Accesso wireless (e wired): autenticazione Layer 3 e soluzione mista

Mirko Corosu

per il gruppo

TRIP

Obiettivo

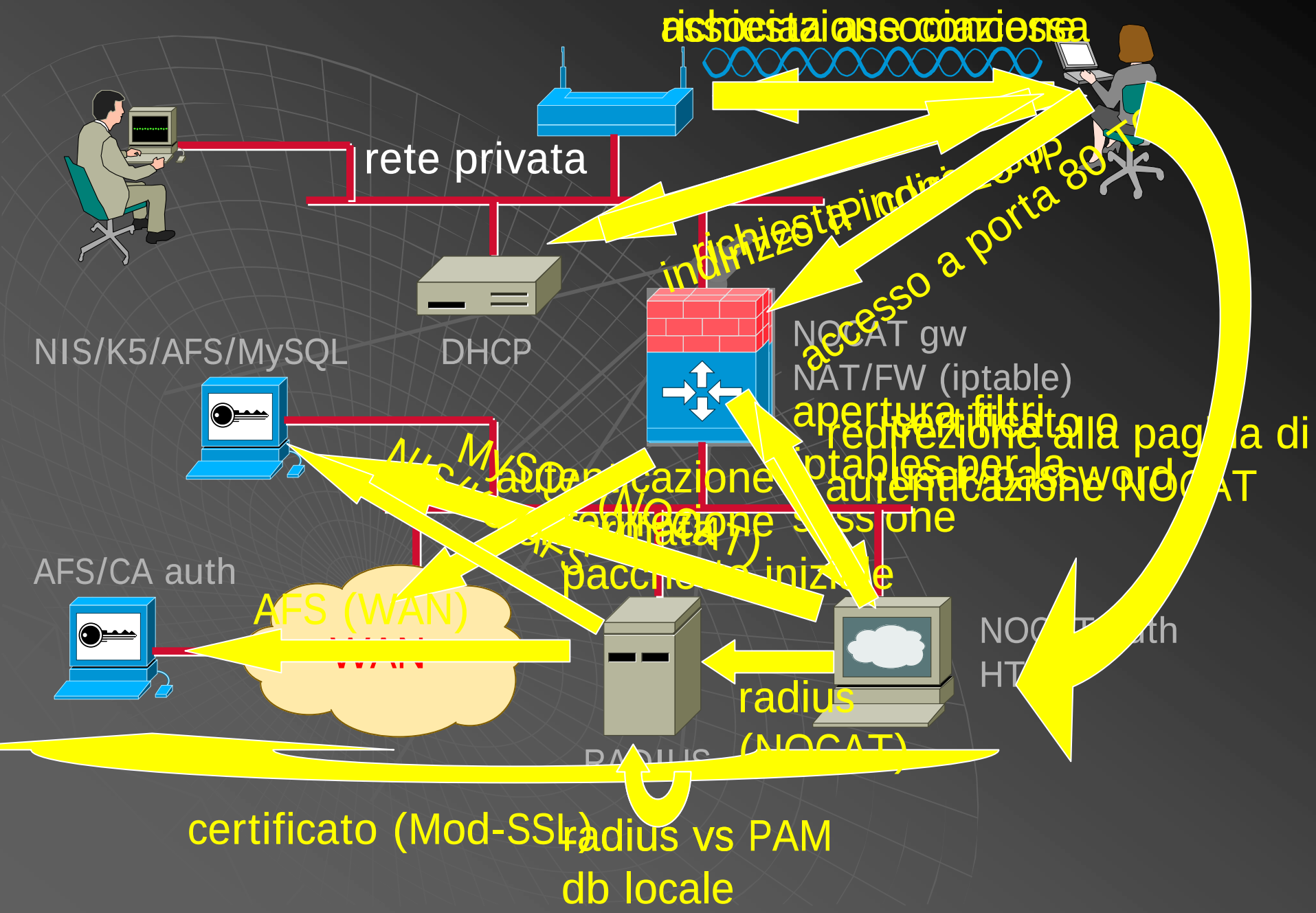
Creare una infrastruttura di accesso wireless layer 3 con caratteristiche:

- autorizzazione/autenticazione
- flessibilita’ (diversi meccanismi di autenticazione)
- fruibilita’ (indipendenza da OS/HW)
- differenziazione accessi
- minimo management a regime
- sicurezza

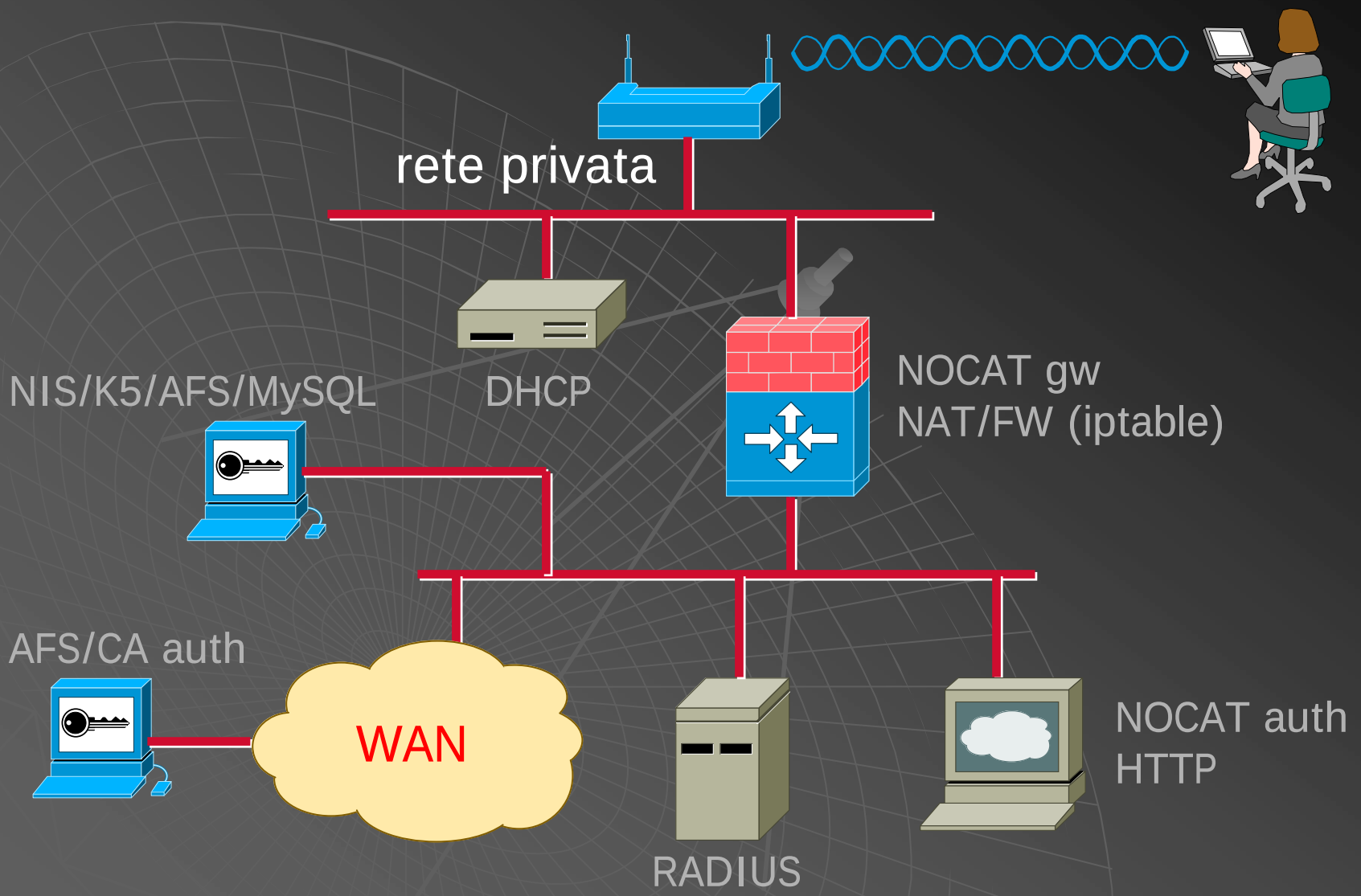
Componenti software

- NOCAT: implementazione di captive portal per reti wireless e wired
- Freeradius: implementazione server di autenticazione ed autorizzazione con protocollo radius
- Apache + mod-SSL: web server con trattamento certificati X.509

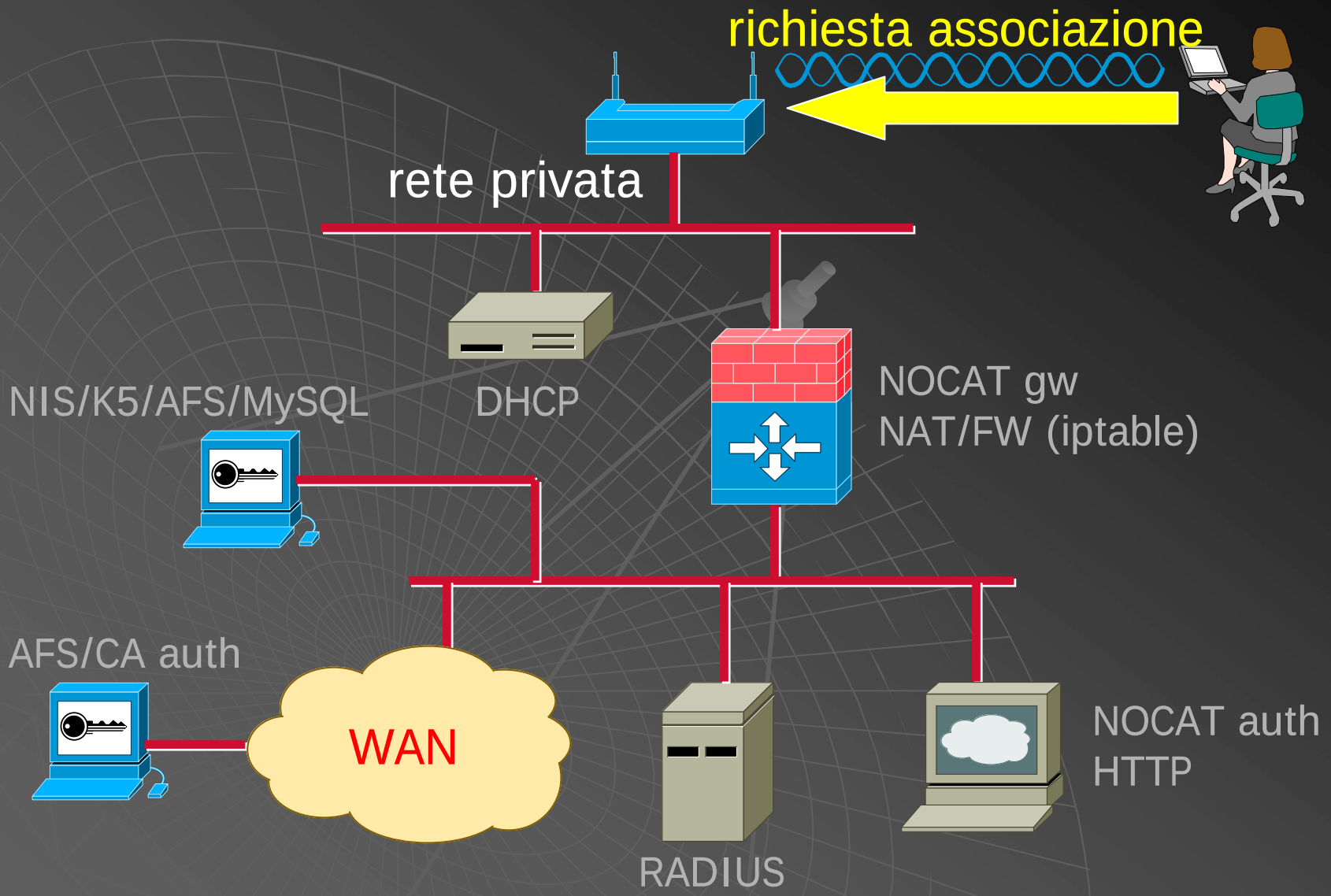
Autenticazione della sessione



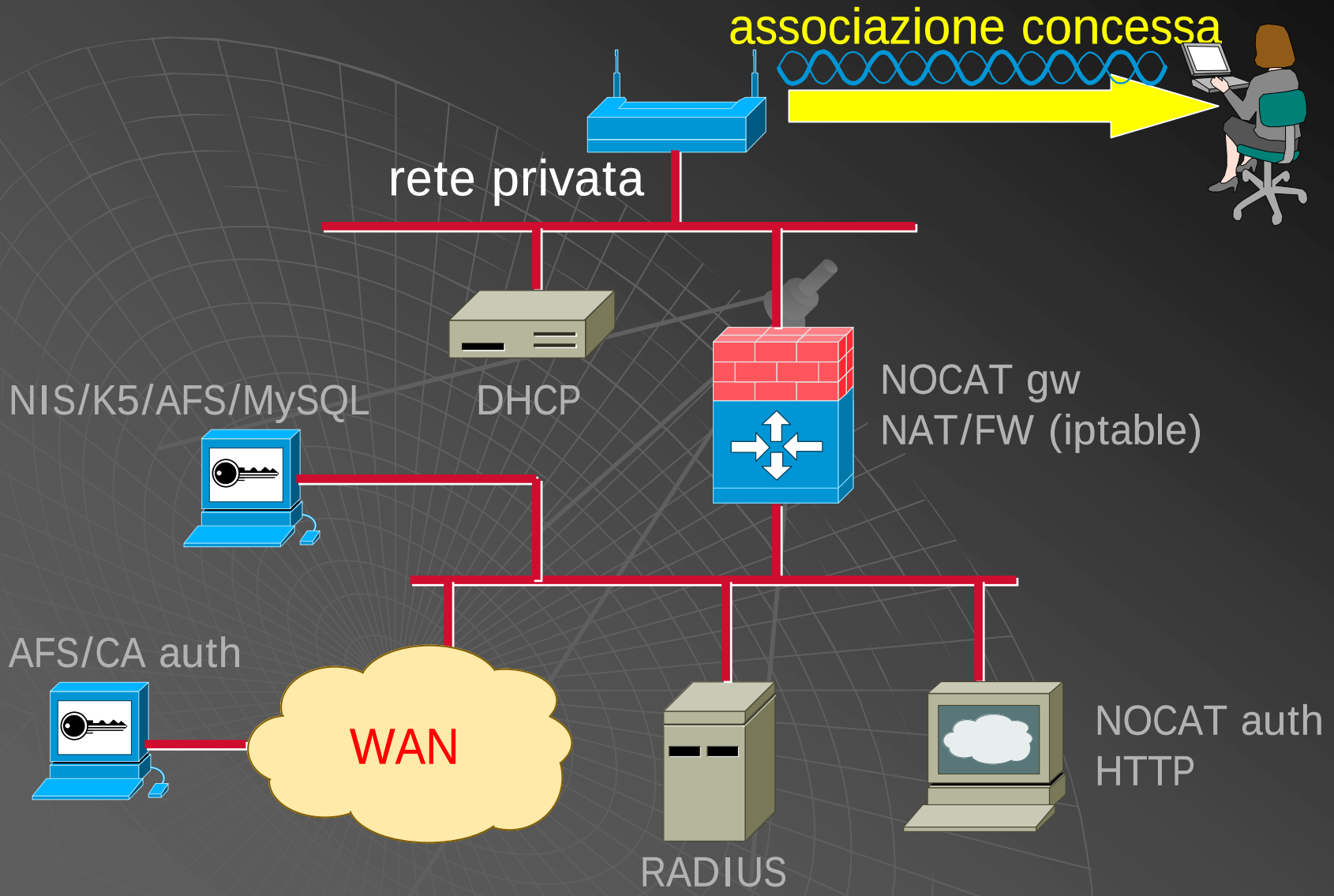
Autenticazione della sessione



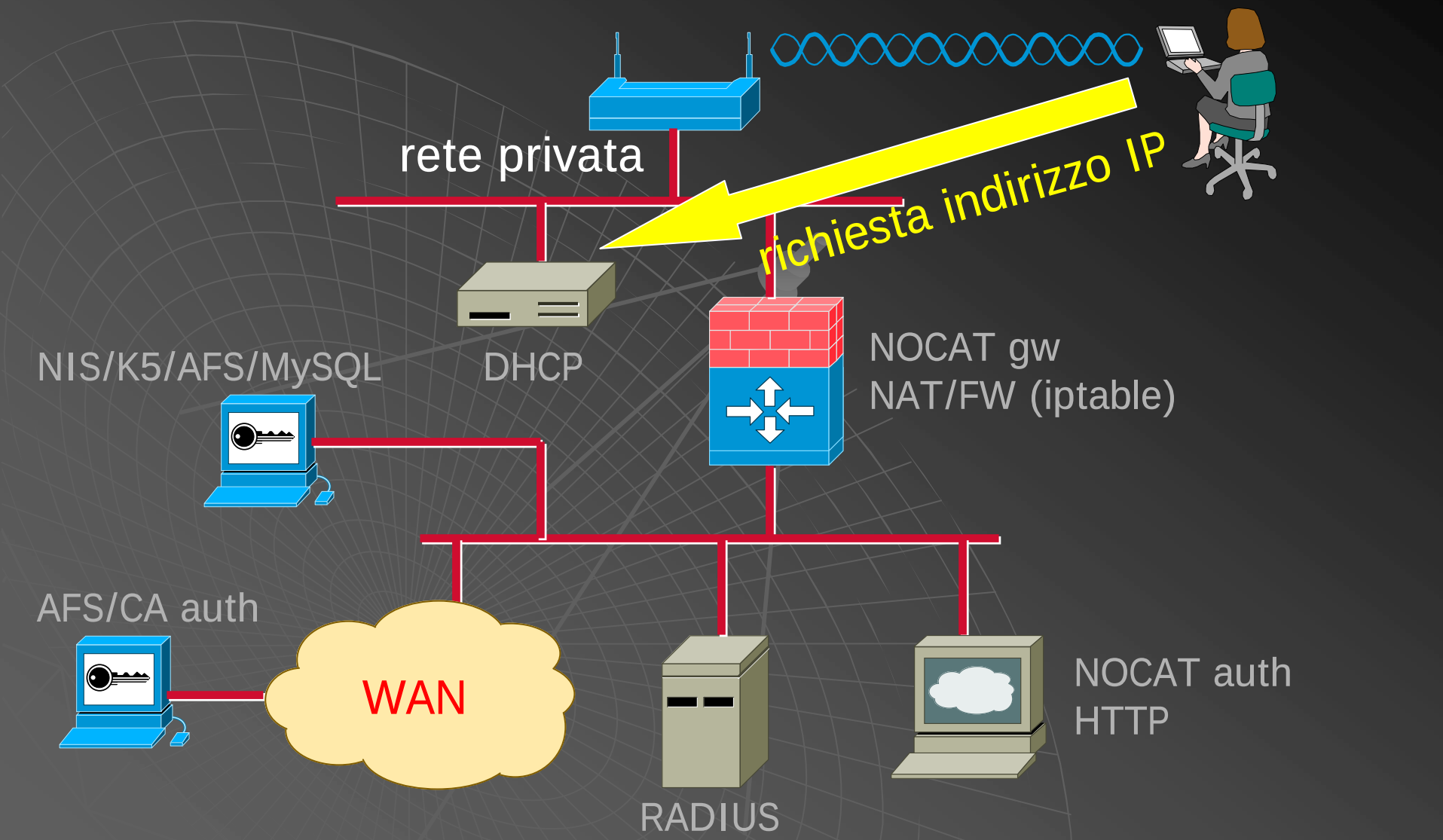
Autenticazione della sessione



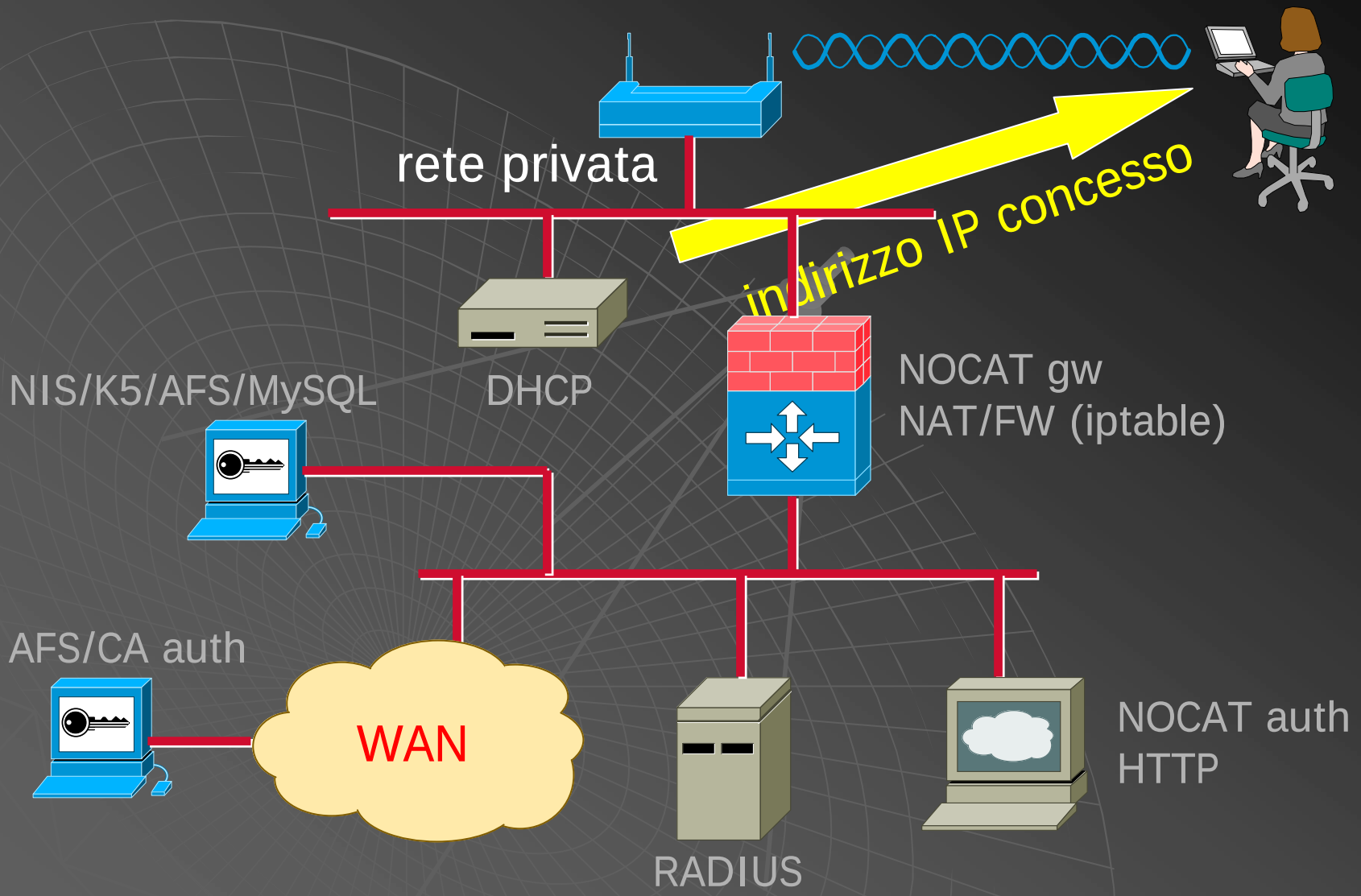
Autenticazione della sessione



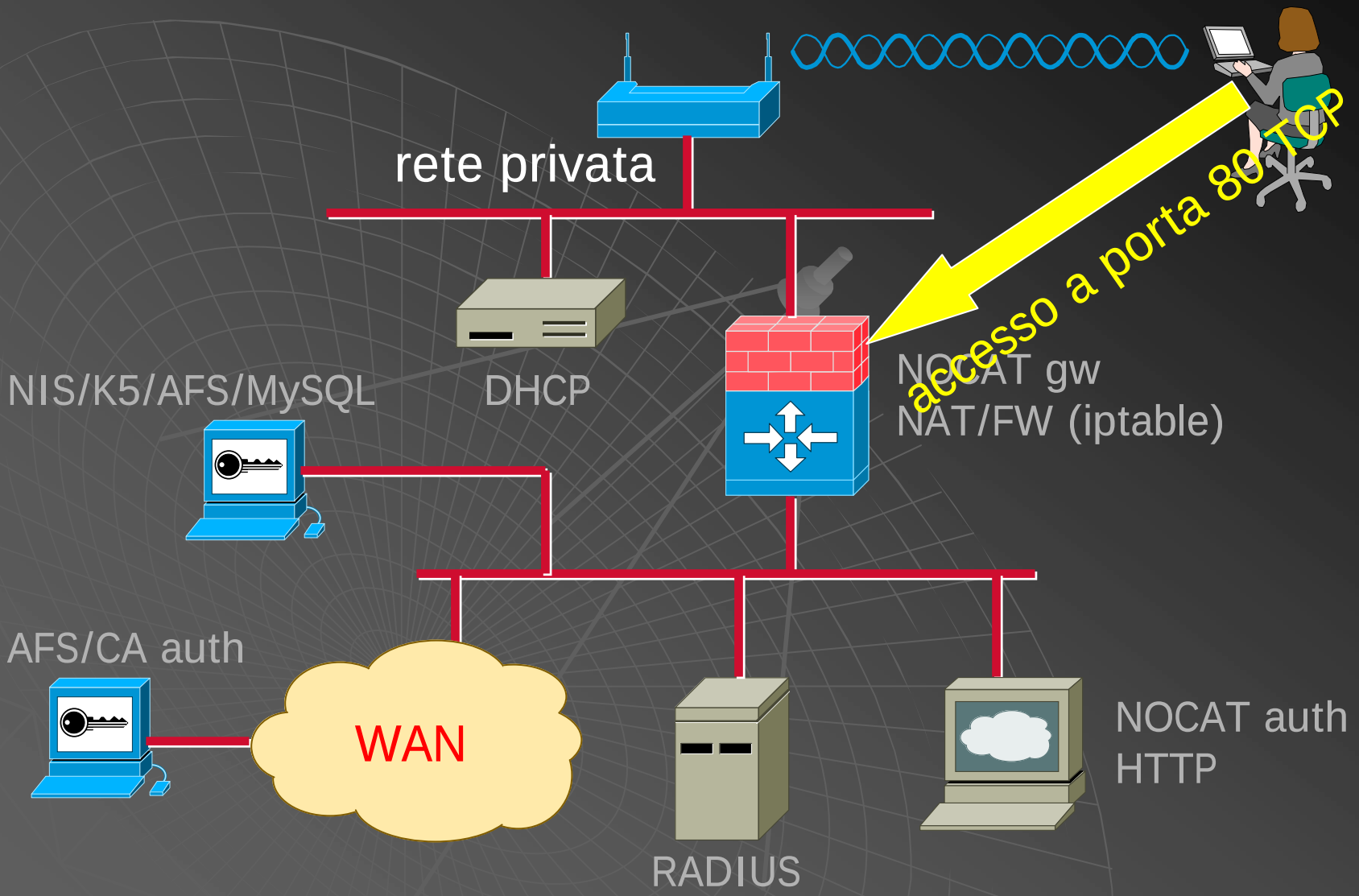
Autenticazione della sessione



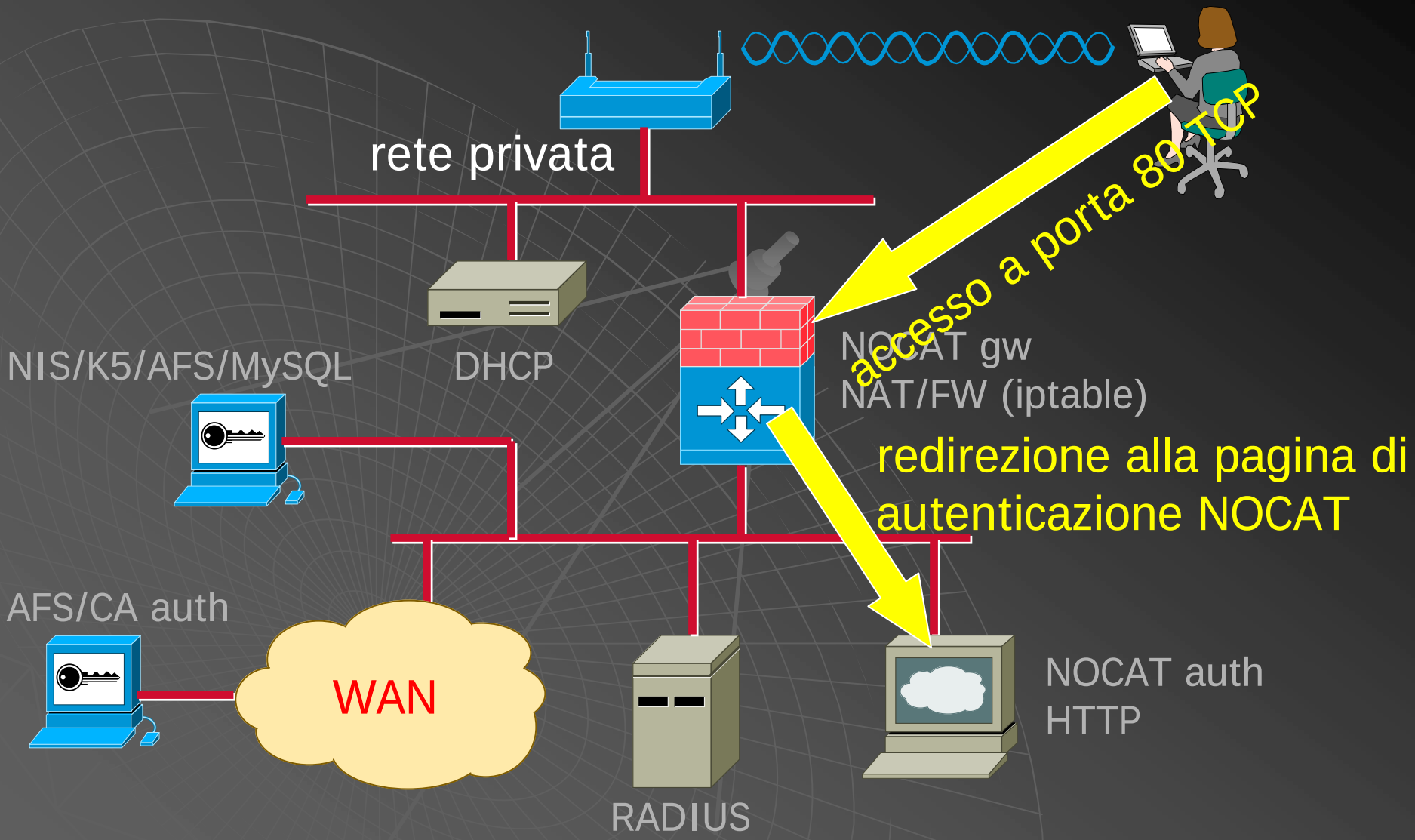
Autenticazione della sessione



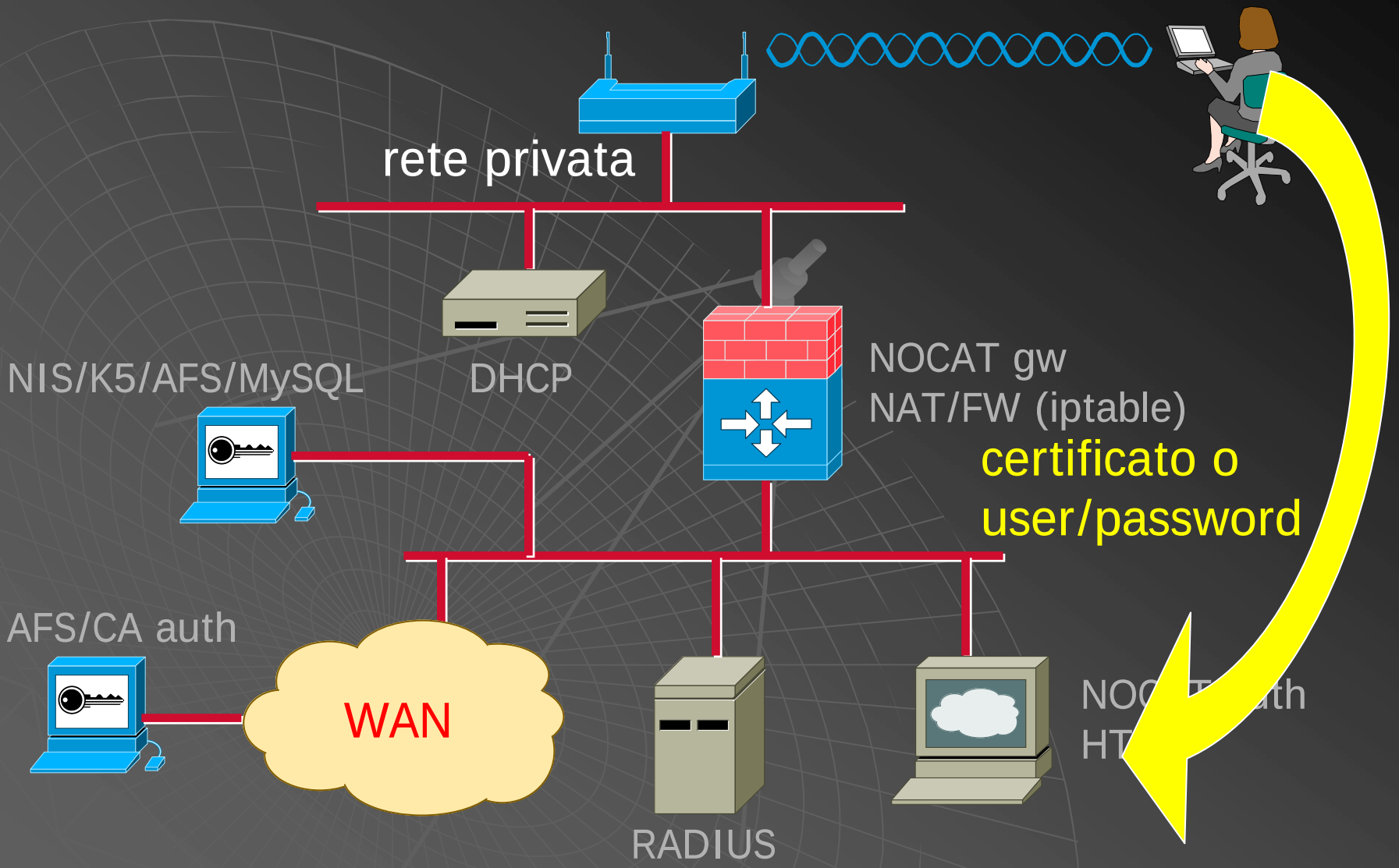
Autenticazione della sessione



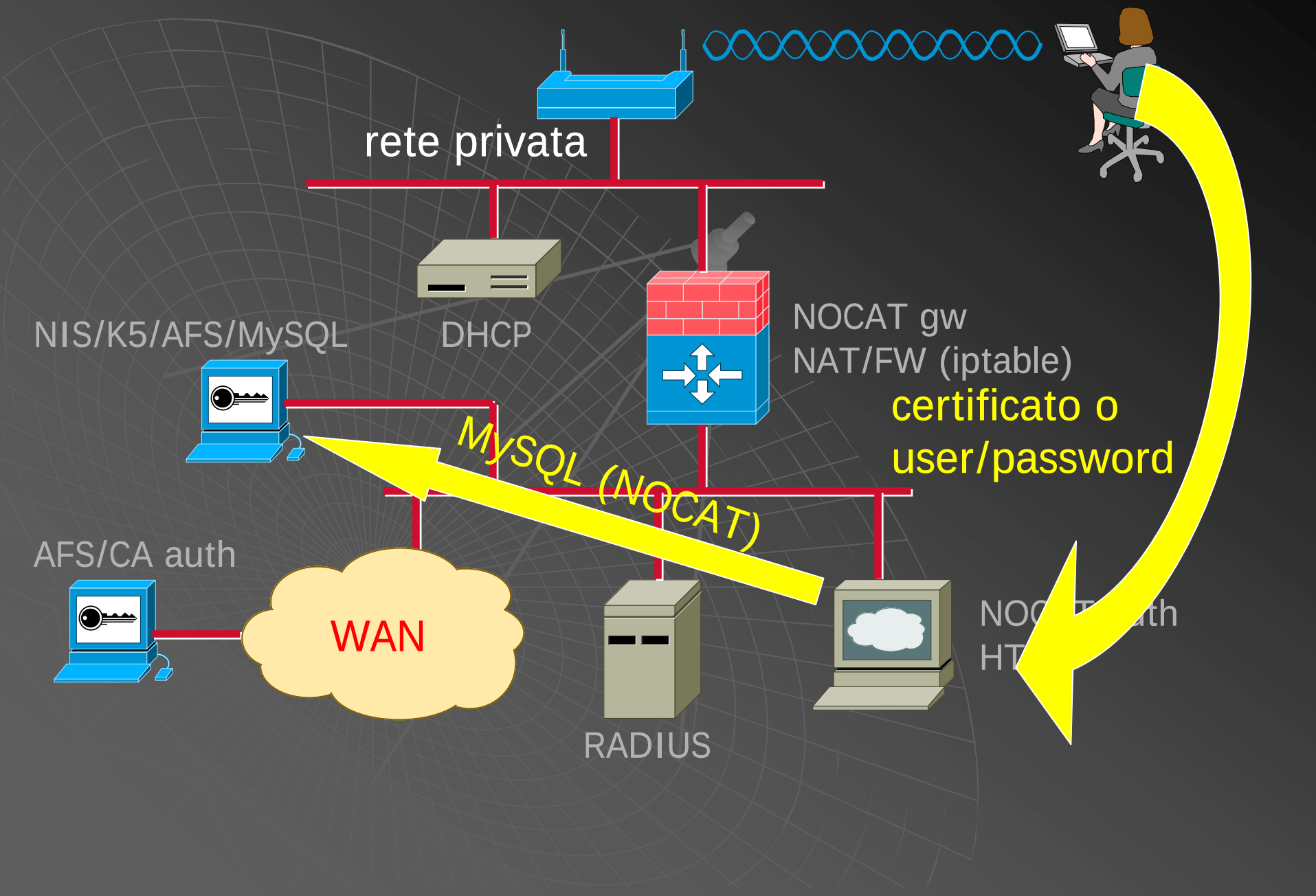
Autenticazione della sessione



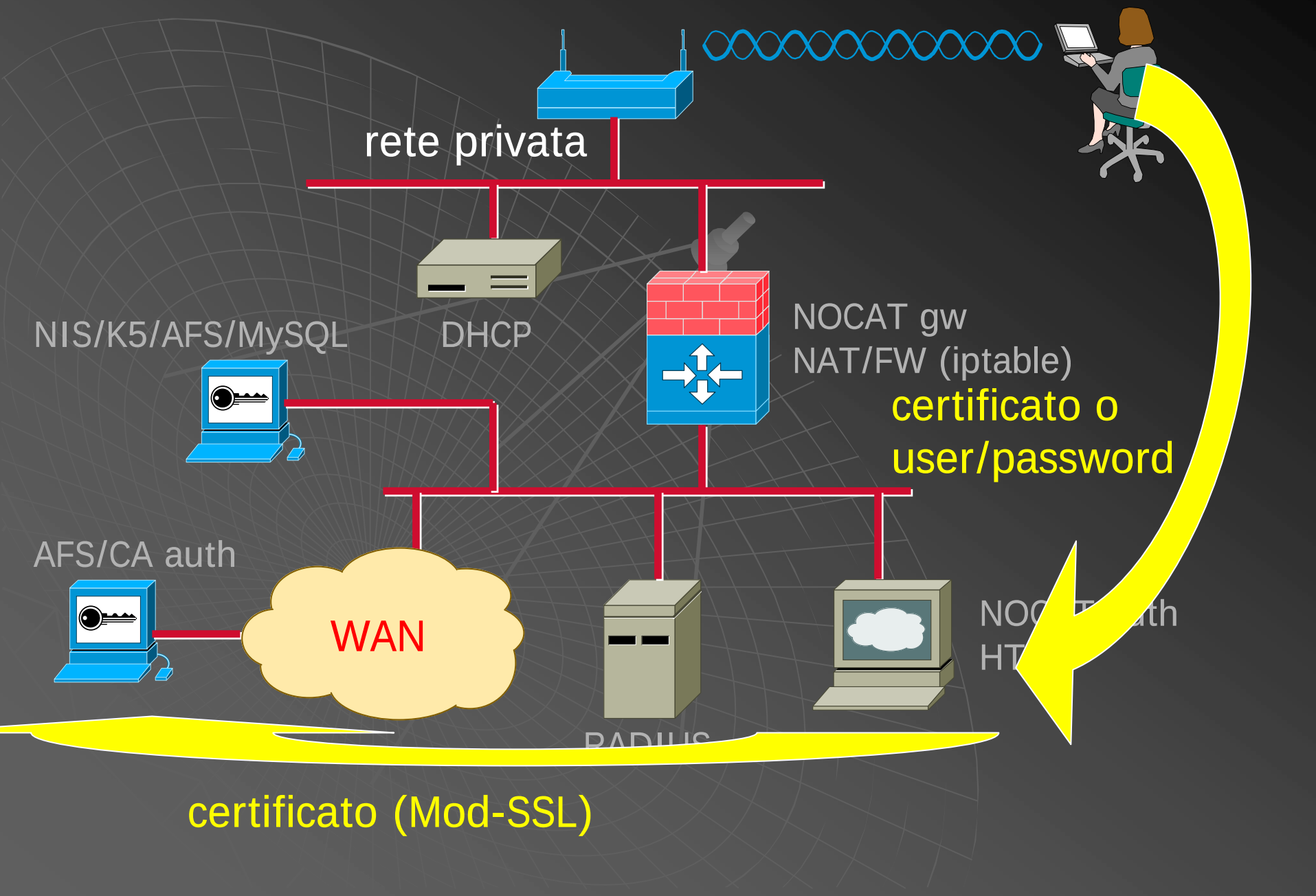
Autenticazione della sessione



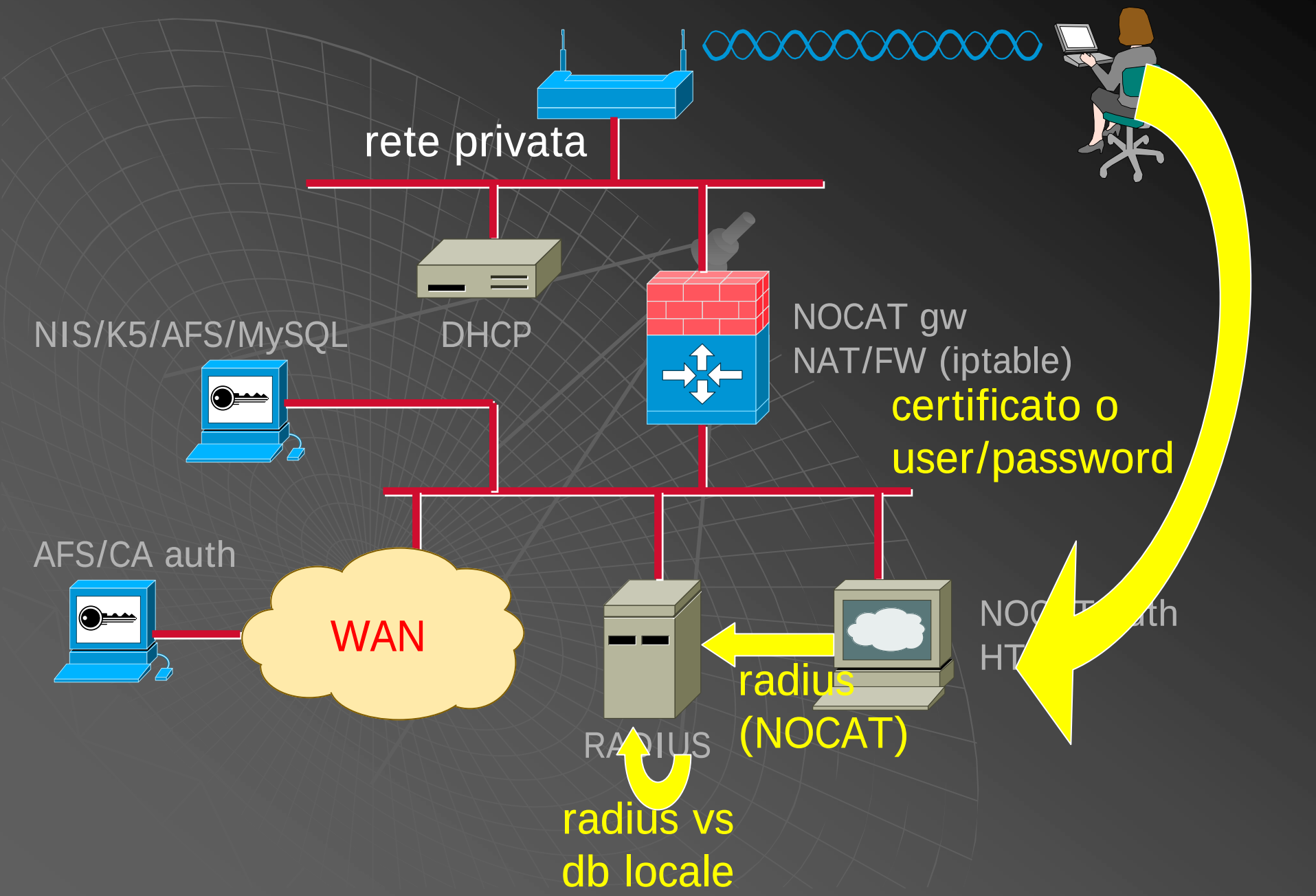
Autenticazione della sessione



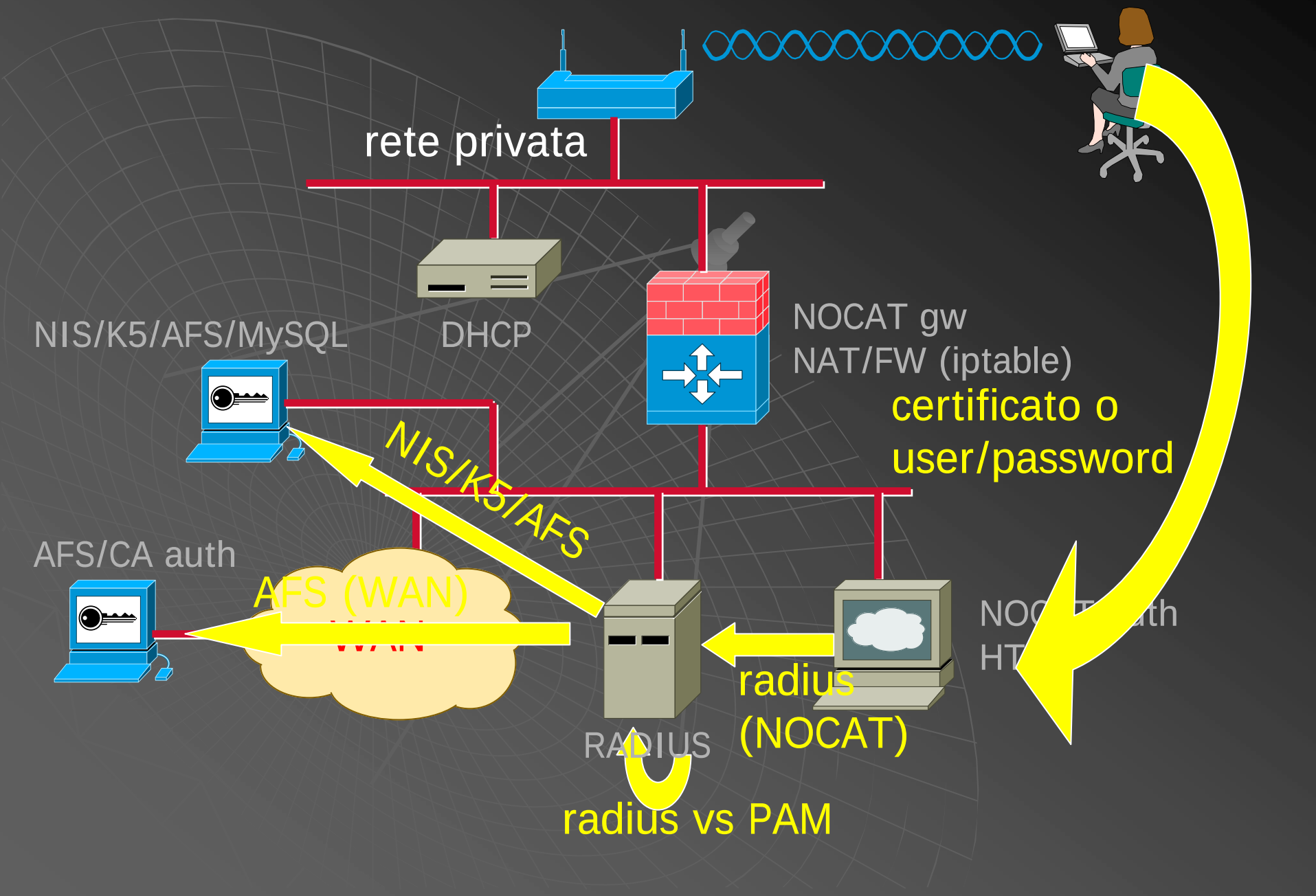
Autenticazione della sessione



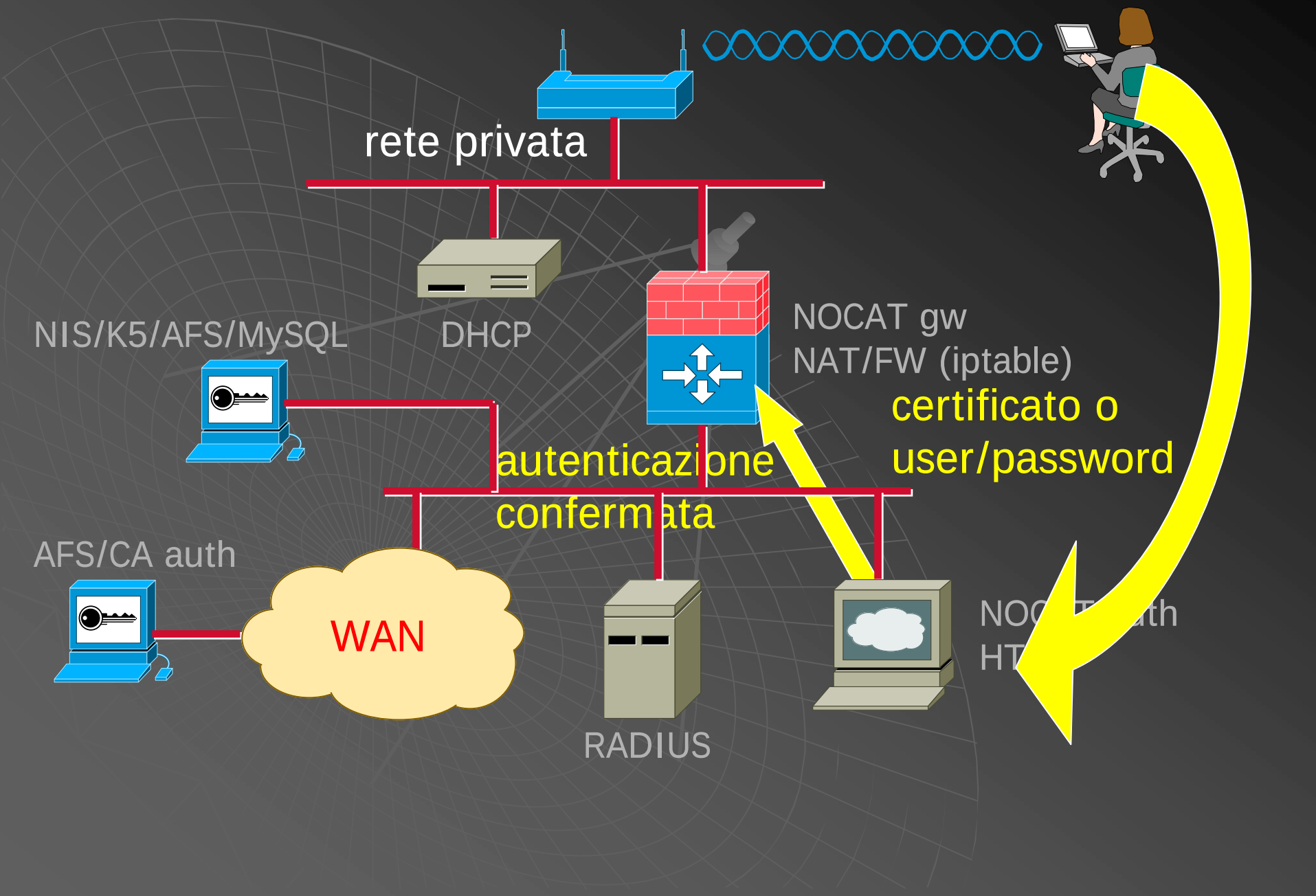
Autenticazione della sessione



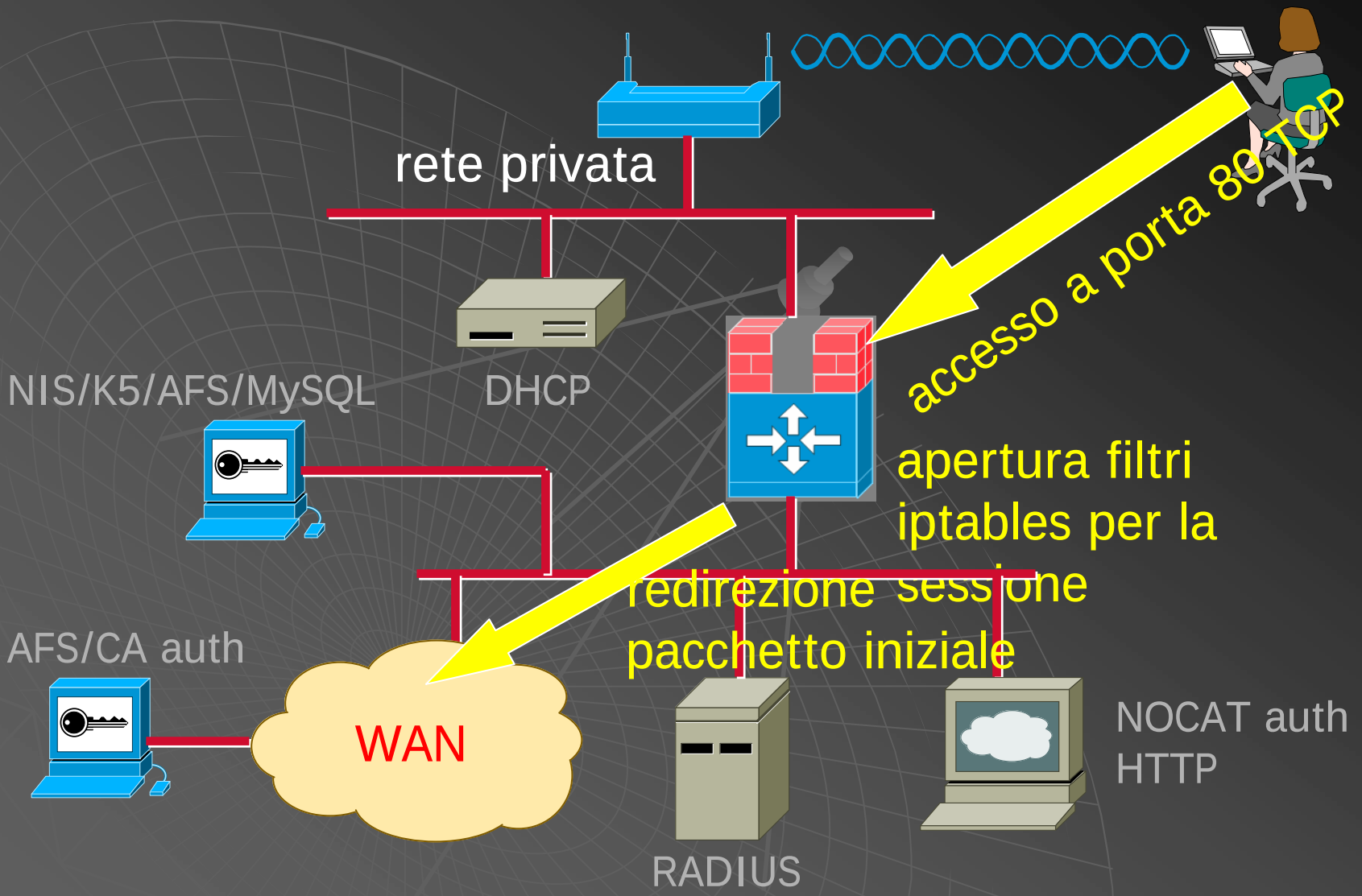
Autenticazione della sessione



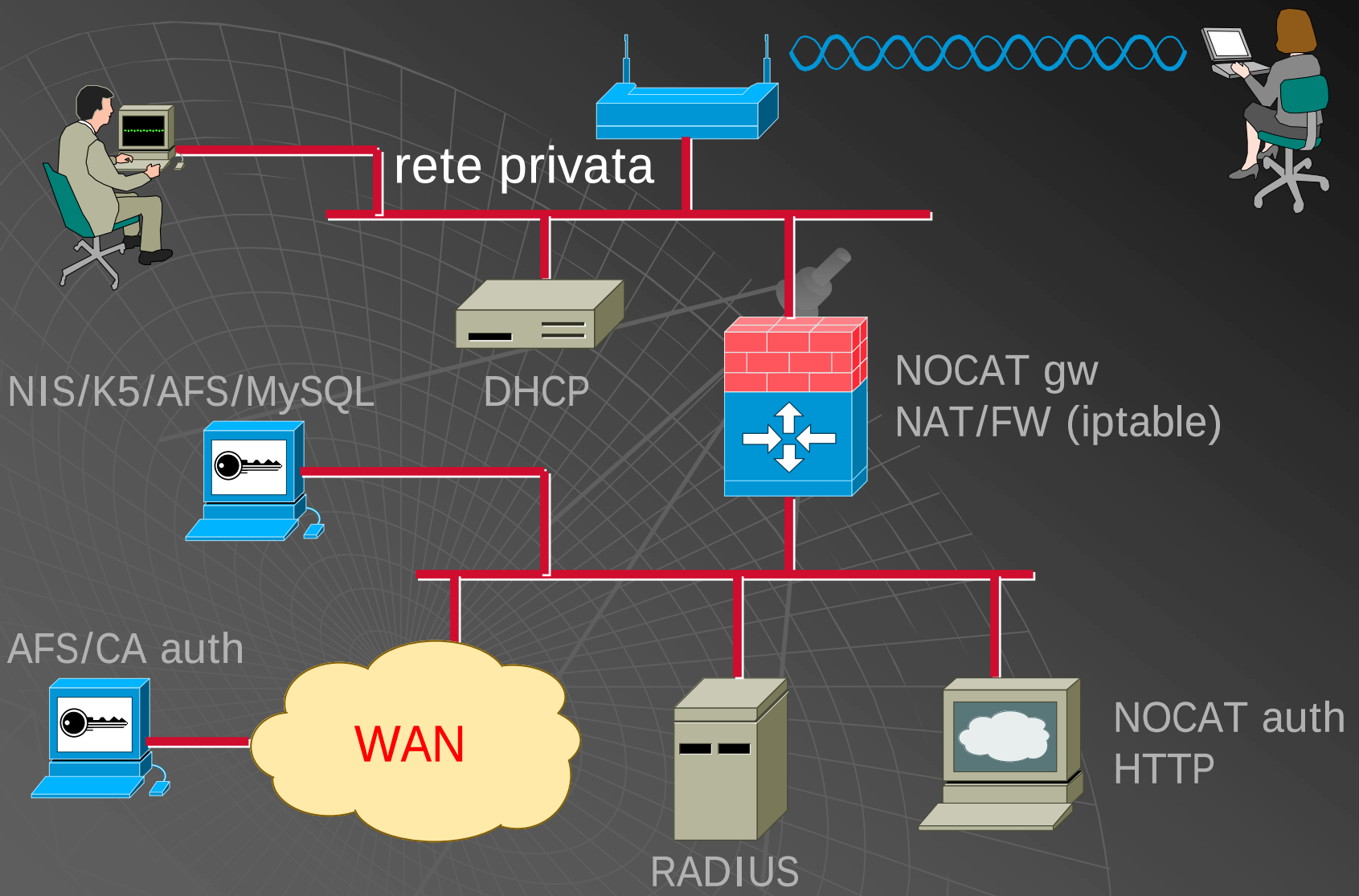
Autenticazione della sessione



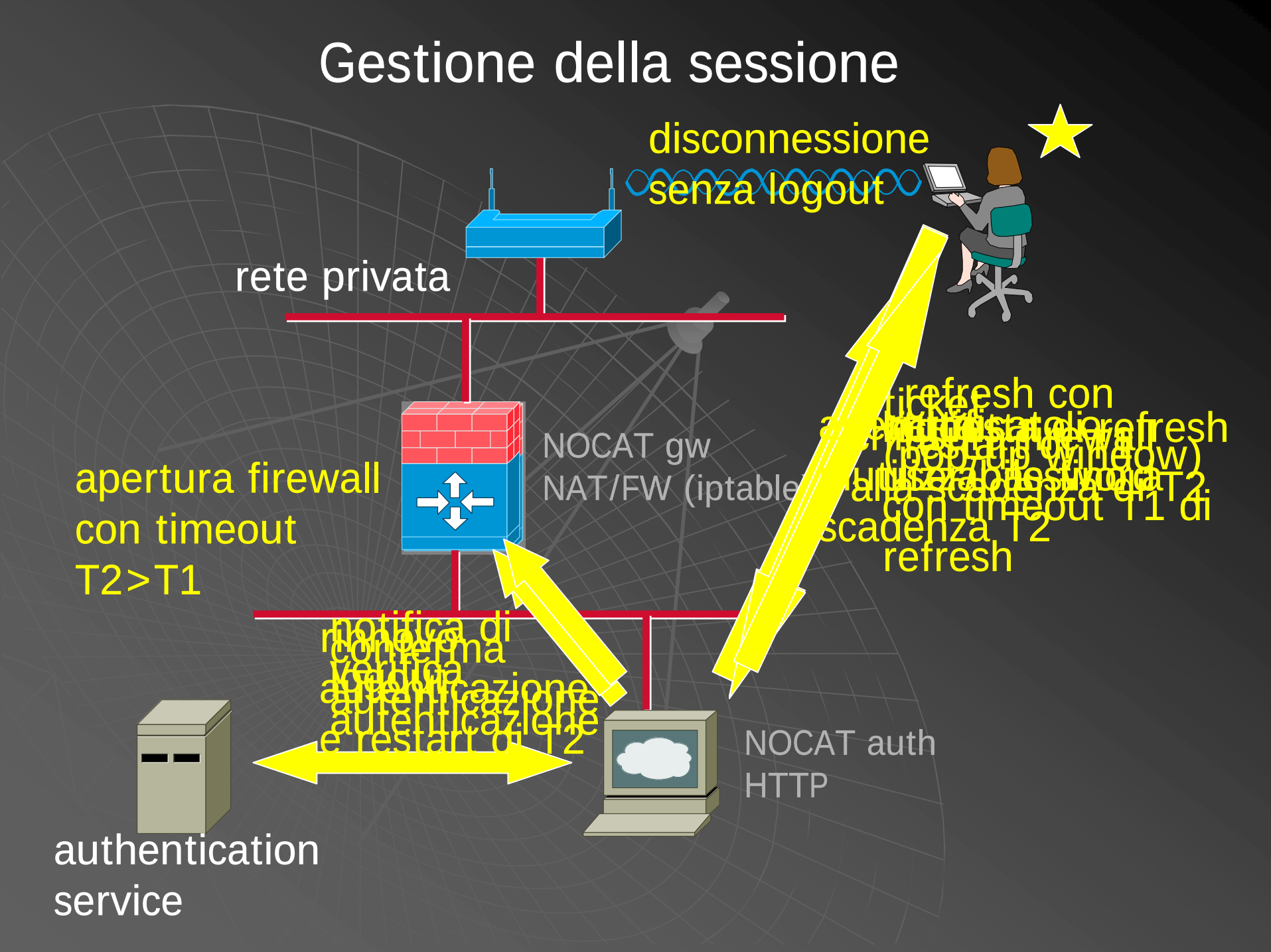
Autenticazione della sessione



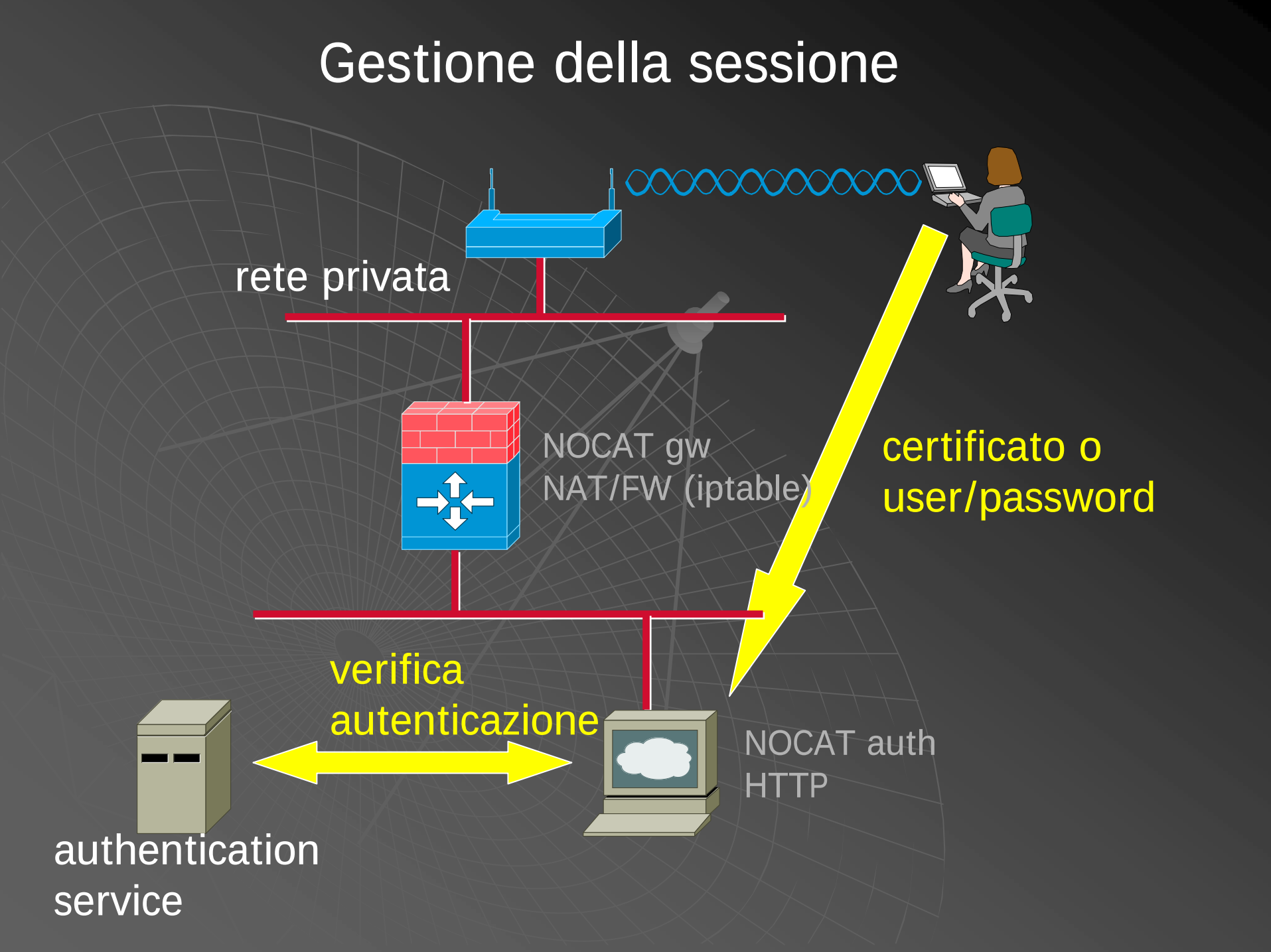
Autenticazione della sessione



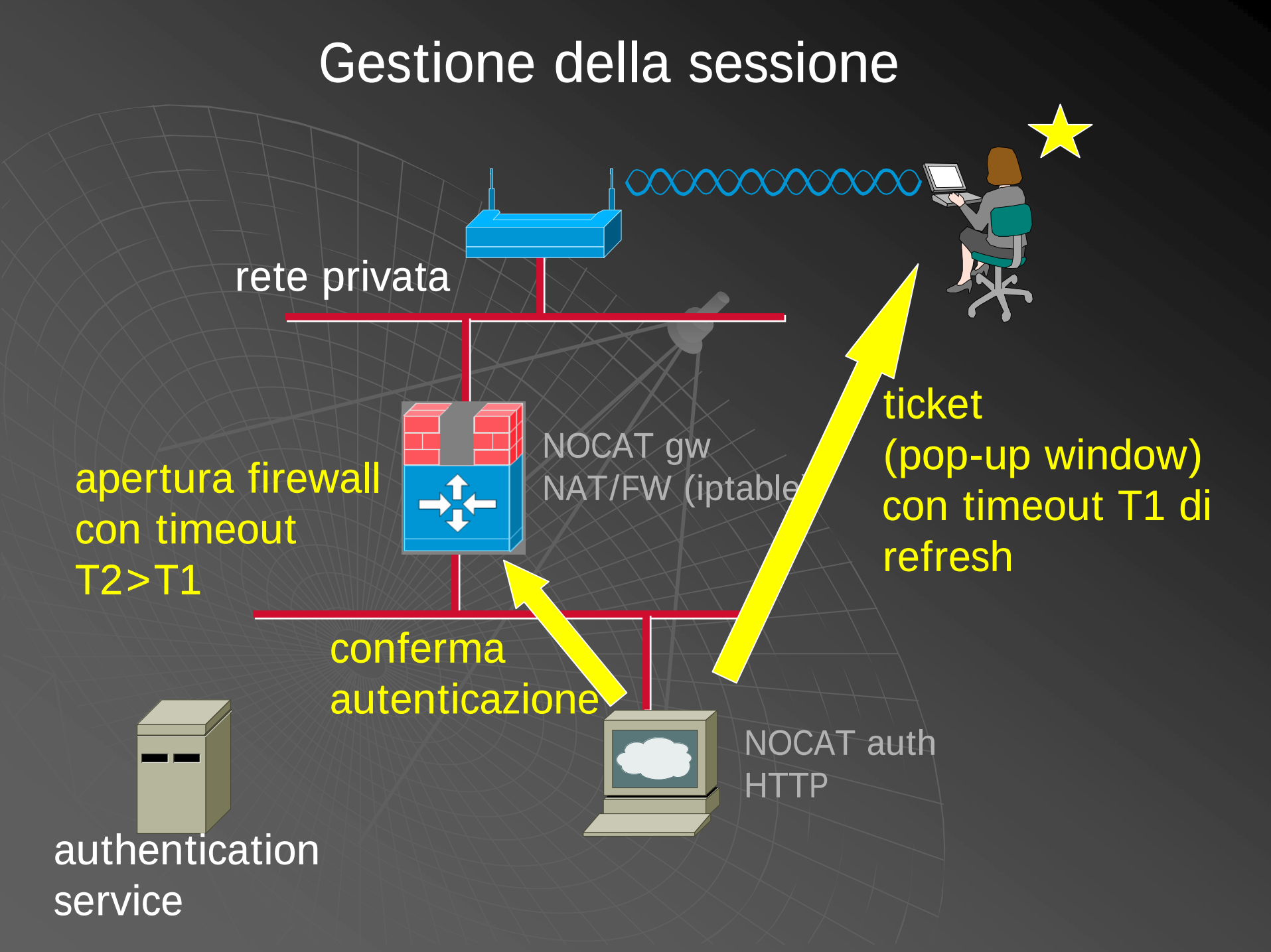
Gestione della sessione



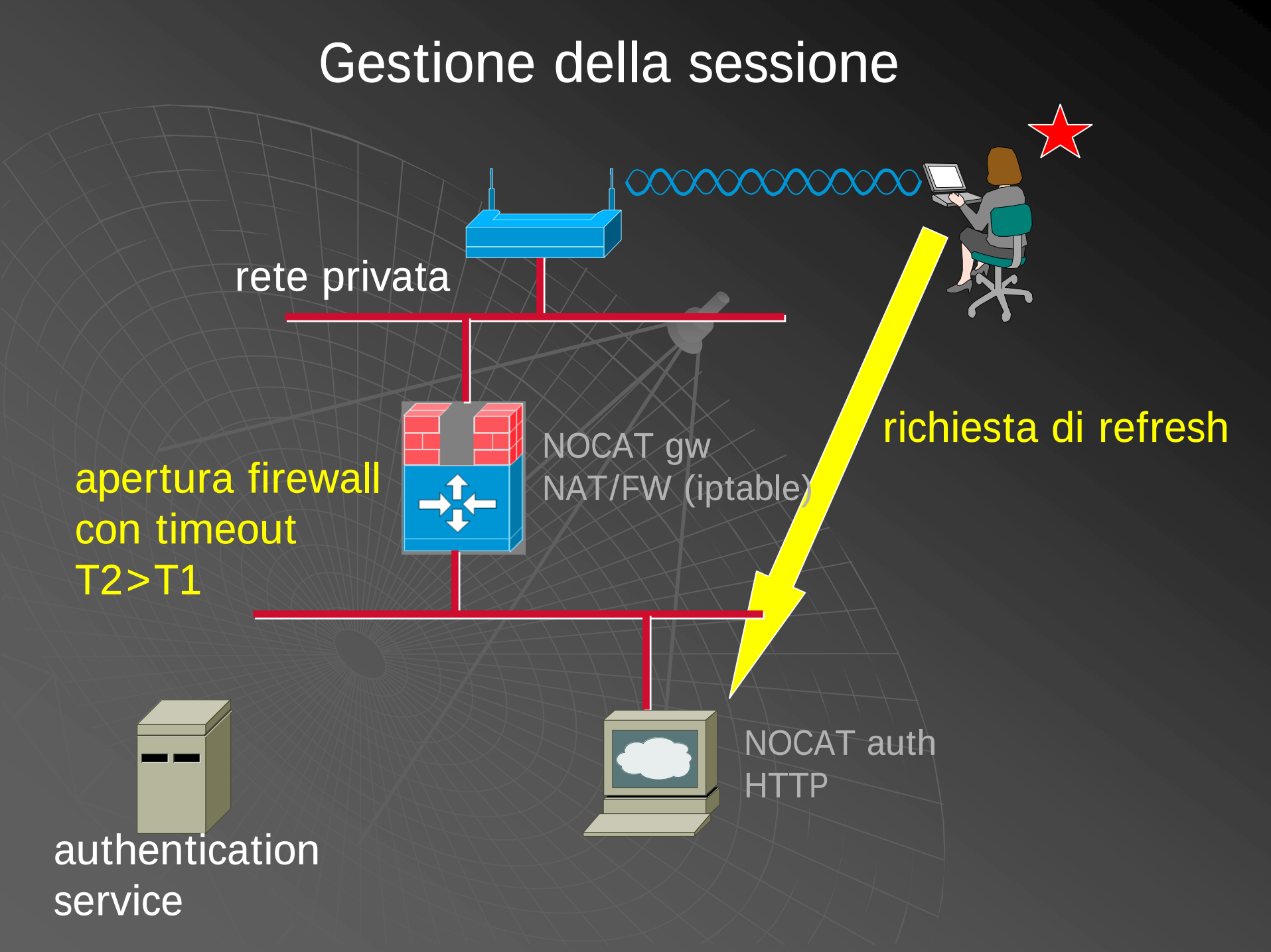
Gestione della sessione



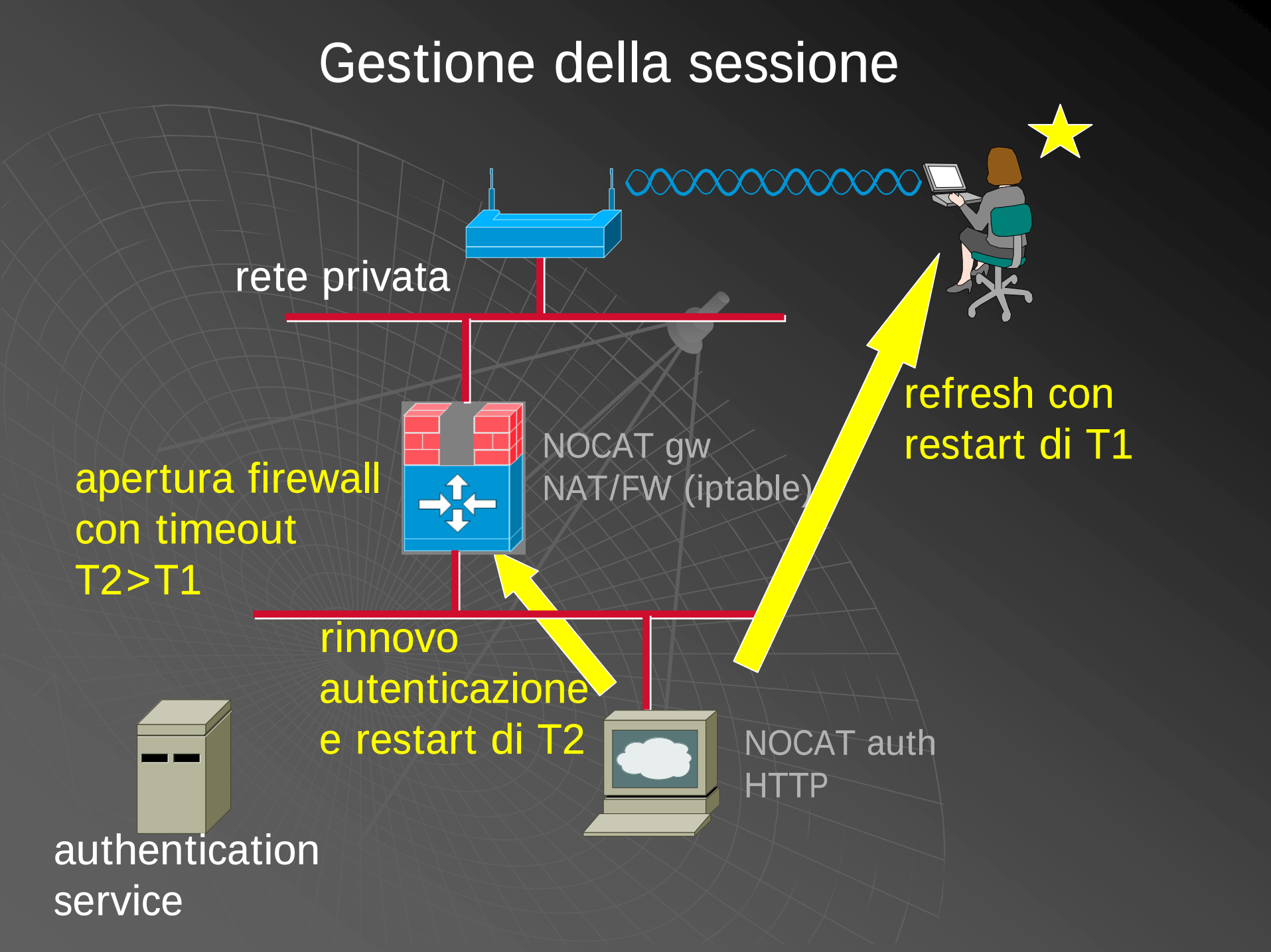
Gestione della sessione



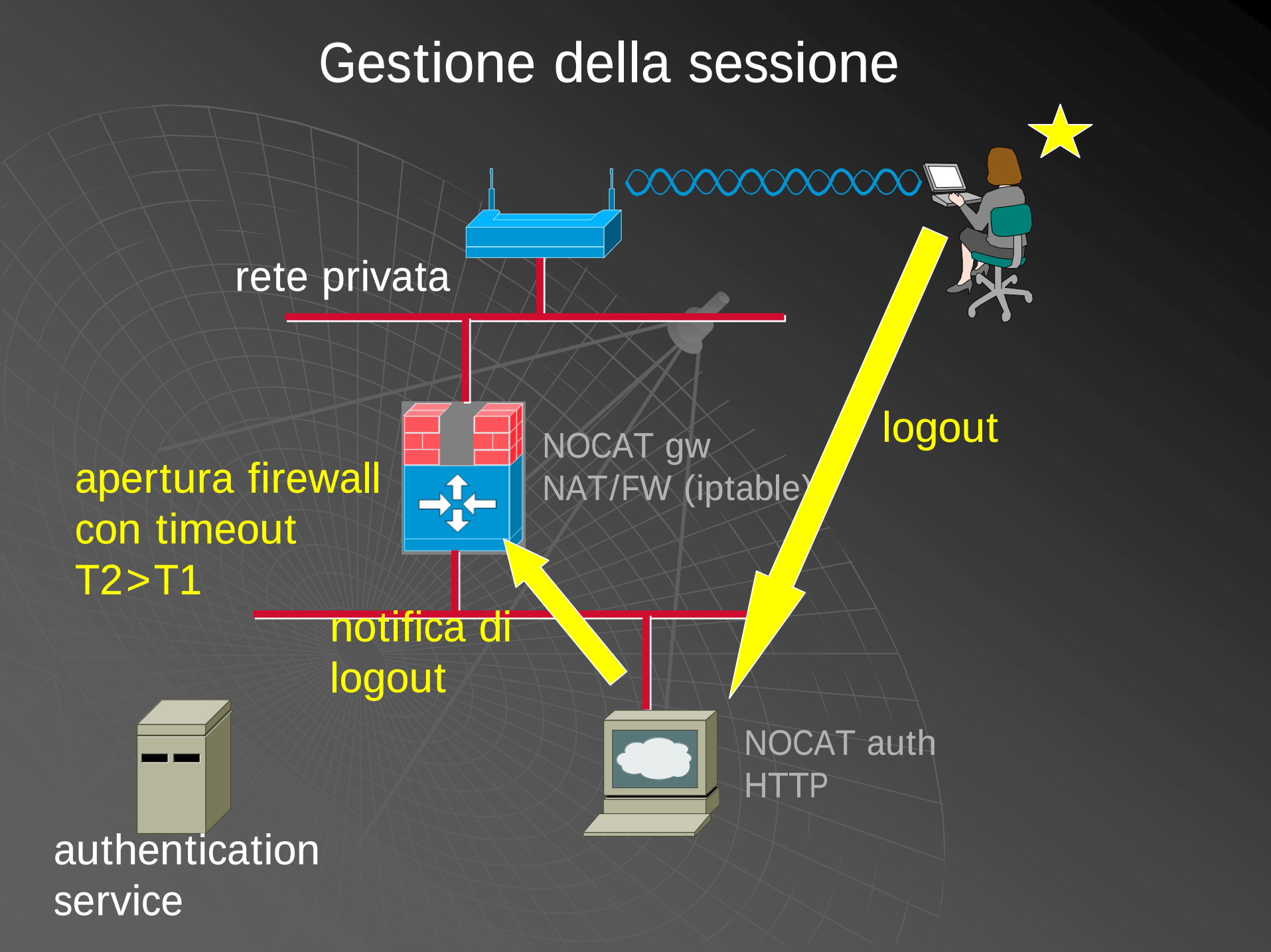
Gestione della sessione



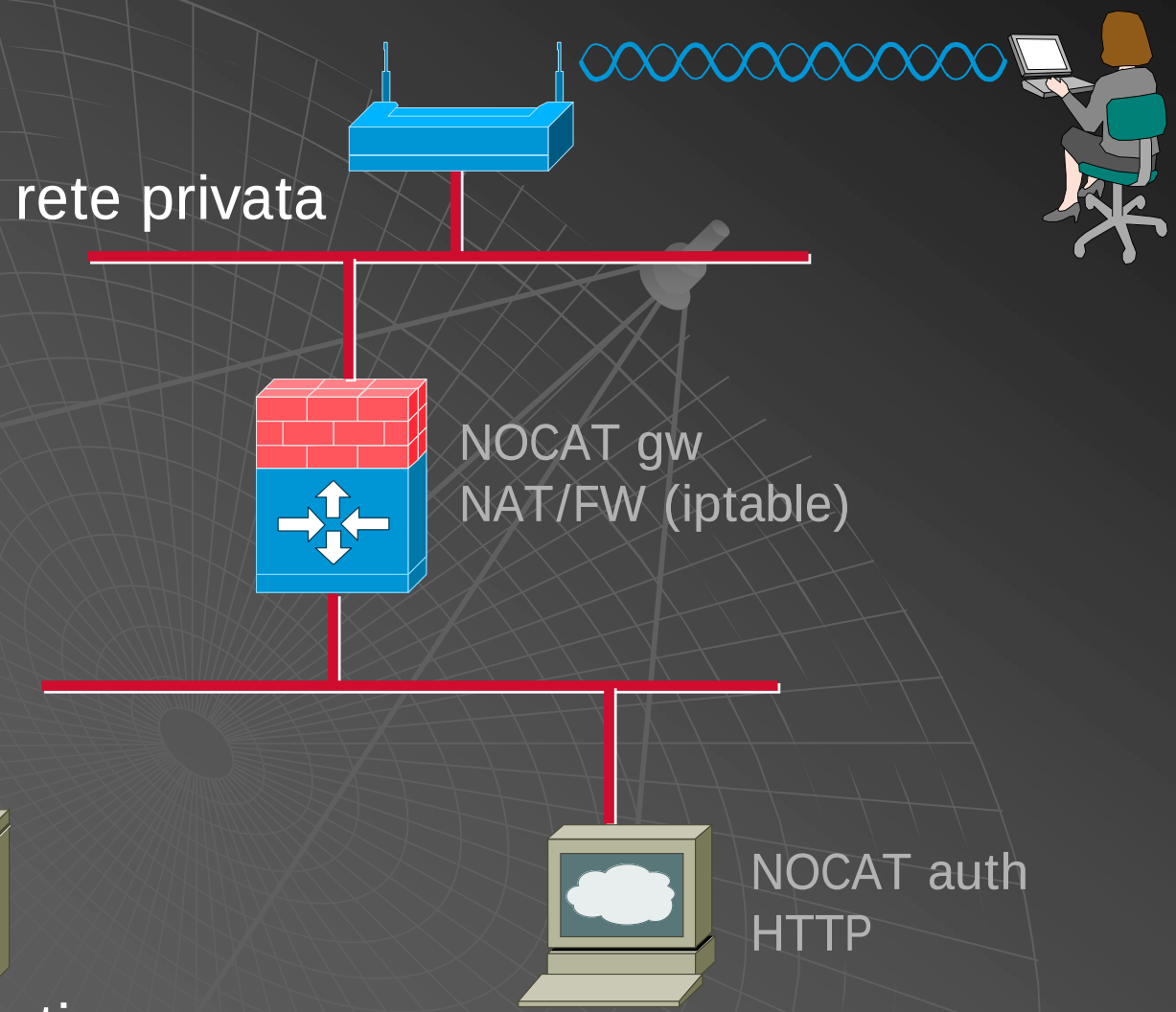
Gestione della sessione



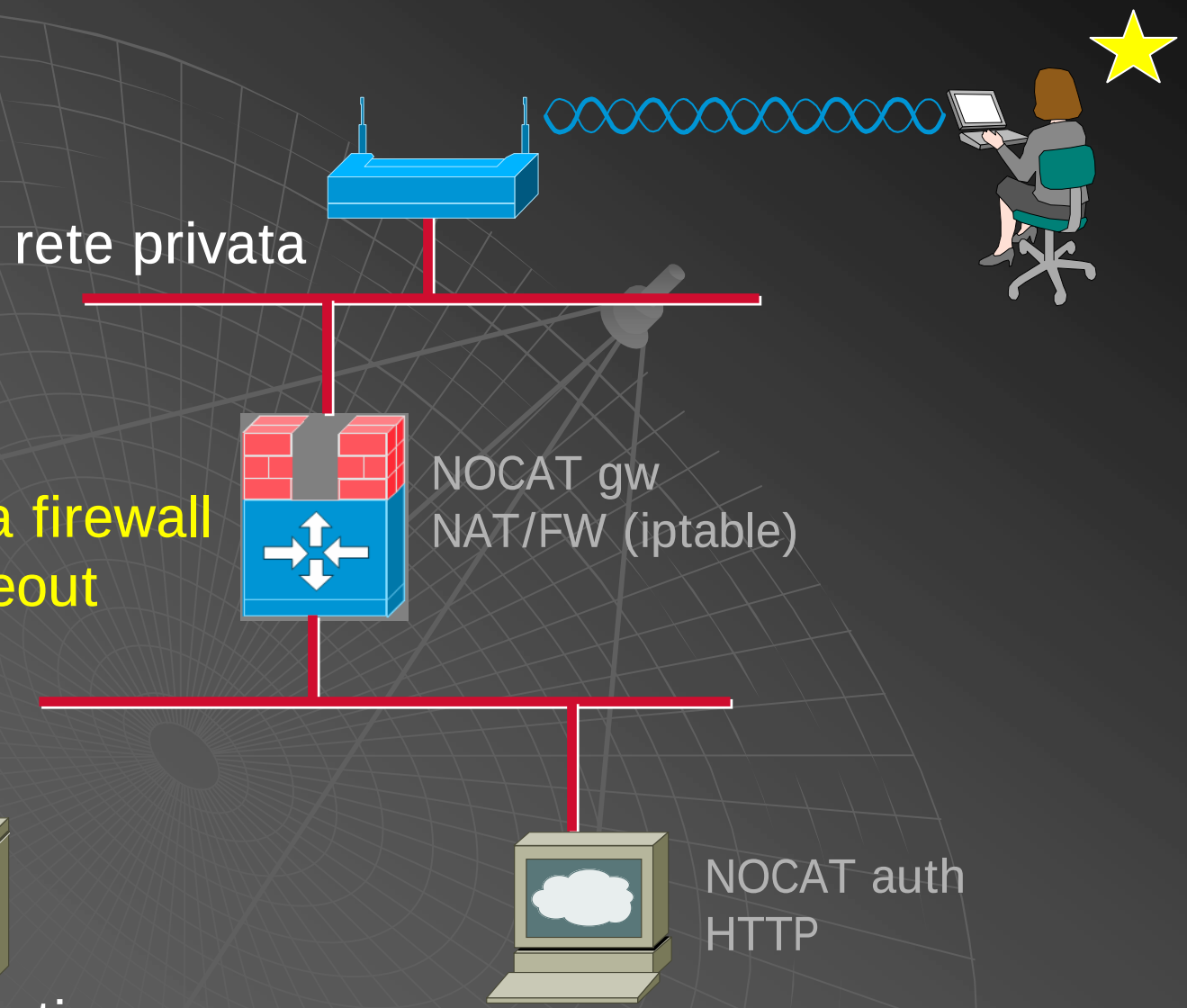
Gestione della sessione



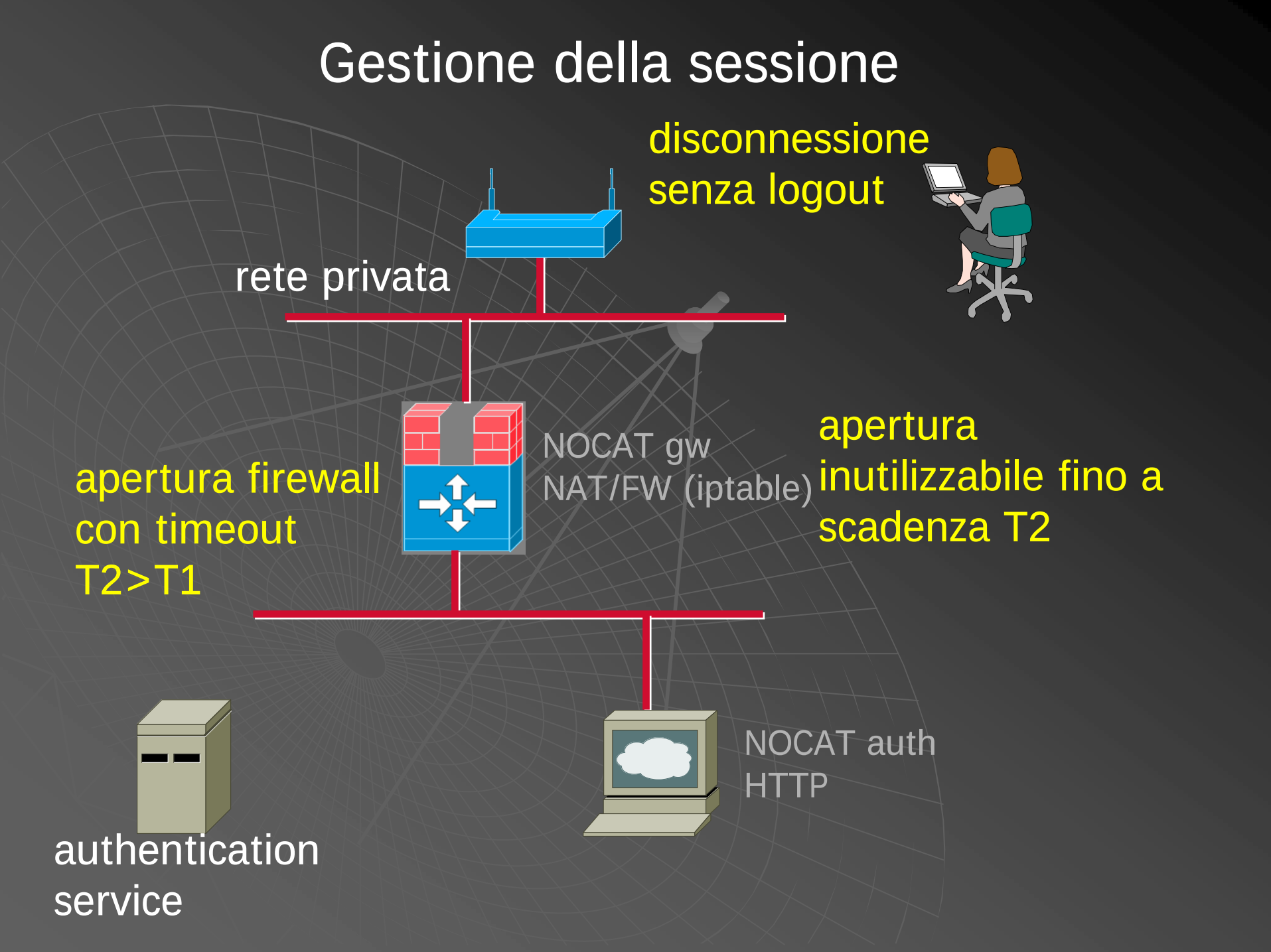
Gestione della sessione



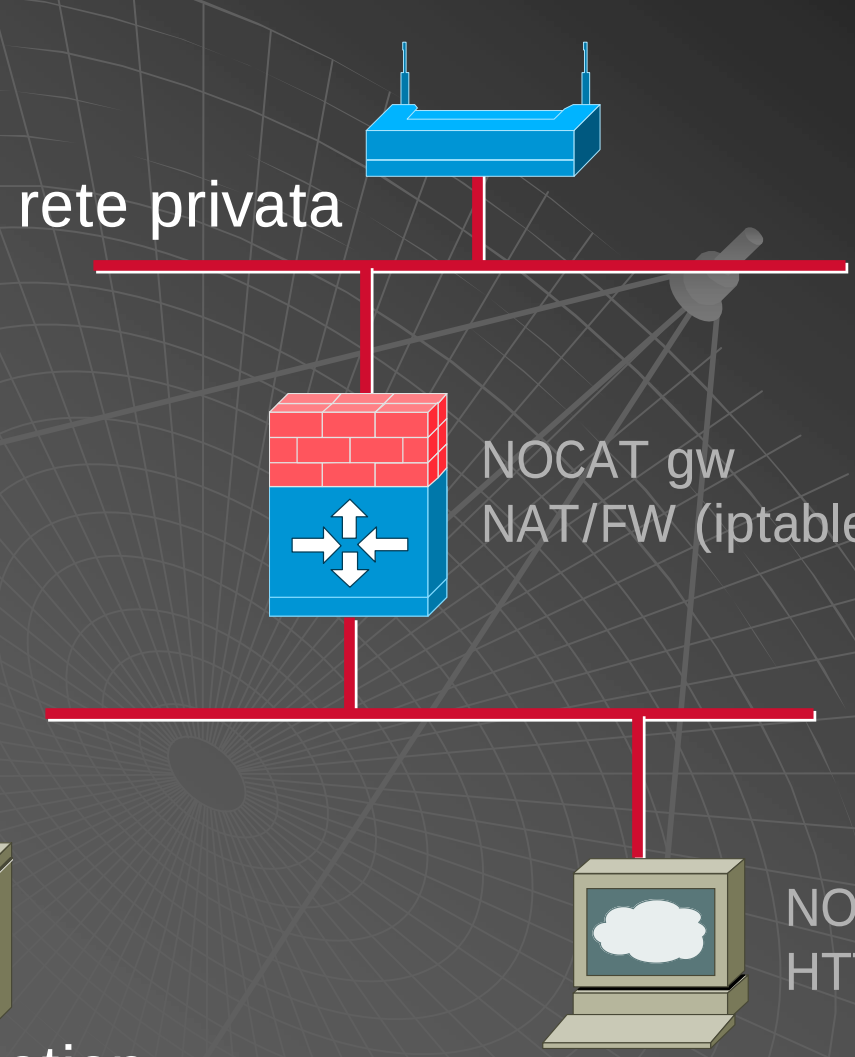
Gestione della sessione



Gestione della sessione

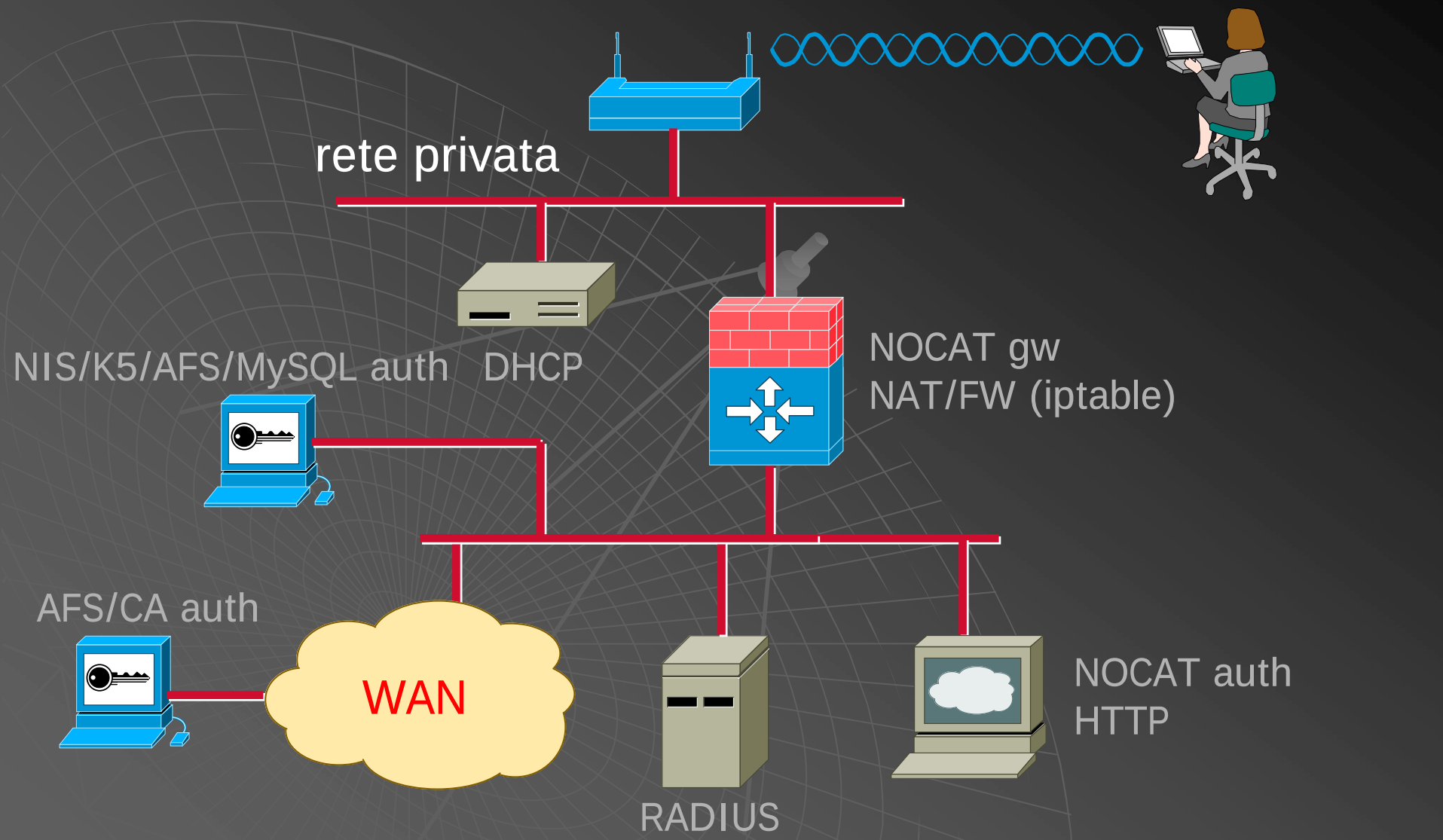


Gestione della sessione

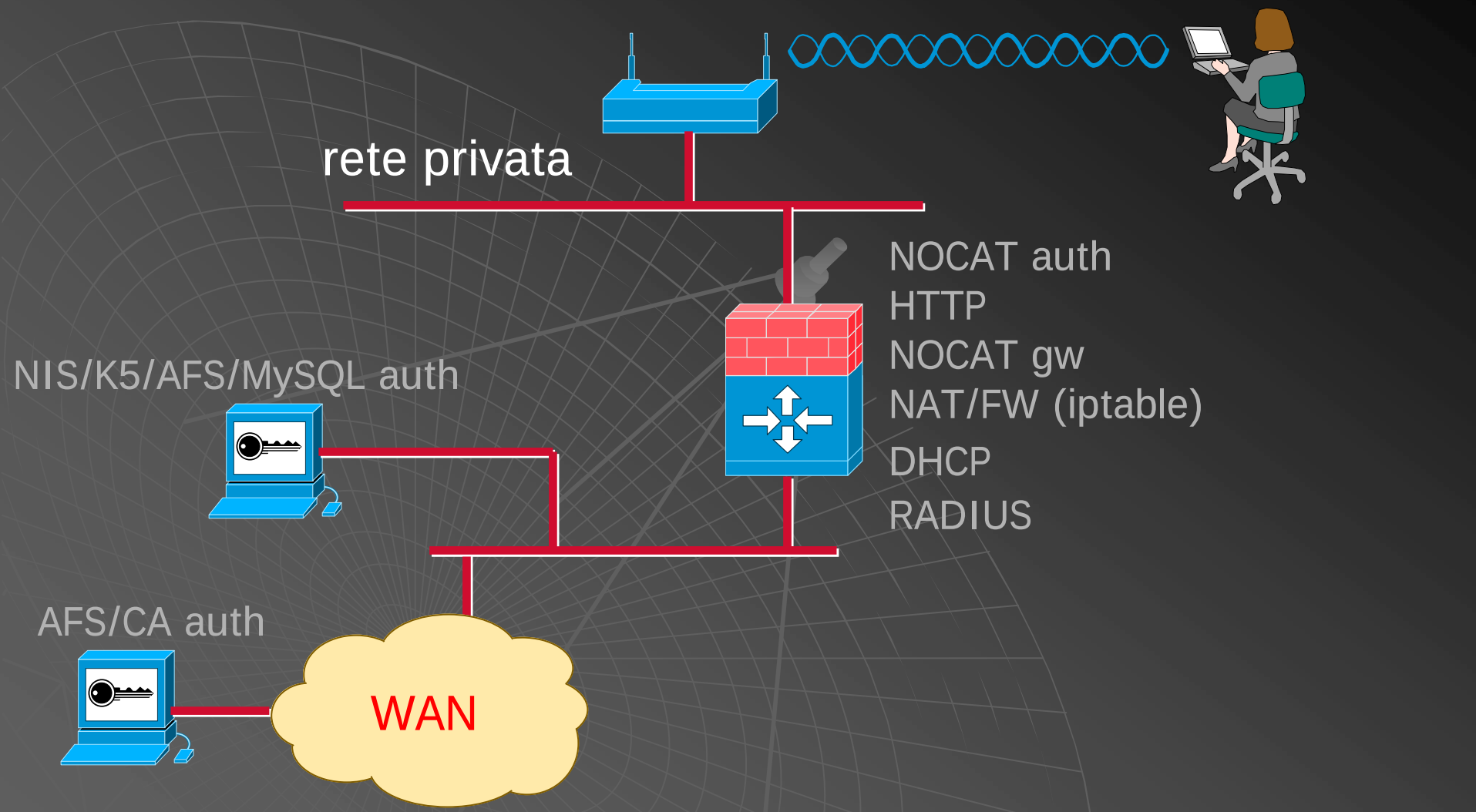


chiusura firewall
alla scadenza di T2

Layout compatto



Layout compatto



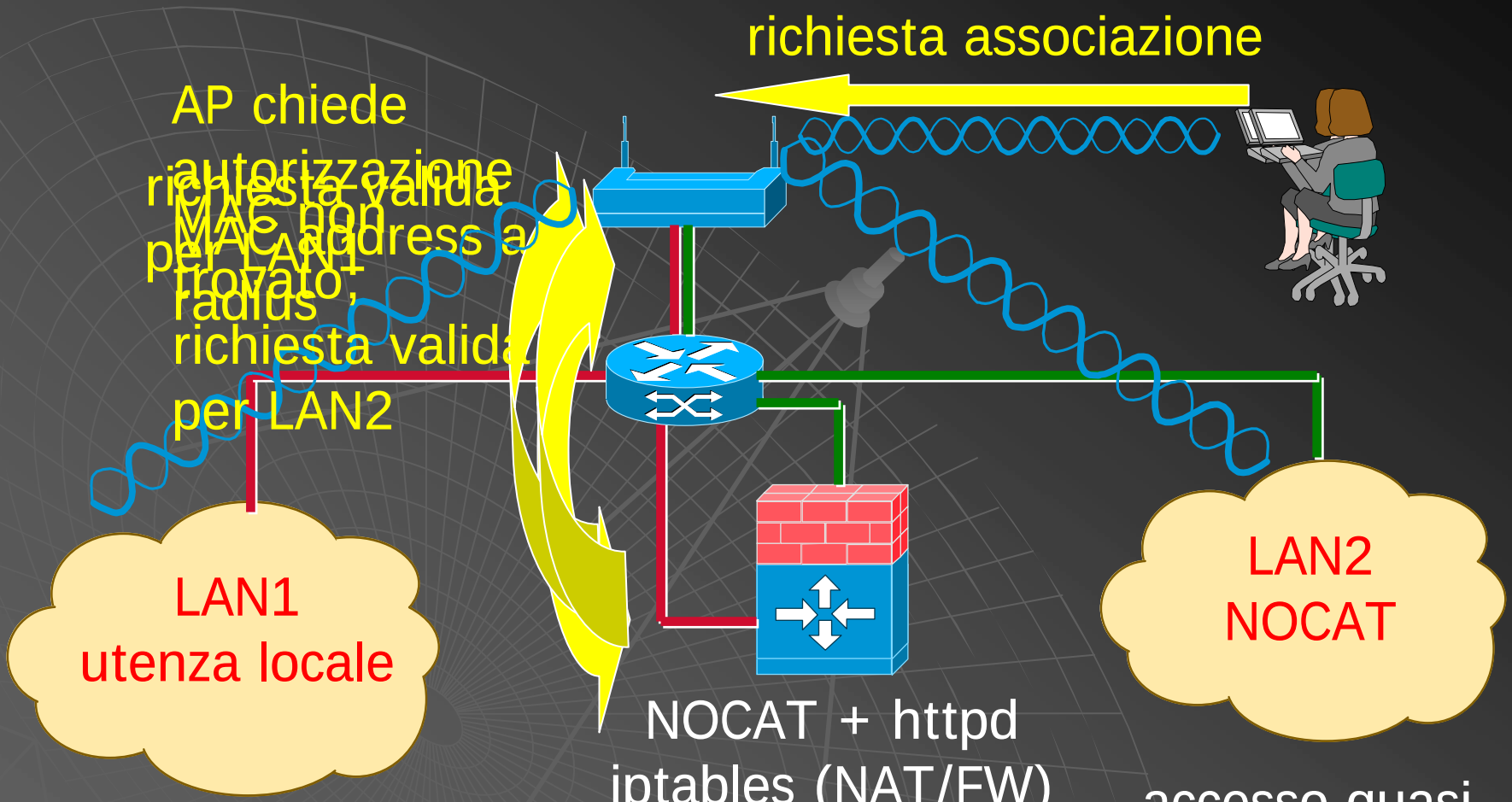
Note

- NOCAT: tratta solo autenticazione via MySQL o via radius (con patch non inserita nell'ultima release). Richiede personalizzazione della pagina HTTP di autenticazione
- Apache + mod-SSL: per trattare certificati X.509 richiede mod-SSL V2.7.x, compatibile solo con apache V1.3 (non con V2.x)
- Non si puo' differenziare gli accessi sulla base delle caratteristiche della autenticazione

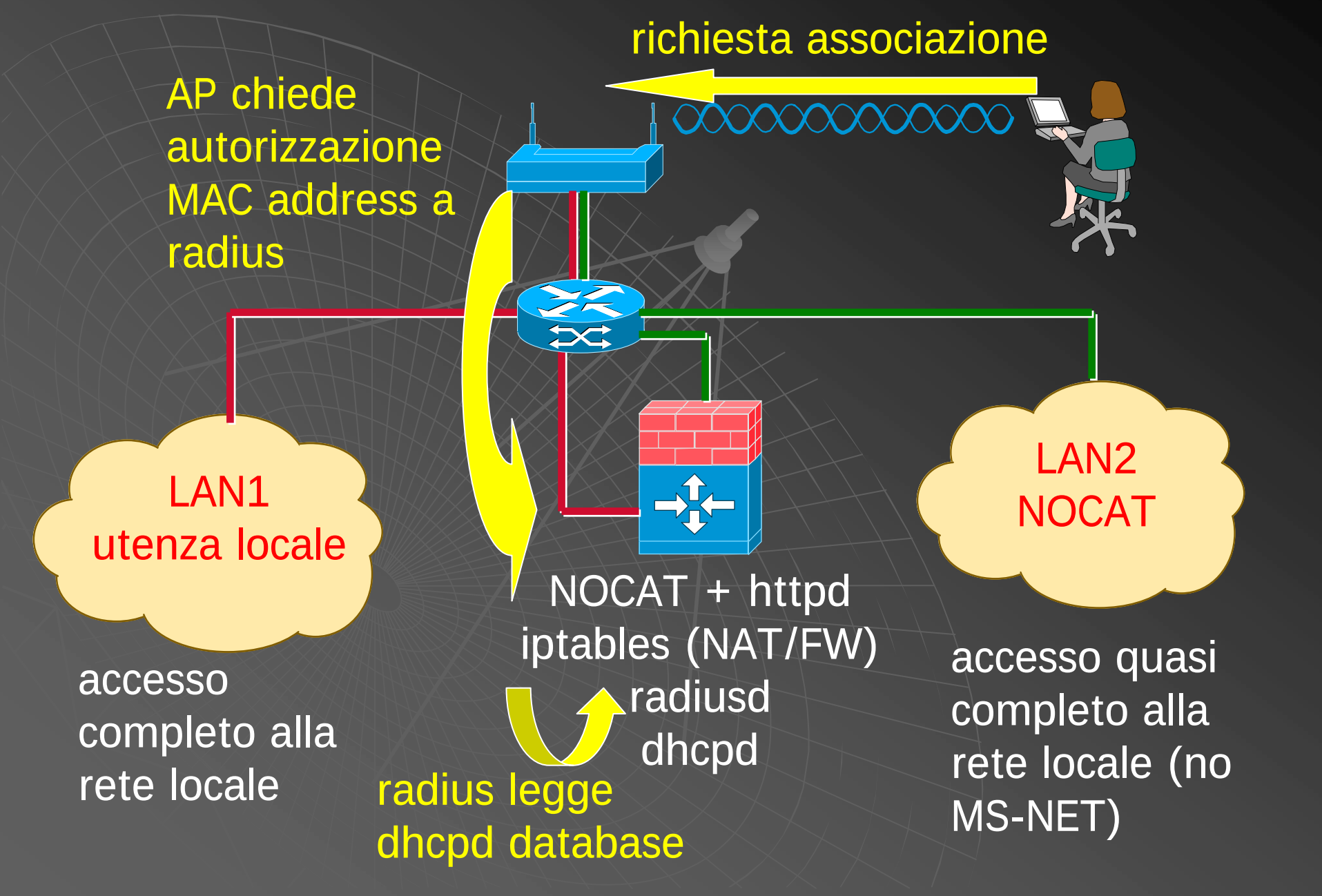
Flessibilita’ e soluzione mista autorizzazione/autenticazione

- Caratteristiche specifiche Cisco Aironet 1120:
  - supporto per SSID multipli e VLAN, con criteri di autorizzazione ed autenticazione indipendenti
  - possibilita’ di collocare dinamicamente il client su una VLAN in base alla autorizzazione radius
- Caratteristiche di freeradius:
  - puo’ fornire all’Aironet le informazioni di VLAN
  - puo’ autorizzare MAC address leggendo il database del dhcpd

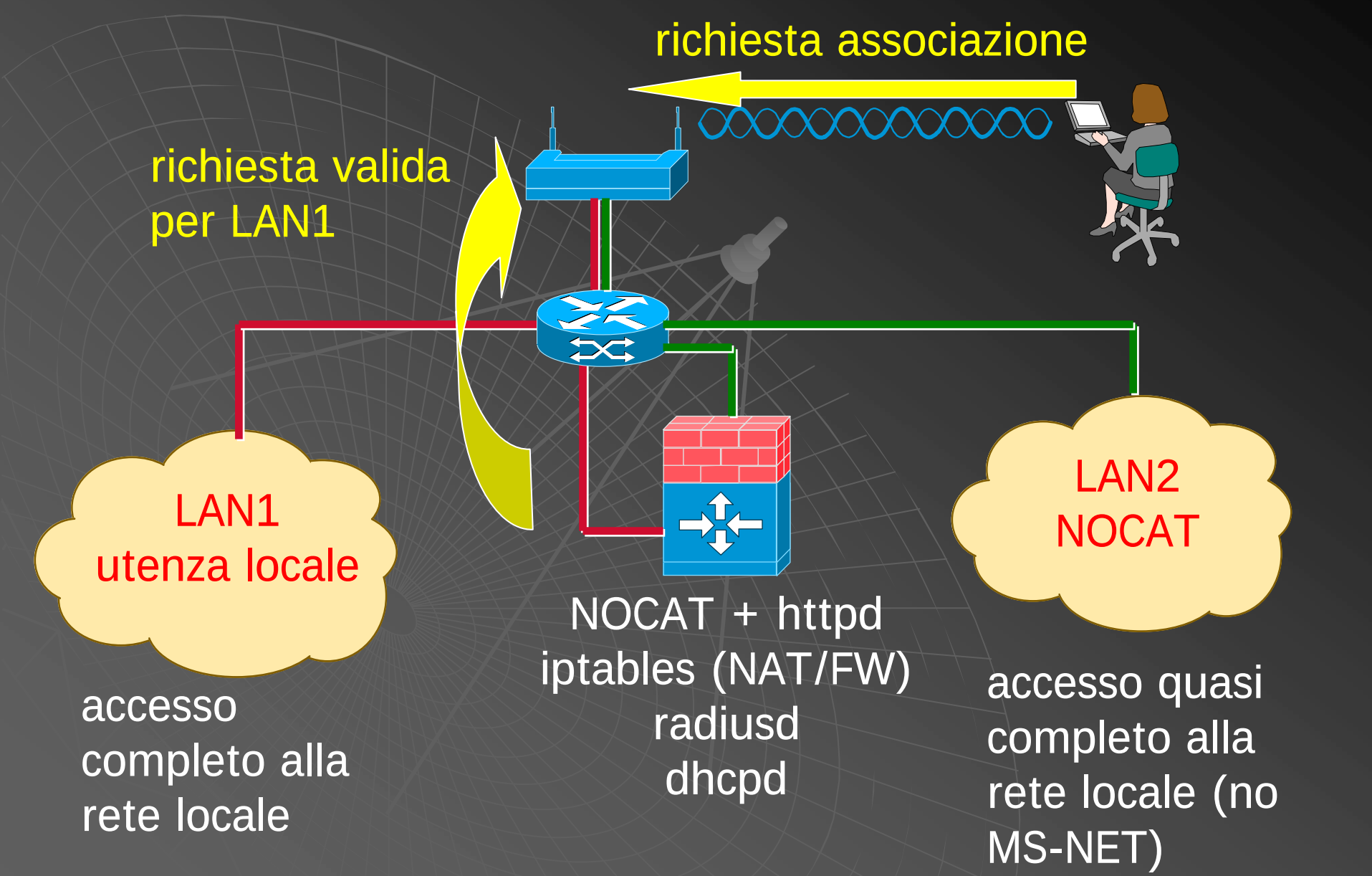
Autorizzazione mista MAC/Layer3



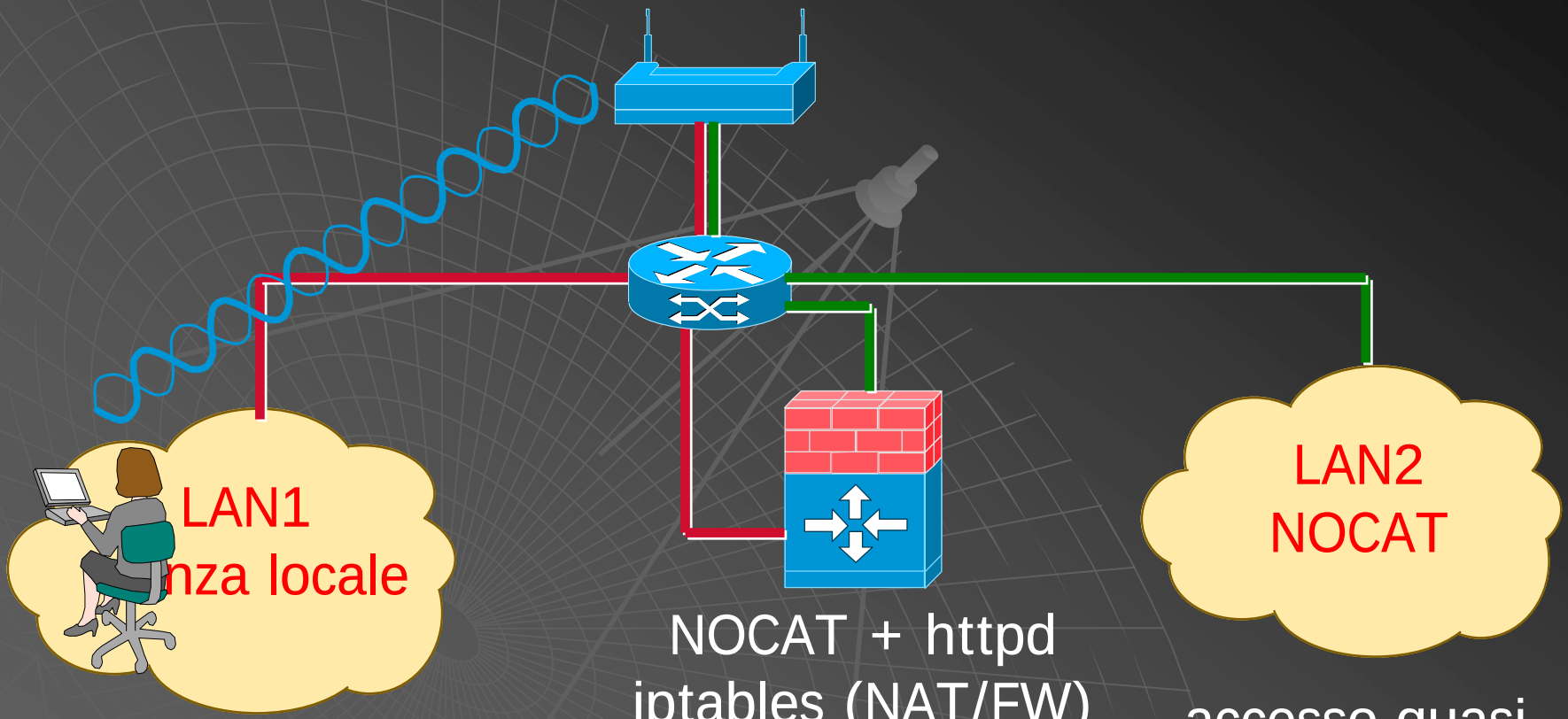
Autorizzazione mista MAC/Layer3



Autorizzazione mista MAC/Layer3



Autorizzazione mista MAC/Layer3

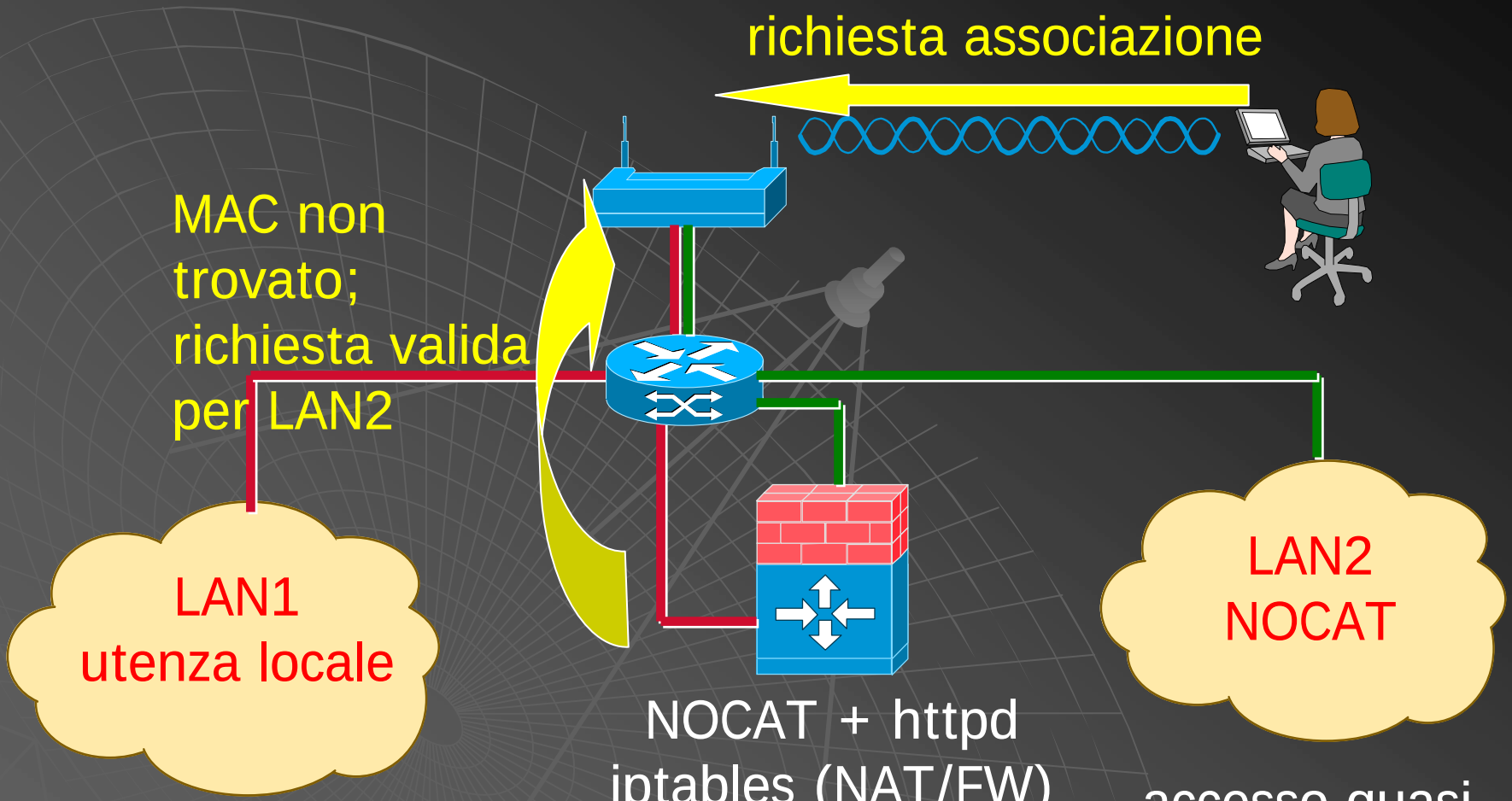


accesso completo alla rete locale

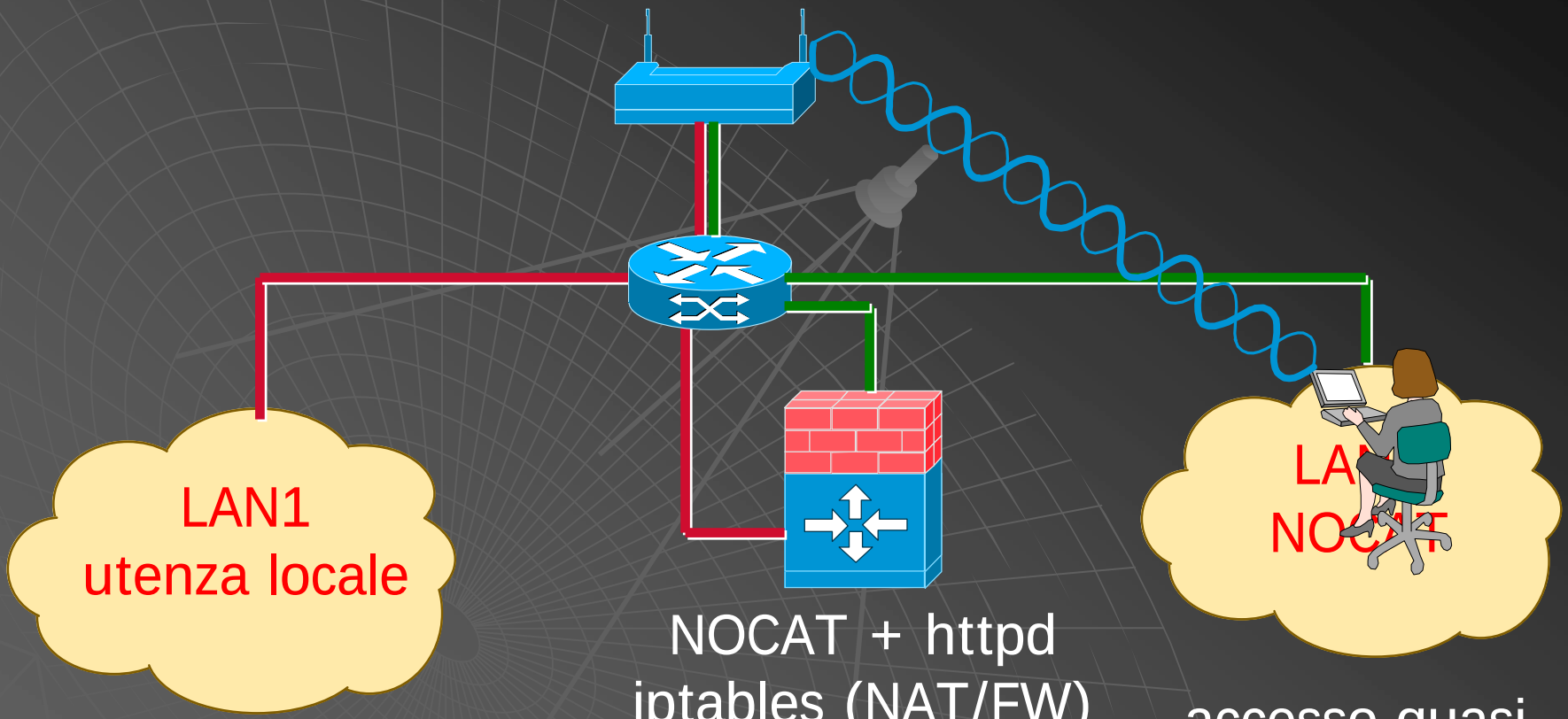
NOCAT + httpd
iptables (NAT/FW)
radiusd
dhcpd

accesso quasi completo alla rete locale (no MS-NET)

Autorizzazione mista MAC/Layer3



Autorizzazione mista MAC/Layer3



accesso completo alla rete locale

NOCAT + httpd
iptables (NAT/FW)
radiusd
dhcpd

accesso quasi completo alla rete locale (no MS-NET)

Risultati

Volevamo una infrastruttura di accesso wireless layer 3 con caratteristiche:

- autorizzazione/autenticazione
- flessibilita' (diversi meccanismi di autenticazione)
- fruibilita' (indipendenza da OS/HW)
- differenziazione accessi
- minimo management a regime
- sicurezza

Problemi

- Sicurezza 1: tutti i client non registrati vengono associati e messi nella LAN filtrata da NOCAT
- Sicurezza 2: la comunicazione tra access point e client non e’ criptata

Sviluppi

- Produzione della documentazione sullo stato di sviluppo del progetto su web
- Produzione di kickstart per l'installazione del software comprensivo di patches (rpm + doc)
- Analisi sulla possiblilita' di differenziare gli accessi gestiti da NOCAT
- Integrazione con associazione via 802.1x
- Interazione NOCAT-Kerberos5

Documentazione

- Progetto ancora in fase di sviluppo
- La documentazione si trova sul sito del progetto (http://www.infn.it/TRIP), in fase di allestimento
- Informazioni sui progressi in questa fase verranno rese pubbliche tramite CCR