WORKSHOP GARR 2026

NET MAKERS

Controllo accessi alla rete cablata: standard aperti ed esperienza all'Università di Verona

Andrea Sartori

Università degli Studi di Verona

Chi è connesso alla tua rete? Lo sai … davvero??



Il nostro punto di partenza

VLAN assegnate staticamente

Inventario incompleto





Poca visibilità



Gestione manuale



Una sola rete, tanti mondi diversi

Sistemi diversi, dispositivi eterogenei, esigenze differenti



I sistemi NAC alla prova dei fatti

POC: i limiti di copertura e di integrazione

Cisco NAC Appliance

Sun Java System Web Proxy



Sophos NAC Advanced

Microsoft NAP
(Network Access Protection)

Enterasys Secure Network

I requisiti che portano a 802.1X e RADIUS

- **Compatibilità con i sistemi presenti.**

Agenti e connettori non coprivano tutte le piattaforme: serviva adattarsi al parco esistente.

- **Identità dell'utente.**

Autenticare la postazione non bastava: occorreva riconoscere i singoli eventi di logon e logoff.

- **Integrazione con gli apparati di rete.**

La policy di autorizzazione doveva effettivamente tradursi nell' applicazione coerente di profili e VLAN.

- **Vincoli sul percorso del traffico.**

Alcune soluzioni richiedevano by design il transito del traffico inline; PBR e PBF non erano sempre praticabili e aggiungevano complessità all'infrastruttura.

- **Controllo operativo.**

Log e configurazioni dovevano essere chiari e comprensibili, per consentire di diagnosticare i guasti e intervenire sul eventuali integrazioni e modifiche.

- **Introduzione graduale.**

Partire dalle workstation offriva la possibilità di iniziare a lavorare all'interno di un perimetro familiare e gestibile, con la possibilità di introdurre gradualmente altre categorie di dispositivi.

- **Sostenibilità economica e gestionale.**

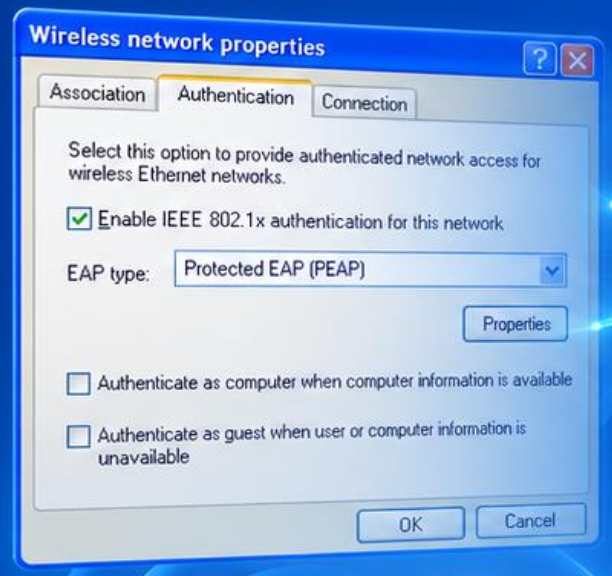
Nella valutazione della soluzione va considerata l'infrastruttura richiesta e lavoro per mantenerla.

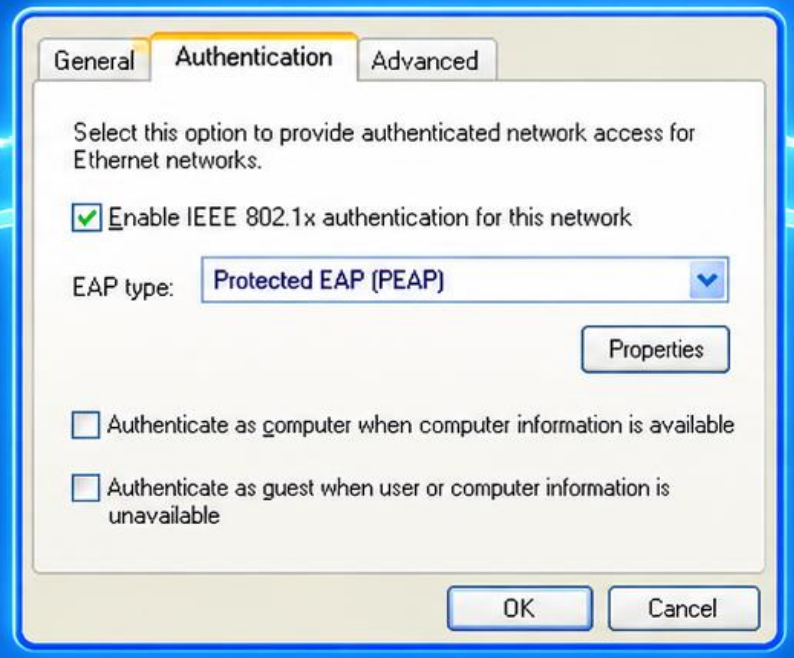
- **Continuità oltre il singolo prodotto.**

Standard condivisi permettevano di far evolvere i componenti conservando una base comune.

Dal Wi-Fi al cablato il denominatore comune

La stessa logica 802.1X del wireless adottata nella rete cablata





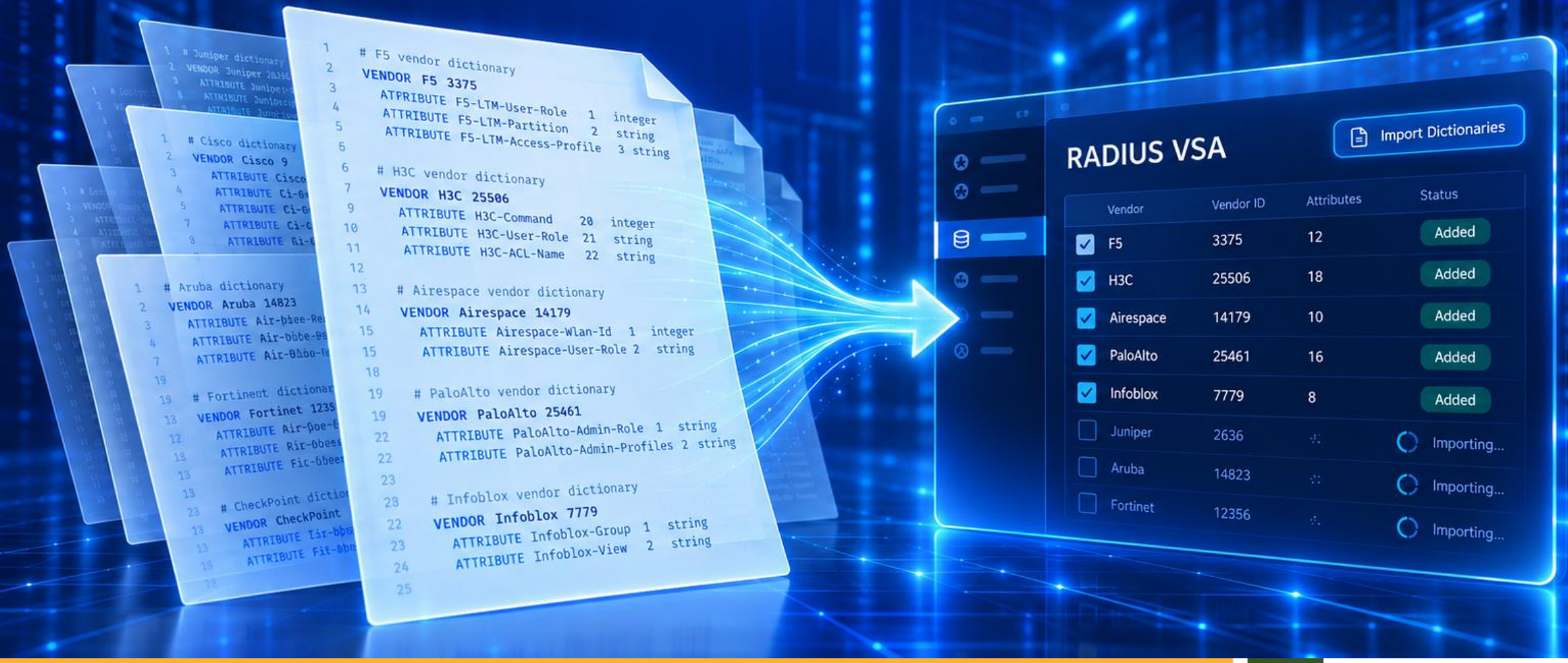






La scelta di RADIUS: i dizionari VSA

Un piccolo sforzo che può risultare decisivo



AAA: prima gli endpoint, poi il resto

Una porta, un host: workstation autenticate VS altri device



Perché partire dalle workstation

Un primo perimetro gestibile

- **Sistemi già capaci di autenticarsi.**

In quel periodo le workstation iniziavano a disporre di supplicant 802.1X nativo; la diffusione di Windows XP SP2 offriva una base uniforme da configurare e verificare.

- **Rispondere al primo obiettivo di riconoscere gli utenti.**

Si potevano distinguere gli accessi autenticati e assegnare VLAN per categoria, prima di classificare ogni apparato.

- **Riutilizzare l'esperienza del Wi-Fi.**

Si sono trasferite nell'ambiente cablato competenze e paradigmi già validati.

- **Ridurre le variabili con il single-host e rendere più semplice il troubleshooting**

Una porta e un unico client erano coerenti con l'infrastruttura e circoscrivevano i casi da gestire. Era più facile seguire il rapporto tra client, autenticazione e VLAN senza introdurre sin da subito dispositivi in cascata

- **Provare prima di estendere.**

Ambienti di test e verifica dei client permettevano di consolidare e raffinare il modello della configurazione applicata prima di una distribuzione più estesa.

- **Accompagnare la migrazione.**

La rete di fallback consentiva comunque di gestire gli apparati ancora da censire e disciplinare.

Lo “switch stampanti”: due reti, due regole

Si accentua la dicotomia tra endpoint e device



Telefoni e aule: più host sulla stessa porta



MAB: compatibilità e inventario



Quando il dispositivo non parla

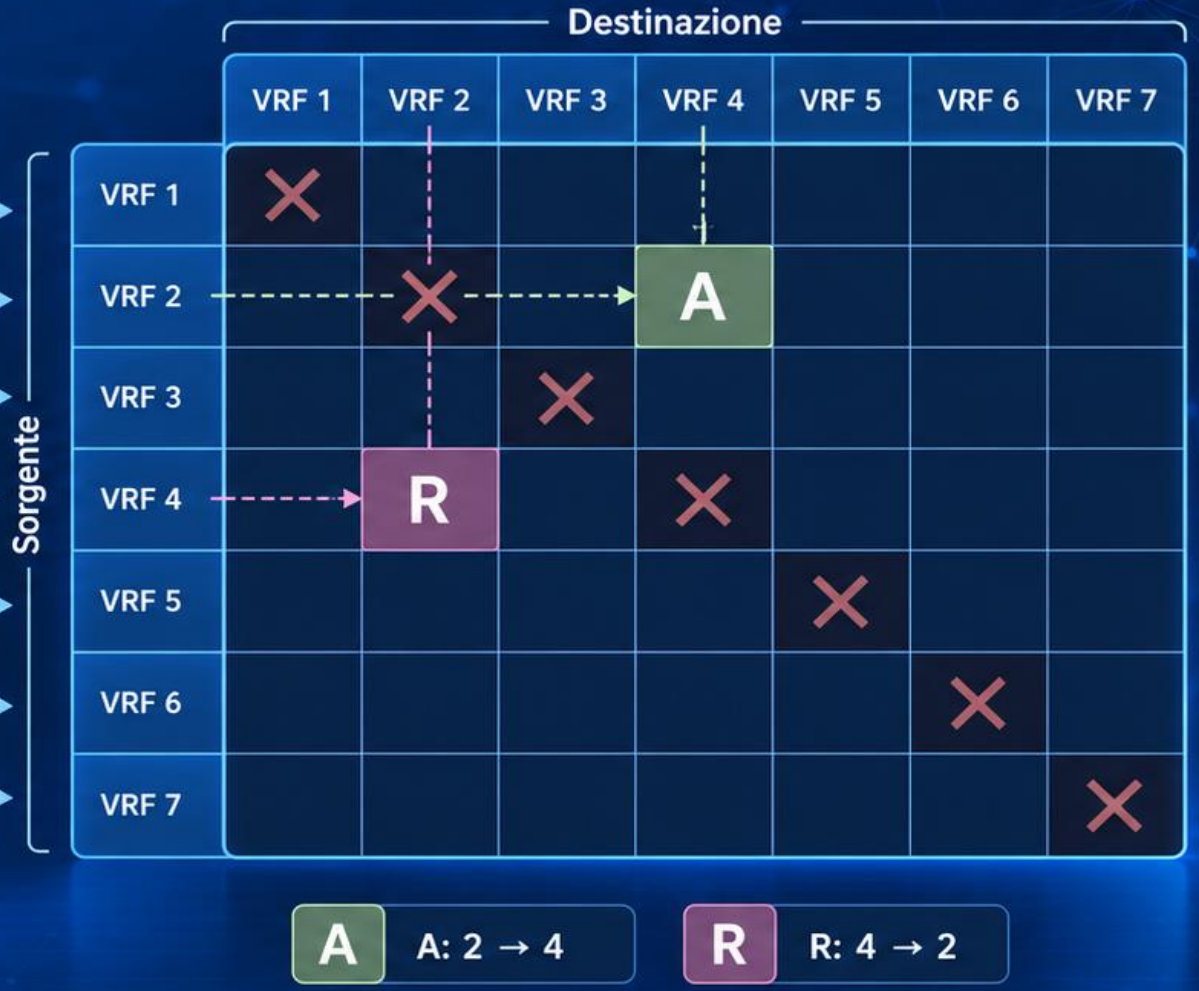
Silent endpoint, workaround con switch managed



I VRF isolano, le intersezioni richiedono disciplina



Raggruppamenti illustrativi

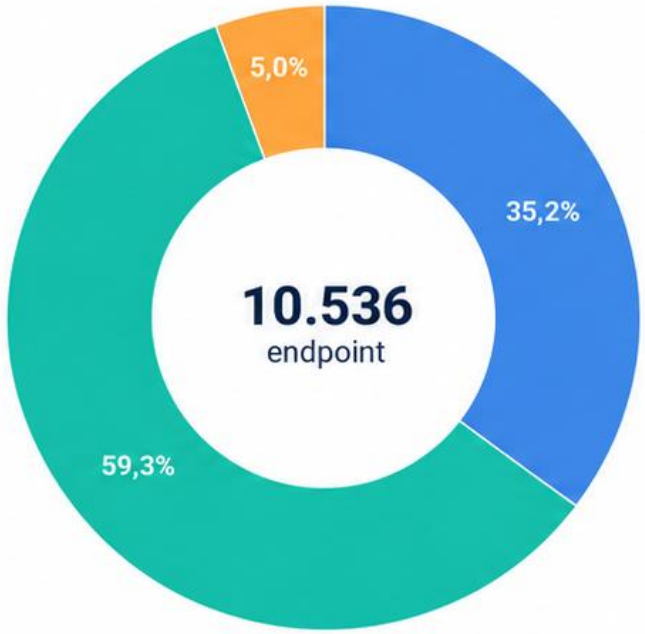


Ritorno di sessione: stato della connessione

Oggi: uniformità e dimensioni

Switch online	Switch offline	Endpoint censiti
332	0	10.536

Metodo di accesso — Tutti gli endpoint



802.1X	35,2%
MAB	59,3%
Fallback	5,0%

Authorization profiles — 10.536 endpoint

#	Profile	Endpoint ▲	%
1	NET-PTA	3.424	32,5%
2	PHONE	1.788	17,0%
3	AP	1.413	13,4%
4	NOAUTH	1.221	11,6%
5	LIVE	655	6,2%
6	PRINT	458	4,3%
7	CCTV	433	4,1%
8	VCONF	299	2,8%
9	SRVEXT	219	2,1%
10	NET-STU	129	1,2%

⌄	Altri profili (11)	Endpoint	%
11	NAS	122	1,2%
12	DOORS	96	0,9%
13	KIOSK	81	0,8%
14	DOT1X	43	0,4%
15	BADGE	34	0,3%
16	ALARMS	32	0,3%
17	NET-ADM	29	0,3%
18	VOIP	24	0,2%
19	NET-WIN	18	0,2%
20	MEETING	10	0,1%
21	SMARTHOME	4	-
22	BADGEAOUI	2	-
23	INSTRUMENTS	2	-

Questioni Aperte e WIP

- Da Authentication Open a Closed, superando la configurazione con VLAN silente.
- Dismissione della VLAN di fallback e gestione dei casi residui.
- Evoluzione oltre PEAP-MS-CHAPv2 e NTLMv1 in ambiente Microsoft AD con passaggio a TEAP
- Riautenticazione periodica e durata della sessione.
- Coerenza del controllo degli accessi anche in IPv6 (DUID).
- Associazione MAC Address ad asset inventory, responsabilità e ciclo di vita dei dispositivi.
- Autenticazione basata su doppio controllo congiunto dell'Identità dell'utente e della postazione.
- Revisione dei raggruppamenti VLAN/VRF per ridurre le policy di traffico tra VRF o, nel caso opposto, per limitare l'accesso a VLAN specifiche.

Domande?

https://www.partici.fi

codice 83995288

Sono a disposizione nella pausa caffè

Informazioni, approfondimenti, contatti
andrea.sartori@univr.it

WORKSHOP GARR 2026
NET MAKERS