

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

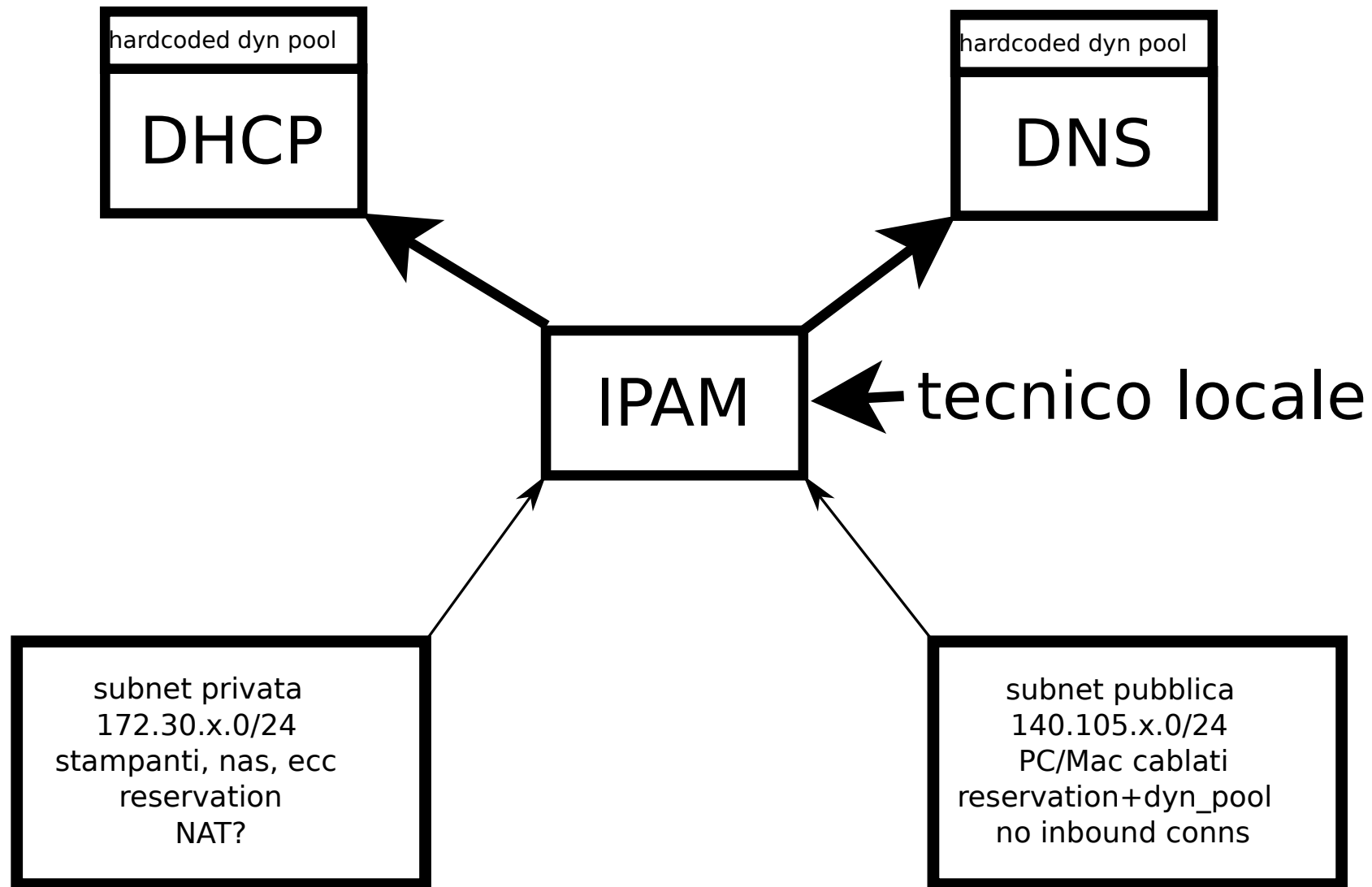
- *Foglio di calcolo per le vlan*
- *File di testo per le subnet*
- *Configurazione manuale del DNS a valle di un ticket di utenti o referenti delegati*
- *Reservation manuali su DHCP*
 - *In parte direttamente editate dai tecnici di Dipartimento con ssh e vim*
- *mac address bypass (MAB) manuale su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

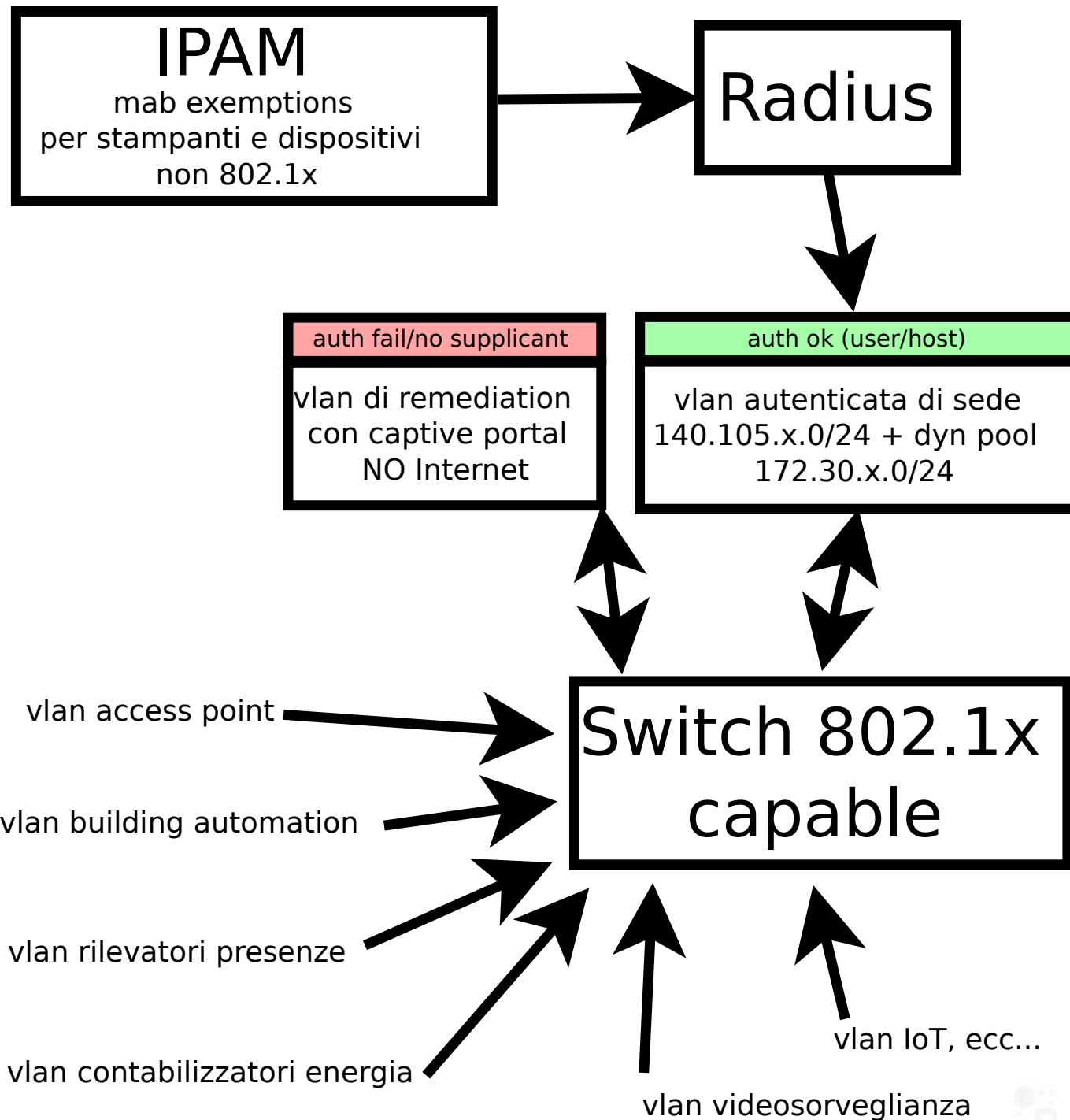
Nuovo modello

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





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*



0. USA
1. ANALIZZA
2. MODIFICA
3. CONDIVIDI

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)*



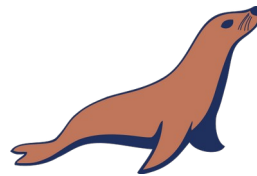
Internet Systems
Consortium

BIND 

freeRADIUS

{php}IPAM

Open-source IP address management



MariaDB



PostgreSQL



BASH
THE BOURNE-AGAIN SHELL

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

{php}IPAM

Open-source IP address management

Statistics

Number of Sections	23
Number of Subnets	585
Number of VLANs	324
Number of IPv4 addresses	9957
Number of IPv6 addresses	2
Number of Devices	9
Number of Locations	47
Number of users	37

Favourite subnets

No favourite subnets selected

— You can add subnets to favourites by clicking star icon in subnet details!

Last 5 change log entries

User	Type	Object	Date	Change
Fabrizio	IP address / edit success	172.31.7	2023-10-24 10:51:32	View
Sebastiano	IP address / add success	140.105.1	2023-10-23 14:06:18	View
Sebastiano	IP address / edit success	140.105.1	2023-10-23 10:46:22	View
Sebastiano	IP address / add success	140.105.1	2023-10-23 09:55:08	View
Alberto	IP address / edit success	140.105.1	2023-10-21 10:47:47	View

Top 10 IPv4 subnets by number of hosts



Top 10 IPv4 subnets by usage



Last 5 informational logs

Severity	Command	Date	Username
Info	AD login	2023-10-24 11:52:57	
Info	Address create	2023-10-24 11:38:35	
Info	Address create	2023-10-24 11:23:42	
Info	Address create	2023-10-24 11:23:42	
Info	AD login	2023-10-24 11:08:15	

Last 5 warning / error logs

Severity	Command	Date	Username
Warn	AD login	2023-10-23 13:06:20	
Err	User login	2023-10-20 08:21:43	
Err	Address create	2023-10-16 18:32:21	
Err	Address create	2023-10-16 18:32:21	
Err	Address create	2023-10-16 18:29:49	

Dashboard

Changelog
dettagliato per
subnet o globale

Available sections

Name	Description	Parent	Strict mode	Show VLANs	Show VRFs	Subnets	Group Permissions
DIA	Ingegneria e Architettura	Root	Yes	Yes	No	34	DIA : Write
DSM	Dipartimento Clinico di Scienze mediche, chirurgiche e della salute	Root	Yes	Yes	No	28	Medicina : Write SBA : Read
Maggiore - ITIS	Ospedale Maggiore e ITIS fisioterapia	DSM	Yes	Yes	No	0	Medicina : Write
MIGe	Reti del Dipartimento di Matematica, Informatica e Geoscienze	Root	Yes	Yes	No	22	MIGe : Write
DEAMS	Scienze Economiche, Aziendali, Matematiche e Statistiche	Root	Yes	Yes	No	5	Didattica Digitale : Read
Tigor	sede di via Tigor	Root	Yes	Yes	No	1	DEAMS-Tigor : Write
Univ1	sede via universita' 1	Root	Yes	Yes	No	1	DEAMS-Univ1 : Write
DISPES	Dipartimento di Scienze Politiche e Sociali	Root	Yes	Yes	No	5	All groups: No access
Fisica	Dipartimento di Fisica	Root	Yes	Yes	No	12	Fisica : Write
IUSLIT	Scienze Giuridiche, del Linguaggio, dell'Interpretazione e della Traduzione via Filzi e ed. A	Root	Yes	Yes	No	4	IUSLIT : Write
Valmaura	Sede di Valmaura	Root	Yes	Yes	No	2	Medicina : Write
Biblioteche	Reti SBA	Root	Yes	Yes	No	11	SBA : Write
San Giovanni	ex-OPP	Root	Yes	Yes	No	1	Operators : Read SBA : Read
Server Pubblici	Server esclusi dalla policy established	Root	No	Yes	No	3	Operators : Read
Studi Umanistici	Reti gestite dal DISU	Root	Yes	Yes	No	9	DISU : Write
Didattica Digitale	Didattica Digitale	Root	Yes	Yes	No	15	Didattica Digitale : Write
Scienze della Vita	Reti di Scienze della	Root	Yes	Yes	No	38	DSV : Write

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

The screenshot displays a network management interface. On the left, there are sections for 'Available subnets' (listing 140.105, 172.30, etc.) and 'Associated VLANs' (showing 'vlanGiur' and 'vlanFilzi'). The main area is titled 'VLAN details' and shows information for 'vlanGiur', including its number, name, domain, and description. Below this, a table lists subnets associated with the VLAN.

Subnet description	Subnet	Hosts check	Used	% Free	Requests
Pubblica ala Nord ed. A Giurisprudenza - vuota ma corrispondente privata usata	140.105.	enabled	7/254	97.24	
Privata ed. A Giurisprudenza 1,2,3 piano ala Nord Ed. A	172.30.	enabled	200/254	21.26	

- *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)*

[Subnet details](#) [Space map](#) [Mask search](#) [Permissions](#) [NAT](#) [Location](#) [Changelog](#)

Subnet details **140.105. (255.255.255.0)**

Hierarchy [Ufficio Reti e Telefontia](#) / [Rete Server ISI \(140.105. \)](#)

Subnet description Rete Server ISI

Permission Admin

Subnet Usage Used: 109 | Free: 145 (57.09%) | Total: 254

Gateway 140.105.

VLAN [vlan Server ISI] default Domain

Nameservers 140.105. , 140.105. , 2001:760:2e03: , 2001:760:2e03: (DNS UNITS)

Customer /

Device (in dismissione)

Location ed. H2

Last edited 2023-10-16 15:30:02

Scan agent localhost (Scanning from local machine)
Last check 2023-10-16 15:38:46

Hosts check enabled Last scan 2023-10-16 15:30:02




Discover new hosts enabled Last scan 2023-10-16 15:30:02

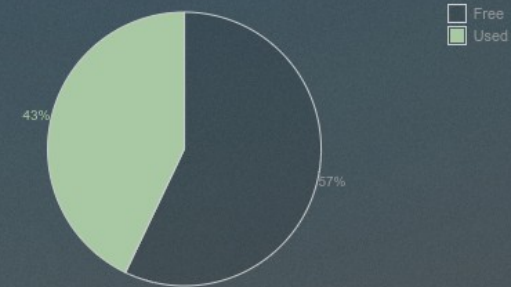
Resolve DNS names enabled

DHCPpush No

NSpush No

dot1x No

Actions           



IP addresses in subnets

Search

⌵

IP address	Hostname	Description	MAC	Device	Location	Owner	AssRespData	SistOperativo	MatricolaUtili	Stanza	SOversione	TipoDevice	AssRespMatr	AssRespChange	Dot1x
140.105. (1)															
140.105.	.univ.trieste.it								5620		Desktop			Yes	

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

Visual subnet display

.1	.2	.3	.4	.5	.6	.7	.8	.9	.10	.11	.12	.13	.14	.15	.16	.17	.18	.19	.20	.21	.22	.23	.24	.25	.26	.27	.28	.29	.30	.31	.32	.33	.34	.35	.36	.37	.38	.39	.40	.41
.42	.43	.44	.45	.46	.47	.48	.49	.50	.51	.52	.53	.54	.55	.56	.57	.58	.59	.60	.61	.62	.63	.64	.65	.66	.67	.68	.69	.70	.71	.72	.73	.74	.75	.76	.77	.78	.79	.80	.81	.82
.83	.84	.85	.86	.87	.88	.89	.90	.91	.92	.93	.94	.95	.96	.97	.98	.99	.100	.101	.102	.103	.104	.105	.106	.107	.108	.109	.110	.111	.112	.113	.114	.115	.116	.117	.118	.119	.120	.121	.122	.123
.124	.125	.126	.127	.128	.129	.130	.131	.132	.133	.134	.135	.136	.137	.138	.139	.140	.141	.142	.143	.144	.145	.146	.147	.148	.149	.150	.151	.152	.153	.154	.155	.156	.157	.158	.159	.160	.161	.162	.163	.164
.165	.166	.167	.168	.169	.170	.171	.172	.173	.174	.175	.176	.177	.178	.179	.180	.181	.182	.183	.184	.185	.186	.187	.188	.189	.190	.191	.192	.193	.194	.195	.196	.197	.198	.199	.200	.201	.202	.203	.204	.205
.206	.207	.208	.209	.210	.211	.212	.213	.214	.215	.216	.217	.218	.219	.220	.221	.222	.223	.224	.225	.226	.227	.228	.229	.230	.231	.232	.233	.234	.235	.236	.237	.238	.239	.240	.241	.242	.243	.244	.245	.246
.247	.248	.249	.250	.251	.252	.253	.254																																	

Visualizzazione degli IP liberi

Add IP address

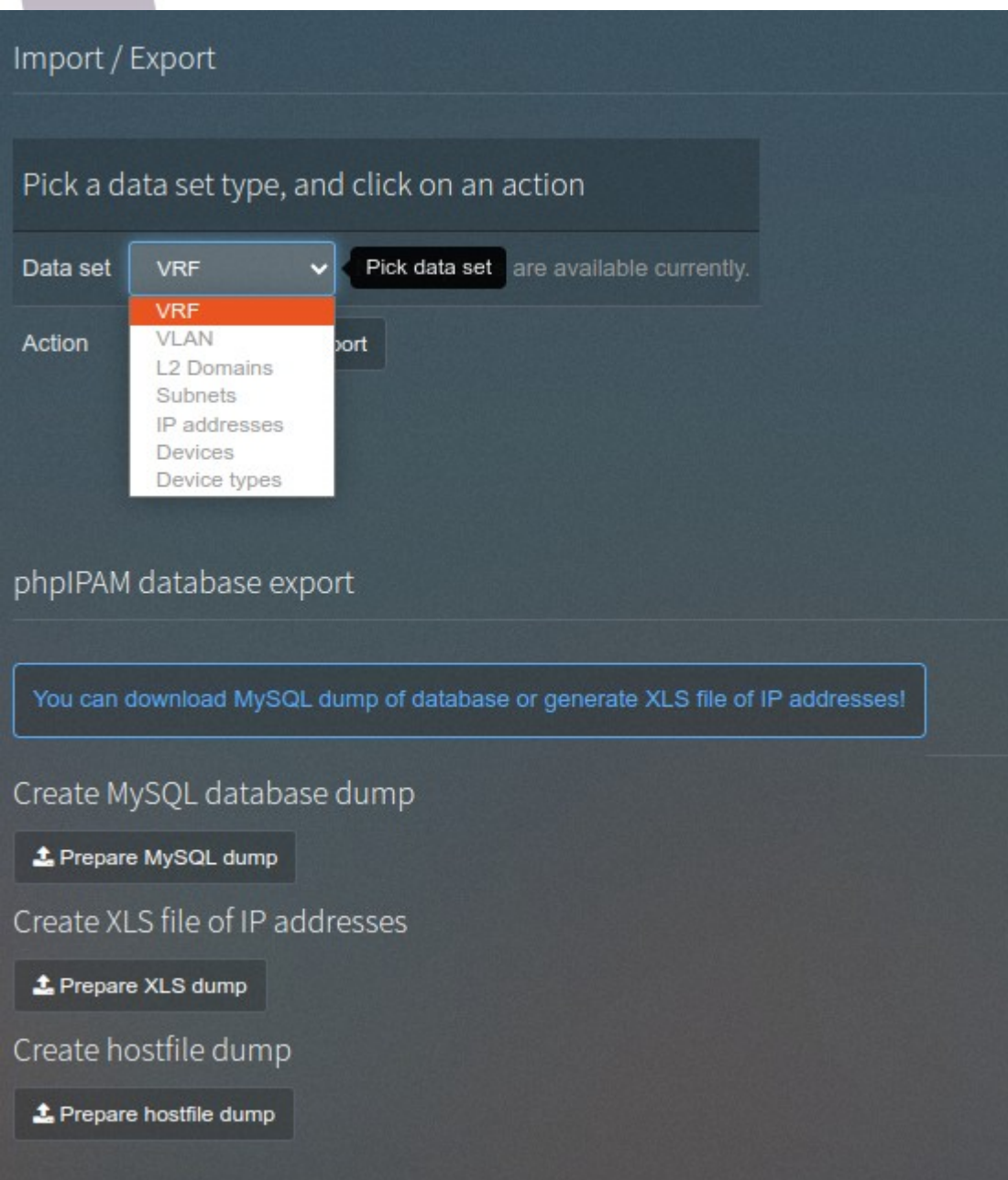
IP address *	<input type="text" value="IP address"/>		
Hostname	<input type="text" value="Hostname"/>		
Description	<input type="text" value="Description"/>		
MAC address	<input type="text" value="MAC address"/>		
Tag	<div>Used </div>		
Is gateway	<div>No </div>		
Ping exclude	<div>No </div> Exclude from ping status checks		
Owner	<input type="text" value="IP address owner"/>		
Device	<div>None </div>		
Location	<div>None </div>		
Note	<input type="text" value="Additional notes about IP address"/>		
AssRespData	<input type="text"/>		
SistOperativo	<div></div>		
MatricolaUtil	<input type="text" value="MatricolaUtil"/>		
Presa	<input type="text" value="Pres"/>		
Stanza	<input type="text" value="Stanza"/>		
SOversione	<input type="text" value="SOversione"/>		
TipoDevice	<div>Desktop </div>		
ProtezStateFul	<div></div>		
Interno	<input type="text" value="interno"/>		
AssRespMatr	<input type="text" value="AssRespMatr"/>		
AssRespChange	<input type="text"/>		
Dot1x	<div>Yes </div>		
Unique	<input type="checkbox"/> Unique hostname		

Cancel Add IP

- *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



- *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 /

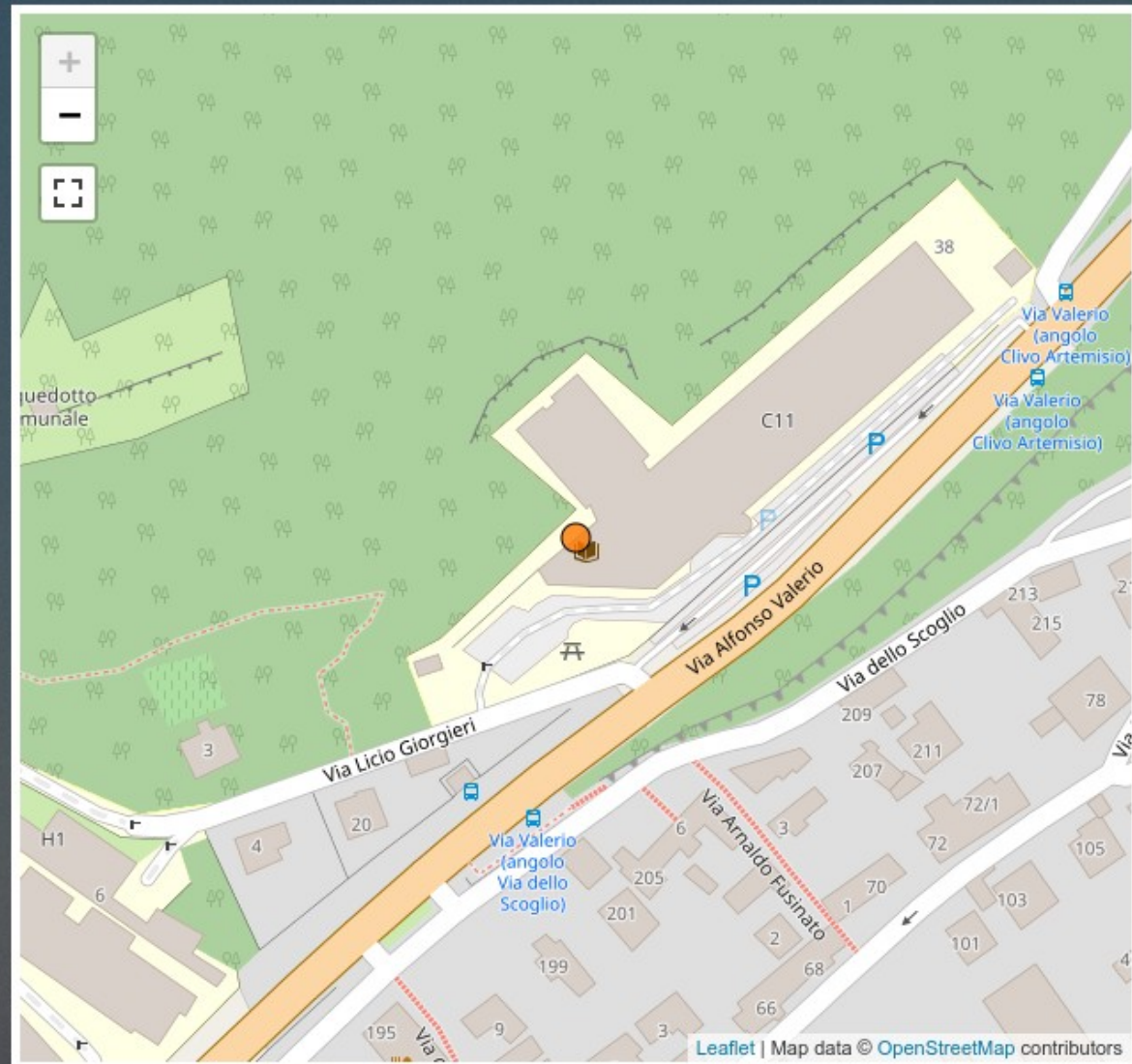
Devices /

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 smettere)
- ✖ 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 *free*RADIUS

- ~~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/>*

Domande?



Daniele Albrizio
albrizio@units.it

Quest'opera è stata rilasciata con licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Italia. Per leggere una copia della licenza visita il sito web <http://creativecommons.org/licenses/by-nc-sa/3.0/it/> o spedisce una lettera a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.