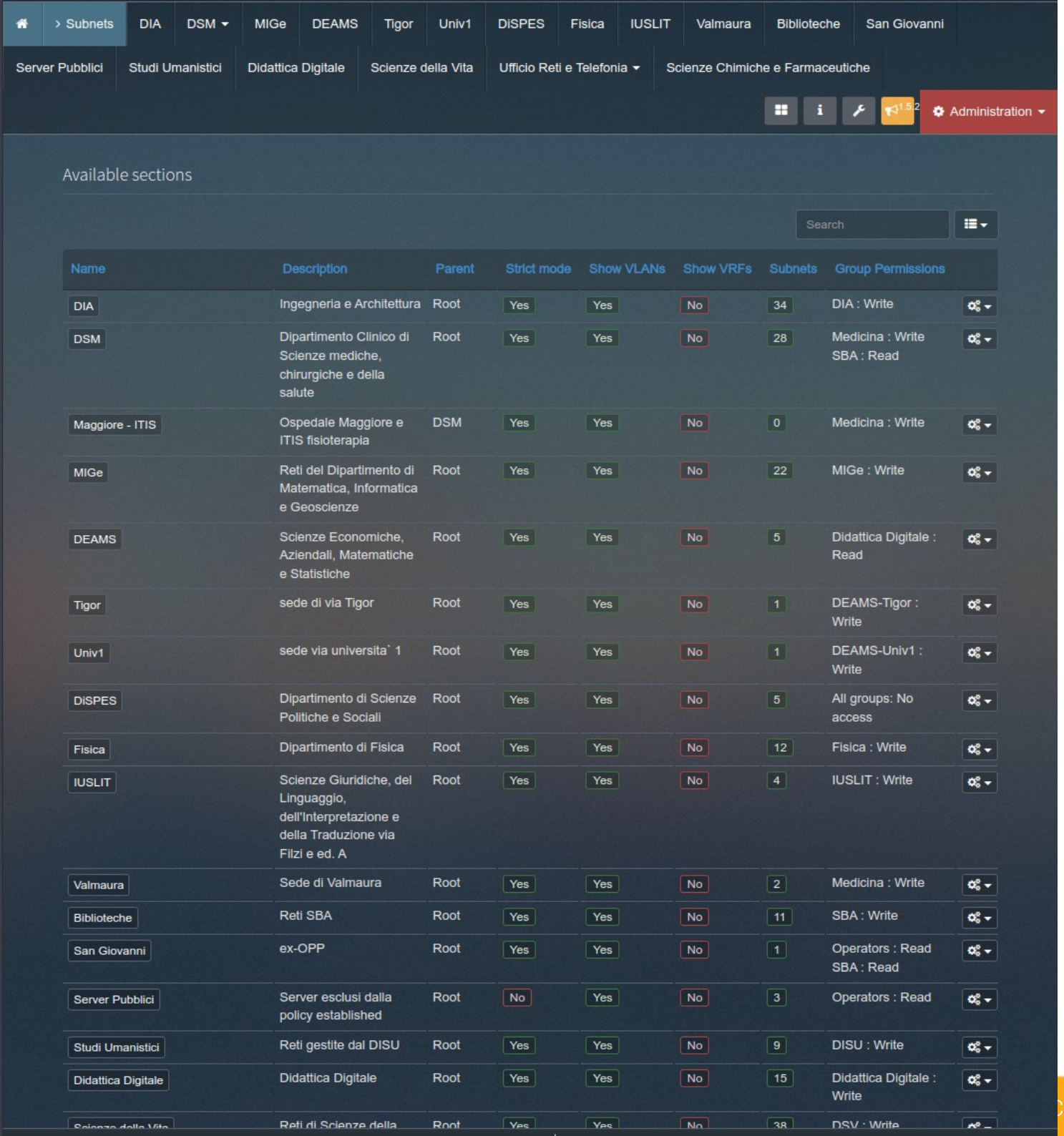
- *Migliorare la gestione della rete*
- *Non indebolire la stabilità dell'infrastruttura esistente*
  - *No dhcp OMAPI e dynDNS con record che scadono*
  - *Script bash a cron ogni 1-5 minuti con controllo di concorrenza di esecuzione*
    - *Scritti con aiuto di intelligenza artificiale (risparmio notevole di tempo ed errori)*

IPAM – IP Address Management

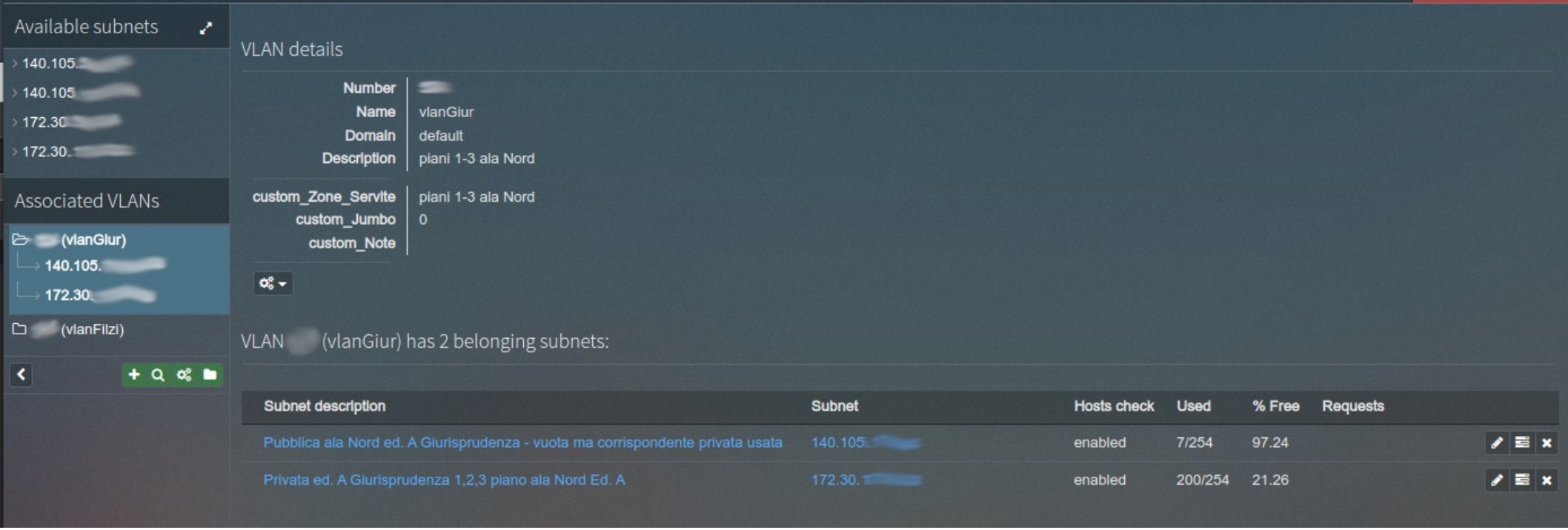


Dashboard

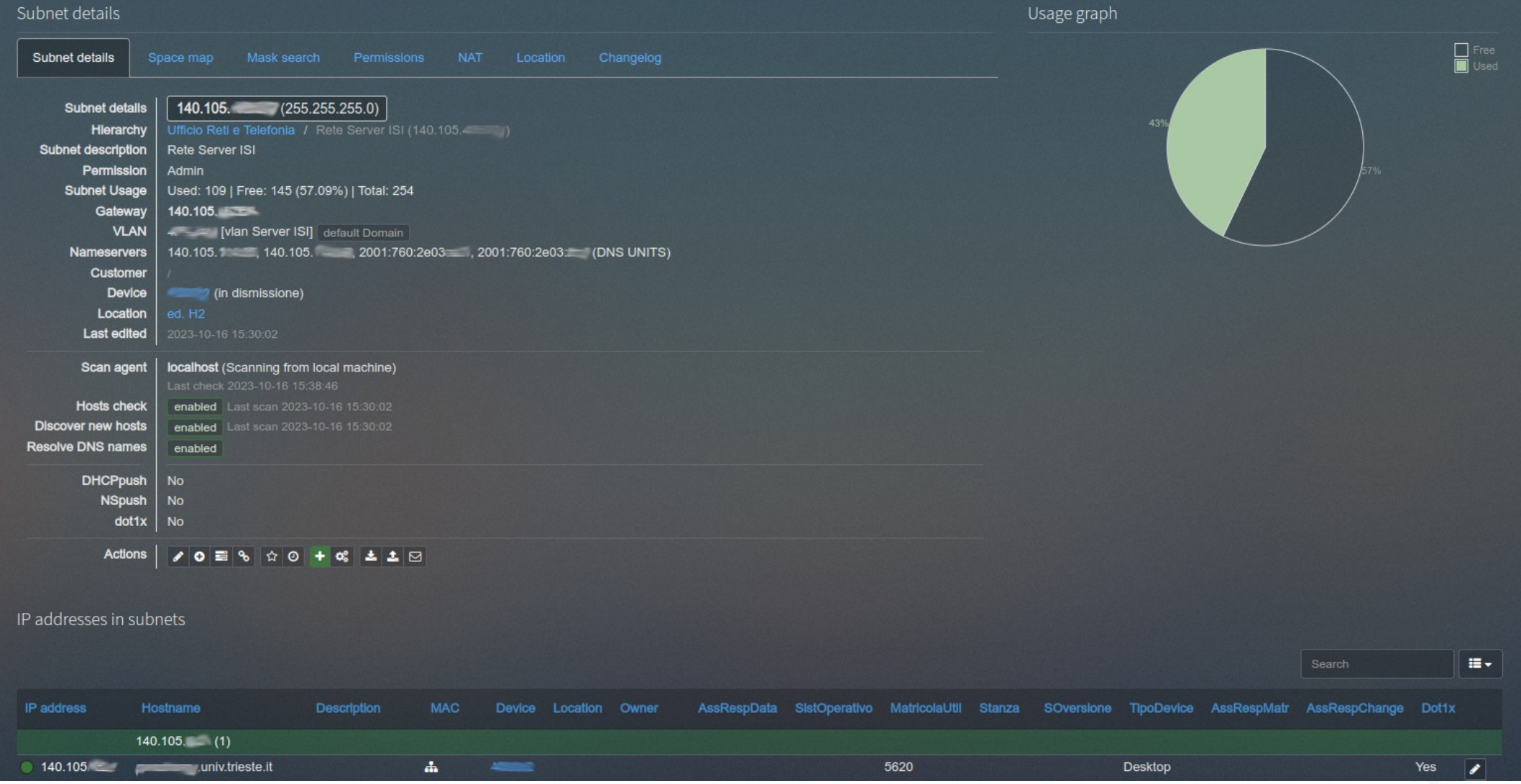
Changelog dettagliato per subnet o globale



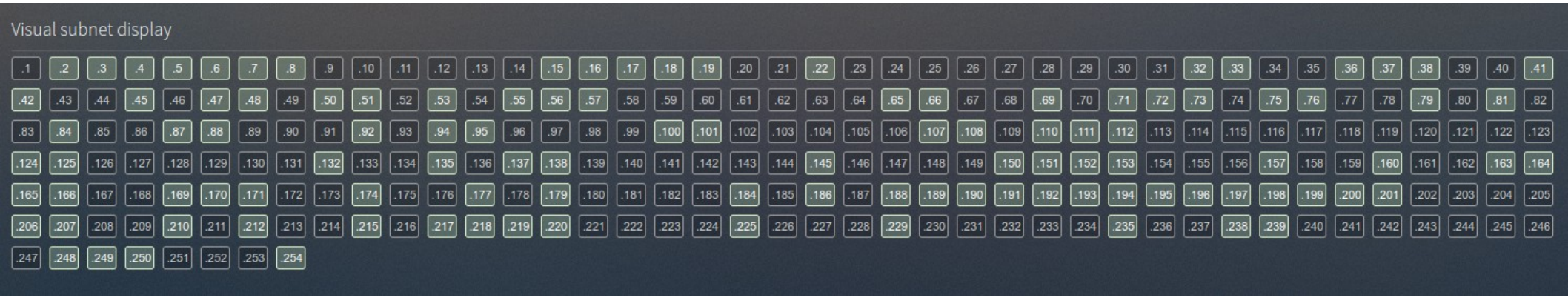
- Sezioni con permessi di accesso e scrittura per gruppi
- Visualizzazioni di dettagli disattivabili per sezione
- Network overlapping control disattivabile



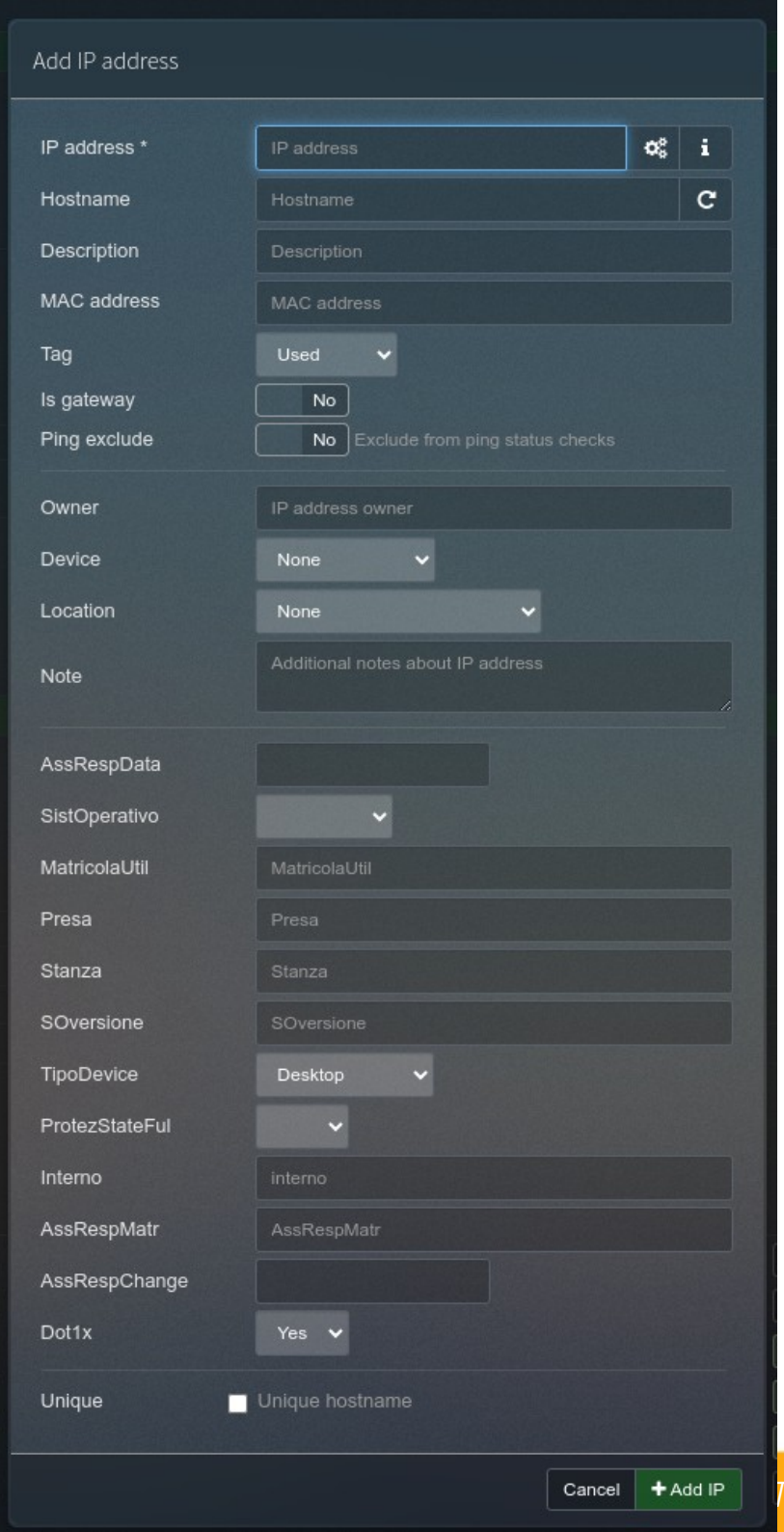
- *Visualizzazione dettagli utili nella comunicazione con i tecnici di Dipartimento come ad es. vlanID, interfacce di routing in quella vlan, stato automazione della subnet*
- *Last seen ARP-table based (no ping)*



- *Dettaglio sottorete con campi personalizzati*
- *Space map aiuta nel subnetting*



Visualizzazione degli IP liberi



- *Maschera di immissione/modifica IP*
- *Tag Used/DHCP/Reserved/ ecc…*
- *Sezione campi personalizzati*

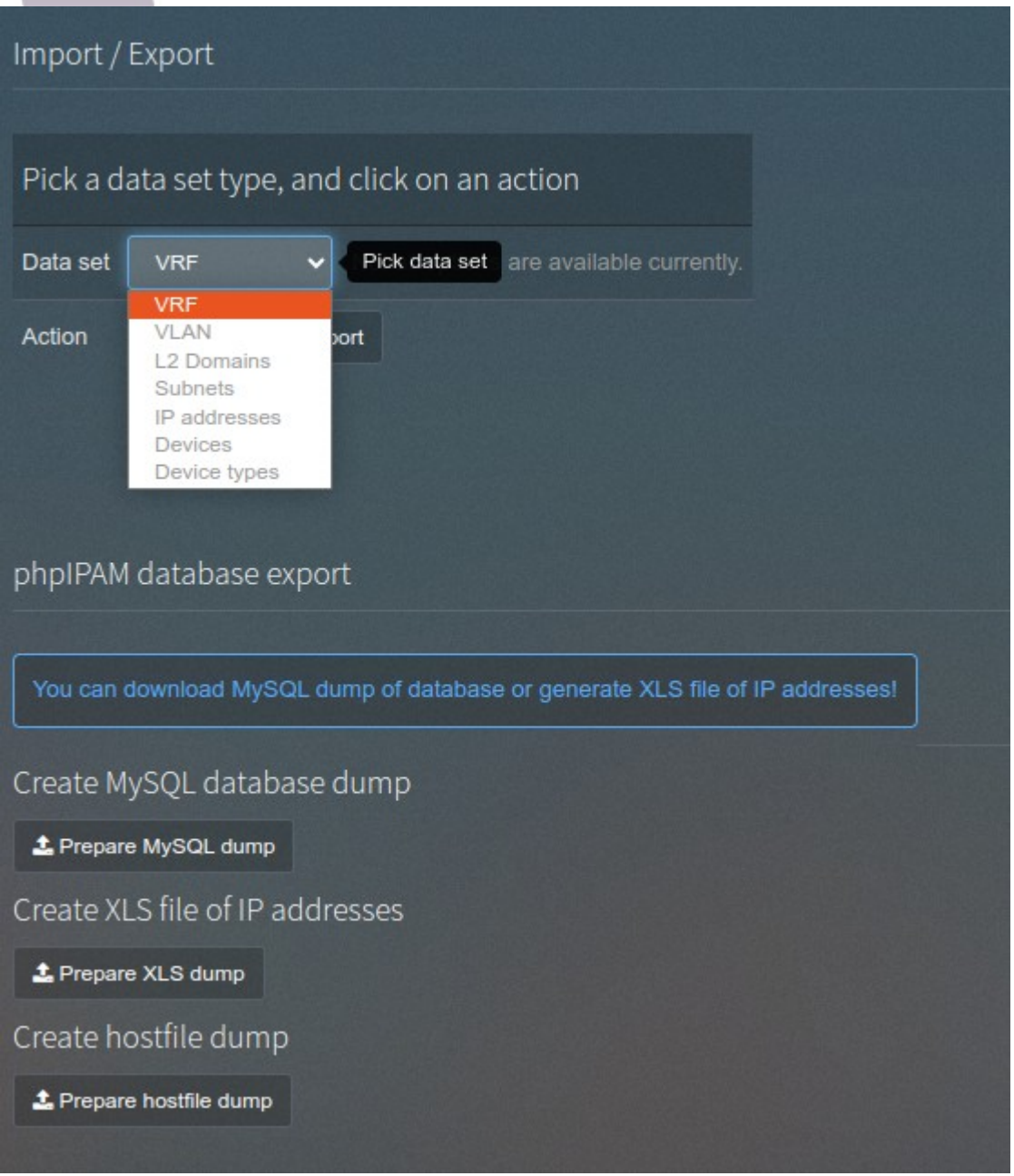
Host, subnet, vlan, ecc. custom fields (e.g. jumbo, zone servite)

Custom fields

You can add additional custom fields to IP addresses and subnets (like CustomerId, location, ...).

Title	Description	Field type	Default	Required	Visible
Custom IP addresses fields					
AssRespData	data assunzione responsabilita` sicurezza	date			Yes
SistOperativo	Major Release	enum('Win7','Win8.x','Win10','Win11','Win2008','Win2012','Win2016','MacOSX','Linux','Altro')			Yes
MatricolaUtil	Numero matricola utilizzatore primario	varchar(31)			Yes
Presa	Numero di presa a muro	varchar(12)			Yes
Stanza	Localizzazione fisica	varchar(32)			Yes
SOversione	Minor Release	varchar(32)			Yes
TipoDevice	Tipo Dispositivo	enum('Desktop','Laptop','Server interno','Server','Stampante','NAS','ThinClient','Altro','Telefono')	Desktop		Yes
ProtezStateFul	Protezione Stateful Firewall	tinyint(1)			Yes
interno	Numero di telefono interno	int(16)			Yes
AssRespMatr	Matricola del responsabile sicurezza host	varchar(31)			Yes
AssRespChange	Ultima modifica all'assunzione responsabilita'	date			Yes
Dot1x	supporta 802.1x	tinyint(1)	1		Yes

Filter



- *Ampio spazio a im/esportazione*
- *NO dump automatici*

ulteriori livelli di dettaglio

Location details

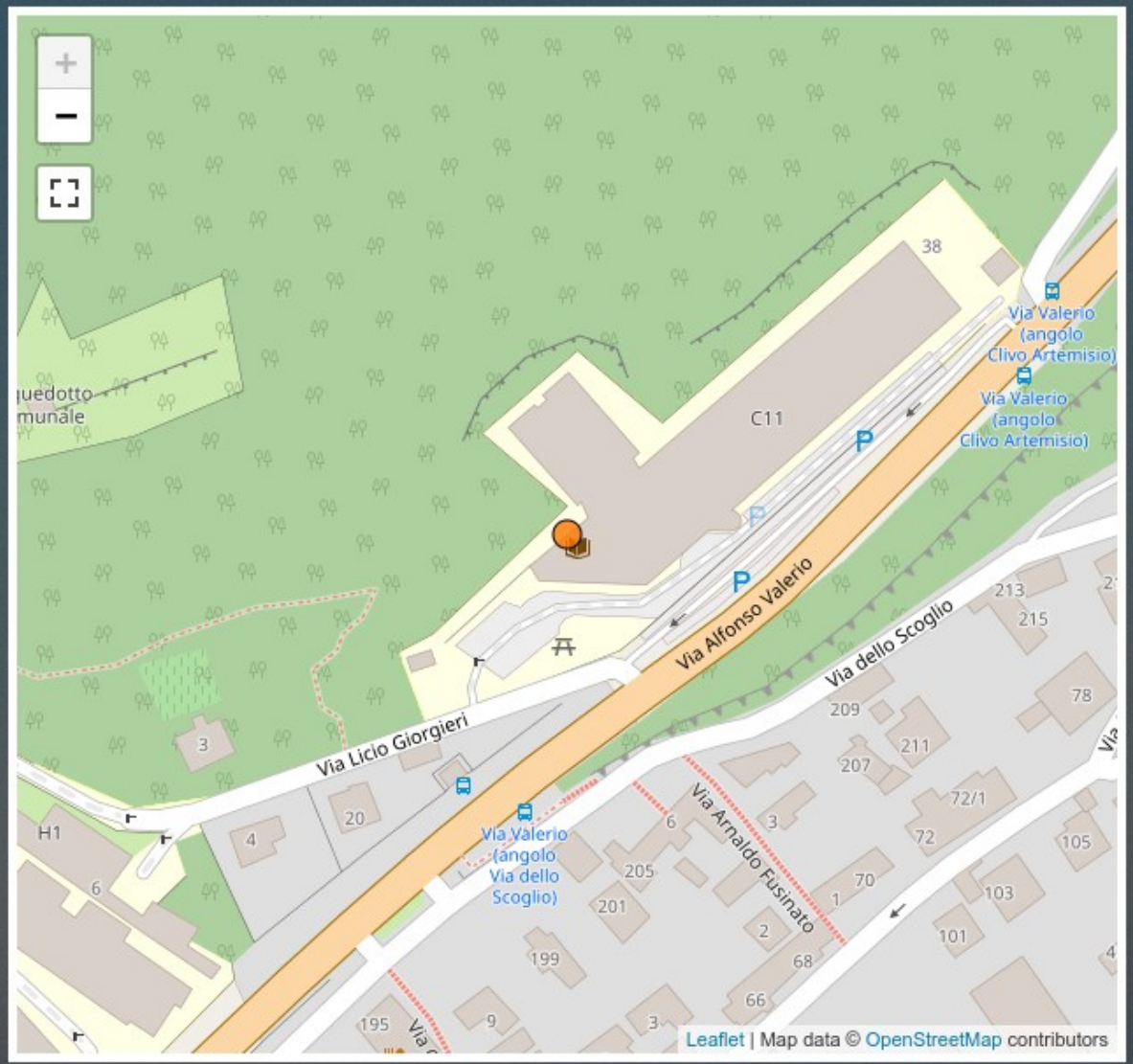
‹ Locations

Name	ed. C11
Address	Trieste, via Giorgieri, 1
Coordinates	45.6605898 / 13.7982976
Description	ed. C11

Actions

Belonging objects

Racks	/
Devices	/
Subnets	140.105. (pubblica DSV C11 (ex BBCM))
	172.30. (privata DSV C11 (ex BBCM))
	172.31 (Telefoni VoIP DSV C11 (ex BBCM))
	172.30 (C11 DSCF ospiti privata)
	172.30. (C11 DSCF privata)
	192.16 (chimici C11 da dismettere)
	140.105 C11 DSCF pubblica)
Addresses	172.31. voip.units.it)
	172.31. voip.units.it)
	172.30 (dscfos .dscf.units.it)
	172.30 (dscfos dscf.units.it)



DHCP

- phpIPAM REST API *(curl+jq per json parsing)*
- *File di configurazione*
  - *<IPAM_subnet_id> <host_file_full_path>*
- *File degli host DHCP*
  - *fqdn-mac_address, mac_address, ip, hostname*

DNS

- phpIPAM *REST API (curl+jq)*
- *File di template della zona di terzo livello con elenco delle subnet e conf statica*

```
$TTL 86400
; Data file of hostnames in valmaura.units.it domain
; Declare here subnets to be parsed from IPAM:
; subnet 140.105.XX.0/24
; subnet 140.105.XXX.0/24
; subnet 140.105.XXX.128/26
@           IN    SOA ns1.units.it. rete.units.it. (
                  SERIAL ; Serial=date e sequenziale 2 cifre
                      57600 ; Refresh secondary
                       7200 ; Retry refresh
                     604800 ; Expire in 4 days
                      86400 ) ; Minimum TTL is 1 day
                IN    NS    ns1.units.it.
                IN    NS    ns2.units.it.
                IN    A     130.186.XXX.XXX
www             IN    CNAME    dmg.units.it.
www.test        IN     CNAME   dmg-www.units.it.
ia              IN     CNAME   dmg-www.units.it.
```

MAC Address Bypass freeRADIUS

- ~~*REST API*~~ *query sql real/runtime (non necessita riavvio radius)*
- *Indipendenza da lentezze o indisponibilità dell'IPAM*
  - *View su MySQL (doppio JOIN)*
    - *Per oggetti con 802.1x=no → mac address, vlan*

MAC Address Bypass - Radius

- *postgres al servizio dei server radius con foreign data wrapper e materialized view concurrently refreshed ogni minuto*
- *Tipizzazione del dato mac address in postgres al posto dell'input filtering*

TBD – Evoluzioni future

- *Integrazione con il Firewall:*
  - *Configurazione del NAT per subnet*
  - *Aperture del traffico entrant per i server*
- *Gestire IPv6 (DNS, IPAM, DHCPv6?)*
- *SAML/openID login*
- *Modulo di richiesta IP da parte dell'utente (wish)*

Ricapitolando

- *Probabilmente ci sono altri strumenti liberi anche più validi (PowerDNS, NetBox*)*
- *Anche sul mercato Solarwinds, Infoblox*
- *La soluzione esposta è quella adottata da UniTS valutando vari aspetti come trade-off ottimale per la propria situazione, probabilmente non coincide con scelte che farebbero altri*
- *Ulteriori info al caffè*

[*] Lorenzo Puccio, Fabio Farina, Netbox, inventory in GARR-T, WS22

Non si fa niente di grande da soli

- *Stefano Catani*
  - *primo deployment e valutazione di phpIPAM*
- *Antenore Bartulovich e Fabrizio Sancin*
  - *sostituzione di centinaia di vecchi switch con nuovi 802.1x compliant*
- *Miha Petkovsek et al per lo sviluppo*
  - *https://github.com/phpipam/*

WORKSHOP GARR 2023

NET MAKERS

Domande?

Daniele Albrizio
albrizio@units.it