802.1x şi NAP

12 aprilie 2010

Cuprins

- EAP
- 802.1x
  - Supplicant
  - Pass-through authenticator
  - Authentication server
- NAP
  - Client
  - Server
- 802.1x şi NAP

Extensible Authentication Protocol

- Standard IETF (RFC 3748)
- Construit initial ca o extensie pentru PPP
- Framework ce suporta diferite metode de autentificare
- Metodele suportate de Windows XP SP3 sunt:
  - Protected EAP (PEAP)
  - EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP)
  - PEAP-Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAP v2)
- PEAP – foloseste un canal TLS pentru criptarea mesajelor EAP (clear text)
  - intai se negociaza folosind PEAP un canal TLS
  - peste acest canal se negociaza o metoda de autentificare

802.1X

- EAP over LAN
- Componentele unei arhitecturi 802.1x
  - Supplicant
    - calculatorul care solicită acces la reţea
  - Pass-through authenticator
    - punct de intrare în reţea, trimite mesajele de autentificare
  - Authentication Server
    - realizează autentificarea si autorizarea
    - poate fi componenta a unui pass-through authenticator sau un server

Supplicant – Windows XP

- Nu are suport pentru 802.1x activat
- Initial suport pentru 802.1x era activat prin serviciul Wireless Zero Configuration
- Serviciul Wired Autoconfig forţează clientul să se autentifice activ la reţea folosind EAPOL
- Serviciul Wired Autoconfig trebuie activat
  - *services.msc→[Wired AutoConfig]→[⇪][Start]*

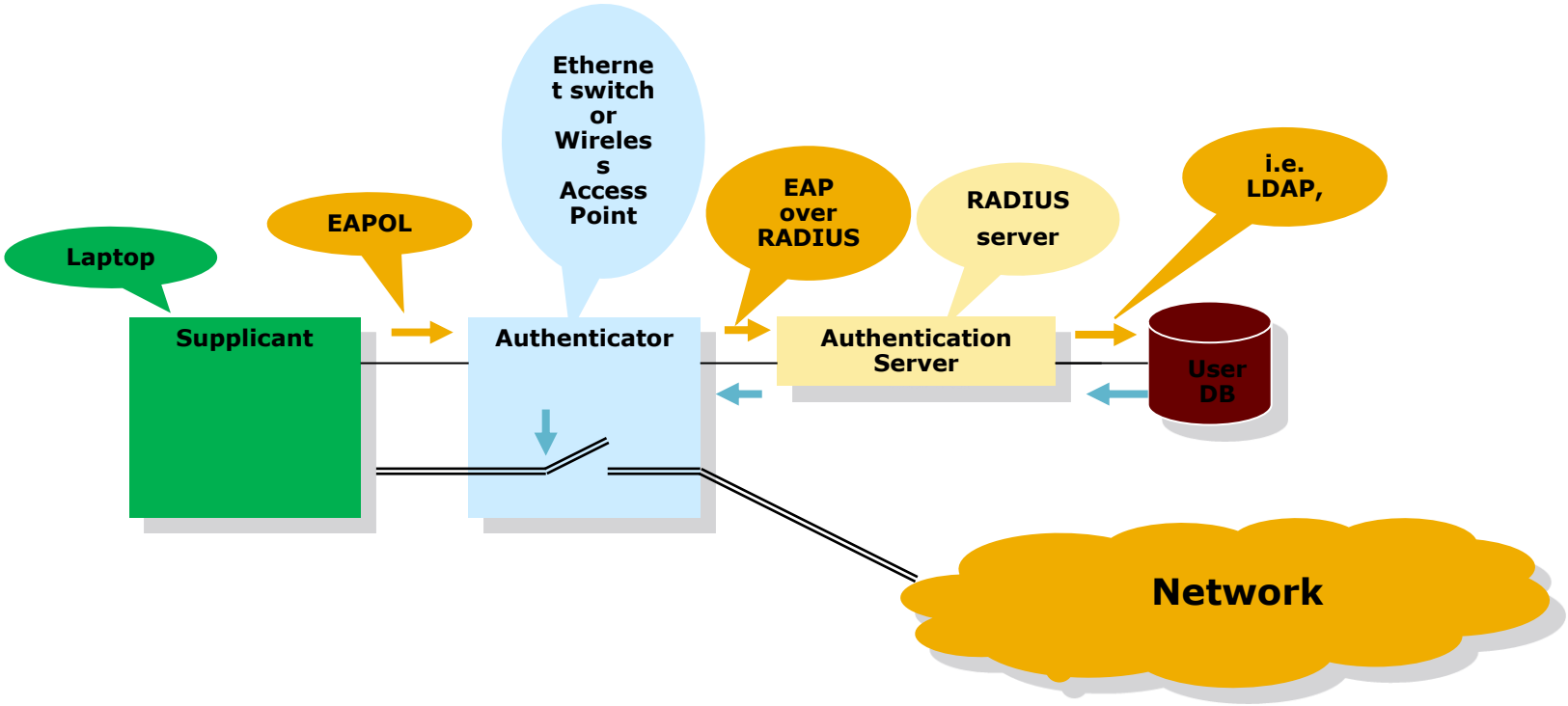
Authentication Server – RADIUS on 2k8

- Integrat in Windows Server 2008 prin serviciul Network Policy Server
- Accepta autentificarea şi monitorizarea clienţilor
- Poate fi configurat ca server RADIUS PROXY
- Schimbul de mesaje se face folosind EAP over RADIUS
- Mesajle sunt trimise folosind UDP
  - porturile 1812, 1645 pentru autentificare
  - porturile 1813, 1646 pentru monitorizare
- Baze de date folosite pentru server
  - Security Accounts Manager
  - Windows NT 4.0 domain
  - Active Directory Domain Services (AD DS)

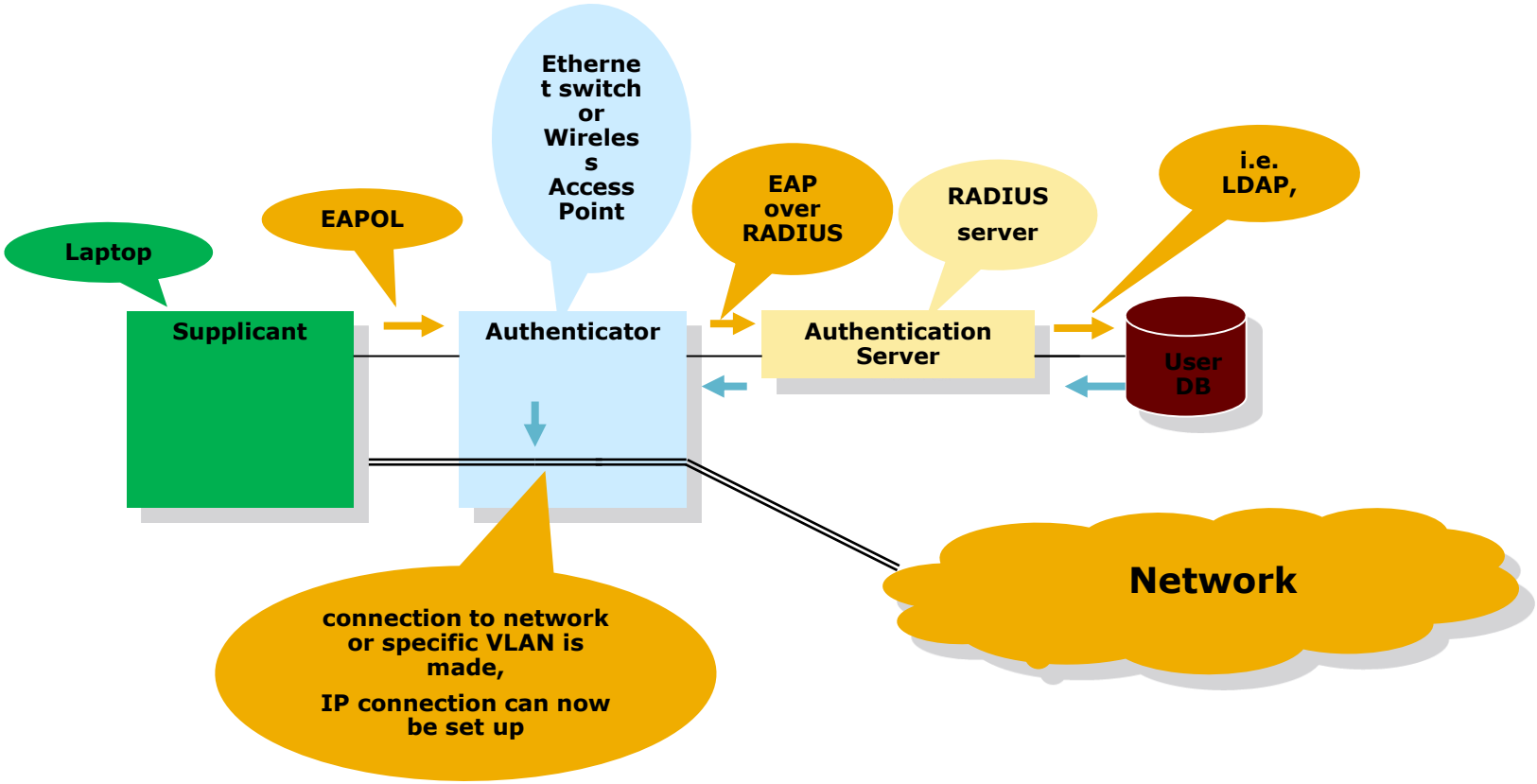
Pass-through autenticator – Cisco switch

- Activarea procesului de autentificare 802.1x
  - *dot1x system-auth-control*
- Folosirea modelului AAA pentru autentificare
  - *aaa new-model*
  - *aaa authentication dot1x default group radius*
- Configurarea serverului de RADIUS
  - *radius-server host X.X.X.X acct-port 1813 auth-port 1812 key PASS*
- Configurarea interfeţelor care necesita 802.1x
  - *dot1x port-control auto*

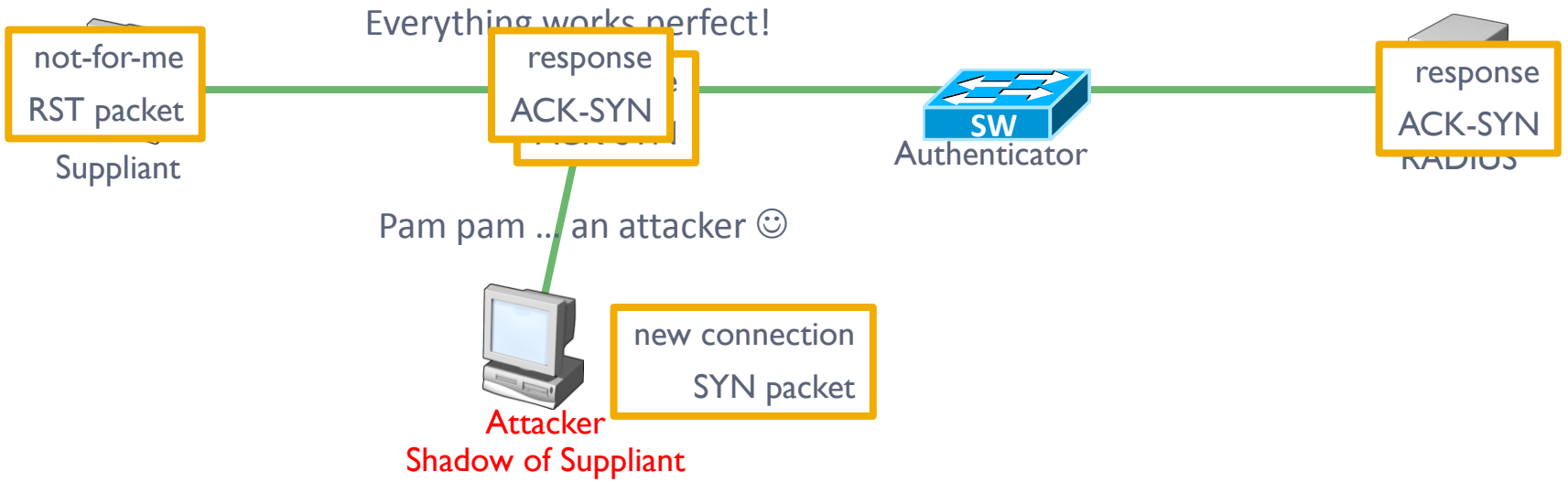
802.1X – How it works



802.1X – How it works



802.1X – Interesting facts



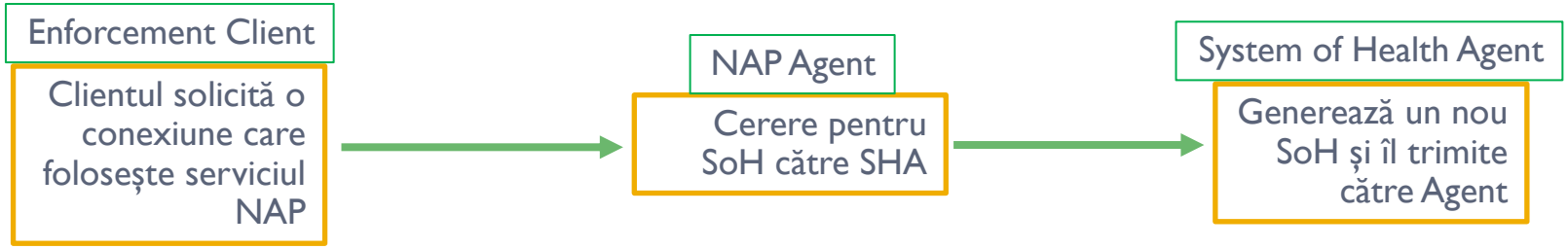
- Atacatorul foloseşte adresele IP şi MAC ale calculatorului
- Ce tip de pachete poate trimite? (ICMP, UDP, TCP)
- Why not TCP?
  - Let's see how TCP works
- Ce se întâmplă dacă victima rulează un firewall ce blochează pachetele ACK-SYN nesolicitate?
  - An that is why you better don't use a firewall …

Network Access Protection

- Arhitectura folosită pentru verificarea "stării de sănătate"
- Trei caracteristicii importante:
  - Validarea stării de sănătate
    - pentru stabilirea nivelului de acces
    - efectuarea este realizată de către server
  - Monitorizarea stării de sănatate
    - client-side, clientul trimite către server orice schimbare de configuraţie
  - Remedierea stării de sănătate
    - folosirea unor servere separate
    - ex. un server cu actualizări de antivirus

NAP – Componente

- Client NAP
  - System Health Agent (SHA) – software care generează raport de sănătate
  - Statement of Health (SoH) – raportul generat
  - NAP Agent – agentul care trimite SoH către server
  - Enforcement Client – clientul care specifică pentru ce tip de conexiune se foloseşte NAP



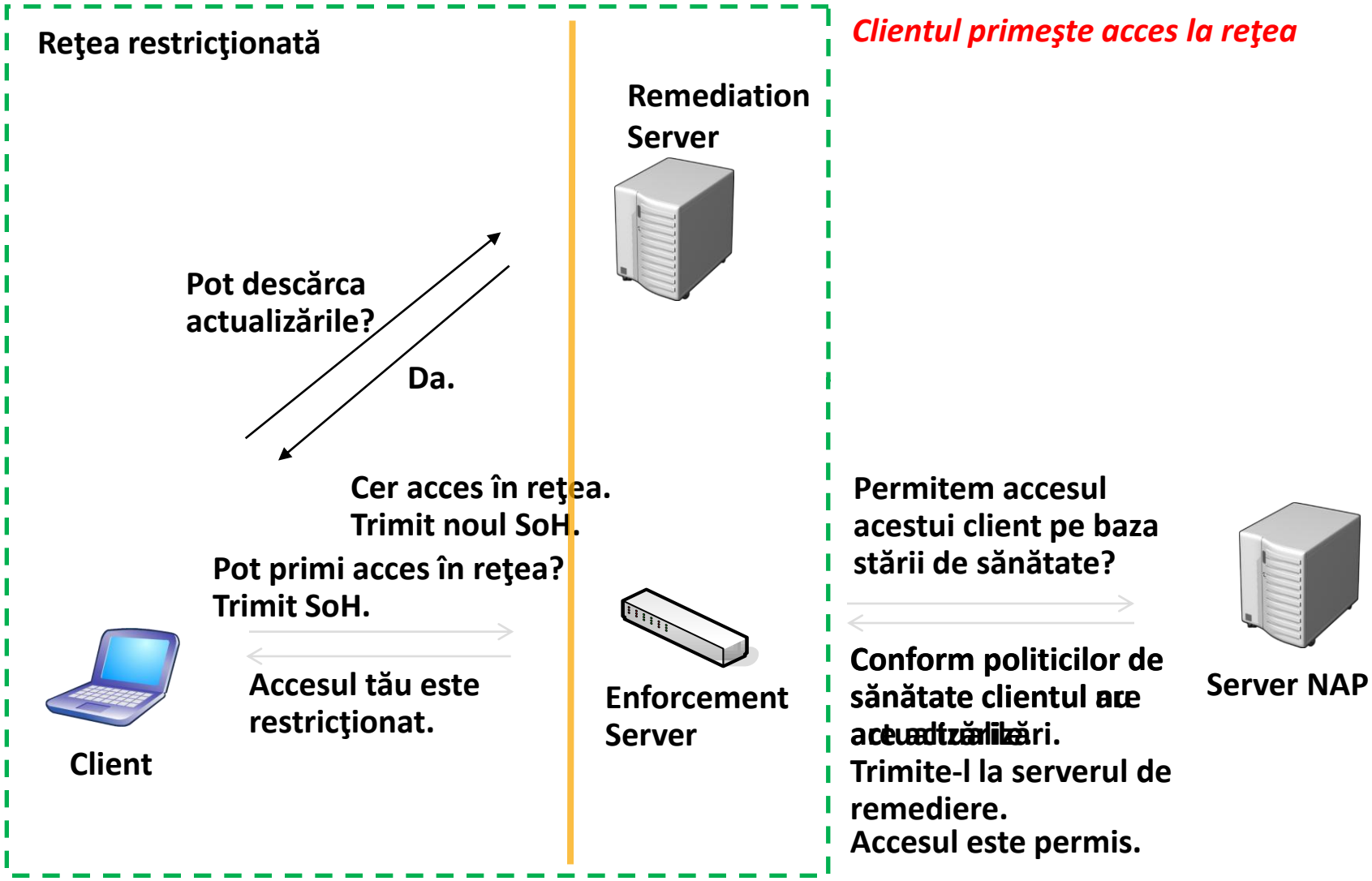
NAP – Componente

- Server NAP
  - System Health Validator – sistemul folosit pentru compararea certificatului de sănătate (SoH) al clientului cu politicile predefinite
  - Statement of Health Response (SoHR) – răspunsul trimis de către server clientului
  - Health Policy – reprezintă diferitele niveluri de sănătate ce pot fi definite de către un administrator, bazat pe deciziile luate de către SHV

NAP – Componente

- Enforcement Server
  - punctul de conectare al clientului la reţea
  - 5 tipuri, definite în funcţie de tipul conexiunii
    - DHCP
    - Remote Access – VPN
    - 802.1x (EAP)
    - Terminal Services Gateway
    - IPSec
- Remediation Server
  - pot fi accesate pentru clienţii non-compatibili
  - furnizează resursele pentru remedierea stării de sănătate

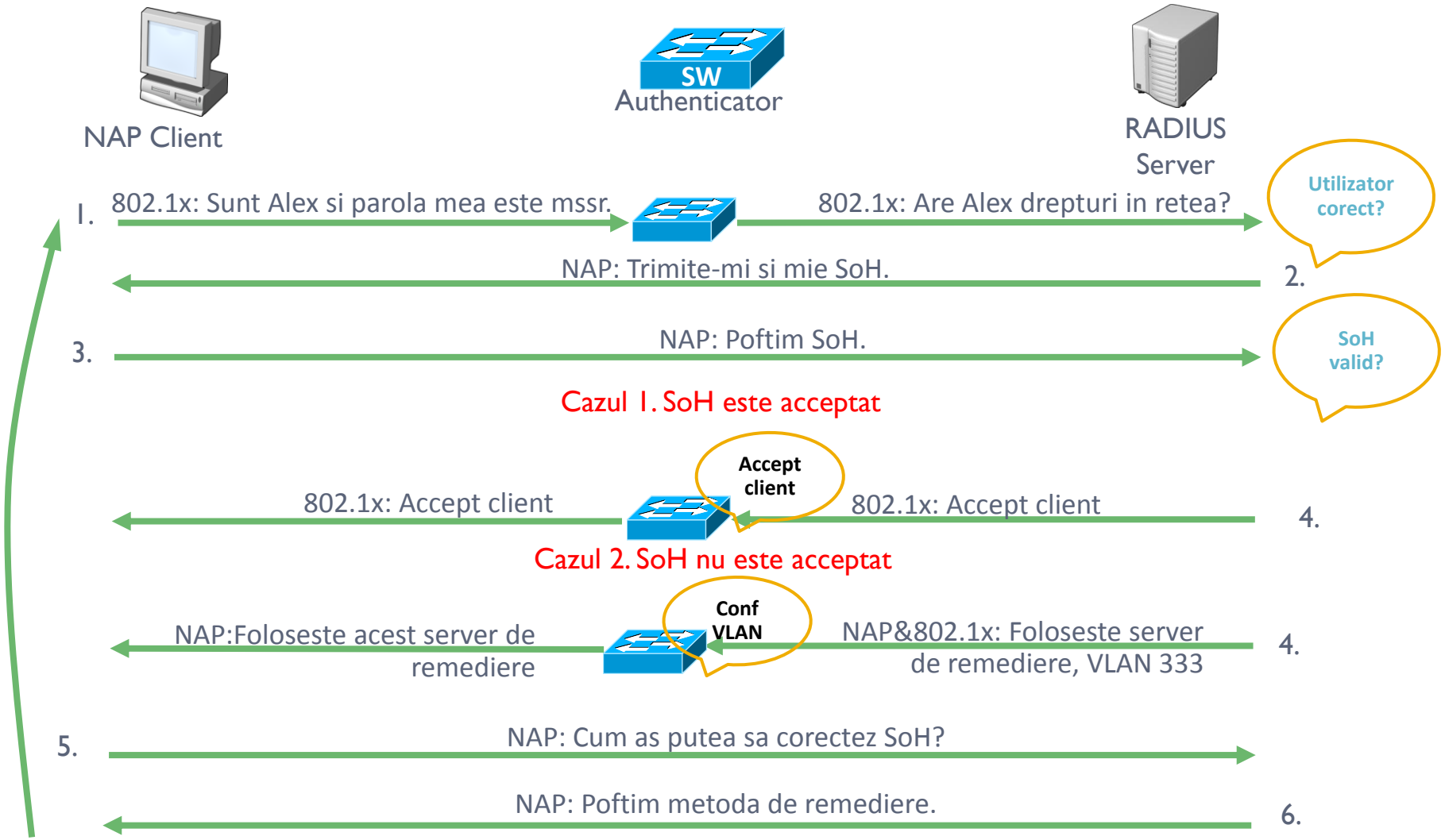
NAP – How it works



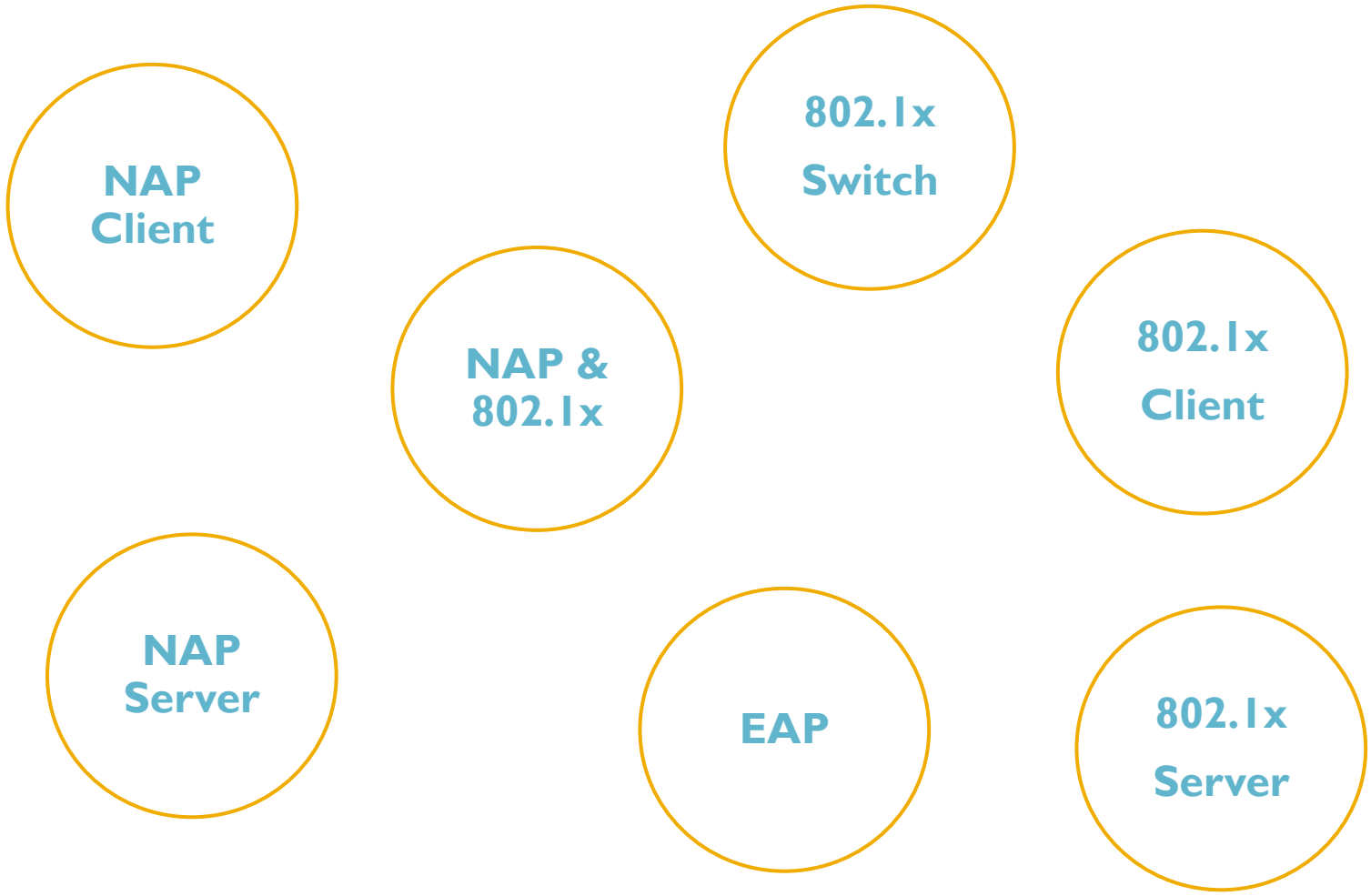
NAP on Windows

- Client
  - SHA = Security Center
    - *gpedit.msc →[Computer Configuration] →[Administrative Templates] →[Windows Components] →[Security Center]→[⇪][Edit] →[Enable]*
  - NAP Agent
    - *services.msc →[Network Access Protection Agent] → [⇪][start]*
  - Enforcement Client
    - *napclcfg.msc* (windows vista)
    - *netsh nap client set enforcement ID = 67213 ADMIN = "DISABLE"*
    - *netsh nap client show configuration*
- Server
  - SHV = Windows SHV

NAP şi 802.1x – How it works



Objective


NAP Client
802.1x Switch
NAP & 802.1x
802.1x Client
NAP Server
EAP
802.1x Server