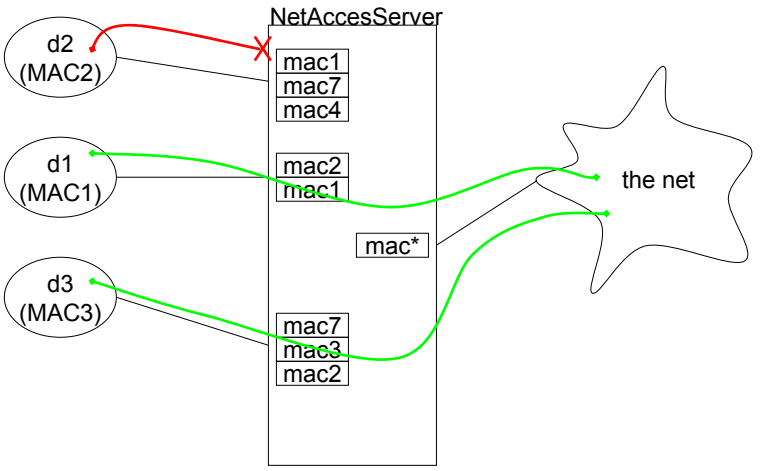
Gente in movimento

La mobilità degli utenti crea ancora difficoltà

- dhcp consente di poter configurare le macchine **1 volta in rete**
- Chiunque può connettere il proprio portatile alla rete
- Come regolamentare l'accesso alla rete?

1 prima soluzione:
Controllo dei mac address che gli apparati di rete possono accettare

Mac access list



ACL MAC:difetti

- Pensato per limitare utilizzo di una porta a poche macchine
- Layer 2 -> forte dipendenza dallo HW
- Non autorizza l'utente ma la macchina
- difficoltà di propagare a tutti gli NAS le ACL
- MAC spesso è alterabile

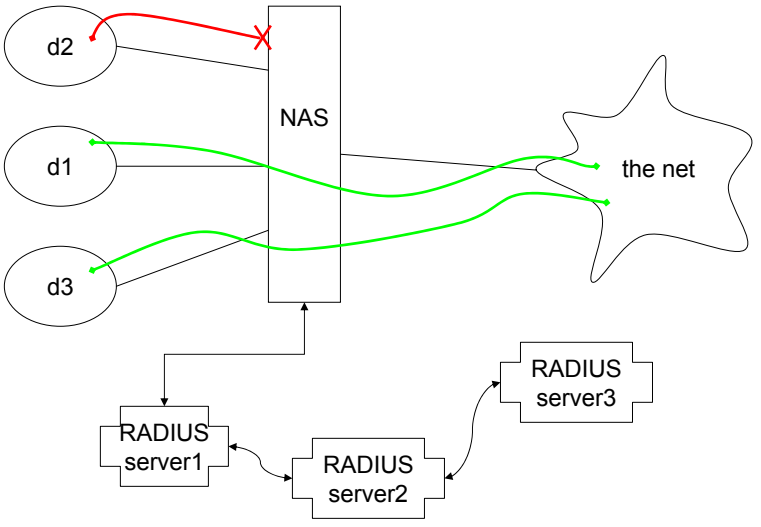
RADIUS

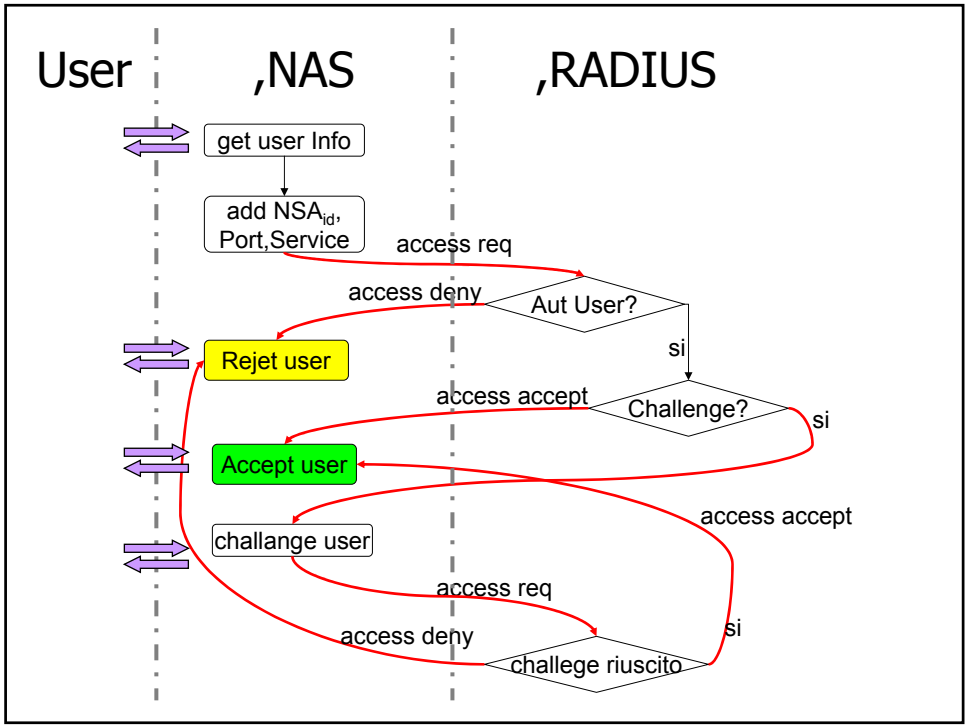
- Remote Authentication Dial In User Service
- Protocollo Layer 3 (UDP port 1812)
- Non autorizza la macchina ma l'utente ad usare la rete
- Traffico cifrato
- Autenticazione client/server tramite shared secret
- Più server (chi non sa tace)

Perché UDP?

- Portare a livello applicativo le ritrasmissioni
- Il protocollo è di natura stateless
- UDP consente di semplificare l'implementazione del server

Scenario Radius

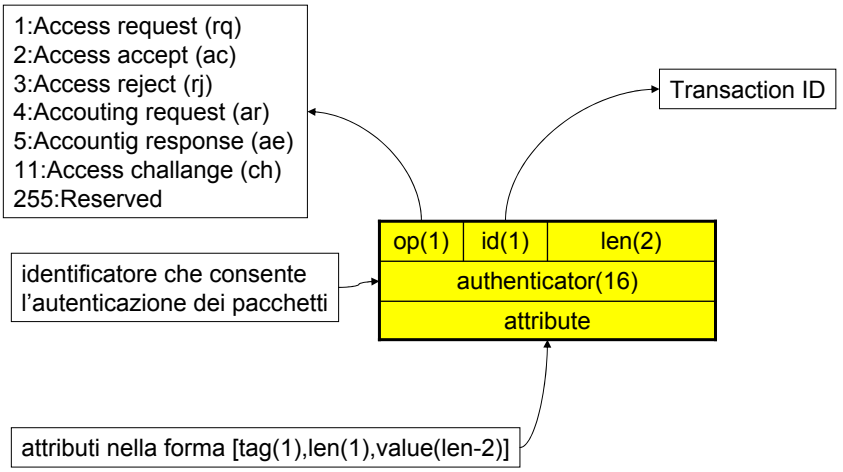




Collaborazione fra server

- Un server prima di dare una risposta può contattare altri server
- Un server diventa dunque client di un altro
- Autenticazione con Shared secret
- Ad ogni passaggio il pacchetto viene decifrato e ricifrato
- Non esiste loop detection
- Meccanismo che consente il roaming
- Ogni server decide se fare il forward oppure no

Formato dei pacchetti



Attributi

tag	nome	significato
1	username	user name (rq)
2	user-password	user password (rq)
5	NAS-port	port used by user (rq)
6	service-type	service req by user (rq,ac) login: connetion to host framed: user use a framed protocol admin: admin the NAS auth: authentication only callback: user want be called back

Attributi

tag	nome	significato
7	frame protocol	Frame protocol (rq,ac): ppp, slip,AppleRAP,etc
8	frame-ip	ip for the user (rq,ac)
9	frame-netmask	netmask for user (rq,ac)
14	ip-login-host	host to connect the user to login (rc,ac)
15	login-service	login service (ac): rlogin,telnet,etc
17	Reply-msg	wellcome msg to user (ac)

Attributi

tag	nome	significato
26	vendor-specific	vendor specific extension
27	session-timeout	len of the session (ac,ch)
28	idle-timeout	idle timeout (rq,ac)
14	ip-login-host	host to connect the user to login (rc,ac)
61	Nas-Port-Type	Type of port used by user: ISDN,ADSL,802.11,etc
17	Reply-msg	wellcome msg to user (ac)

Account

- Possibilità di gestire l'accounting degli utenti in modo centralizzato
- Accouting request: client passa al server i dati
- Accountig respons: il server conferma memorizzazione
- Se il server non memorizza NON risponde nulla
- I messaggi sono codificati come attributi (40-51)
- Nei pacchetti di accuting si possono usare la maggior parte degli attributi. Di interesse:
- username
- NAS-Port
- NAS-Port-Type

Attributi per accountig

tag	nome	significato
40	acc-type	tipo di messaggio: 1: start account 2: stop account
42	Acc-input-octect	Byte inviati dallo user (ar+acc stop)
43	Acc-output-octet	Byte ricevuti dallo user (ar+acc stop)
44	Acc-session-id	Id per facilitare le cose
46	Acc-session-time	Durata sessione in sec. (ar+acc stop)
49	Acc-term-cause	tipo di fine sessione (User req, session timeout,admin reset, NAS err, user err,Port Preempted,etc)