Kontrola pristupanja mreži

NAC, Network Access Control

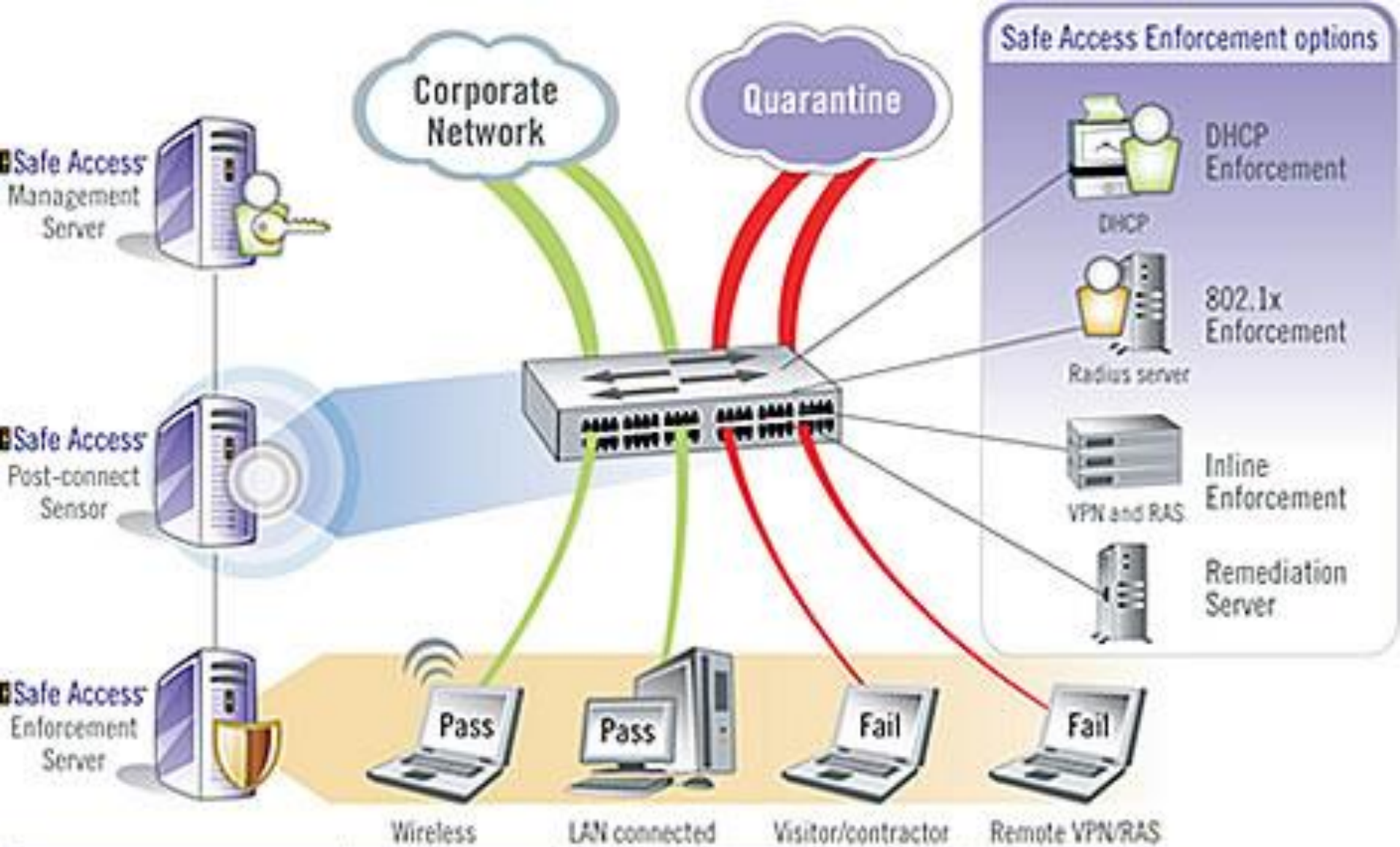
Elementi sistema

- Tražilac pristupa (AR, Access requestor) – supplicant ili klijent
- Server polise (Policy server) – utvrđuje kakav pristup treba odobriti
- Server za pristup mreži (NAS, Network access server) – tačka kontrole pristupa za korisnike na udaljenim lokacijama
  - mrežni prolaz za medij (media gateway)
  - server za daljinski pristup (RAS, remote access server

- Klijenti traže pristup mreži uglavnom tako što se prijavljuju nekoj vrsti NAS-a
- Prvi korak je autentifikacija
- NAS može da obavi autentifikaciju ili da posreduje u procesu autentifikacije između klijenta i servera za autentifikaciju
- Proverava se identitet klijenta, na osnovu koga se odrede privilegije, a onda se uglavnom razmene ključevi sesije
- Proverava se i zdravstvena ispravnost klijenta

Metodi nametanja pristupa mreži – aktivnosti koji regulišu pristup mreži

- IEEE 802.1X
  - Protokol sloja veze koji nameće odobravanje pre dodele IP adrese. Za proces autentifikacije koristi EAP
- Virtuelne lokalne mreže (VLAN)
  - Sistem NAC odlučuje u koji od VLAN-ova u mreži da usmeri AR
- Mrežna barijera (Firewall)
  - Dopušta ili odbija saobraćaj između nekog mrežnog resursa i spoljnog korisnika
- DHCP upravljanje
  - Dinamički dodeljuje IP adrese korisnicima, ali je podložan raznim oblicima lažiranja IP adresa



Authentication:	Pass	Pass	Fail	Fail
Pre-connect testing:	Pass	Pass	Pass	Fail
Post-connect traffic inspection	Pass	Pass	Fail	NA

Proširivi protokol autentifikacije (EAP)

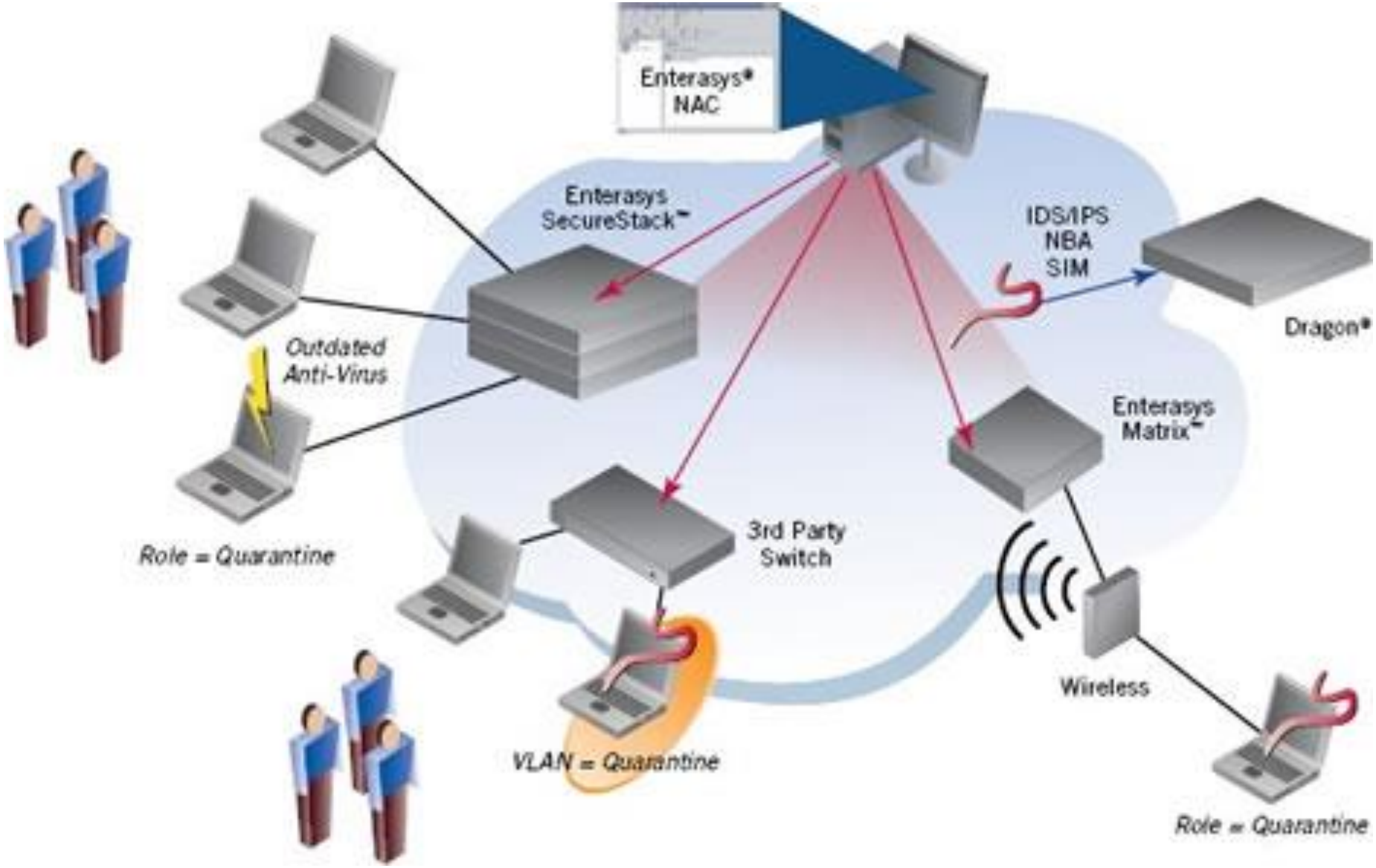
- Metodi autentifikacije
  - EAP bezbednost transportnog sloja (EAP-TLS) – klijent i server se međusobno autentifikuju pomoću digitalnih sertifikata. Klijent pravi pre-master tajni ključ tako što šifruje slučajan broj pomoću serverovog javnog ključa i pošalje serveru. I klijent i server koriste taj pre-master i prave isti tajni ključ
  - EAP tunelovani TLS (EAP-TTLS) – server ima sertifikat i prvo se on autentifikuje klijentu, uspostavlja se bezbedna veza sa tajnim ključem koja sada služi za nastavak autentifikacije
  - EAP opšti unapred deljeni ključ (EAP-GPSK) – uspostavljanje unapred uparenih tajnih ključeva (Pre-Shared Key PSK) je deo registracije učesnika. Koristi kriptografske algoritme tajnih ključeva. Ako je međusobna autentifikacija uspešna obezbeđuje se zaštićen komunikacioni kanal
  - EAP internet razmena šifara (EAP-IKEv2) – zasnovan na protokolu razmene šifara na Internetu

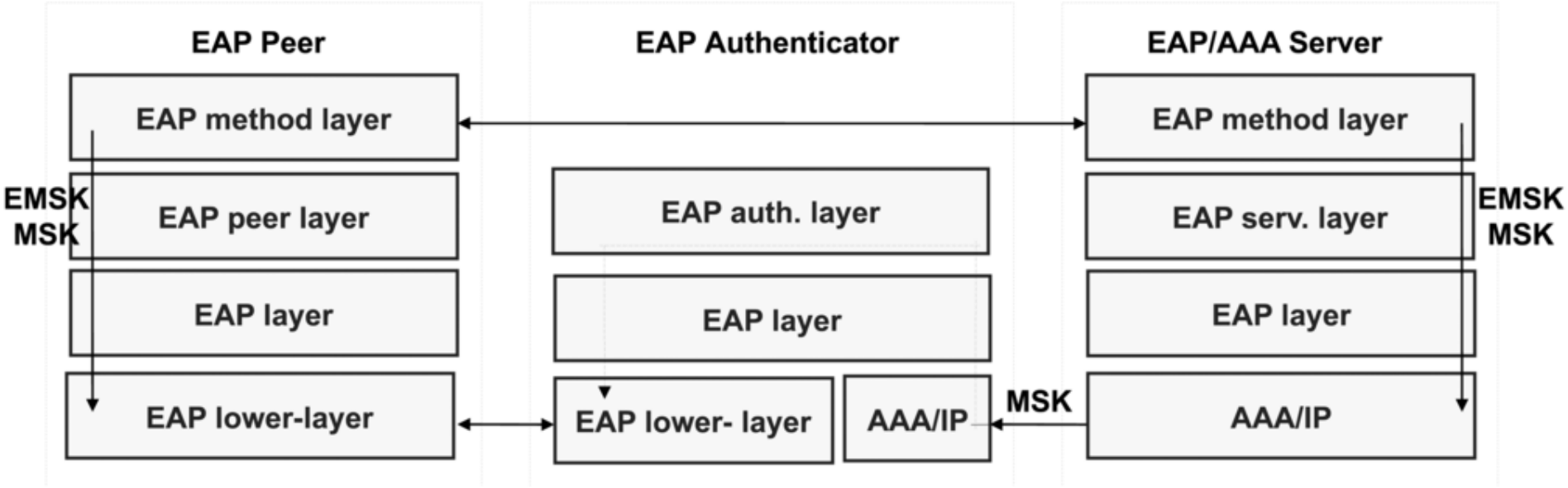
Proširivi protokol autentifikacije (EAP)

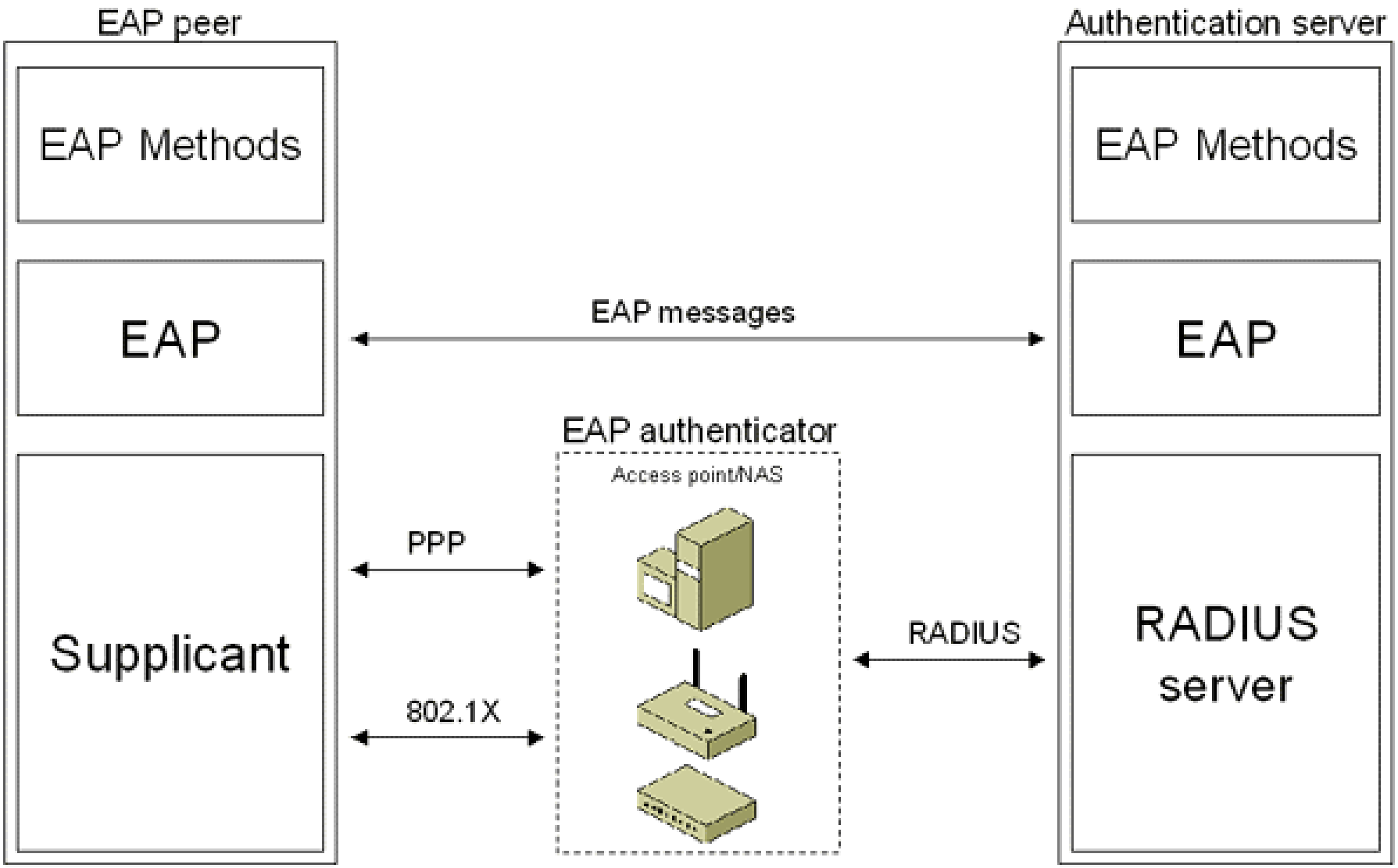
- EAP razmene
  - EAP učesnik – klijentski računar koji pokušava da pristupi mreži
  - EAP autentifikator – pristupna tačka ili NAS koji zahteva EAP autentifikaciju pre odluke odobravanja pristupa mreži
  - Server za autentifikaciju – server koji predlaže određeni EAP metod, proverava ovlašćenja klijenta i odobrava pristup mreži. Jedan server može da vrši autentifikaciju za veći broj EAP autentifikatora. Ovo je obično RADIUS (Remote Authentication Dial-in User Service) server

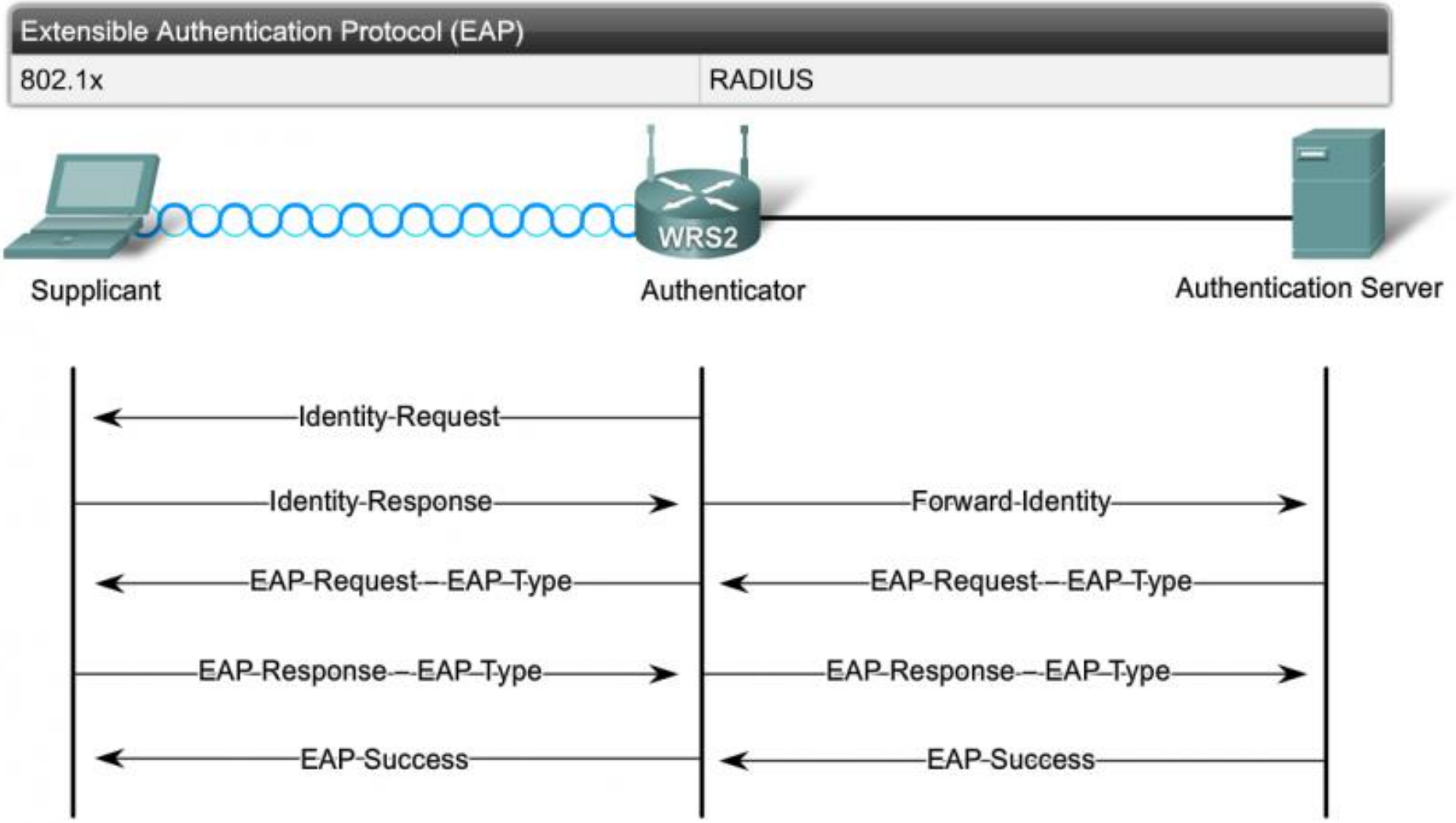
EAP poruke sadrže sledeća polja:

- Kod – ukazuje na tip EAP poruke (Zahtev, Odgovor, Uspeh, Neuspeh)
- Identifikator – uparuje odovor sa zahtevom
- Dužina – dužina EAP poruke u oktetima
- Podaci – informacije vezane za autentifikaciju


Enterasys®
NAC
Enterasys
SecureStack™
IDS/IPS
NBA
SIM
Dragon®
Outdated
Anti-Virus
Role = Quarantine
Enterasys
Matrix™
3rd Party
Switch
VLAN = Quarantine
Wireless
Role = Quarantine

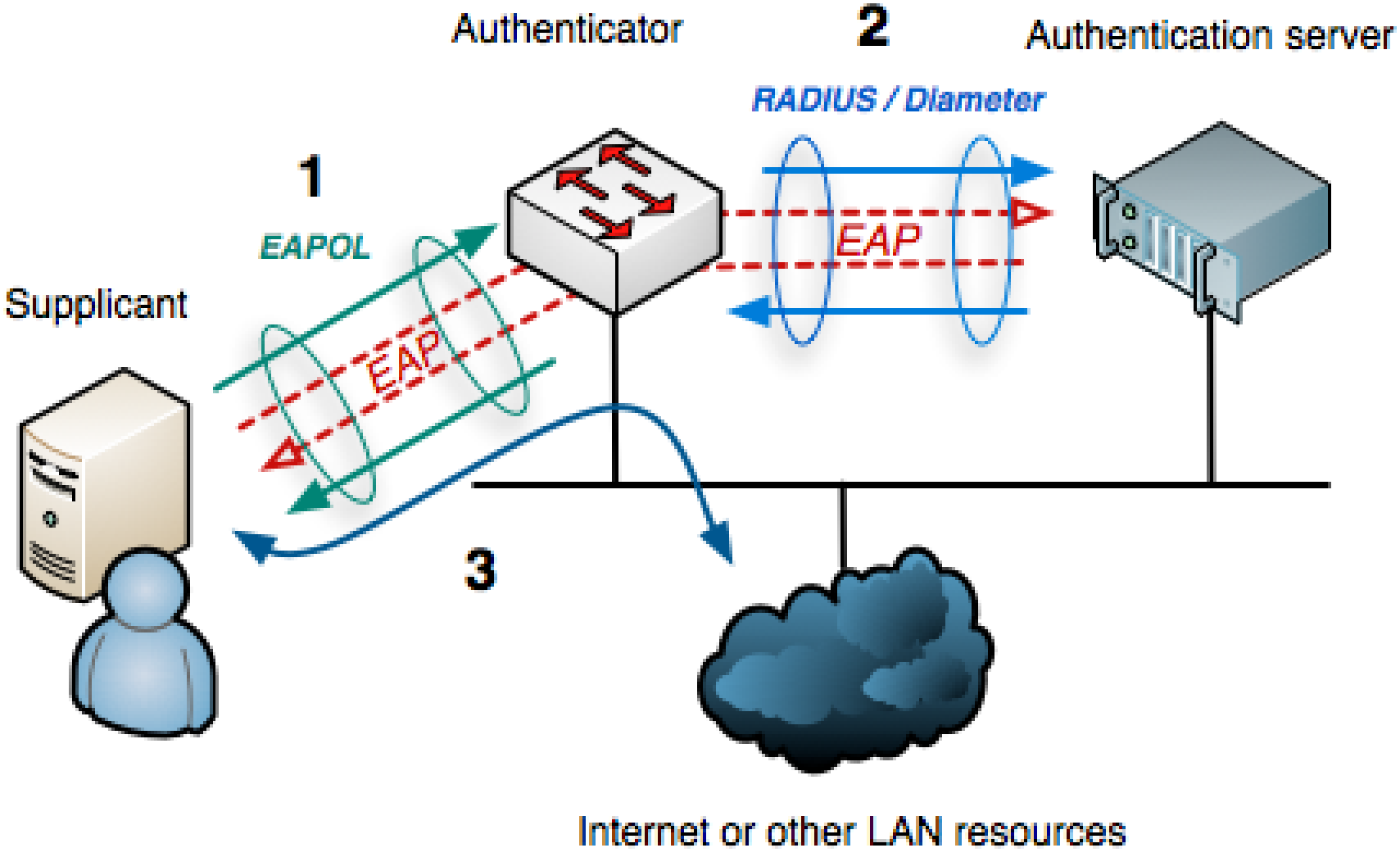

EAP Peer
EAP Authenticator
EAP/AAA Server
EAP method layer
EAP method layer
EMSK
MSK
EAP peer layer
EAP auth. layer
EAP serv. layer
EMSK
MSK
EAP layer
EAP layer
EAP layer
EAP lower-layer
EAP lower- layer
AAA/IP
MSK
AAA/IP


EAP peer
EAP Methods
EAP
Supplicant
EAP messages
PPP
802.1X
EAP authenticator
Access point/NAS
RADIUS
Authentication server
EAP Methods
EAP
RADIUS server


Extensible Authentication Protocol (EAP)
802.1x
RADIUS
WRS2
Supplicant
Authenticator
Authentication Server
Identity-Request
Identity-Response
Forward-Identity
EAP-Request--EAP-Type
EAP-Request--EAP-Type
EAP-Response--EAP-Type
EAP-Response--EAP-Type
EAP-Success
EAP-Success

Kontrola pristupa mreži na osnovu porta (IEEE 802.1X)

- Autentifikator
- Razmena autentifikacije
- Proces autentifikacije
- Server za autentifikaciju
- Prenos autentifikacije
- Bridge port
- Edge port
- Network access port
- Port access entity
- Suplikant


Authenticator
2
Authentication server
RADIUS / Diameter
1
EAPOL
EAP
EAP
Supplicant
3
Internet or other LAN resources

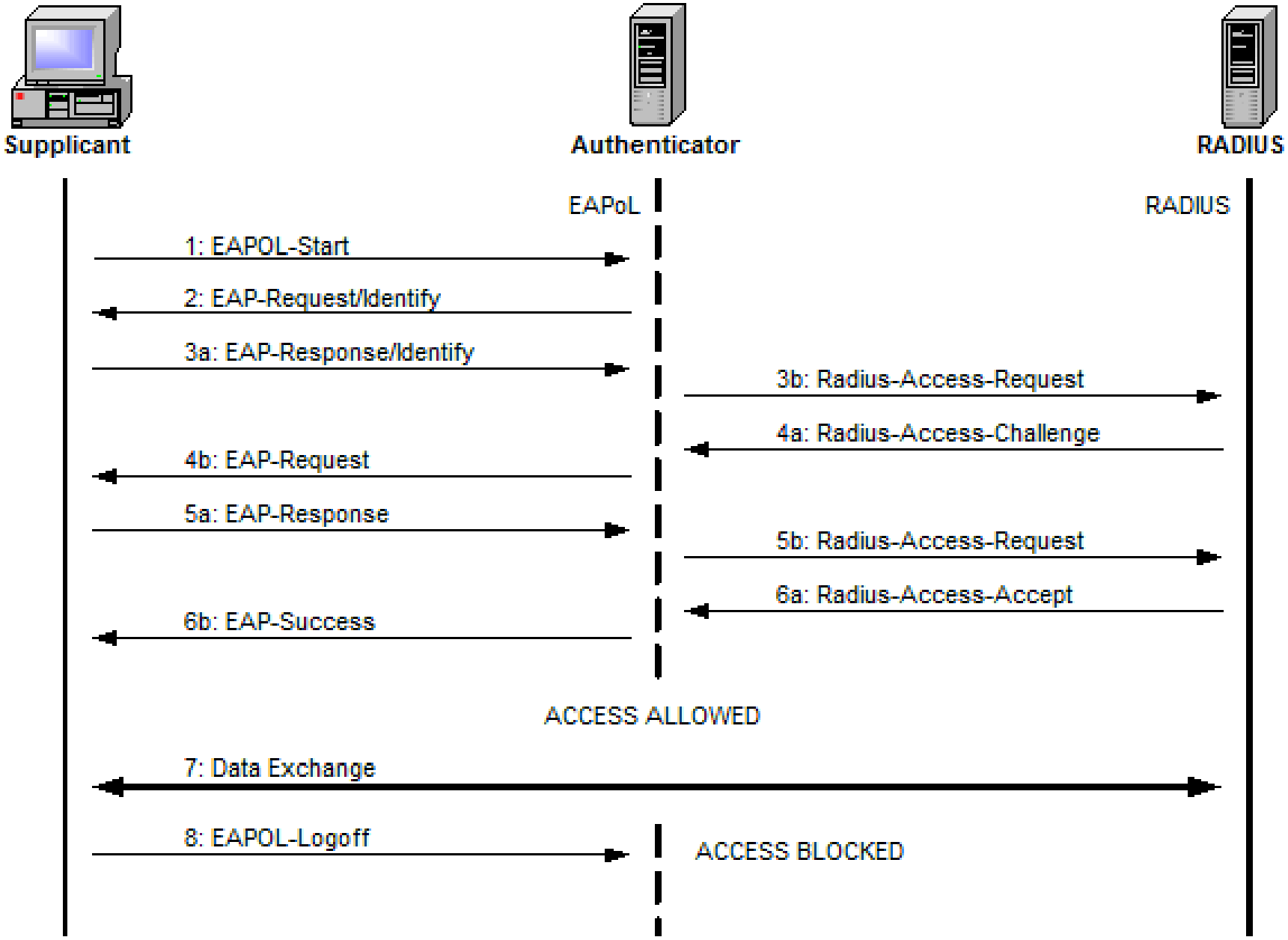
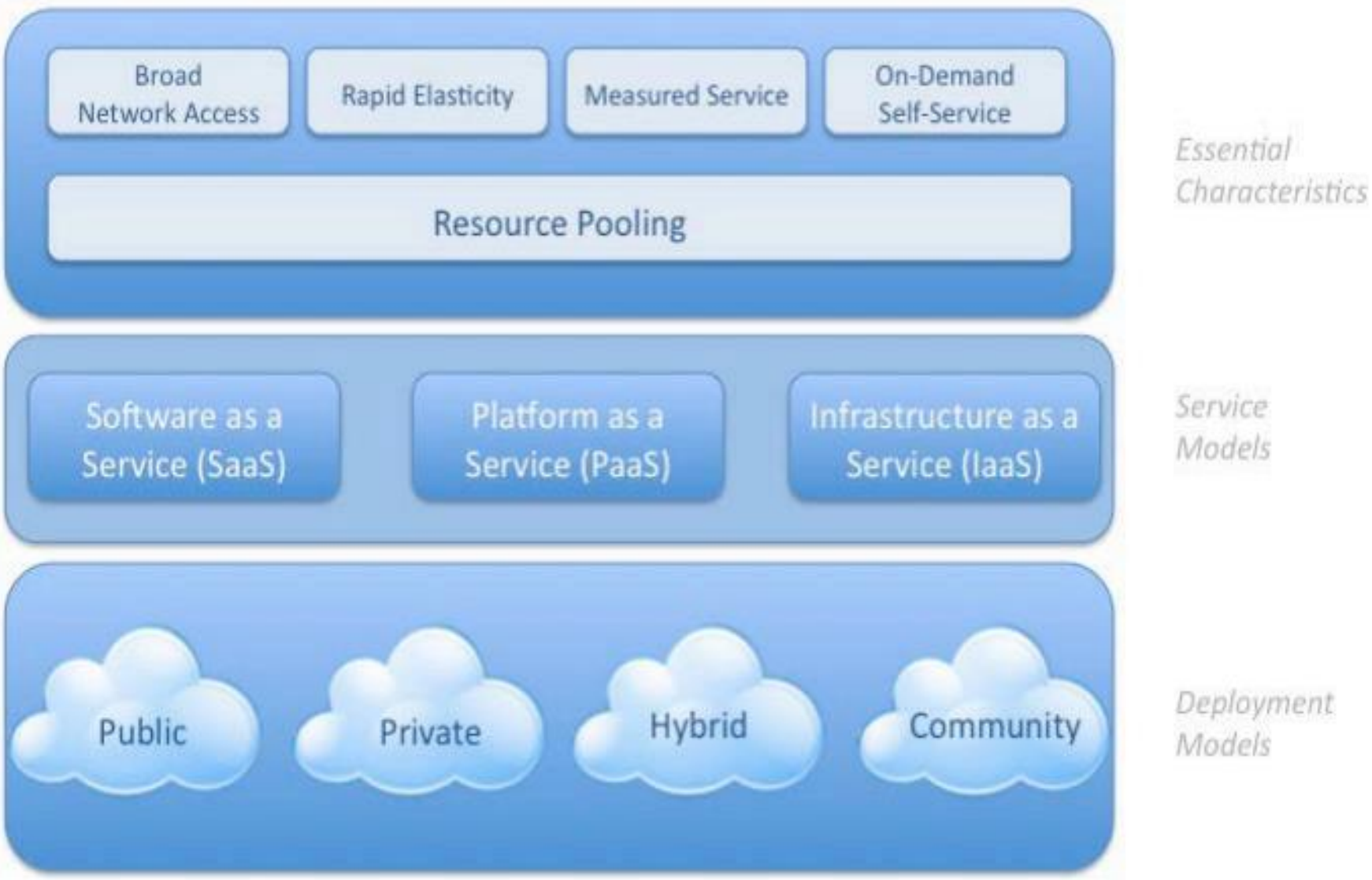


Figure 2: Sample EAPoL Exchange

Računarstvo u oblaku

- Definicija
  - Model da se omogući sveprisutan, prikladan, mrežni pristup na zahtev zajedničkom pulu podesivih računarskih resursa koji mogu brzo da se pribave i oslobode sa minimalnim upravljačkim naporom ili interakcijom sa dobavljačem servisa.
  - Ovaj model oblaka promoviše dostupnost i sastoji se od
    - 5 bitnih karakteristika,
    - 3 modela usluga i
    - 4 modela primene

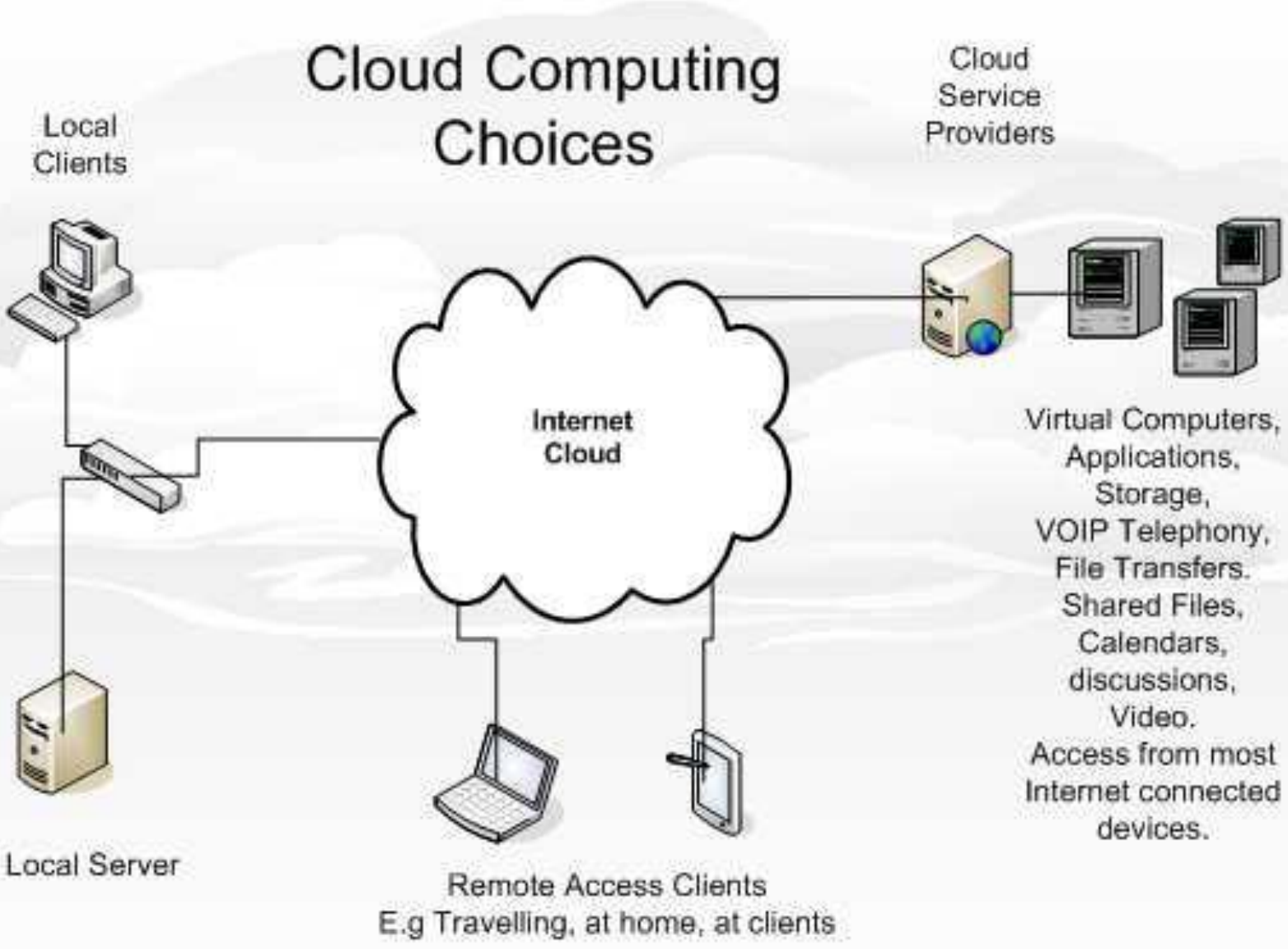

Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

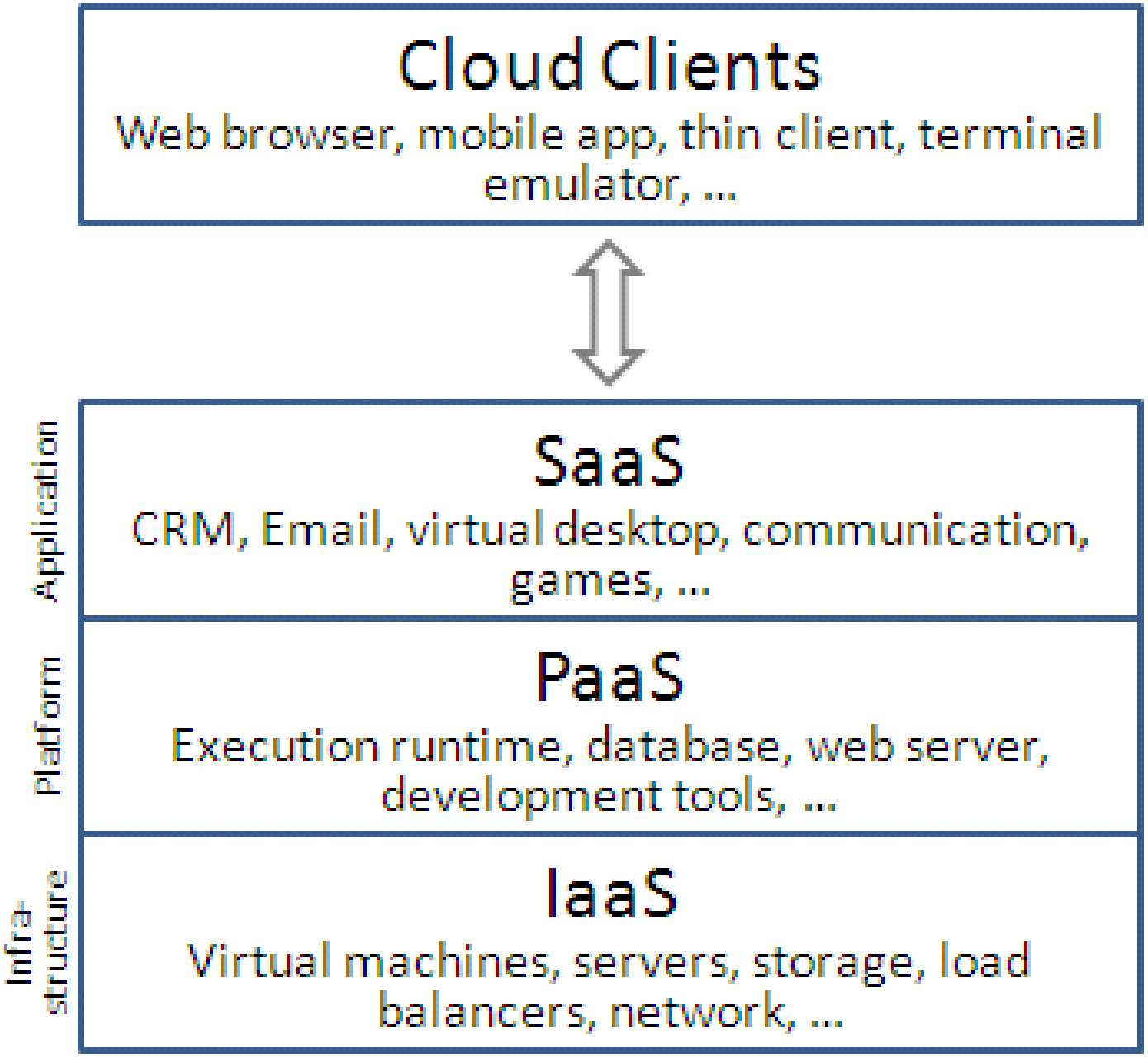
Računarstvo u oblaku - karakteristike

- Širok pristup mreži
- Brza elastičnost
- Merene usluge
- Samousluga na zahtev
- Udruživanje resursa

modeli servisa i modeli primene

- Modeli servisa
  - SaaS – softver kao servis
  - PaaS – platforma kao servis
  - IaaS – infrastruktura kao servis
- Modeli primene
  - Javni oblak
  - Privatni oblak
  - Oblak zajednice
  - Hibridni oblak


Cloud Computing Choices
Local Clients
Cloud Service Providers
Internet Cloud
Virtual Computers, Applications, Storage, VOIP Telephony, File Transfers. Shared Files, Calendars, discussions, Video. Access from most Internet connected devices.
Local Server
Remote Access Clients
E.g Travelling, at home, at clients


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

SaaS

Software as a Service

- Email
- CRM
- Collaborative
- ERP

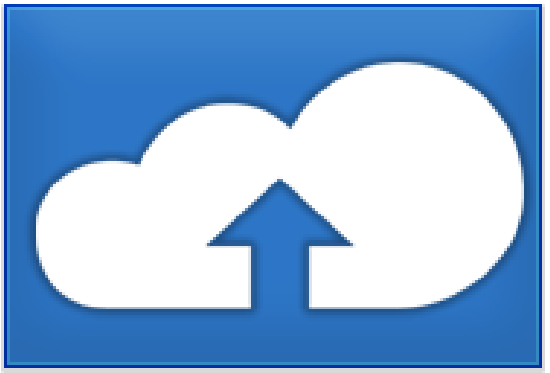
CONSUME

PaaS

Platform as a Service

- Application Development
- Decision Support
- Web
- Streaming

BUILD ON IT



IaaS

Infrastructure as a Service

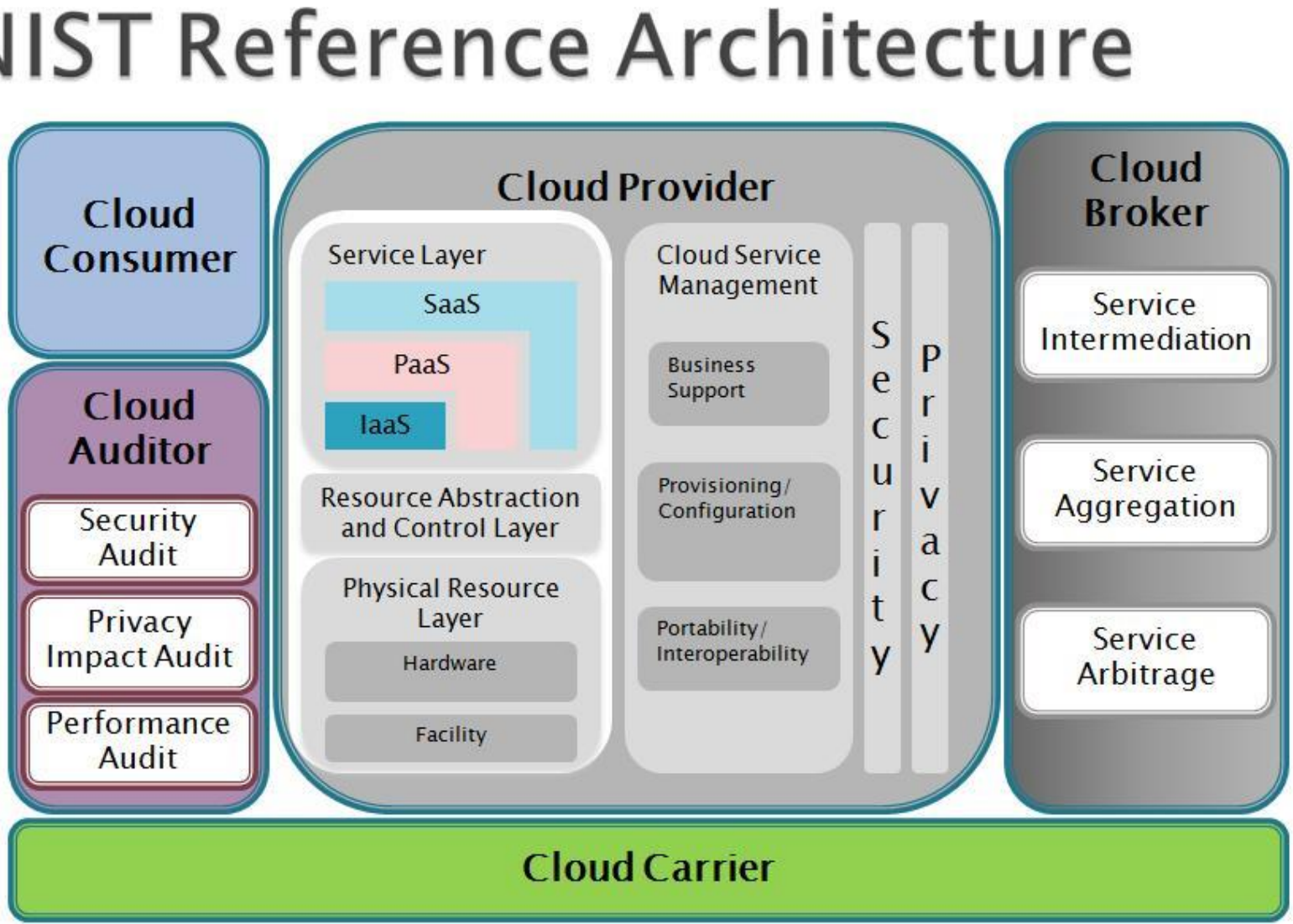
- Caching
- Legacy
- File
- Networking
- Technical
- Security
- System Mgmt

MIGRATE TO IT

Ciljevi referentne arhitekture

- Da se ilustruju i razumeju raznovrsni servisi u oblaku
- Da se potrošačima pruži tehnička referenca da bi shvatili, razmatrali, kategorisali i poredili servise u oblaku
- Da se olakša analiza kandidata standarda za bezbednost, interoperabilnost i prenosivost i reference implementacija

Referentna arhitektura računarstva u oblaku



Glavni akteri u smislu uloga i odgovornosti

- Korisnik oblaka (Cloud consumer)
- Dobavljač oblaka (Cloud provider)
- Revizor oblaka (Cloud auditor)
- Broker oblaka (Cloud broker)
- Nosilac oblaka (Cloud carrier)

Bezbednosni rizici u oblaku i protivmere

- Zloupotreba i neprimereno korišćenje računarstva u oblaku
  - Mnogi dobavljači omogućavaju lako registrovanje ili besplatni probni period, što omogućava napadačima da lako uđu u oblak i napadnu zlonamernim kodom, neželjenim porukama ili uskraćivanjem usluge (DoS)
  - Protivmere su:
    - Srožiji procesi registracije
    - Poboljšano nadgledanje i koordinacija zloupotrebe kreditnih kartica
    - Samoispitivanje kupčevog mrežnog saobraćaja
    - Kontrolisanje javnih crnih lista

Bezbednosni rizici u oblaku i protivmere

- Nesigurni interfejsi i API-ji
  - Bezbednost opštih servisa u oblaku zavisi od bezbednosti osnovnih API-ja
  - Protivmere su:
    - Analilza modela bezbednosti dobavljačevih interfejsa
    - Provera jačine autentifikacija i kontrole pristupa
    - Razumevanje lanca zavisnosti povezanog sa API-jem

Bezbednosni rizici u oblaku i protivmere

- Zlonamerni insajder
  - Organizacije se odriču direktne kontrole nad mnogim aspektima bezbednosti i imaju visok stepen poverenja u dobavljača. To dovodi do rizika od aktivnosti zlonamernih insajdera
  - Protivmere su:
    - Sveobuhvatna procena dobavljača i upravljanje lancem snabdevanja
    - Preciziranje kadrovskih zahteva u pravnom ugovoru
    - Zahtevanje transparentnosti
    - Proces obaveštavanja o povredama bezbednosti

Bezbednosni rizici u oblaku i protivmere

- Pitanja deljenih tehnologija
  - IaaS servis deli infrastrukturu sa drugim korisnicima. Izolovane virtualne mašine nisu dovoljno pouzdane.
  - Protivmere su:
    - Primene bezbednih tehnika za instalaciju i konfiguraciju
    - Nadgledanje neovlašćenih aktivnosti u okruženju
    - Jaka autentifikacija i kontrola pristupa
    - SLA ugovori
    - Skeniranje ranjivosti
    - Revizija konfiguracije

Bezbednosni rizici u oblaku i protivmere

- Gubitak ili curenje podataka
  - Ovo je jedan od najvećih rizika
  - Protivmere su:
    - Jaka kontrola API pristupa
    - Šifrovanje podataka u tranzitu
    - Analiza zaštite podataka
    - Jake tehnike za generisanje, skladištenje, upravljanje i uništavanje ključeva

Bezbednosni rizici u oblaku i protivmere

- Otmice naloga ili usluga
  - Najčešće pomoću ukradenih ovlašćenja ugrožava se poverljivost, integritet i dostupnost
  - Protivmere su:
    - Zabrana deljenja ovlašćenja za više korisnika i servisa
    - Jaka autentifikacija
    - Aktivno nadgledanje
    - Razumevanje bezbednosne polise i SLA ugovora

Bezbednosni rizici u oblaku i protivmere

- Profili nepoznatih rizika
  - Zaposleni kod klijenta mogu neodgovorno da se ponašaju pa je važno definisati uloge i odgovornosti
  - Protivmere su:
    - Nadgledanje i upozoravanje na neophodne mere
    - Objavljivanje primenljivih evidencija
    - Objavljivanje detalja infrastrukture (firewall, zakrpe...)

Zaštita podataka u oblaku

- Upravljanje
- Pridržavanje
- Poverenje
- Arhitektura
- Upravljanje identitetom i pristupanjem
- Izolacija softvera
- Zaštita podataka
- Raspoloživost
- Reagovanje na incidente

Bezbednost u oblaku kao servis (SecaaS)

- Upravljanje identitetom i pristupom
  - Proverava se identitet entiteta i odobrava odgovarajući nivo pristupa
- Sprečavanje gubitaka podataka
  - Nadgledanje, zaštita i proveravanje bezbednosti podataka
- Veb bezbednost
  - Dodatna zaštita u realnom vremenu, pored antivirusa
- Bezbednost e-pošte
  - Kontrola dolaznog i odlaznog saobraćaja
- Procenjivanje bezbednosti
  - Nezavisne revizije servisa u oblaku

Bezbednost u oblaku kao servis (SecaaS)

- Kontrola upada
  - Sistem za detekciju upada (IDS-intrusion detection systems) i sistem za sprečavanje upada (IPS-intrusion preventions systems) otkriva, sprečava i reaguje na upade na ulaznim tačkama oblaka i na serverima u oblaku
- Upravljanje informacijama o bezbednosti i o događajima
  - Sakuplja podatke o događajima, povezuje ih i analizira radi izveštavanja u realnom vremenu i alarmiranja
- Bezbednost mreže
  - Mrežne barijere koje dodeljuju pristup, nadgledaju i štite osnovne resurse servisa

Bezbednost u oblaku kao servis (SecaaS)

- Šifrovanje
  - Ovaj servis uključuje:
    - Upravljanje ključevima
    - Primena VPN-a
    - Šifrovanje aplikacija
    - Pristup sadržaju podataka
- Kontinuitet poslovanja i oporavak od katastrofe
  - Obezbeđuje operativnu otpornost u slučaju zastoja pomoću:
    - Fleksibilne infrastrukture
    - Redundanse
    - Nadzranog rada
    - Geografski distribuiranih centara
    - Mogućnosti preživljavanja mreže