Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Mechanizmy autentifikácie a autorizácie (v sieťach)

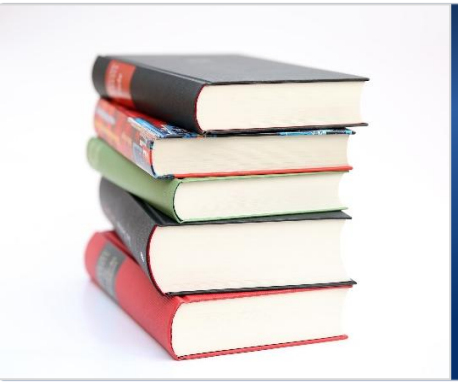
Sieťová bezpečnostná architektúra

Kurz: Špecialista kybernetickej bezpečnosti

Pavel Segeč

KC KYB UNIZA https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk



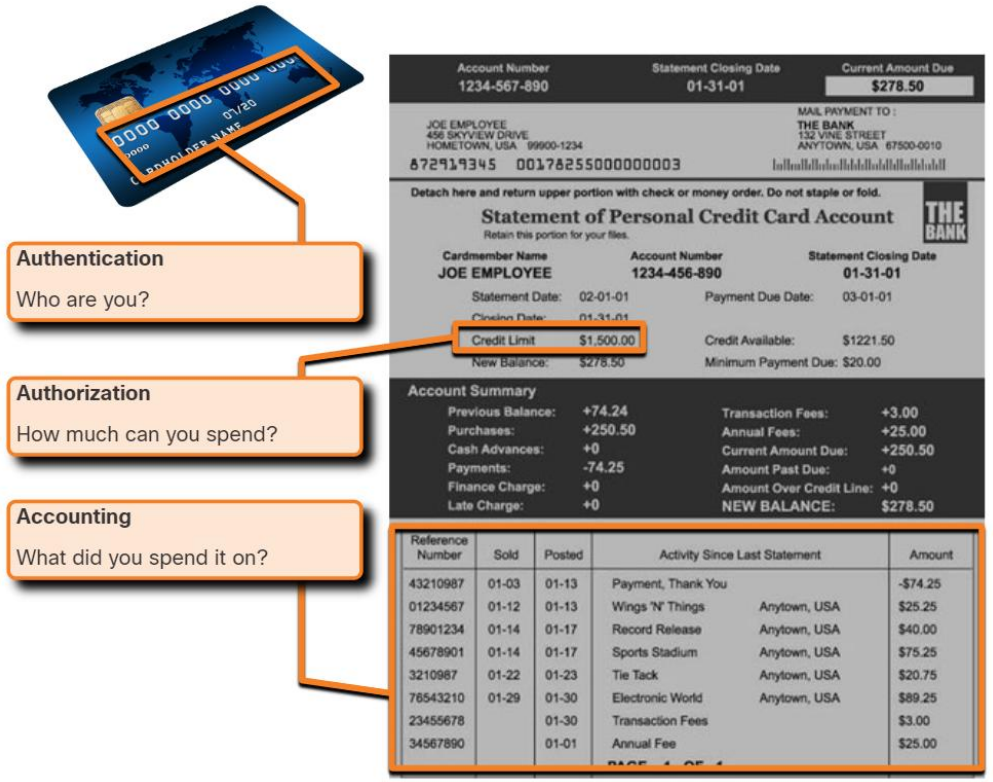
Čo nás čaká ...

- Úvod do autentifikácie a autorizácie
- Faktory autentifikácie
- Mechanizmy autentifikácie
- **Autorizácia a kontrola prístupu**
- Implementácia a technológie

Úvod a rámec AAA

AAA: Prehľad a komponenty

- AAA = rámec pre **Autentifikáciu, Autorizáciu a Účtovanie**
  - V sieťach sa používa ako základ pre **riadenie prístupu** (Access Control)
  - **A**uthentication - Autentifikácia – *Kto si?*
    - Overenie identity
    - Faktory: niečo čo viem / mám / som / robím
    - MFA ako štandard (heslo + token/sms/biometria)
  - **A**uthorization - Autorizácia - *Čo môžeš robiť?*
    - Práva na zdroje podľa roly, atribútov alebo vlastníctva
  - **A**ccounting (Auditing/Účtovanie) - *Čo si urobil?*
    - Evidencia a zodpovednosť
    - Kto čo spravil, kedy, kde a prečo
  - Účel AAA:
    - **Kto** sa môže pripojiť (admini, používatelia, partneri)
    - **Kedy** majú prístup
    - **Čo** môžu vykonávať



AAA Lifecycle: Authentication → Authorization → Accounting

- V sieťovej praxi dva rozmery AAA:
  - **Sieťový prístup** - kto smie vstúpiť do siete (používateľ, zariadenie)
  - **Administrátorský prístup** – kto smie spravovať zariadenia a aké príkazy môže používať

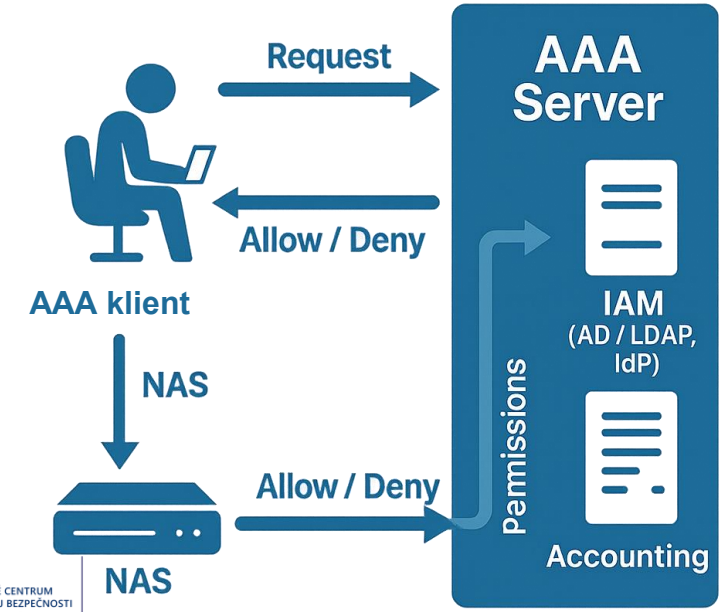
- **Lifecycle**
  - **Authentication (Autentifikácia)**
    - Overenie identity používateľa alebo zariadenia
    - Faktory: heslo, token, certifikát, biometria
    - Výsledok = dôveryhodná identita
  - **Authorization (Autorizácia)**
    - Rozhodnutie, čo môže identita vykonať
    - Priradenie práv (exec, konfigurácia, VLAN, prístup k zdrojom)
    - Realizované
      - Lokálne
      - Remote - cez AAA server (RADIUS AV-pairs, TACACS+ policies)
  - **Accounting (Účtovanie)**
    - Logovanie aktivít: kto, čo, kedy, odkiaľ
    - Záznamy pre audit, compliance a troubleshooting
    - Podpora fakturácie (ISP, telco prostredia)
  - **Lifecycle ako celok:**
    - „Kto si?“ → „Čo smieš robiť?“ → „Čo si vykonal?“
    - AAA uzatvára bezpečnostnú slučku od identity po audit.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra AAA - Základné komponenty a tok

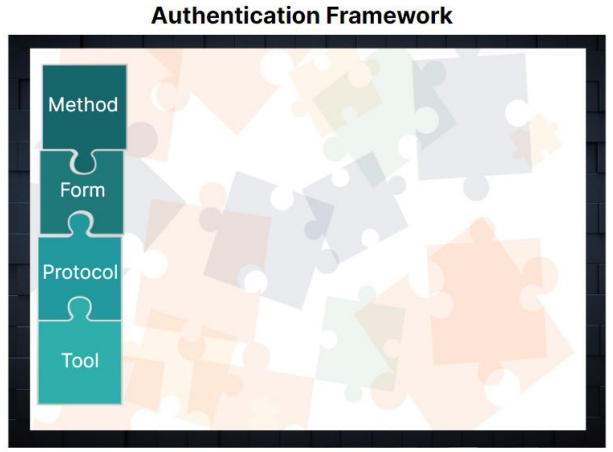
- **Architektúra AAA**
  - Umožňuje centralizované riadenie prístupu
  - Politiky na jednom mieste
  - Vynucované vo všetkých NAS zariadeniach
- **Základné komponenty**
  - **AAA Klient**
    - Proces v NAS sprostredkujúci komunikáciu používateľa s AAA serverom
  - **Network Access Server (NAS)**
    - Zariadenie prijímajúce žiadosť o pripojenie (switch, router, firewall, VPN gateway, WLC)
    - Policy Enforcement Point – PEP (vynucuje rozhodnutie)
  - **AAA Server**
    - Centrálny systém na autentizáciu, autorizáciu a accounting
      - RADIUS/TACACS+ server,
      - napr. Cisco ISE, FreeRADIUS, Microsoft NPS
    - Policy Decision Point – PDP (rozhoduje o prístupe)

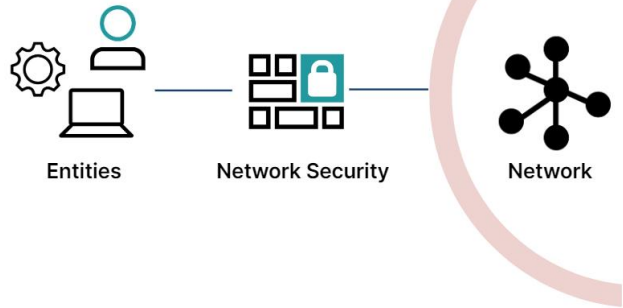
- **Tok komunikácie**
  - Používateľ sa prihlási na NAS
    → NAS pošle požiadavku na AAA server
    → server overí identitu voči IAM (AD/LDAP, IdP)
    → povolenie/odmietnutie + pridelenie oprávnení
  - Všetky akcie sa logujú pre accounting (audity, reporting).



AAA v autentifikačnom frameworku

- **Autentifikačný framework**
  - Schéma na overovanie identít (používateľov/aplikácií) v systéme
  - AAA je jeho súčasťou, jadrom – poskytuje mechanizmy a protokoly
- **Obsahuje**
  - **Metódy -** konkrétne spôsoby overenia
    - Spôsoby autentizácie: Heslá, biometria, tokeny – HW/SW; protokoly ako PPP PAP/CHAP, EAP-TLS
  - **Formy -** ako sú metódy implementované
    - Implementácie autentifikačných metód: SFA, 2FA, MFA, certifikáty, username
  - **Protokoly -** prenos a správa identít
    - RADIUS, TACACS+, Kerberos, LDAP
  - **Nástroje** - riešenia
    - Softvérové riešenia (IAM/IMS, SSO, MFA; frameworky ako **802.1X,** EAP, ISE, FreeRadius, MS NPS)





Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY

AAA a Identity Aaccess Management (IAM)

- ***IAM***
  - ***Proces*** (systém, technológia a politika)
  - Zabezpečuje:
    - správu digitálnych identít v celom životnom cykle
    - riadenie prístupu k systémom, dátam a službám,
    - overovanie a vynucovanie oprávnení používateľov a zariadení
- **AAA**
  - Podmnožina / komponent v rámci IAM
  - Technická implementácia IAM princípov v sieťach a infraštruktúre
    - Overovanie, povoľovanie a sledovanie prístupu **v sieťovom kontexte**
    - Zabezpečuje centrálne riadenie prístupu k zariadeniam alebo sieti
    - Autentifikácia:
      - Využíva identitu z IAM IdP (napr. Active Directory, LDAP, Azure AD)
    - Autorizácia
      - Aplikuje IAM politiky – priradí práva podľa role (RBAC) na prístup k CLI
    - Účtovanie
      - Zaznamenáva všetky prístupy a akcie

- *IAM definuje čo by malo platiť, AAA zabezpečí že sa to naozaj vynúti v reálnej sieti*

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA v bezpečnostných štandardoch

- **NIST SP 800-53 (USA)**
  - Kontrolné rodiny:
    - AC (Access Control) – pravidlá prístupu k zdrojom
    - IA (Identification & Authentication) – overenie identít
    - AU (Audit and Accountability) – záznamy aktivít
  - AAA je jadrom týchto kontrol – zabezpečuje identitu, oprávnenia a audit
- **ISO/IEC 27001 (globálny štandard)**
  - A.9 Riadenie prístupu – politiky, autentifikácia, autorizácia
  - A.12 Prevádzková bezpečnosť – monitoring a logovanie
  - AAA pomáha plniť požiadavky na kontrolu a audit prístupu
- **CISSP Common Body of Knowledge (CBK)**
  - AAA = základná téma v doméne „Security and Risk Management“ a „Identity and Access Management“
  - Kľúčový koncept pre bezpečnosť sietí a compliance
- **ENISA odporúčania (EÚ)**
  - AAA súčasť Zero Trust Architecture – vždy overuj používateľa, zariadenie a aktivitu
  - Dôraz na integráciu s IAM a monitoring

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autentifikácia

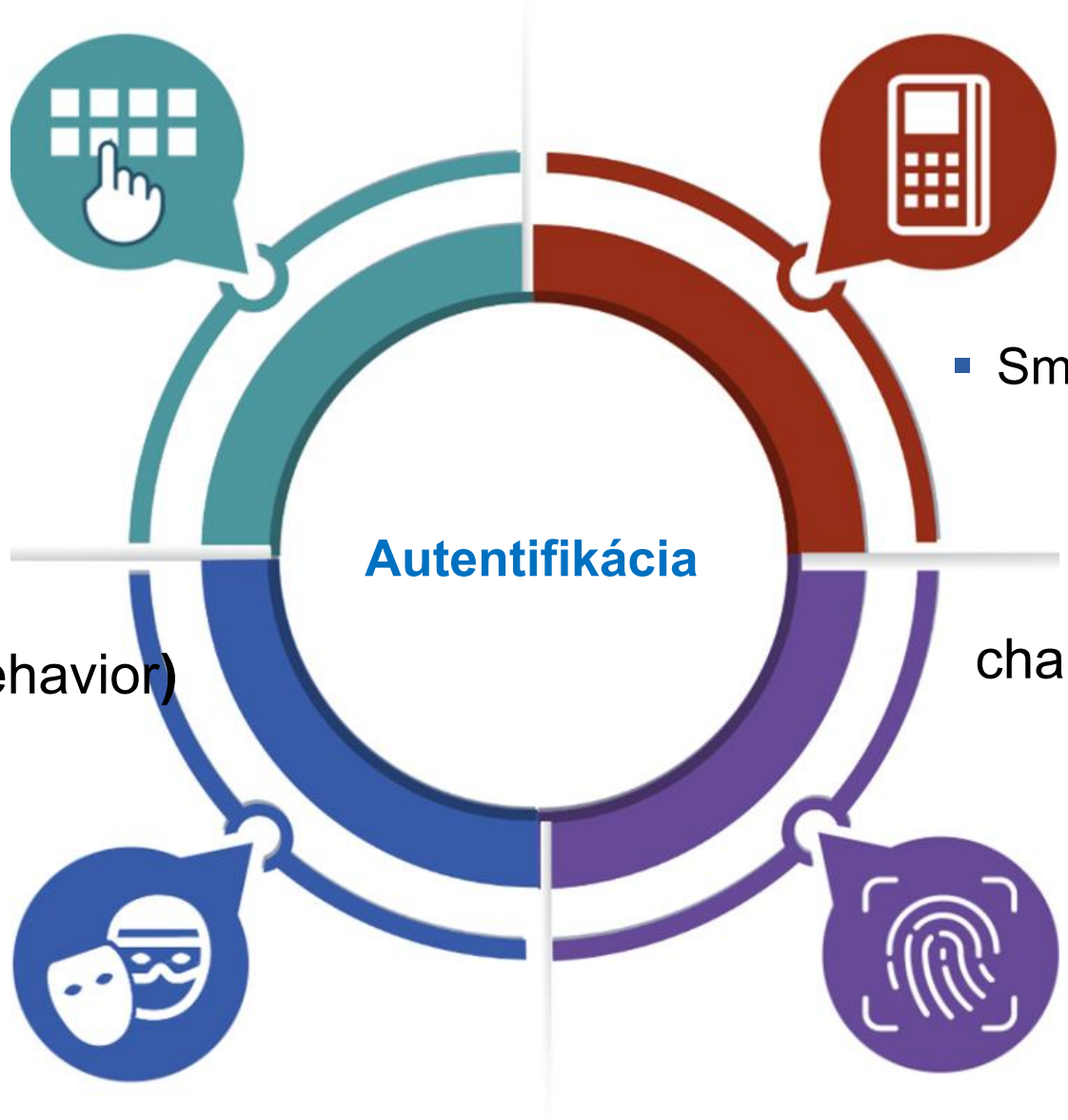
Autentifikácia

- **Autentifikácia** = proces overenia identity používateľa alebo zariadenia
  - Cieľ: potvrdiť, že entita je tým, za koho sa vydáva
  - Pozostáva
    - **Identifikácia** (identification, identity proofing)
      - Procedúra kde používateľ/systém alebo entita prezentuje svoju totožnosť
      - napr. meno, ID, email
    - **Verifikácia** (verification) alebo autentizácia
      - Proces overenia totožnosti používateľa (Potvrdenie dôveryhodnosti Identity)
      - Zadaním napr. hesla alebo kódu zo SMS
- **Úloha -** Prvý krok v AAA
  - Bez úspešnej AuthN nasleduje odmietnutie
- **Realizácia autentifikácie**
  - Na základe jedného alebo viacerých faktorov (čo viem / mám / som / robím)
- **Výsledok**
  - Dôveryhodná identita, ktorú možno ďalej použiť na autorizáciu a účtovanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Metódy autentifikácie

- **Niečo, čo viem len ja** (tajomstvo) **- KBA**
  - PIN
  - Heslo
  - Fráza
  - Kód
  - Jednorazové heslo
  - ...
- **Niečo, čo robím** (čo ma charakterizuje - behavior)
  - Ako rozprávam
  - Ako píšem na klávesnici
  - Pohyb myšou
  - Rukopis ...



- **Niečo, čo mám / vlastním**
  - Mobil, SMS
  - Pamäťová karta (s chipom) + reader (i.e. banková karta)
  - Smart karta (napr. NFC karty)
  - OTP token
  - ...
- **Niečo, čo som** (moja jedinečná charakteristika - biometrika)
  - Odtlačok prsta
  - Sken sietnice
  - Sken tváre
  - Veľkosť prsta/dlane
  - ....

Autentifikácia založená na znalosti (Something You Know)

- **Definícia:**
  - Autentifikačné metódy založené na **tajnej informácii, ktorú pozná iba používateľ**
- **Metódy**
  - **Heslá (passwords)**
    - Reťazec znakov, ktorý pozná len používateľ
    - Najčastejšia metóda, ale zároveň najzraniteľnejšia
  - **Prístupové frázy (passphrases)**
    - Dlhší a zmysluplný text (napr. „RánoPijemZelenýČaj“)
    - Ľahšie zapamätateľný / ťažšie uhádnuteľný
  - **PIN kódy**
    - Krátky číselný kód
    - Používaný v mobiloch, bankomatoch alebo smart kartách
  - **Kognitívne otázky (cognitive passwords)**
    - Otázky na osobnú históriu používateľa (napr. „meno prvého psa“)
    - Používajú sa najmä pri obnove hesla alebo pri nepravidelnom prístupe
  - **CAPTCHA** (na odlíšenie človeka od robota)
    - Obrázkový alebo textový test na odlíšenie človeka od robota
      - Nie je primárna metóda, ale doplnková forma overenia identity
- **Nevýhody autentifikácie založenej na znalosti**
  - 🔓 **Slabé alebo predvídateľné heslá** (napr. „123456“, „admin“)
  - 🔁 **Zdieľanie alebo opakované používanie** hesiel medzi službami
  - 📋 **Zapisovanie hesiel** kvôli zlej zapamätateľnosti (najmä zložitých hesiel)
  - 🎣 **Zraniteľnosť voči phishingu, shoulder surfing a social engineeringu**
  - 🕵️ **Statické údaje – raz kompromitované → trvalo ohrozené**
  - 🧠 **Používatelia si často neuvedomujú riziká a zanedbávajú hygienu hesiel**

Koncept hesiel – Best practise

- **Politika zloženia hesiel**
  - Min. 8-10 znakov (odporúčané), kombinácia znakov
  - Rotácia len pri podozrení z kompromitácie (NIST SP 800-63B)
  - Max/min vek hesla, zákaz opätovného použitia
- **Zakázanie slabých alebo kompromitovaných hesiel**
  - Kontrola proti známym databázam (HaveIBeenPwned, wordlisty)
  - NIST: rotácia len pri podozrení z kompromitácie
- **Ochranné mechanizmy**
  - Account Lockout: po 3–5 chybách dočasná blokácia
  - Session Timeout / Inactivity logout
  - AAA Accouting - Logovanie pokusov o prihlásenie – dátum, čas, user ID, zariadenie
- **Vzdelávanie používateľov a adminov**
  - Bezpečné používanie hesiel, phishing awareness
- **Cisco „Gold config“**
  - Zakázať plaintext heslá (no service password-recovery, kde je vhodné)
  - Povoliť len bezpečné prístupy (SSHv2, žiadny Telnet)
  - Centrálne AAA (RADIUS/TACACS+) → vyhnúť sa lokálnym účtom
- FINAL => **Vyhýbaj sa zbytočne zložitým politikám a pravidlám**
  - Začnú sa hľadať cesty na obchádzanie
  - Rovnováha medzi **bezpečnosťou** a **použiteľnosťou**

Niečo, čo mám / vlastním (Something You Own)

- **Definícia**
  - Založené na **vlastníctve objektu** – fyzický alebo logický dôkaz identity
- **Metódy**
  - **OTP (One-Time Password)**
    - Jednorazový kód generovaný zariadením alebo
      - Google / MS authenticator, SMS kód, atď.
    - Použitie: VPN prístup (AnyConnect, SSL/IPsec VPN), privilegovaný admin login
    - Výhoda: odolné voči replay útokom, phishing sťaženejší
  - **Smart karty a bezpečnostné kľúče**
    - Karty s čipom alebo USB kľúče \
      - Obsahujú **privátny kľúč** a kryptomodul (napr. YubiKey / FIDO2)
    - Uchovávajú privátny kľúč, autentifikácia cez PIN alebo challenge–response
    - V sieťach: použitie s 802.1X (EAP-TLS), VPN, prístup na zariadenia
  - **Hardvérové tokeny (NFC/RFID, fobs)**
    - Klientske zariadenia, ktoré generujú alebo prenášajú kód
    - Typicky doplnok k heslu (2FA) – login do AAA servera (RADIUS/TACACS)

HW autentifikácia

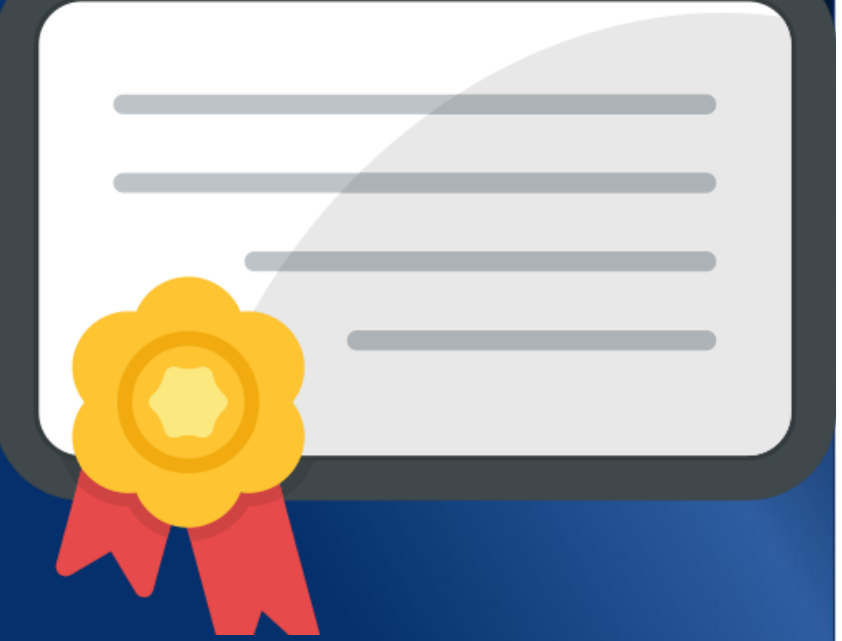
- Klasický **druhý faktor** – používajú sa tam, kde je potrebná vyššia úroveň bezpečnosti než heslá
  - V praxi => najčastejšie sa viažu na **VPN a admin prístupy**.
- **Výhody:**
  - Silnejšie než len použitie hesla (2FA)
  - Odolnosť voči phishingu (najmä OTP)
  - Možnosť offline generovania OTP
  - Hardvérové tokeny – vyššia fyzická bezpečnosť

- **Nevýhody:**
  - Riziko straty, krádeže alebo poškodenia tokenu
  - Softvérové OTP môžu byť zneužité pri kompromitovanom zar
  - Potreba synchronizácie (synchronné tokeny)
  - Náklady na infraštruktúru (napr. čítačky kariet, správa PKI)
  - Falošné čítačky – *skimming* (napr. pri kartách)

- **AAA súvislosť**
  - AAA server (RADIUS/ISE) integruje OTP/MFA riešenia → pridáva faktor k heslu
  - Politiky umožňujú: admin login vyžaduje heslo + OTP, bežný user len heslo

Best Practice pre HW tokeny a bezpečnostné kľúče

- **Použitie HW tokenov (OTP/TOTP/HOTP)**
  - Vhodné pre **VPN prístupy** (AnyConnect, SSL/IPsec) a **privilegovaný admin prístup** na sieťové zariadenia
  - Integrácia cez AAA server (RADIUS/TACACS+) → politika „heslo + OTP“
- **Smart karty / USB kľúče (YubiKey, CAC, PIV)**
  - Obsahujú **privátny kľúč** a kryptomodul (FIDO2, PKCS#11, PIV štandardy)
  - Podpora pre **EAP-TLS (802.1X)** a **IKEv2/IPsec VPN**
  - Chránia pred phishingom a replay útokmi
- **Cisco best practice**
  - Nasadzovať HW tokeny pre **vysoko privilegovaných používateľov** (admini, root access)
  - Používať AAA integráciu – Cisco ISE/ACS + RSA SecureID, Duo, YubiKey
  - Politiky viazať na role (admin login vyžaduje token, bežný user nie)
- **Prevádzkové zásady**
  - Token musí byť **vždy v držbe používateľa** – never share!
  - Nastaviť životnosť OTP kódov (30–60 sekúnd TOTP)
  - Vynucovať ochranu PIN-om (smart karty, USB kľúče)
  - Centrálne monitorovať stratu/odcudzenie tokenu → okamžitá deaktivácia
- **Výhody**
  - Silná ochrana proti krádeži hesiel (phishing, keylogging)
  - Bezpečná integrácia s AAA (RADIUS Challenge/Response)
- **Nevýhody**
  - Náklady na HW + správu tokenov
  - Logistika distribúcie a správy (obnova pri strate)



Certifikáty v sieťovej autentifikácii

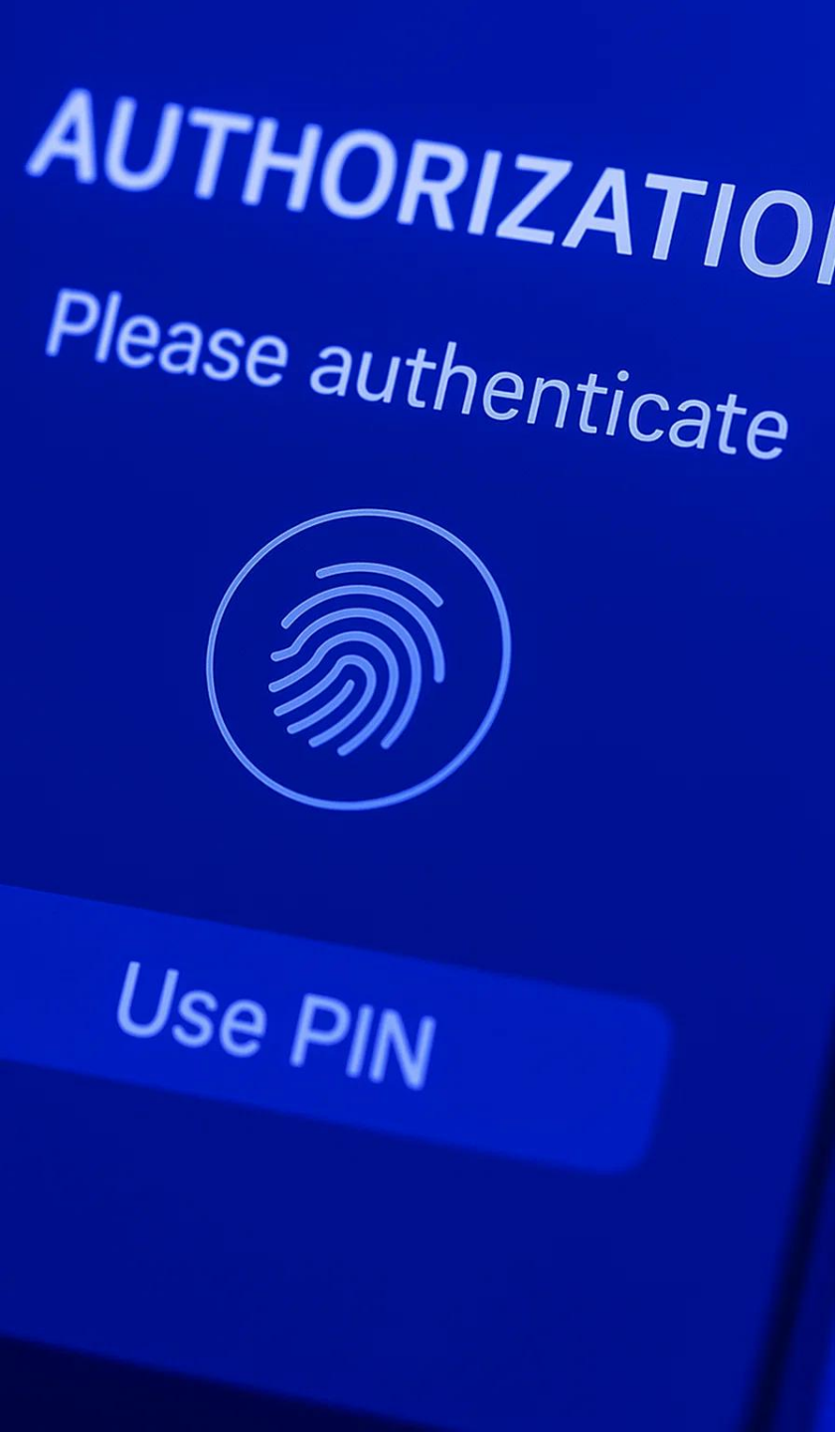
- **Certifikáty**
  - Digitálny certifikát = kryptografický dôkaz identity (X.509 štandard)
  - Vydaný certifikačnou autoritou (CA), viaže identitu na verejný kľúč
  - Zlatý štandard pre sieťovú autentifikáciu
- **Použitie v sieťach**
  - **802.1X / EAP-TLS** – klientsky certifikát overuje zariadenie/používateľa
  - **VPN (IKEv2, SSL/TLS)** – obojstranná autentifikácia klient/server
  - **Zariadenia** – autentifikácia sieťových prvkov (switch, router, firewall, AP)
  - **IoT a priemyselné siete** – identita zariadení zabezpečená certifikátom
- **Princíp fungovania**
  - Privátny kľúč uložený na klientovi (TPM/HSM)
  - Overenie identity prebieha kryptografickým podpisom a validáciou CA reťazca
  - Podpora revokácie cez CRL/OCSP
- **Výhody**
  - Silná ochrana pred phishingom a MITM útokmi
  - Integrácia s AAA (RADIUS + EAP-TLS, ISE/ACS)
  - Vysoká úroveň dôveryhodnosti pri autentifikácii
  - Najvyššia úroveň bezpečnosti (EAP-TLS je odolný proti phishingu a MITM)
- **Nevýhody**
  - Potreba správy PKI (životný cyklus certifikátov)
  - Zložitejšia administrácia a distribúcia
  - Vyššia komplexita pre používateľov a admino

Best Practice pre certifikáty v sieťovej autentifikácii

- **Cisco best practice**
  - Vždy používať **silné algoritmy** – RSA ≥ 2048 bit, alebo ECDSA P-256/P-384
  - Nastaviť **maximálnu dobu platnosti** certifikátu (≤ 1–2 roky)
  - Automatizovať vydávanie/obnovu cez **SCEP/EST alebo certifikačný agent (ISE, MS ADCS)**
  - Validovať certifikáty voči CRL/OCSP → zabrániť používaniu zrušených certifikátov
  - Používať **separačné CA pre infra** a oddeliť internú CA od verejnej
- **Prevádzkové zásady**
  - Uchovávať privátne kľúče v **HSM alebo TPM** (nie v plaintext súboroch)
  - Používať unikátne certifikáty pre každé zariadenie a používateľa
  - Segmentovať PKI hierarchiu (Root CA offline, Subordinate online)
  - Implementovať proces revokácie (CRL publikácia, OCSP responder)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autorizácia



Autorizácia

- **Autorizácia**
  - **Autentifikácia (Kto?) ≠ Autorizácia (Čo?)**
    - Autorizácia => **vykonáva sa po úspešnej autentifikácii**
  - Rozhoduje, či má ***overená entita*** (používateľ, systém, služba) ***právo (oprávnenie, povolenie)*** vykonať určitú akciu nad daným zdrojom
    - Kto => môže robiť Čo, Kde a Kedy?
    - Určuje tzv. prístupové práva po overení identity
- **Cieľ autorizácie**
  - Obmedziť prístup len na nevyhnutné funkcie (least privilege)
  - Znížiť riziká z nadmerných alebo nesprávne pridelených práv
- **Praktický príklad**
  - Junior Admin sa prihlási cez SSH (AuthN = meno/heslo)
  - TACACS+ určí, že môže spúšťať len príkazy „show“ (AuthZ)

Mechanizmy autorizácie v sieťach (a sieť. zariadeniach)

- **AAA kontext**
  - AuthZ rozhodnutie vydáva AAA server (RADIUS, TACACS+)
  - Enforcement vykonáva sieťové zariadenie (NAS, switch, firewall, WLC)
- Mechanizmy
  - **RADIUS Attributes / AV-Pairs**
    - Určujú, **aké oprávnenia alebo parametre** má mať užívateľ po úspešnej autentifikácii
      - VLAN assignment, ACL, QoS parametre
      - Použitie pri 802.1X (užívateľ po AuthN dostane VLAN alebo ACL
      - `cisco-avpair = "attribute=value" (napr. shell:priv-lvl=15)`
  - **TACACS+ Command Authorization**
    - Jemnozrnná kontrola príkazov na zariadení
    - Admin A: povolené len „show“ príkazy
    - Admin B: povolené aj „configure“ príkazy
    - Vhodné pre správu routerov, switchov, firewallov
- Autorizačné modely, hlavne
  - **RBAC (Role-Based Access Control)**
    - Oprávnenia podľa roly → admin, operator, guest
      - WiFi, prístup k CLI
    - Jednoduché, ale menej flexibilné
    - Najrozšírenejší model (jednoduchý na správu)
  - **ABAC (Attribute-Based Access Control)**
    - Prístup na základe atribútov: čas, miesto, typ zariadenia, skupina používateľov
    - Príklad: partner má prístup len z VPN, len v pracovnom čase
    - Väčšia flexibilita ako RBAC, napr. Firewall policy či pre Zero Trust
- Iné
  - RuleBAC, PolicyDAC ...

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autorizácia

Odporúčania a osvedčené postupy (Best practise)

- **Pravidlo najnižších oprávnení (Least privilege)**
  - Udeľovať iba minimálne nevyhnutné oprávnenia potrebné na vykonanie úloh
  - Zabraňuje prideleniu rozsiahlych oprávnení a hrozbám
- **Pravidelná revízia prístupových práv**
  - Detekcia nadbytočných a neaktuálnych práv (napr. po zmene roly)
- **Pravidelná kontrola a aktualizácia prístupových politík**
  - Reaguje na zmeny v rolách, štruktúre organizácie, systémoch
- **Segregácia právomocí (Separation of Duties)**
  - Prevencia kolúzie a neoprávnenej eskalácie práv
  - Napr. schvaľovanie vs. vykonávanie transakcií
- **Časovo obmedzené práva (Just-in-Time access)**
  - Práva udeľované na obmedzený čas (napr. incident response, support)
- **Kritické prístupy chrániť pomocou MFA**
  - Kombinácia faktorov (napr. heslo + token) na silnejšie overenie
- **Command-level Authorization (Cisco TACACS+)**
  - Best practice je nepovoľovať všetkým adminom príkazy **conf t**
- **Zero Trust Access**
  - Autorizácia už nie je len o role → ale aj **o kontexte** (device posture, geolokácia, čas

Accounting / Audit a loging

Audit a logging (Accounting)

- **Audit (Accounting / Accountability)**
  - Systematické zaznamenávanie relevantných aktivít používateľov a adminov
  - Poskytuje spätnú stopu pre audit, compliance a troubleshooting
    - Kto, kedy, čo robil a s akým výsledkom
- Účel logovania a auditovania
  - **Operatíva**
    - Výkonový baseline a odchýlky
  - **Trasovanie**
    - Čo sa dialo v systéme
  - **Zodpovednosť**
    - Transparentnosť operácií a možnosť priradiť akcie konkrétnym identitám.
  - **Forenzná analýza**
    - Rekonštrukcia incidentov (kto čo spravil pred únikom dát)
  - **Detekcia anomálií, incidentov a poručení politík**
    - Identifikácia podozrivého správania (napr. neobvyklé prihlásenia, prístupy)
- **AAA súvislosť**
  - **RADIUS / TACACS+ Accounting** – start/end session, spustený príkaz (command=show run)
  - Logy sa ukladajú centrálne (AAA server, SIEM, syslog)

%LINK-3 UPDOWN: Interface FastE

Čo sa loguje v sieťových systémoch?

- **Operatívne logy (Operational Logs)**
  - Zamerané na spoľahlivosť, výkon a prevádzku infraštruktúry.
  - **Syslog správy**
    - Udalosti zo sieťových zariadení (link up/down, port error, restart)
    - Stavové hlásenia protokolov (OSPF, BGP, DHCP, DNS, SNMP)
    - Varovania a chyby (CRC errors, interface drops, congestion)
  - **Prevádzkové ukazovatele**
    - CPU, RAM, využitie portov, disková kapacita
    - Latencia, jitter, packet loss – základ pre SLA a QoS monitoring
    - SNMP traps, NetFlow/IPFIX záznamy, telemetria
  - **Systémové udalosti**
    - Reštart, upgrade firmware, reload zariadenia
    - Inštalácia alebo zmena konfigurácie služby / modulu
    - Hardvérové zlyhania (ventilátor, PSU, teploty)
- **Bezpečnostné logy (Security Logs)**
  - Slúžia na detekciu, vyšetrovanie a prevenciu incidentov.
  - **Autentifikácia a prístup**
    - Úspešné / neúspešné login pokusy (meno, IP, čas)
    - Viacnásobné zlyhania – indikácia brute-force
    - Zmeny oprávnení, role, account lockouts
  - **Autorizácia a účtovanie (AAA)**
    - Každý vykonaný príkaz (exec/config) pre audit a troubleshooting
    - VPN/Wi-Fi relácie – používateľ, IP, pridelený VLAN
  - **Incidenty a anomálie**
    - Prístupy z neštandardných lokalít / časov (anomaly detection)
    - IDS/IPS alerts – signature matches, policy violation
    - Neautorizované zmeny v konfigurácii alebo politike ACL

Čo obsahujú auditné záznamy ?

- Musí obsahovať **kto, čo, kedy, kde a s akým výsledkom**
  - **Časové údaje**
    - Presný čas udalosti (login, logout, command)
    - Dĺžka trvania relácie
  - **Identifikáciu používateľa alebo účtu**
    - Username / User ID (z AAA servera)
    - Zdrojová IP/MAC adresa klienta
  - **Identifikáciu zariadenia**
    - NAS (switch, WLC, VPN gateway), hostname, IP adresa zariadenia
    - Session ID alebo číslo portu
  - **Akciu alebo udalosť**
    - Príkazy spustené adminom (pri TACACS+)
    - Zmena konfigurácie alebo role
    - Prístup k zdroju, začiatok a koniec session
  - **Výsledok akcie**
    - Success / Fail (napr. login OK alebo neúspešný pokus)
    - Odmietnutý príkaz alebo zamietnutý prístup
  - **Bezpečnostný kontext**
    - Použitá autentifikačná metóda (heslo, OTP, certifikát)
    - VLAN assignment, ACL, dACL aplikovaná cez RADIUS AV-Pair

Best practise

Osvedčené postupy

- **Logovanie všetkých pokusov o prístup** – aj zamietnutých
  - Mal by trackovať „ideálne“ všetky aktivity (všetko čo sa deje)
- **Integrácia s časovou synchronizáciou (NTP/PTP)**
  - Bez správneho času sú logy nepoužiteľné pri forenznej analýze
  - Cisco odporúča všade NTP + časová zóna UTC + auth
- **AAA logy vždy centralizovať**
  - Neponechávať iba na zariadení (buffer limited)
  - **Centralizovať do špecializovaného nástroja**
    - **Logstash/Elasticsearch + Kibana (ELK stack)**
    - **Graylog** (open-source, s web UI)
    - **Splunk, IBM QRadar, ArcSight** (komerčné SIEM)
- **Bezpečné ukladanie logov**
  - Immutable, hashované
  - Zabezpečená komunikácia
- **Retencia a archív logov**
  - Minimálne 90 dní pre prevádzkové účely, 1 rok pre bezpečnostné/compliance účely
  - ISO 27001 a GDPR môžu mať špecifické požiadavky
- **Pravidelný review logov + alertovanie**:
  - Prístup mimo pracovných hodín
  - Zmeny práv administrátora
  - Vysoký počet pokusov o prihlásenie

- **Nevýhoda**
  - Big data: Ak logujem všetko
    - => zahltenie dátami
- Challenge
  - **Vypracovať riešenie ktoré dáva zmysel a nájsť vhodný nástroj**
    - Napr. zadanie zlého hesla
      - Potrebujem vedieť o všetkých zle zadaných heslách všetkými používateľmi?
      - Alebo až keď jeden zadá veľa krát za sebou?
      - ==> Allerting
  - **Monitoring a korelácia**
    - Vysoký počet login pokusov → alert (možný brute-force útok)
    - Zmena práv administrátora → kritický alert
    - Session hijack / anomálie (veľký objem dát prenesený v krátkom čase)

AAA protocols

RADIUS (RFC 2865)

TACACS+ (RFC 8907)

DIAMETER (RFC 6733

AAA - protokoly a rámce

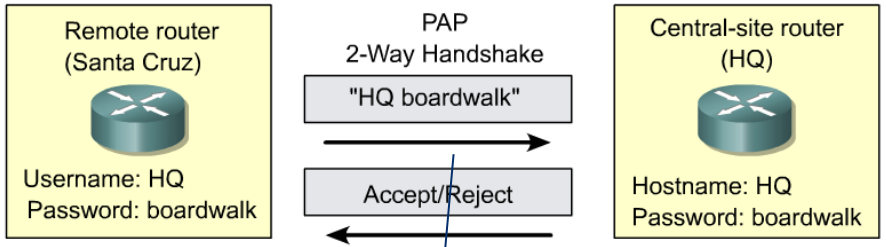
Protokoly v AAA

- **Autentifikačné protokoly**
  - Určujú, **ako** sa preukazuje totožnosť (heslo, certifikát)
  - Definujú mechanizmy na overenie identity
- Hlavné protokoly
  - **PAP (Password Authentication Protocol)** – jednoduchý, heslo v plaintext forme
  - **CHAP (Challenge Handshake Authentication Protocol)** – challenge/response, bezpečnejší než PAP
  - **Kerberos** – ticketing systém, používaný v doménach (AD, enterprise)
  - **EAP (Extensible Authentication Protocol)** – rámec pre rozšíriteľnú autentifikáciu (802.1X, Wi-Fi, VPN)
  - **LDAP** – adresárový protokol, backend pre identity (Active Directory, OpenLDAP)
- **Kategórie použitia**
  - **Jednoduché prenosy hesiel** – PAP, CHAP
  - **Doménové/enterprise prostredie** – Kerberos, LDAP
  - **Sieťový prístup (LAN, Wi-Fi, VPN)** – EAP, 802.1X

- **Transportné protokoly**
  - Prenos autentifikačných, autorizačných a accounting dát medzi zariadeniami
- Hlavné protokoly
  - **RADIUS** – UDP/1812, 1813; VPN, Wi-Fi (802.1X); šifruje len heslo
  - **TACACS+** – TCP/49; plne šifrovaný; granularita až na príkazy (admin prístupy)
  - **DIAMETER** – TCP/SCTP; nástupca RADIUS (telco, LTE/5G)

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Password Authentication Protocol (PAP)

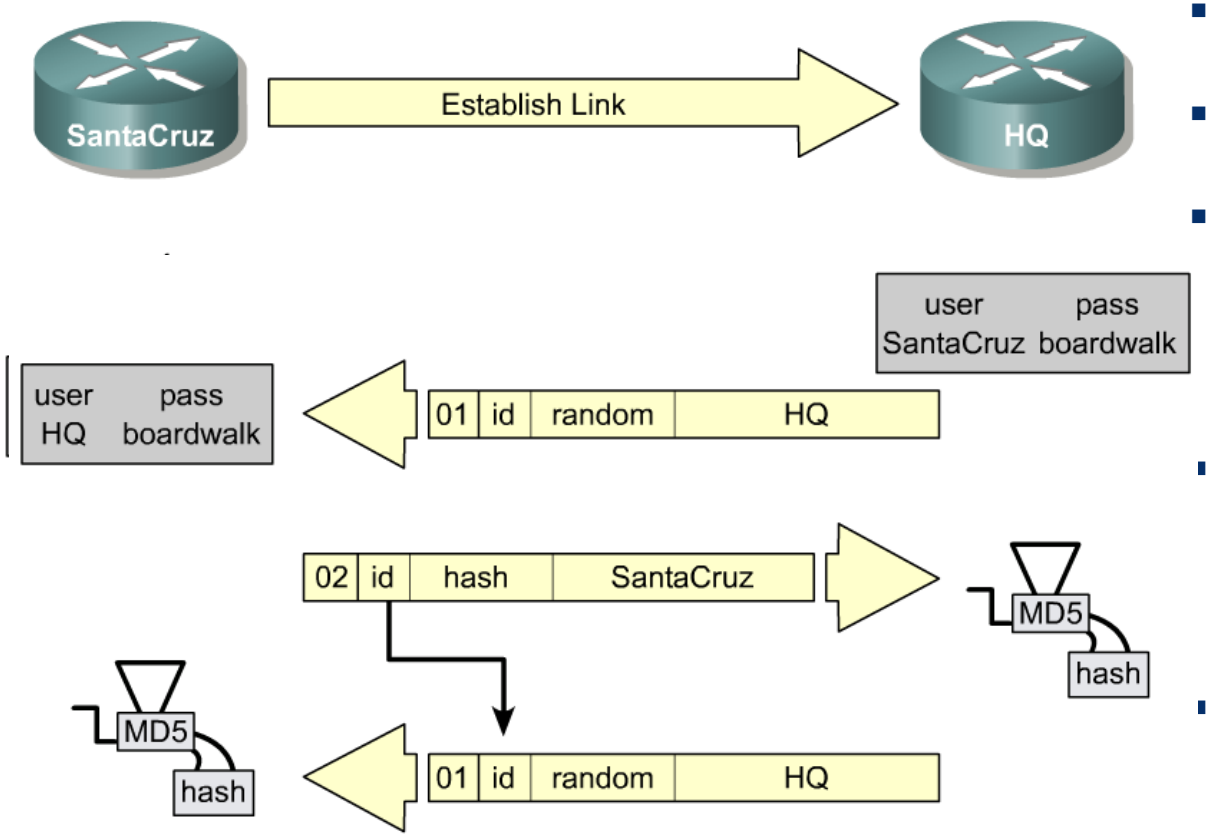


- Heslo posielané ako plaintext
- Opakovane posielané až kým druhá strana nepotvrdí = PROBLÉM (trial-and-error attacks)

- Prvý pokus o sieťovú autentifikáciu
- Najjednoduchší „two-way handshake“ autentifikačný protokol (RFC 1334)
- Klient posiela **meno a heslo v cleartexte** na server
  - Proces autentifikácie začína klient
  - Strana, ktorá požaduje preukázanie identity (ISP), toto meno a heslo overí a informuje klienta o (ne)úspechu
- **Výhody**
  - Jednoduchá implementácia
  - Podpora vo všetkých zariadeniach
- **Nevýhody / slabiny**
  - Heslo prenášané v plaintext forme → odpočúvanie = kompromitácia
  - Žiadna ochrana proti replay útokom
  - Nepodporuje viacfaktorovú autentifikáciu
- **Použitie**
  - Historické (PPP/PPPoE, dial-up)
  - Dnes už len pre testy alebo laby
  - V produkcii sa **neodporúča** – nahradený CHAP/EAP

Financované Európskou úniou NextGenerationEU PLÁ

CHAP (Challenge Handshake Authentication Protocol)



- Autentifikačný protokol založený na **challenge–response** mechanizme - *three way handshake*
- Zavedený v PPP (RFC 1994) ako bezpečnejšia alternatíva k PAP
- **Princíp fungovania**
  - Server (NAS) pošle klientovi **náhodný challenge**
  - Klient odpovie **hashom (MD5)** z challenge + hesla
  - Server overí hash porovnaním s uloženou hodnotou
  - Heslo sa nikdy neposiela v plaintext forme
- **Výhody**
  - Heslo neprechádza sieťou v cleartexte
  - Odolnejší proti odpočúvaniu než PAP
  - Challenge je náhodný → zabraňuje jednoduchému replay útoku
- **Nevýhody / slabiny**
  - Používa zastaraný **MD5 hash** (slabé proti moderným útokom)
  - Neodolný voči **dictionary/brute-force** útokom, ak heslá slabé
  - Nepodporuje moderné MFA mechanizmy
- **Použitie**
  - Historické (PPP, staršie dial-up, niektoré DSL/ISDN)
  - Dnes už prakticky nepoužívaný, nahradený EAP metódami

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY

CHAP Autentifikácia

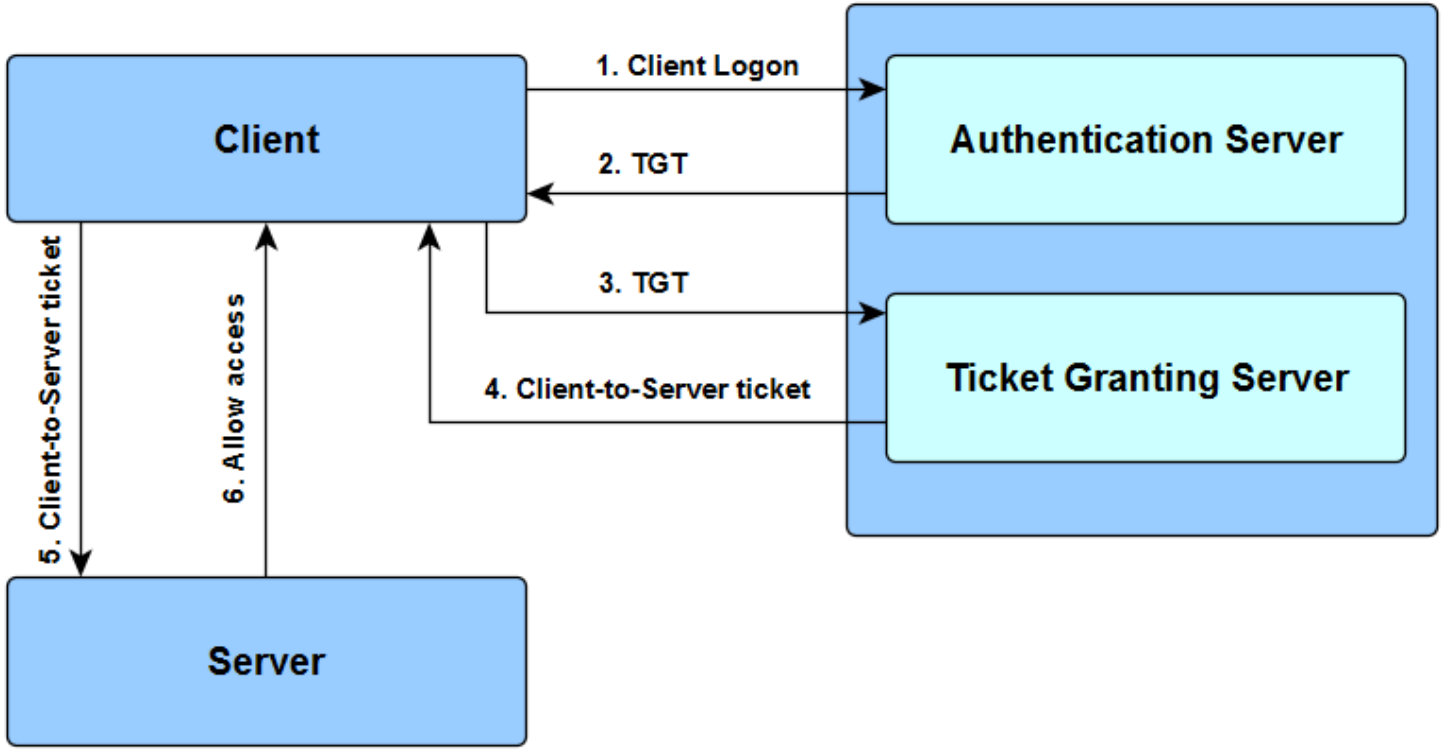
```
ca:01:9c:3a:00:08    ca:02:9e:fa:00:08    PPP CHAP    60 Challenge (NAME='ISP', VALUE=0x7fe39ba70da9310da5e9ad0ab5e644f6)
ca:02:9e:fa:00:08    ca:01:9c:3a:00:08    PPP CHAP    60 Response (NAME='Pouzivatel_1', VALUE=0x558b4db060c579457d03d0208d2d8fd1)
ca:01:9c:3a:00:08    ca:02:9e:fa:00:08    PPP CHAP    60 Success (MESSAGE='')
```

```
▾ PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0002
    Payload Length: 26
▾ Point-to-Point Protocol
    Protocol: Challenge Handshake Authentication Protocol (0xc223)
▾ PPP Challenge Handshake Authentication Protocol
    Code: Challenge (1)
    Identifier: 1
    Length: 24
  ▾ Data
      Value Size: 16
      Value: 7fe39ba70da9310da5e9ad0ab5e644f6
      Name: ISP
```

```
▸ PPP-over-Ethernet Session
▸ Point-to-Point Protocol
▾ PPP Challenge Handshake Authentication Protocol
    Code: Response (2)
    Identifier: 1
    Length: 33
  ▾ Data
      Value Size: 16
      Value: 558b4db060c579457d03d0208d2d8fd1
      Name: Pouzivatel_1
```

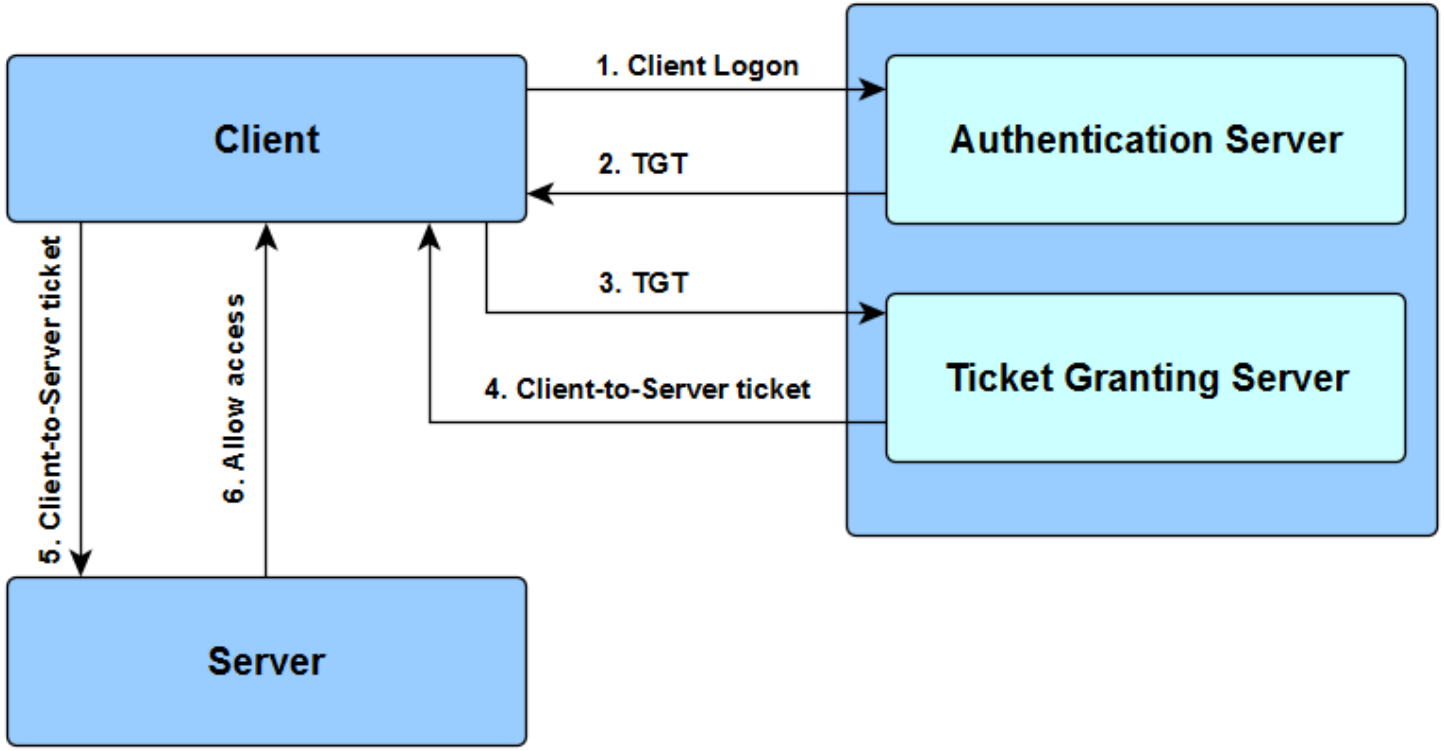
```
▸ PPP-over-Ethernet Session
▸ Point-to-Point Protocol
▾ PPP Challenge Handshake Authentication Protocol
    Code: Success (3)
    Identifier: 1
    Length: 4
```

Kerberos: Prehľad



- Sieťový autentifikačný protokol K/S založený na systéme **ticketov**
- Vyvinutý na MIT (projekt Athena), štandardizovaný (RFC 4120)
- Používa symetrické šifrovanie (zdieľané tajomstvá) na poskytnutie bezpečnej autentifikácie
- Základ pre sieťové SSO (infra, nie aplikácie)
- Architektúra
  - **Klient**: Užívateľ alebo služba, ktorá žiada o prístup
  - **Server služby:** Prostriedok, ku ktorému sa klient chce dostať (napr. súborové úložisko, mail server)
  - **KDC** (Key Distribution Center) – centrálna autorita (napr. MicroSoft DC)
    - **AS (Authentication Service)** – overuje totožnosť používateľa, vydáva TGT (Ticket Granting Ticket)
    - **TGS (Ticket Granting Service)** – vydáva Service Tickets pre jednotlivé služby

Kerberos



- **Login klienta**
  - Používateľ zadá meno/heslo
  - Klient žiada **AS (Authentication Server)** o TGT
  - AS overí prihlasovacie údaje a vydá **TGT (Ticket Granting Ticket)**
- **Žiadosť o službu**
  - Klient predloží TGT na **TGS (Ticket Granting Server)**
  - Požiada o prístup ku konkrétnej službe (napr. file server)
- **Service Ticket**
  - TGS vydá **Service Ticket** pre danú službu
  - Ticket obsahuje session key pre komunikáciu
- **Prístup k službe**
  - Klient sa preukáže Service Ticketom priamo službe
  - Server overí ticket (proti KDC) → prístup povolený

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kerberos

- Použitie
  - Active Directory (Windows domény) a SSO – základný autentifikačný mechanizmus
  - AAA servery (RADIUS/TACACS+) => overenie na AD/Kerberos
  - Umožňuje centrálne riadenie prístupu pre VPN, Wi-Fi (802.1X), aj administrátorsky prístup
  - Unix/Linux – integrácia do AD alebo vlastné KDC
  - Sieťové služby: NFS, SSH GSSAPI, Kerberized apps
- **Výhody**
  - Vzájomná autentifikácia
    - Klient i server navzájom preukazujú svoju totožnosť.
  - Heslá sa neprenášajú sieťou – používajú sa tikety
  - Single Sign-On (SSO) v doménovom prostredí
    - Používateľ sa prihlási raz (získa TGT) a počas životnosti tiketu má prístup ku všetkým povoleným službám
  - Škálovateľné, vhodné pre enterprise
- **Nevýhody**
  - Zložité nasadenie a správa KDC
  - Jediný bod zlyhania = KDC
  - Vyžaduje presnú časovú synchronizáciu (NTP)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

EAP (Extensible Authentication Protocol) protokol

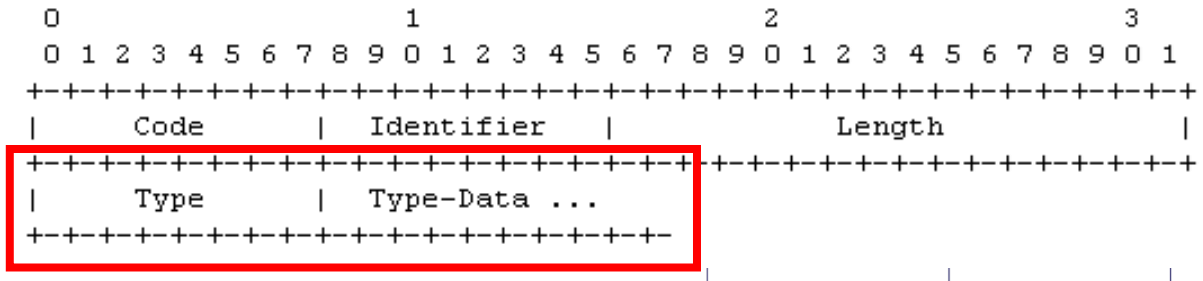
- Nie je samostatný protokol, či auth metóda
- **=>** EAP
  - **rámec pre prenos autentifikačných metód**
  - Štandardizovaný v RFC 3748
  - Flexibilita - umožňuje používanie rôznych metód autentifikácie
    - Napr. Pre WiFI či VPN
  - Funguje priamo na linkovej vrstve prostredníctvom Point-to-Point Protocol (PPP) alebo IEEE 802, bez potreby IP

- **Charakteristiky**
  - Prenáša sa cez **EAPOL (LAN/WLAN)** alebo **EAP over RADIUS**
  - Štruktúra: **Request–Response**
  - Flexibilný: desiatky štandardizovaných aj vendor metód
- **Výhody**
  - Modularita, možnosť pridávať nové metódy bez zmeny protokolu
  - Podpora silných metód (certifikáty, TLS)
- **Nevýhody**
  - Komplexita implementácie (napr. pri cert.-och)
  - Niektoré EAP metódy sú slabé (napr. EAP-MD5)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

EAP PDU

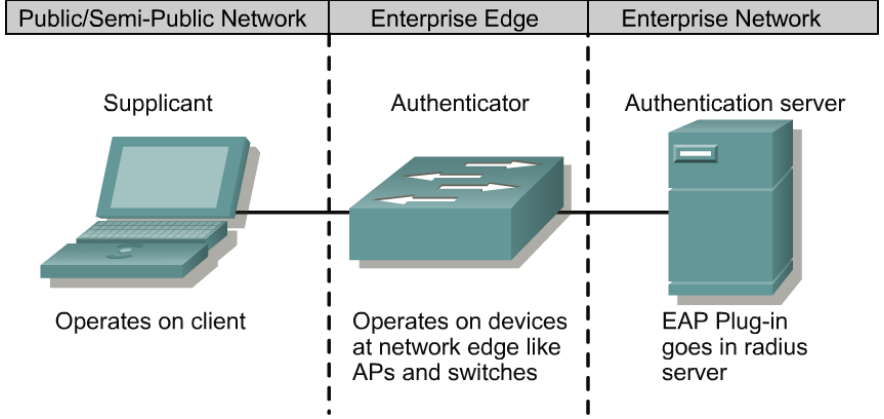
- Code – typ EAP paketu
  - 1: Request
  - 2: Response
  - 3: Success
  - 4: Failure
- Identifier - prepája žiadosti a odpovede
  - Pomáha odlišovať Žiadosti od Odpovedí
- Length – dĺžka EAP paketu
  - Zahŕňa Code, Identifier, Length, and Data.
- Data – mení sa podľa Code
  - Napr. EAP meeóda



- **Metódy EAP**
  - Konkrétne definujú, ako sa autentifikácia vykonáva v rámci EAP rámca
  - **EAP-Method** v EAP pakete - Štruktúra
    - Type
    - Type-data / EAP-Method dáta
      - Informácie súvisiace s autentifikáciou.

Type	EAP-Method
1	Identity
2	Notification
3	Nak (iba v Response pakete)
4	MD5-Challenge
5	One Time Password (OTP)
6	Generic Token Card (GTC)
13	EAP-TLS
17	EAP-Cisco Wireless/LEAP
21	EAP-TTLS
25	PEAP
43	EAP-FAST
254	Expanded Types
255	Experimental use

EAP architektúra



- **Supplicant (Žiadateľ)**
  - Softvér na strane klienta, ktorý žiada o prístup do siete
    - Koncové zariadenie: PC, notebook, mobil, IoT
  - Posiela autentifikačné údaje (heslo, certifikát)
  - Príklad: Native "Wi-Fi" nastavenia v Windows, macOS, alebo aplikácie ako Cisco AnyConnect Secure Mobility Client.
- **Authenticator (Overovateľ) (NAS / PEP)**
  - Sieťové zariadenie, ktoré kontroluje prístup do siete
  - Úloha:
    - Prenaša autentifikačné správy medzi Supplicantom a Authentication Serverom.
    - Na základe výsledku autentifikácie otvára alebo blokuje prístup k sieti (typicky zmenou VLAN alebo povolením portu).
  - Príklad: Wi-Fi prístupový bod (Access Point), switch podporujúci 802.1X, VPN koncentrátor
- **Authentication Server (Autentifikačný server) (DB / PDP)**
  - Overuje prihlasovacie údaje voči backendu (AD/Kerberos, LDAP, databáza)
  - Rozhoduje o výsledku: Access-Accept / Access-Reject.
  - Príklad: RADIUS server (napr. Cisco ISE, FreeRADIUS, Microsoft NPS) alebo TACACS+ server

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

EAP - autentifikačné protokoly / metódy

- **EAP-MD5 (Message Digest 5) - jednoduchý**
  - Používa MD5 hash hesiel
  - Nešifruje komunikáciu, menej bezpečný
  - Neodporúča sa pre citlivé aplikácie
- **EAP-TLS (Transport Layer Security) - bezpečný**
  - Poskytuje obojstrannú autentifikáciu (mutual authentication) pre zvýšenú ochranu
  - Veľmi bezpečný
  - Často používaný
    - **802.1X v LAN a WLAN (Enterprise Wi-Fi)**
    - **VPN (SSL, IKEv2)** – klientsky certifikát namiesto hesla
- **PEAP (Protected EAP)**
  - Vytvára šifrovaný TLS tunel na ochranu autentifikačných údajov (napr. hesiel) (EAP-TLS)
  - Podporuje vnútorné metódy: MS-CHAPv2
  - Autentifikuje iba na strane servera (pomocou jeho certifikátu)
  - Vhodné tam, kde certifikát klienta nie je možný
    - Enterprise Wi-Fi (WPA2/WPA3-Enterprise), VPN
- **EAP-PEAP (Protected PEAP)**
  - Kombinácia EAP a PEAP
  - Umožňuje autentifikáciu pomocou používateľského mena a hesla v chránenom režime.
- **EAP-TTLS (Tunneled Transport Layer Security)**
  - Umožňuje autentifikáciu v tunelovacom režime
  - Vyžaduje certifikát len na strane servera
  - Umožňuje tunelovanie starších autentifikačných protokolov (napr. PAP, CHAP) cez TLS.
- **EAP-FAST (Flexible Authentication via Secure Tunneling)**
  - Umožňuje rýchlu autentifikáciu v bezdrôtových sieťach
  - Používa TLS na zabezpečenie komunikácie.
  - Používa Protected Access Credential (PAC) namiesto certifikátov na rýchlu autentifikáciu
  - Vyvinuté spoločnosťou Cisco
  - Optimalizované pre efektívnosť a jednoduché nasadenie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Porovnanie EAP metód

Metóda	Mechanizmus	Výhody	Nevýhody	Použitie
EAP-TLS	Vzájomné overenie pomocou **digitálnych certifikátov**	Najvyššia bezpečnosť, odolné proti phishingu, MITM, replay	Vyžaduje PKI, náročná správa certifikátov	Enterprise Wi-Fi, VPN, Zero Trust siete
PEAP (EAP-MSCHAPv2)	Serverový certifikát + heslo v TLS tuneli	Jednoduchšie než PKI, široká podpora OS	Slabšie než EAP-TLS, závislosť od hesiel, riziko rogue AP	Enterprise Wi-Fi (WPA2/WPA3-Enterprise), VPN
EAP-FAST (Cisco)	TLS tunel s PAC (Protected Access Credential) namiesto certifikátov	Rýchla autentifikácia, nepotrebuje PKI, vhodné pre veľké nasadenia	Cisco proprietárne, menej rozšírené mimo Cisco prostredia	Cisco WLAN, NAC (ISE), BYOD scenáre
EAP-MD5	Heslo → MD5 hash	Jednoduché, nízka latencia	Slabá bezpečnosť, odpočúvanie = kompromitácia	Testy, laby (neodporúča sa v produkcii)
EAP-TTLS	TLS tunel, vnútri heslá alebo iné EAP metódy	Flexibilný, alternatíva k PEAP	Menej rozšírený než PEAP	Niektoré enterprise Wi-Fi, VPN

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA protocols

RADIUS (RFC 2865)

TACACS+ (RFC 8907)

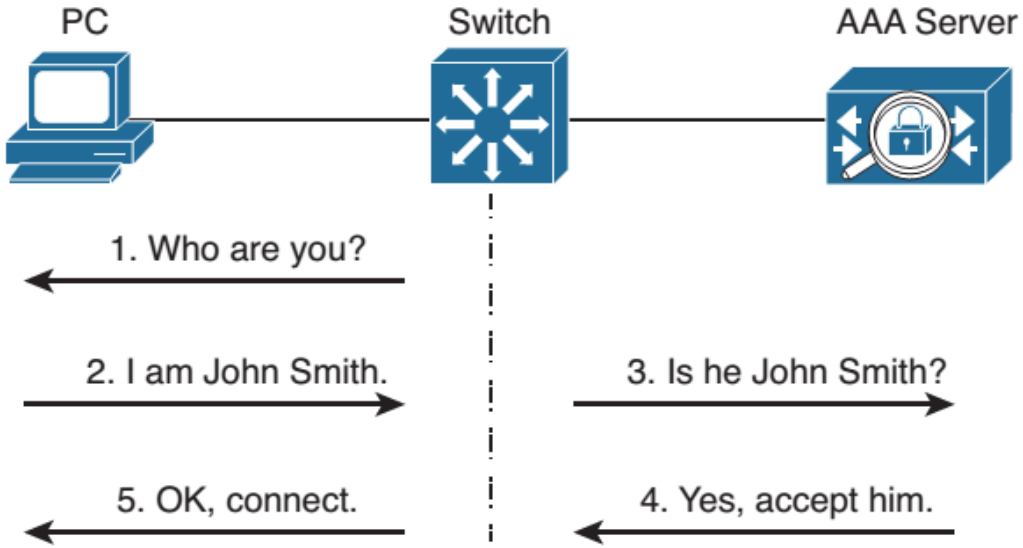
DIAMETER (RFC 6733)

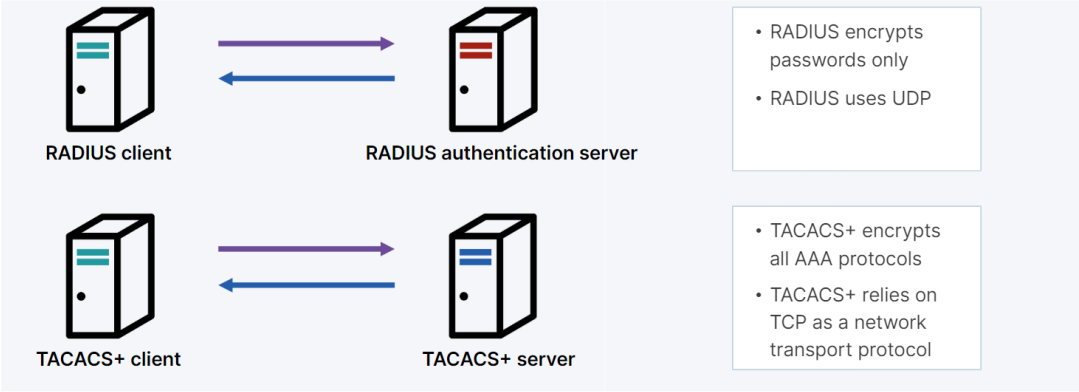
AAA - Transportné protokoly

AAA transportné protokoly

- **RADIUS (RFC 2865)**
  - Remote Authentication Dial-In User Service
- **TACACS+ (RFC 8907 / from 2020)**
  - The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol
- **DIAMETER (RFC 6733)**
  - Diameter Base Protocol

- ***LDAP** môže byť tiež súčasťou*





RADIUS (Remote Authentication Dial-In User Service)

- Otvorené klient/server riešenie
- Zvyčajne používaný na autentifikáciu a účtovanie
  - Je „session oriented“ a nie „Command“ orientovaný
  - Podporuje riešenia vzdialeného prístupu (dot1x) pre NAC systémy, WiFi či admin access
  - RADIUS accounting
    - často **povinný z hľadiska compliance (ISO 27001, NIS2, SOC 2)**
- Technické detaily
  - Používa UDP porty:
    - IANA 1812 (autentifikácia) / 1813 (účtovanie)
    - Cisco def. 1645 (autentifikácia) / 1646 (účtovanie)
  - AV-Pairs určujú VLAN, ACL, QoS, Session timeout

- **Výhody**
  - Široko podporovaný a štandardizovaný
  - Centralizovaná správa používateľských poverení
  - Vhodný pre veľké nasadenia, ako sú ISP a podniky
  - Ponúka robustné accouting funkcie
- **Nevýhody**
  - Obmedzené šifrovanie (šifrujú sa iba heslá)
  - Nie je granularita per command v porovnaní s TACACS+

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

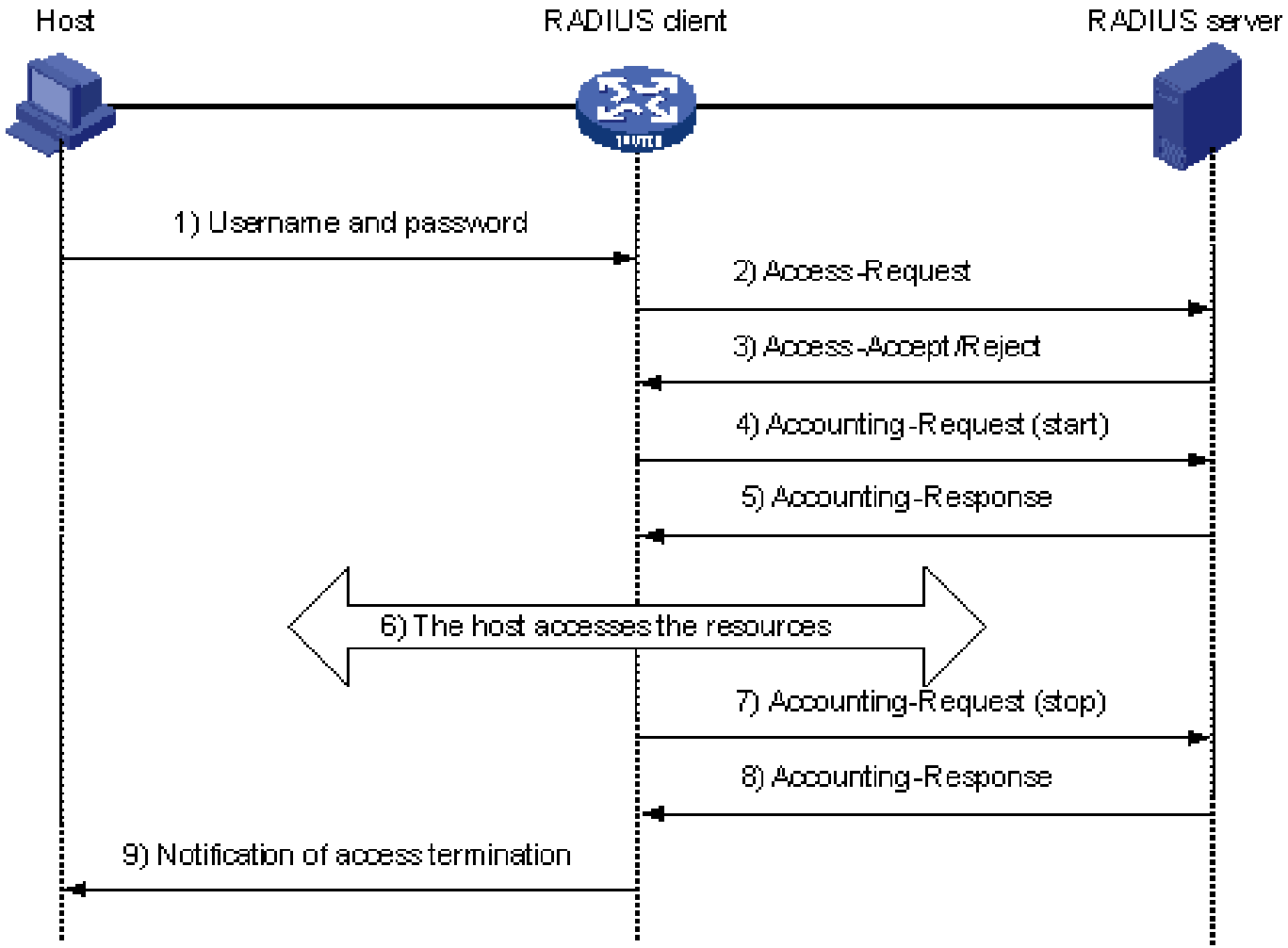
RADIUS architektúra a správy – Request/response model

- Architektúra RADIUS
  - **RADIUS klienti**: Zariadenia požadujúce autentifikáciu
  - **RADIUS server:** Server vykonávajúci autentifikáciu a autorizáciu, niekedy funguje ako RADIUS Proxy, obsahuje databázy používateľov, klientov a slovníkov
  - **RADIUS databáza:** Ukladá informácie o používateľoch

- Access-Request
  - Odosiela RADIUS klient na server
  - Obsahuje prihlasovacie údaje používateľa a žiadosť o prístup
- Access-Accept
  - Odpoveď od RADIUS servera pri úspešnej autentifikácii/autorizácii
  - Obsahuje oprávnenia (napr. VLAN, ACL, QoS parametre)
- Access-Reject
  - Odpoveď servera pri neúspešnej autentifikácii/autorizácii
  - Prístup sa zamietne
- Access-Challenge
  - Server žiada od klienta dodatočné údaje (napr. OTP, PIN, certifikát)
  - Používa sa pri viacfaktorovej autentifikácii
- Accounting-Request
  - NAS posiela serveru záznamy o aktivitách používateľa
  - Štart/stop session, prenesené dáta, doba pripojenia
- Accounting-Response
  - Potvrdenie prijatia Accounting-Request správ zo strany servera
- Change of Authorization (CoA)
  - Umožňuje dynamicky zmeniť oprávnenia používateľa počas aktívnej relácie
    - Napr. pridanie ACL, zmena VLAN bez odhlásenia
  - Dôležité pre NAC

Financované Európskou úniou NextGenerationEU
PLÁN

Basic RADIUS message exchange process



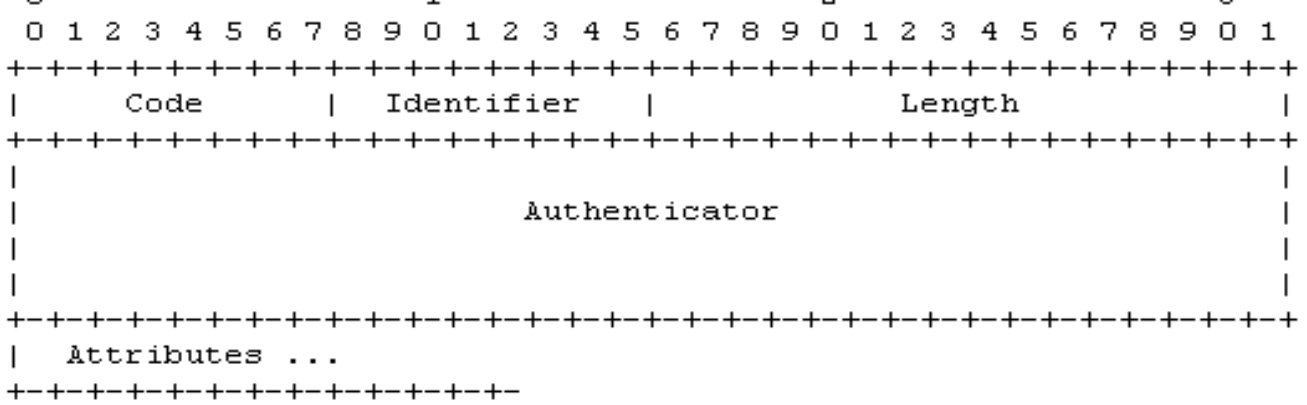
https://support.hpe.com/techhub/eginfolib/networking/docs/routers/msrv5/cg/5200-2323_security-cg/content/459369118.htm

- Klient posiela **požiadavky** na autentifikáciu serveru
- Server overí identitu používateľa
- Server rozhodne o oprávneniach a pošle **odpoveď** klientovi
  - **Prijať / odmietnuť**
- Platí počas trvania relácie

- Voliteľné: **Účtovacie záznamy** zaznamenávajú udalosti
  - (Start / Stop value)

RADIUS PDU

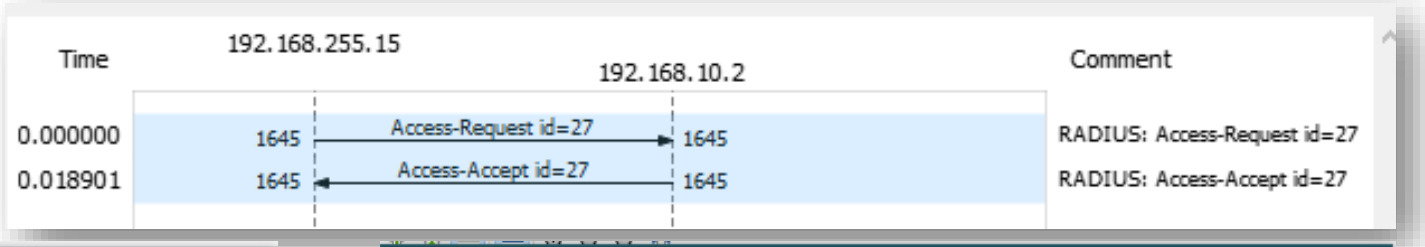
- Jedna RADIUS správa je zapuzdrená v jednom UDP datagrame
- **Code**
  - Identifikuje typ RADIUS správy
- **Identifier**
  - Pomáha spájať odpovede s požiadavkami
  - RADIUS server používa túto hodnotu spolu so zdrojovou IP adresou a UDP portom na detekciu duplikátov, ak sú prijaté v krátkom časovom intervale
- **Length**
  - Dĺžka RADIUS paketu
  - Zahŕňa polia Code, Identifier, Length, Authenticator a atribúty



- **Authenticator**
  - Používa sa na autentifikáciu odpovede od RADIUS servera
  - Tiež sa používa v algoritme na skrytie hesla
- **Attributes**
  - Nesú špecifické informácie o autentifikácii, autorizácii a konfiguračné detaily pre požiadavku a odpoveď
    - AVP pairs
  - Koniec zoznamu atribútov je určený hodnotou poľa Length

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

RADIUS



Wireshark · Packet 1 · radius.pcapng

```
> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on inter
> Ethernet II, Src: Fortinet_ec:20:94 (90:6c:ac:ec:20:94), Dst: 6a:48:96:09:2e:
> Internet Protocol Version 4, Src: 192.168.255.15, Dst: 192.168.10.2
> User Datagram Protocol, Src Port: 1645, Dst Port: 1645
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1b (27)
    Length: 68
    Authenticator: 7fc5bbdc9b4a49e225b9985626d3be7c
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=6 val=palo
    v AVP: t=User-Password(2) l=18 val=Encrypted
        Type: 2
        Length: 18
        User-Password (encrypted): ed379                              c23c
    > AVP: t=NAS-Port(5) l=6 val=1
    > AVP: t=NAS-Port-Id(87) l=6 val=tty1
    > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
    v AVP: t=NAS-IP-Address(4) l=6 val=192.168.255.15
        Type: 4
        Length: 6
        NAS-IP-Address: 192.168.255.15
```

No.: 1 · Time: 0.000000 · Source: 192.168.255.15 · Destination: 192.168.10.2 · Protocol: RADIUS · Length: 110 · Info: Access-Request id=27

Show packet bytes

Close Help

Wireshark · Packet 2 · radius.pcapng

```
> Frame 2: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on int
> Ethernet II, Src: 6a:48:96:09:2e:3c (6a:48:96:09:2e:3c), Dst: Fortinet_ec:20:
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.255.15
> User Datagram Protocol, Src Port: 1645, Dst Port: 1645
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1b (27)
    Length: 109
    Authenticator: ca10688b9f4be9a559da6555b4590a11
    [This is a response to a request in frame 1]
    [Time from request: 0.018901000 seconds]
  v Attribute Value Pairs
    > AVP: t=Idle-Timeout(28) l=6 val=600
    > AVP: t=Port-Limit(62) l=6 val=1
    > AVP: t=Service-Type(6) l=6 val=Dialback-Framed-User(4)
    > AVP: t=Class(25) l=46 val=dad50b2                              0200000000fd50bc
    v AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
        Type: 26
        Length: 25
        Vendor ID: ciscoSystems (9)
      v VSA: t=Cisco-AVPair(1) l=19 val=shell:priv-lvl=15
          Type: 1
          Length: 19
          Cisco-AVPair: shell:priv-lvl=15
```

No.: 2 · Time: 0.018901 · Source: 192.168.10.2 · Destination: 192.168.255.15 · Protocol: RADIUS · Length: 151 · Info: Access-Accept id=27

Show packet bytes

Close Help

RADIUS - Accounting

- Zaznamenáva začiatok, priebeh a koniec každej relácie
  - Start – kto sa pripojil, odkiaľ, cez aký port, akú službu
  - Interim-Update – priebežné štatistiky (traffic, čas)
  - Stop – koľko preniesol dát, ako dlho trval login, prečo sa ukončil
- Poskytuje údaje pre:
  - Audit – „kto, kedy, kde, čo a ako dlho robil “
  - Billing – časové alebo dátové účtovanie (ISP, VPN, Wi-Fi)
  - Monitoring výkonu – koľko relácií je aktívnych, koľko prenášajú
  - Compliance – záznamy pre ISO 27001 / NIS2 / SOC 2
  - Incident response – spätné dohľadanie, kto bol prihlásený počas útoku
- Môže zaznamenávať aj špecifické udalosti:
  - Network accounting – prenesené bajty/packety, QoS class
  - Problém
    - System accounting – reštarty, reloady, konfiguračné zmeny
    - Command accouting

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

RADIUS - Accouting

Accouting-Request (Acct-Status-Type = Start)

```
! Začiatok relácie používateľa po úspešnej autentifikácii
Acct-Status-Type = Start

! Meno autentifikovaného používateľa
User-Name = palo

! IP adresa NAS zariadenia (switch, router)
NAS-IP-Address = 192.168.255.15

! Fyzický alebo logický port, cez ktorý je používateľ pripojený
NAS-Port = 11

! Typ pripojenia (Ethernet, Wireless, Virtual)
NAS-Port-Type = Ethernet

! Jedinečný identifikátor relácie, koreluje Start/Stop páry
Acct-Session-Id = 0018C0A9

! Typ autentifikácie, ktorou bol používateľ overený
Acct-Authentic = RADIUS

! Typ služby – prihlásenie na zariadenie, PPP, VPN, atď.
Service-Type = Login-User

! Časové oneskorenie medzi vznikom udalosti a odoslaním záznamu
Acct-Delay-Time = 0

! MAC adresa klienta alebo CPE zariadenia
Calling-Station-Id = 00:24:E8:7A:34:91

! IP adresa pridelená používateľovi (pri L3 pripojení)
Framed-IP-Address = 10.0.10.55

! Čas začiatku relácie (synchronizácia cez NTP)
Event-Timestamp = Oct 23 2025 14:00:33
```

Accouting-Request (Acct-Status-Type = Stop)

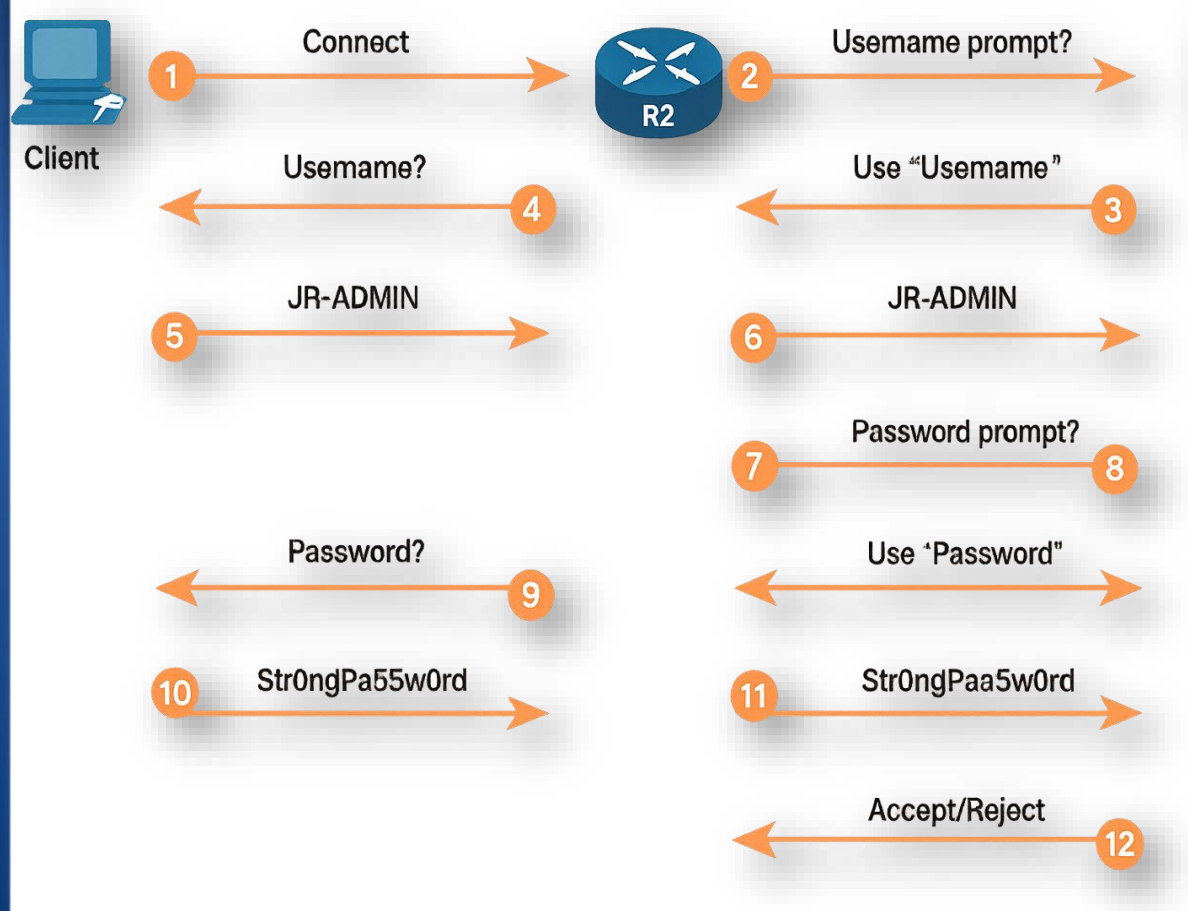
```
! Označuje ukončenie relácie
Acct-Status-Type = Stop

! Rovnaký používateľ ako v Start zázname
User-Name = palo

! IP adresa NAS zariadenia
NAS-IP-Address = 192.168.255.15

! Identifikátor relácie – zhodný so Start správou
Acct-Session-Id = 0018C0A9

! Dĺžka trvania relácie v sekundách
Acct-Session-Time = 360

! Počet prijatých bajtov od používateľa
Acct-Input-Octets = 105340

! Počet odoslaných bajtov používateľovi
Acct-Output-Octets = 98760

! Počet prijatých paketov
Acct-Input-Packets = 1293

! Počet odoslaných paketov
Acct-Output-Packets = 1201

! Dôvod ukončenia relácie (User-Request, Lost-Carrier, Idle-
Timeout...)
Acct-Terminate-Cause = User-Request

! Čas ukončenia relácie
Event-Timestamp = Oct 23 2025 14:06:33
```

TACACS+: Prehľad

- **TACACS+**
  - štandard RFC8907 (2020) (pôvodne Cisco proprietary)
  - AAA protokol pre **administrátorský prístup**
- **Technické detaily**
  - Transport: **TCP port 49**
  - Celá komunikácia je šifrovaná
  - Oddelenie funkcií: Authentication, Authorization, Accounting → samostatne
- **Architektúra**
  - Klient (NAS) = sieťové zariadenie (router, switch, firewall, WLC)
  - TACACS+ server (Cisco ISE, ACS, TACACS.net)
  - Backend: databáza účtov (AD, LDAP, lokálne DB)
- **Použitie v sieti**
  - Administrátorský prístup na sieťové zariadenia (SSH, konzola)
  - Kontrola príkazov (command-level authorization)
    - Operátor = iba show príkazy / Senior admin = plný prístup conf t
  - Auditing všetkých zmien konfigurácie
- **Výhody**
  - Granulárna autorizácia (kontrola konkrétnych príkazov)
  - Plne šifrovaná komunikácia – celý payload
  - Jasné oddelenie AAA funkcií
- **Nevýhody**
  - Cisco proprietárny protokol (obmedzená dostupnosť riešení mimo Cisco)
  - Zložitejšia konfigurácia než lokálne účty
  - Nedostatok server implementácií

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

TACACS+ architektúra



- **TACACS+ Klient (Sieťové zariadenia)**
  - Smerovače, prepínače, firewally
  - Požadujú AAA službu
  - Autentifikácia používateľov, autorizácia príkazov a zaznamenávanie účtovných informácií
- **TACACS+ Server**
  - Centrálna autorita pre AAA funkcie
  - Spracováva požiadavky od klientov
  - Komunikuje s používateľskými databázami a presadzuje prístupové politiky
- **Databáza (Úložisko používateľov)**
  - Ukladá prihlasovacie údaje používateľov, roly, oprávnenia a účtovné záznamy
  - Môže sa integrovať s externými adresármi:
    - **Active Directory**, **LDAP** alebo lokálne databázy spravované serverom TACACS+

Návod implementácie na https://nil.uniza.sk/en/tacacs-for-ubuntu-20-04/

https://lostintransit.se/2024/11/20/tacacs-on-ise-deep-dive/

TACACS+ - príklad autorizácia príkazu

Bob chce použiť show privilege:

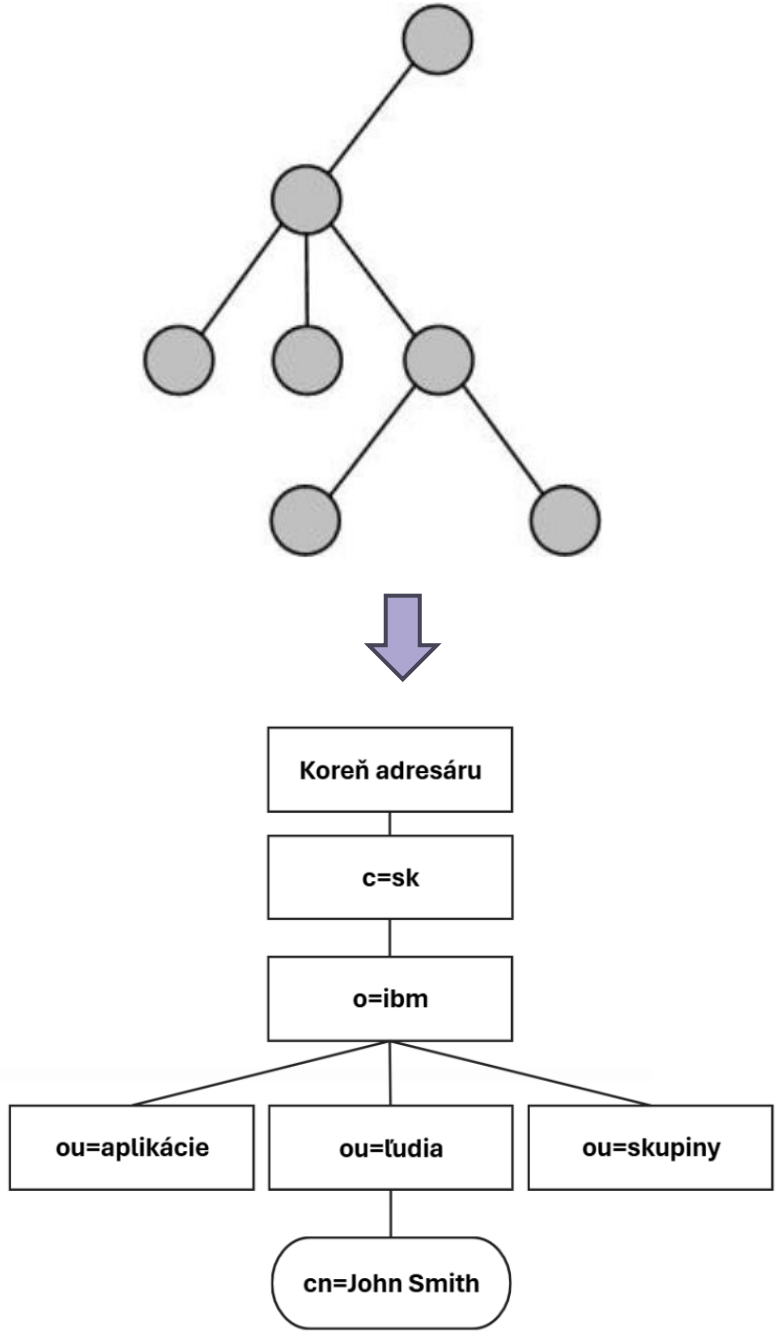
```
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple
Connections)
    Session ID: 3893996130
    Packet length: 78
    Encrypted Request
    Decrypted Request
        Auth Method: NONE (0x01)
        Privilege Level: 1
        Authentication type: ASCII (1)
        Service: TAC_PLUS_AUTHEN_SVC_NONE (0)
        User len: 3
        User: bob
        Port len: 4
        Port: tty1
        Remaddr len: 9
        Remote Address: 10.10.0.1
        Arg count: 4
        Arg[0] length: 13
        Arg[0] value: service=shell
        Arg[1] length: 8
        Arg[1] value: cmd=show
        Arg[2] length: 17
        Arg[2] value: cmd-arg=privilege
        Arg[3] length: 12
        Arg[3] value: cmd-arg=<cr>
```

Príkaz je autorizovaný

```
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 3893996130
    Packet length: 6
    Encrypted Reply
    Decrypted Reply
        Auth Status: PASS_ADD (0x01)
        Server Msg length: 0
        Data length: 0
        Arg count: 0
```

LDAP – adresárový protokol

- Adresár = špecializovaná databáza navrhnutá na vyhľadávanie a prechádzanie
- Otvorený štandard pre adresáre (RFC 4510+) – **Lightweight Directory Access Protocol**
  - Základný „zdroj pravdy“ pre IdP a aplikácie
  - **Ukladá** záznamy o identitách (DN, OU) a ich atribútoch do hierarchického stromu
    - DN – distinguished name, OU – organization unit, cn – common name
  - **Typické objekty & dáta**
    - **Users, Groups, OrganizatUnits** + atribúty (napr. e-mail, department, role v tvare typ a hodnota)
    - Odvolávka na objekt cez jeho DN
- **Použitie**
  - **Backend pre IdP** (Azure/AD, OpenLDAP, FreeIPA, Keycloak)
    - Slúži aj ako **PIP** zdroj atribútov pre autorizáciu
  - Integrácie aplikácií: vyhľadávanie používateľov, skupín a rolí
- **Bezpečnosť & prevádzka**
  - **LDAPS/TLS**, princípy „least privilege“ pre bind účty
  - Replikácia a vysoká dostupnosť (HA) pre spoľahlivosť
- **Limity (čo LDAP nie je)**
  - Nie je to SSO ani engine autorizácie - je to **adresár/úložisko** identít a atribútov
- Príklady: MS Actvie Directory, OpenLDAP ...



DIAMETER - prehľad

- **DIAMETER**
  - Nástupca RADIUSu (RFC 6733)
  - Primárne pre telekomunikačné siete (IMS, LTE, 5G core)
- **Architektúra**
  - Klienti (NAS, sieťové elementy) ↔ DIAMETER servery ↔ backend databázy (HLR, HSS, AAA DB)
  - Komunikácia na báze AVP (Attribute-Value Pairs) – podobne ako RADIUS, ale rozšírené
- **Technické detaily**
  - Transport: **TCP alebo SCTP** (spoľahlivý, na rozdiel od UDP v RADIU)
  - Porty: 3868 (default)
  - Podpora zabezpečenia: IPsec, TLS
- **Použitie v sieti**
  - **Mobilné siete (3G/4G/5G)** – autentifikácia SIM kariet, billing, mobility management
  - **Policy kontrola** (PCEF/PCF v LTE/5G architektúre)
  - V enterprise prostredí takmer nepoužívaný

- **Výhody**
  - Spoľahlivý transport (TCP/SCTP)
  - Viac flexibility – rozšírené AVP, lepšia škálovateľnosť
  - Podpora roamingu a komplexných billing modelov
- **Nevýhody**
  - Zložitosť implementácie
  - Menšia podpora v enterprise sieťach → relevantné najmä pre telco operátorov
  - Integrácia s existujúcou AAA infraštruktúrou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Porovnanie transportných AAA protokolov

Feature	RADIUS	TACACS+	DIAMETER
Primárne použitie	Sieťový prístup (VPN, Wi-Fi, 802.1X)	Administrátorský prístup na zariadenia (SSH, konzola)	Telco AAA (IMS, LTE/5G)
Transport	UDP 1812 (Auth), 1813 (Acct)	TCP 49	TCP/SCTP 3868
Šifrovanie	Len heslá	Celý payload	Celá komunikácia
AAA funkcie	Auth + AuthZ + Acct v jednej správe	Auth, AuthZ, Acct oddelené	Kombinované + rozšíriteľné
Granularita	Obmedzená (user access, VLAN/ACL)	Vysoká (command-level control)	Vysoká (viac funkcií než TACACS+)
Škálovateľnosť	Veľké enterprise siete	Stredné až veľké siete	Veľmi vysoká – moderné telco
Komplexita	Jednoduchšia konfigurácia	Zložitejšia – oddelené AAA	Najzložitejší, mnoho funkcií
Integrácia	Široká podpora všetkými vendormi	Primárne Cisco & podobné	Telco infra, pokročilé siete
Accounting	Silné účtovanie (VPN, Wi-Fi sessions)	Limitované (skôr admin logy)	Rozšírené, billing v telco

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

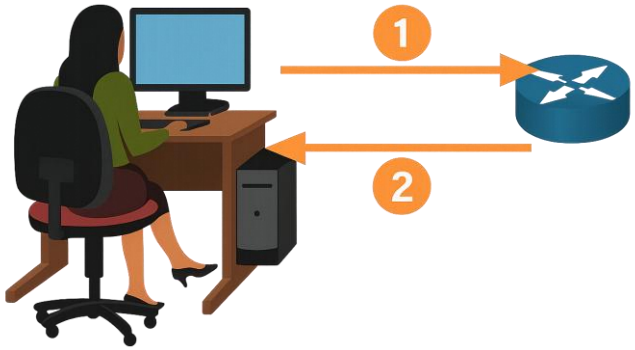
Príklady implementácií

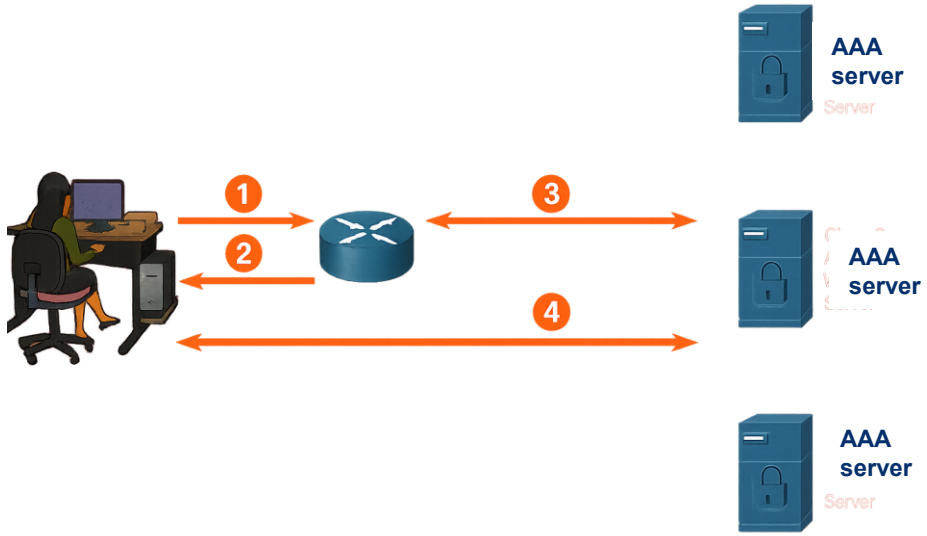
Produkt / Platforma	Dodávateľ	Podporované protokoly	Typ	Kľúčové vlastnosti / poznámky
Cisco ISE	Cisco	RADIUS, TACACS+, LDAP	Komerčný	Centrálna AAA platforma, NAC, správa prístupu k zariadeniam, profilovanie
Microsoft Entra ID	Microsoft	LDAP (cez AD), RADIUS (cez NPS)	Komerčný	Cloud identita, MFA, podmienený prístup, integrácia s NPS
Microsoft NPS	Microsoft	RADIUS, LDAP	Komerčný	Windows RADIUS server, integrácia s Active Directory
Radiator AAA Server	Radiator Software	RADIUS, Diameter, TACACS+, LDAP	Komerčný	Modulárny dizajn, telco-grade, podpora EAP, RadSec, roaming, VoWiFi
FreeRADIUS	InkBridge Networks	RADIUS, LDAP, TACACS+ (modulárne)	Open-source	Najrozšírenejší open-source RADIUS server, škálovateľný, používaný v eduroam, ISP
daloRADIUS	Komunita	RADIUS (GUI pre FreeRADIUS)	Open-source	Webové rozhranie, správa používateľov, billing, hotspot podpora
tac_plus	Shrubbery Networks	TACACS+	Open-source	Ľahký daemon, vhodný pre Cisco zariadenia, jednoduchá konfigurácia
OpenTACACS+	Komunita (fork Cisco)	TACACS+	Open-source	Minimalistické riešenie, vhodné pre laboratóriá alebo malé siete
aaaEngine (GitHub)	Komunita	RADIUS, TACACS+	Open-source	C++ AAA engine, klientsky orientovaný, škálovateľný dizajn

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA na sieťových zariadeniach (Cisco)

Lokálna vs. serverové AAA





- **Lokálna autentifikácia**
  - Zariadenie má lokálnu DB
  - Používateľ sa pripojí na router/switch (konsola, SSH, Telnet)
  - Zariadenie vyžiada meno a heslo
  - Overenie prebehne **voči lokálnej databáze účtov** v zariadení
    - Jednoduché, nepotrebuje infraštruktúru
    - Nevhodné pre väčšie prostredia (účty treba spravovať na každom zariadení)
- **Server-based autentifikácia**
  - Používateľ sa pripojí na router/switch
  - Zariadenie vyžiada meno a heslo
  - Zariadenie odošle prihlasovacie údaje na **AAA server** (napr. Cisco ISE, ACS, FreeRADIUS, Microsoft NPS).
  - AAA server overí používateľa voči backendu (AD, LDAP, databáza).
  - Server vráti výsledok (Access-Accept/Reject, prípadne autorizačné atribúty – VLAN, ACL)
    - Centralizovaná správa účtov, škálovateľné
    - Vyžaduje infraštruktúru (AAA server, integrácia s AD/PKI).

Financované Európskou úniou NextGenerationEU
PLÁ

Lokálna vs. Server-based AAA

Lokálne AAA

- **Výhody:**
  - Jednoduchá konfigurácia (stačí username / password v IOS)
  - Funguje aj bez siete alebo servera (offline režim)
  - Vhodné pre laby alebo malé siete
  - Vhodné ako fallback pri nedostupnosti AAA servera
- **Nevýhody:**
  - Účty spravované na každom zariadení zvlášť → vysoká administratívna záťaž
  - Neškálovateľné vo väčších sieťach
  - Obmedzené možnosti autorizácie (žiadne granular policies, AV-pairs)
  - Slabšie možnosti účtovania/logovania (Accounting)

AAA server (server based)

- **Výhody:**
  - Centralizovaná správa účtov (napr. integrácia s AD/LDAP (IAM))
  - Škálovateľné pre veľké enterprise prostredia
  - Podpora komplexných politík (VLAN assignment, dACL, per-command authorization)
  - Podpora Accounting (logovanie aktivít, compliance)
  - Jednotné pravidlá bezpečnosti v celej sieti
  - Enterprise štandard
- **Nevýhody:**
  - Závislosť od dostupnosti AAA servera a siete
  - Vyššia komplexita konfigurácie
  - Potreba AAA infraštruktúry (RADIUS/TACACS+ server, PKI, integrácia s AD)
  - Vyššie náklady na správu a licencie (Cisco ISE, ACS)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA modely nasadenia – Central vs. Distributed

- **Centralizovaný model**
  - Všetky NAS zariadenia smerujú na jeden/jeden cluster AAA serverov
  - Jednoduchšia správa, jednotná politika
  - Riziko single point of failure → nutná redundancia (HA, load balancing)
- **Distribuovaný model**
  - AAA servery umiestnené v rôznych lokalitách (DC, pobočky)
  - Nižšia latencia, lepšia odolnosť voči výpadkom WAN
  - Zložitejšia správa politík (synchronizácia DB, konzistencia configov)
- **Hybrid**
  - Centrálna politika (AD, ISE) + lokálne fallback mechanizmy (caching, local DB)
  - Najčastejší prístup v enterprise (napr. Cisco ISE s distrib. Policy Service Nodes)s

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Modely AAA implementácie v Cisco IOS / IOS XE

- Na Cisco zariadeniach je možné prepínať sa medzi dvomi modelmi AAA
- Pozn. Platí aj pre iných vendorov

- Starší model
  - Autentifikácia len voči lokálnej databáze
  - Autorizácia len voči lokálnej databáze
  - Minimálne (ak vôbec nejaké) možnosti pre účtovanie

- Novší model
  - Komplexná konfigurácia, ktorá umožňuje rôzne služby nasmerovať na AAA voči rôznym databázam
  - Ponúka
    - Lepšiu flexibilitu a škálovateľnosť
    - Využitie viacerých systémov či riadenie ich záloh

```
aaa new-model
```

    - podpora pre moderné AAA backendy (ISE, TACACS+, IPv6).Možnosti integrácie (napr. s Active Directory, PKI

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nový model AAA

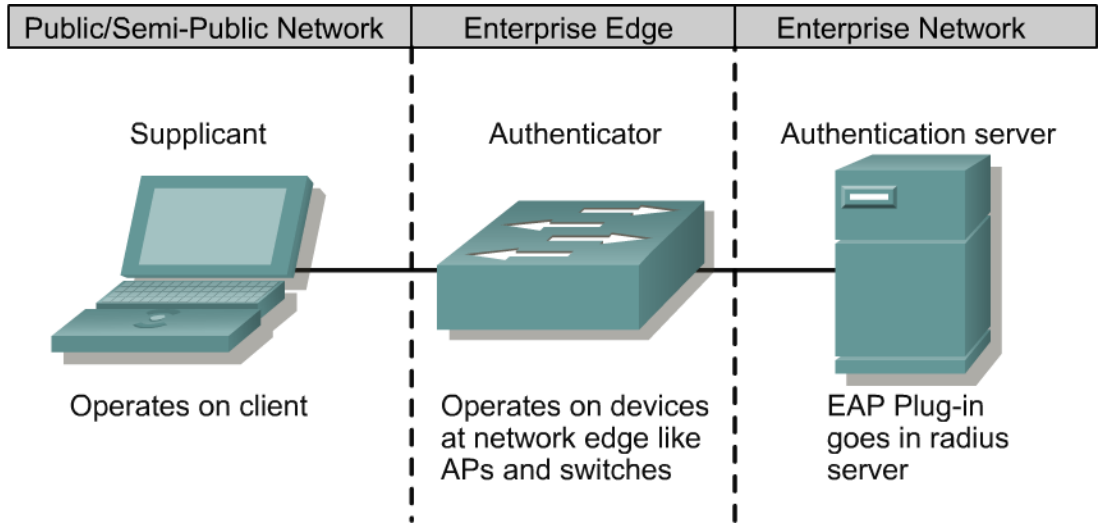
- „*Nový model AAA*“ vychádza z týchto predpokladov
  - Na jednej strane máme isté druhy služieb, ktoré vedia na základe autentifikácie pomocou istého mechanizmu riadiť prístup (dot1x, enable, login, ppp)
  - Na druhej strane máme rôzne databázy s evidenciou používateľov a ich práv (RADIUS, TACACS, lokálna databáza)
  - My chceme mať možnosť konkrétnej službe vysvetliť, v akej databáze má používateľa vyhľadať
- Napríklad:
  - Konzolové prihlásenia sa overia voči lokálnej databáze
  - SSH prihlásenia sa overia voči RADIUS serveru s IP 1.2.3.4
  - PPP prihlásenia sa overia voči RADIUS serveru s IP 5.6.7.8
  - Ethernet klienti sa overia voči RADIUS serveru s IP 9.8.7.6

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA v sieťach - 802.1X Framework

802.1X (dot1x) v skratke

- Robustný štandardizovaný rámec pre „port-based network access control“ na L2
  - LAN port aj WiFi (WPA2/3-Enterprise)
  - Pred prístupom do siete musí koncové zariadenie preukázať identitu
- Účel
  - Zabránenie neautorizovanému prístupu
  - Centrálna politika
  - Podpora rôznych metód (heslo, certifikát, token)
- Základ pre NAC systémy

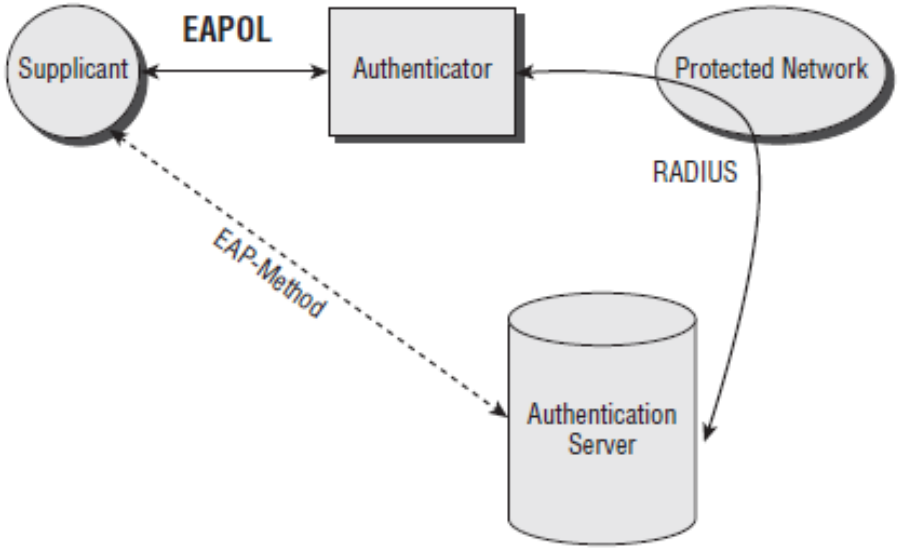


- Štandardy a špecifikácie, ktoré tvoria kompletný systém portovej autentifikácie 802.1X
  - **Institute of Electrical and Electronics Engineers (IEEE)**
    - 802.1X – Port-based Network Access Control
    - EAPOL (EAP over LAN) protokol
  - **Internet Engineering Task Force (IETF)**
    - EAP (Extensible Authentication Protocol)
    - EAP metódy
    - RADIUS protokol

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

802.1X - Komponenty

- **Supplicant (klient)**
  - Zariadenie, ktoré sa pokúša získať prístup do siete
  - Softvérový klient v OS (napr. Windows supplicant, wpa_supplicant), ktorý odosiela autentifikačné údaje
- **Authenticator (sprostredkovateľ)**
  - Sieťové zariadenie, ktoré sprostredkuje proces autentifikácie
  - Zariadenie, na ktoré sa klient fyzicky pripája a ktoré od klienta vyžaduje overenie (switch alebo access point)
- **Authentication Server (AAA server)**
  - Obsahuje databázu informácií o používateľoch/identitách
  - Overuje identitu klienta a vracia rozhodnutie (Accept/Reject) + autorizačné atribúty
  - Typicky **RADIUS** server (napr. Cisco ISE, FreeRADIUS, Microsoft NPS)
- EAP + EAPOL
  - Autentifikačné informácie (username, password) sa postupne zapuzdrujú od klienta k autentifikujúcemu zariadeniu v rámci protokolov 802.1X:
  - **EAP methods**
    Špecifické protokoly alebo mechanizmy, ktoré definujú, ako sa autentifikácia vykonáva v rámci rámca EAP
  - **EAP protocol**
    Komunikačný prostriedok
  - **EAPOL** L2 protokol

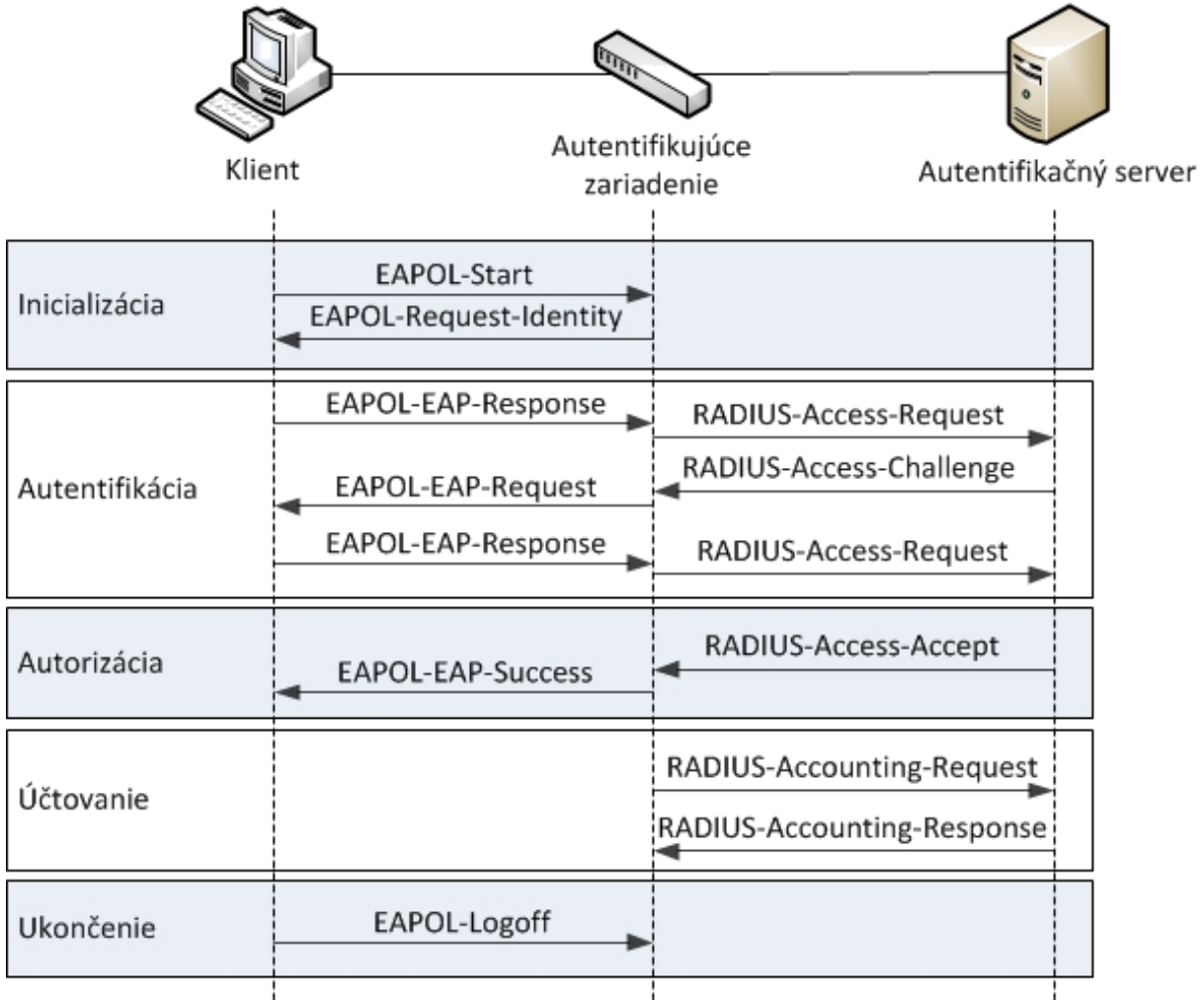


EAPOL (EAP over LAN)

EAPOL Message Type	Description
1. EAPOL-Start	Initiates the authentication process. Sender: Supplicant (client device). Function: Signals the authenticator that the supplicant wishes to begin authentication.
2. EAPOL-Logoff	Terminates the authentication session. Sender: Supplicant. Function: Informs the authenticator that the supplicant is disconnecting from the network, allowing the authenticator to clean up session data.
3. EAPOL-Key	Manages key exchange for encryption. Sender: Authenticator and Supplicant. Function: Facilitates the generation and distribution of cryptographic keys used to secure the communication channel (e.g., during EAPOL handshake).
4. EAPOL-EAP (Encapsulated EAP)	Carries EAP messages. Sender: Both Authenticator and Supplicant. Function: Encapsulates EAP-Request and EAP-Response messages to exchange authentication information between the supplicant and the authentication server via the authenticator.
5. EAPOL-Success	Indicates successful authentication. Sender: Authenticator. Function: Notifies the supplicant that authentication has been successfully completed, granting network access.
6. EAPOL-Failure	Indicates failed authentication. Sender: Authenticator Function: Notifies the supplicant that authentication has failed, denying network access.

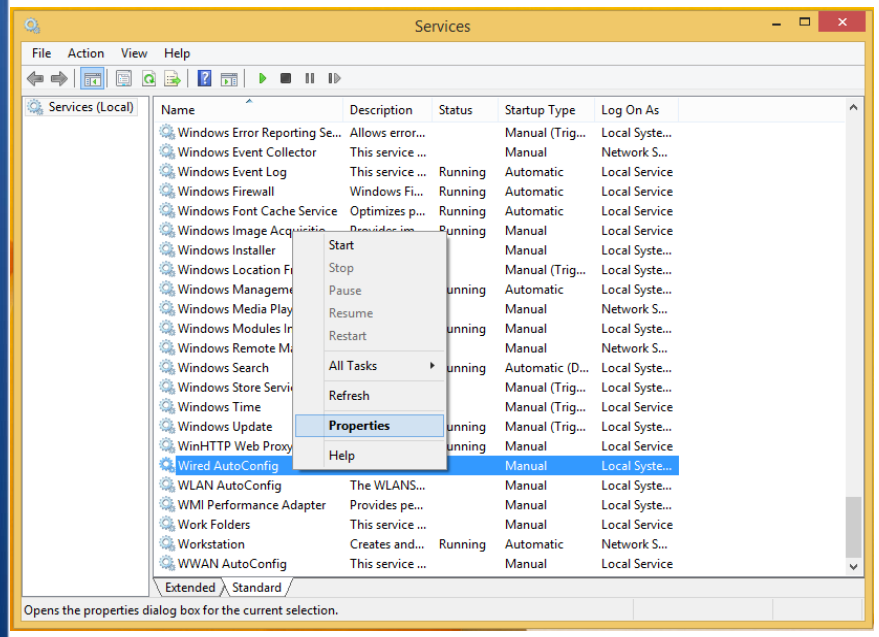
802.1X Port-Based Authentication

- **Klient odošle EAPOL-Start**
  - Alebo najprv **odpovie na EAP-Request/Identity** z authenticatora
- **Switch/AP vyžiada identitu**
  - Kým nie je overený, cez port prejdú len riadené rámce: **EAPOL** (a L2 kontrolné BPDU/CDP/LLDP podľa politiky)
- **Switch zabalí EAP do RADIUS** a pošle **Access-Request** na AAA server
- **RADIUS server** môže overiť hneď **alebo** prebehne výmena **Challenge/Response** (viac krokov podľa EAP metódy)
- Po úspechu server pošle **Access-Accept** (+ autorizačné atribúty: **VLAN/voice-VLAN, dACL/SGT, session-timeout**)
- **Switch otvorí port** (stav *authorized*), priradí politiku a informuje klienta
- Voliteľne sa odošlú **RADIUS Accounting** správy (**Start/Stop**, prípadne **Interim-Update**)
- Ukončenie relácie: **EAPOL-Logoff** (alebo timeout/reauth)

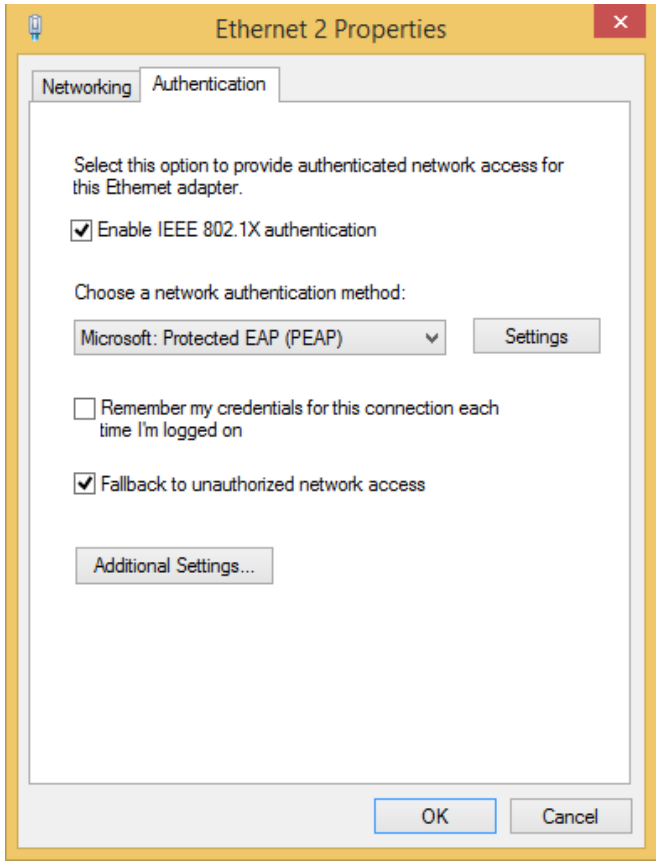


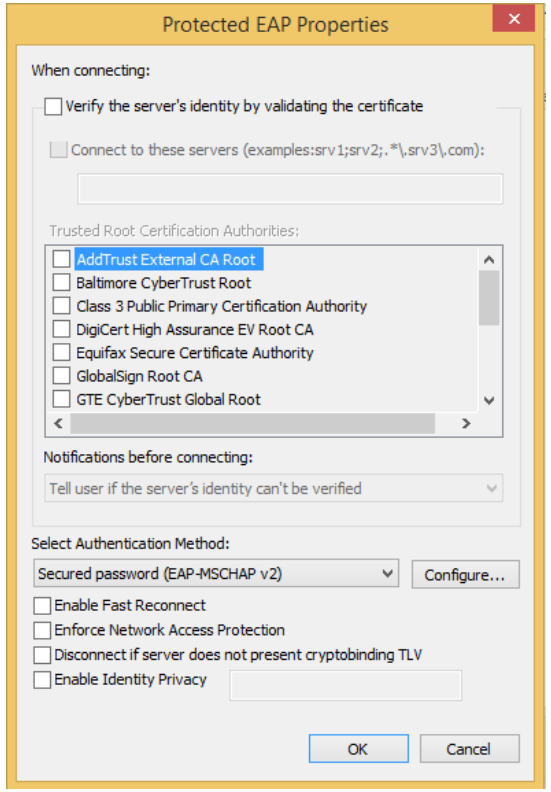
Konfigurácia – klient

- Hľadať „services.msc“
- Zapnúť službu „Wired AutoConfig“



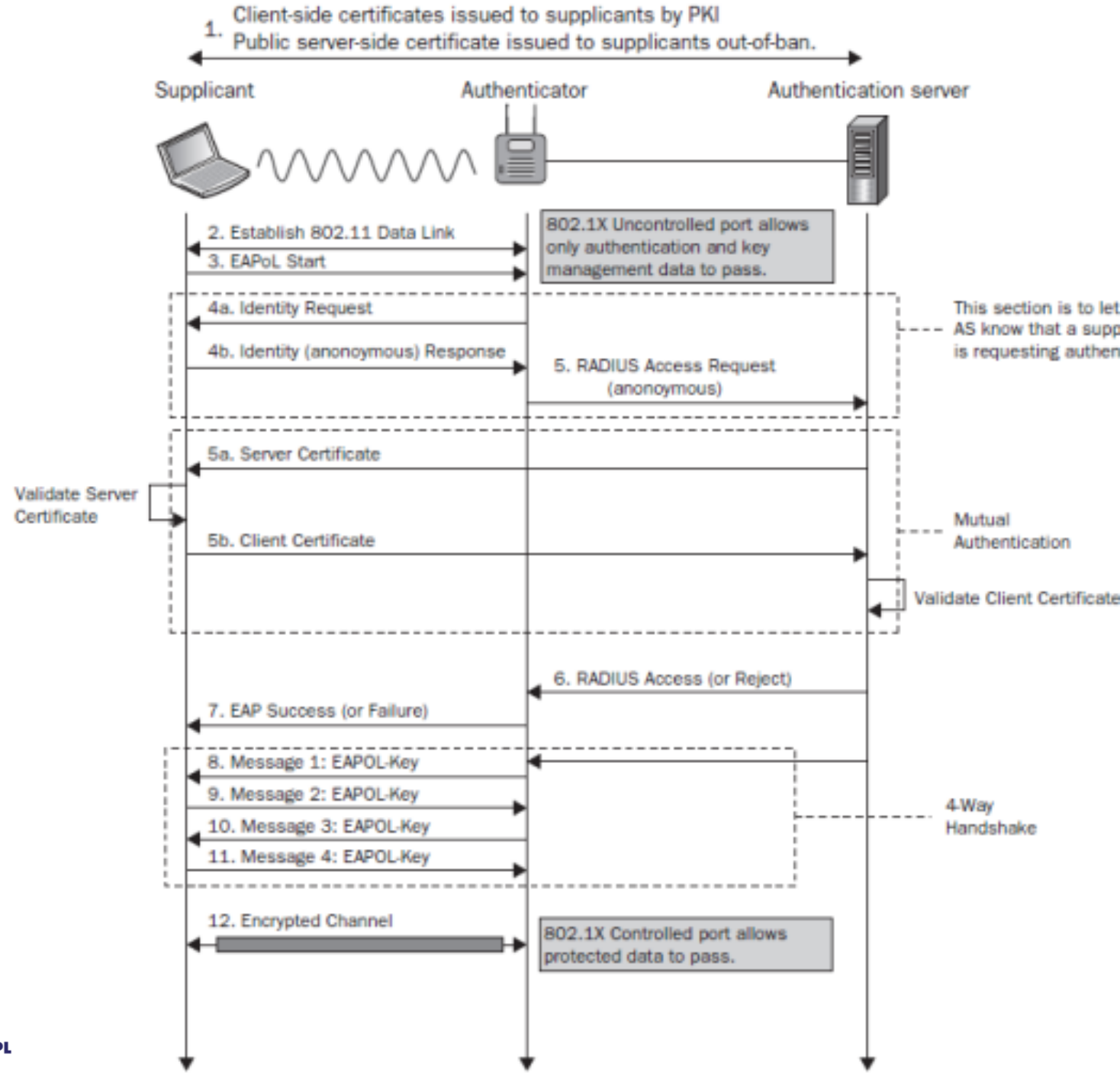
- V nastaveniach pripojenia zapnúť autentifikáciu 802.1X a vybrať EAP metódu





Dot1x s EAP TLS

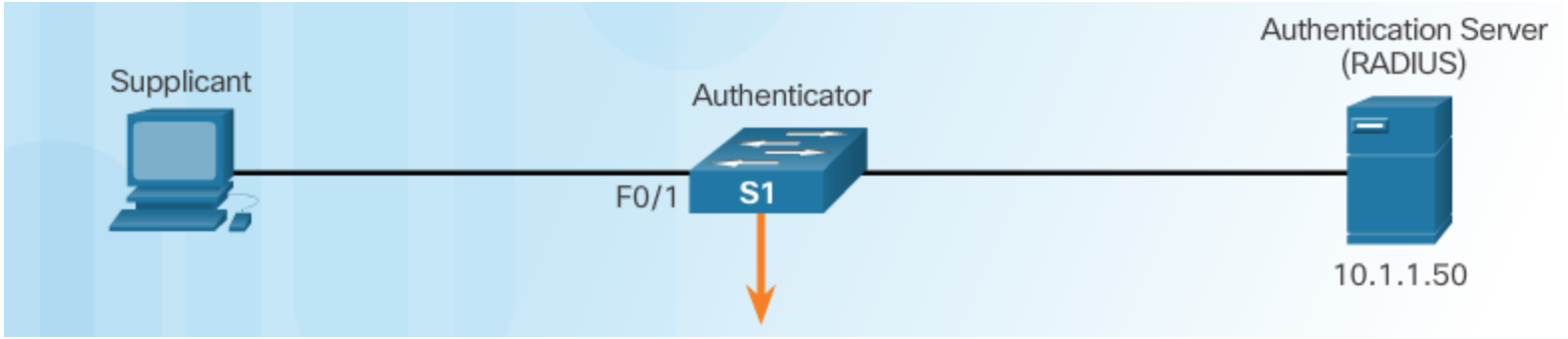
- EAP-TLS flow:
  - Založenie dátového spojenia (EAPOL Start)
  - Identity exchange (anon. request/response)
  - RADIUS Access-Request (EAP-Message)
  - Výmena certifikátov (server ↔ client)
  - EAP Success a 4-way handshake
  - Vytvorenie šifrovaného kanála (protected port)



Financované Európskou úniou NextGenerationEU

PL

Configuring 802.1X – an example




```
aaa new-model
!
radius-server SERVER-R
   address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
   key HESLO
!
aaa authentication dot1x default group radius
! Nasledujúci riadok netreba, ak nechceme dynamicky prideľovať VLAN
aaa authorization network default group radius
!
dot1x system-auth-control
!
interface FastEthernet 0/1
 switchport mode access
! Zapni dot1x na porte
 authentication port-control auto
 dot1x pae authenticator
```

Minimalistická konfigurácia – freeRADIUS server

```
apt-get install freeradius

/etc/freeradius/clients.conf
            client 192.168.99.253 {
            secret = kluc123
            shortname = klient2
      }
/etc/freeradius/users
            meno        Cleartext-Password := „heslo"
                        Tunnel-Type = VLAN,
                        Tunnel-Medium-Type = IEEE-802,
                        Tunnel-Private-Group-Id = číslo_vlan

; V prípade použitia tunelovanej metódy:
/etc/freeradius/eap.conf
            use_tunneled_reply = yes

/etc/init.d/freeradius restart
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zhrnutie

- **Mechanizmy autentifikácie a autorizácie**
- **AAA rámec**
  - **Autentifikácia:** overenie identity („Kto si?“)
  - **Autorizácia:** určenie oprávnení („Čo môžeš robiť?“)
  - **Accounting:** záznam aktivít („Čo si urobil?“)

- **Kľúčové body**
  - **RADIUS** – prístup používateľov (VPN, Wi-Fi)
  - **TACACS+** – správa zariadení, príkazová kontrola
- **AAA new-model** – centralizácia, audit, fallback
- **MFA a certifikáty** – vyššia úroveň zabezpečenia

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Sieťová bezpečnostná architektúra

Kurz: Špecialista kybernetickej bezpečnosti

Pavel Segeč

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk

Autentifikácia na sieťových zariadeniach (Cisco IOS)

Prístup na zariadenie

Kroky konfigurácie AAA autentifikácie v CLI

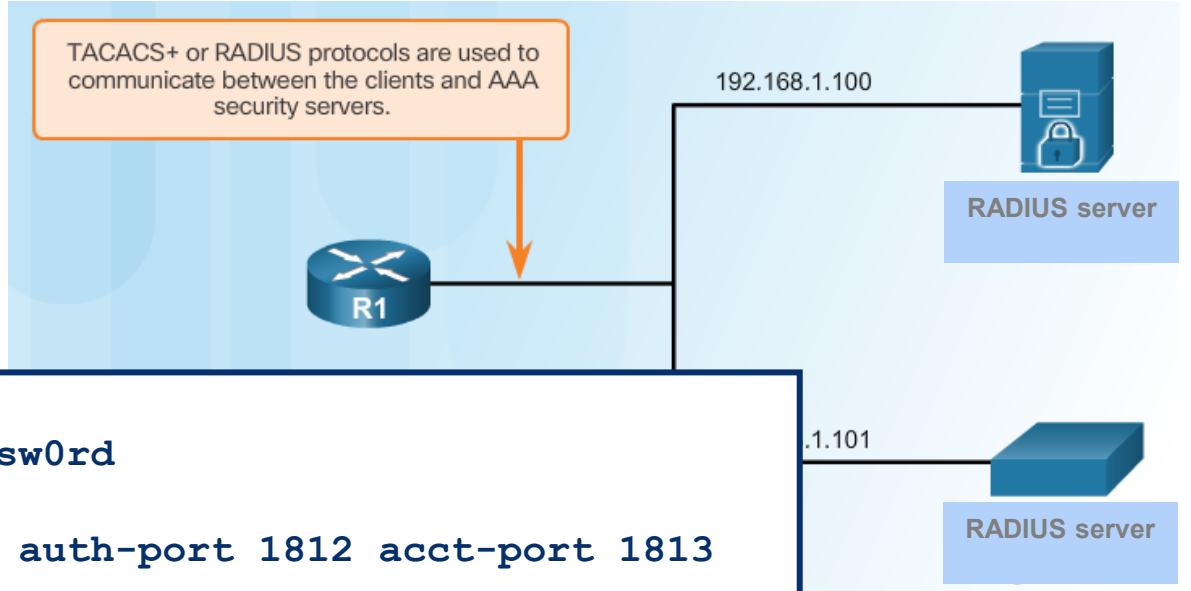
1. Definuj zdroje (ciele) AAA autentifikácie **– lokal, server, alebo oba**
   - Zadaj IP adresu/adresy AAA servera
   - Nakonfiguruj tajný kľúč
2. Aktivuj AAA model
3. Definuj zoznam metód autentifikácie (databáz) pre danú službu (login, ppp, dot1.x...), ktoré sa budú pri overení skúšať
   - Lokal DB, alebo RADIUS alebo TACACS+ server, alebo oba
4. Aplikuj metódy autentifikácie na **con / vty / aux** a over ich funkčnosť

- ***Poznámka:*** *Konfigurácia autentifikácie umožňuje používateľom prístup* ***iba po úspešnom prihlásení****, ale* ***neumožňuje vykonávať žiadne príkazy!***
  - *Na kontrolu toho,* ***ktoré príkazy sú povolené****, je potrebné nastaviť* ***autorizáciu****!*

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autentifikácia voči dvom RADIUS serverom

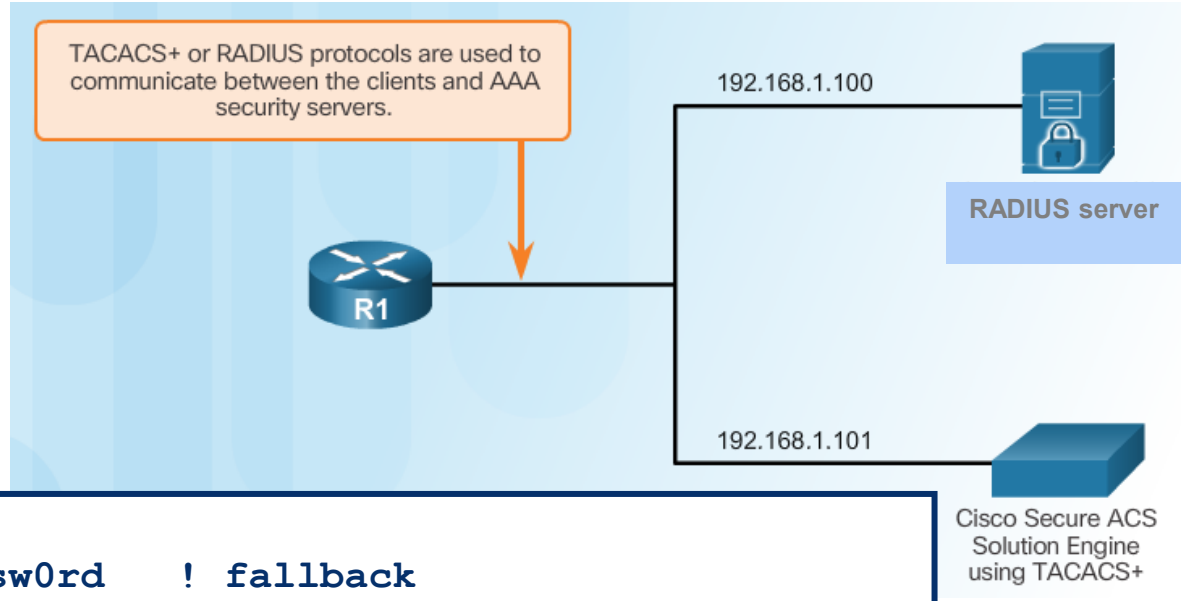
Server-Based AAA
Reference Topology




```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd
Router(config)# radius server SERVER-R1
Router(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# radius server SERVER-R2
Router(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa group server radius RADIUS-SERVERS
Router(config-sg)# server name SERVER-R1
Router(config-sg)# server name SERVER-R2
Router(config-sg)# exit
Router(config)# aaa authentication login MY_RADIUS_AUTH group RADIUS-SERVERS local-case
Router(config)# aaa authentication enable MY_RADIUS_AUTH group RADIUS-SERVERS local-case
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_RADIUS_AUTH
```

Autentifikácia voči TACACS+ a RADIUS Server

Server-Based AAA
Reference Topology

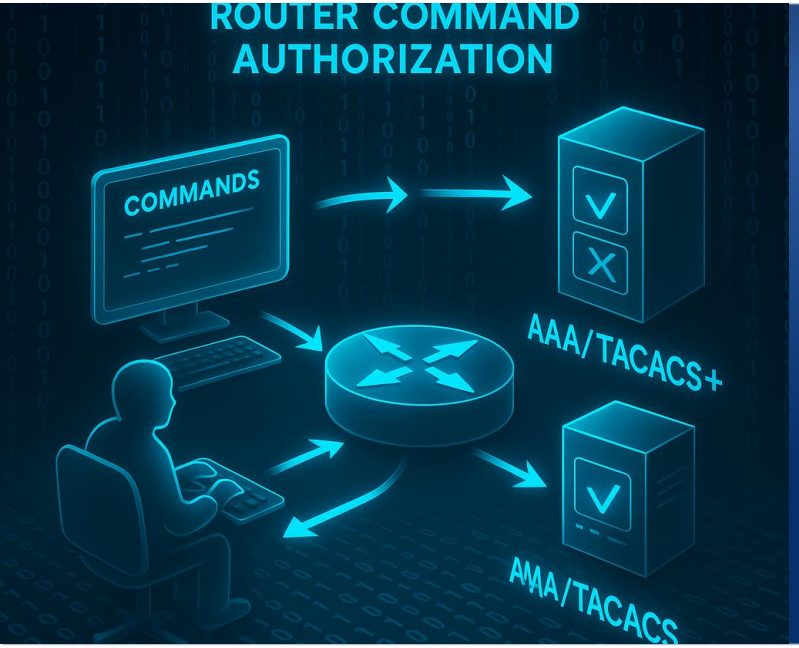



```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd   ! fallback
Router(config)# radius server SERVER-R
Router(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
Router(config-radius-server)# key RADIUS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# tacacs server SERVER-T
Router(config-radius-server)# address ipv4 192.168.1.101
Router(config-radius-server)# single-connection
Router(config-radius-server)# key TACACS-pa55w0rd
Router(config-radius-server)# exit
Router(config)# aaa authentication login MY_AUTH_RAD+TAC group radius group tacacs+ local
Router(config)# line vty 0 15
Router(config-line)# login authentication MY_AUTH_RAD+TAC
```

Naše príklady

- Tacacs+
  - Tacacs for Ubuntu 20.04
    - Tacacs for Ubuntu 20.04 | NIL - Network Information Library
- Radius
  - Riešenie autentifikácie a privilege-levels oprávnení v Cisco IOS voči Windows NPS Radius serveru na Win 2019
    - Riešenie autentifikácie a privilege-levels oprávnení v Cisco IOS voči Windows NPS Radius serveru na Win 2019 | NIL - Network Information Library
  - ASA AAA authentication against Windows 2016 server (AD)
    - ASA AAA authentication against Windows 2016 server (AD) | NIL - Network Information Library

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Autorizácia na sieťových zariadeniach (Cisco IOS)

Prístup na zariadenie + server based AAA + autorizácia príkazov (Cisco IOS)

Autorizácia príkazov (v Cisco IOS)

- Tri mechanizmy
  - **Lokálne:**
    - Privilege Levels (0–15)
    - Role-Based CLI (Parser Views)
  - **Server-based:**
    - **TACACS+ Command Authorization**
    - RADIUS?
      - **Pozn.:** RADIUS neumožňuje per-command kontrolu; vie len úroveň shell:priv-lvl

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cisco Privilege Levels (0–15) – čo to je, plusy/mínusy

- Lokálny mechanizmus riadenia prístupu k príkazom v IOS/IOS XE
- **Predvolené úrovne:**
  - **Level 0**
    - len disable, enable, exit, logout, help
  - **Level 1** - user EXEC mode
    - “>“ – základné „show“
  - **2 – 14 - používateľsky definovateľné úrovne**
  - **Level 15 - privileged EXEC**
    - “#” plný prístup
- **Dôležité**
  - **Levely 2–14 = default rovnaké ako level 1**
    - pokiaľ sa **nepriradía iné príkazy** (privilege … level … <cmd>)
  - Dedí sa smerom nahor
    - príkazy z nižšej úrovne sú vždy dostupné na vyššej
- **Plusy**
  - jednoduché, offline (bez AAA), minimálna záťaž
- **Mínusy**
  - hrubozrnné, bez auditu, ťažko udržiavateľné naprieč zariadeniami, neintegrujú sa s AD/IAM
- **Obmedzenia**
  - Nie je kontrola na úrovni konkrétneho rozhrania/slotu
  - Príkaz s viacerými kľúčovými slovami dáva prístup ku všetkým príkazom, ktoré ich používajú
  - Nedokážeš rozlišovať argumenty príkazu (na to slúžia Parser Views)
- **Best practice**
  - Používať len doplnkovo (break-glass)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

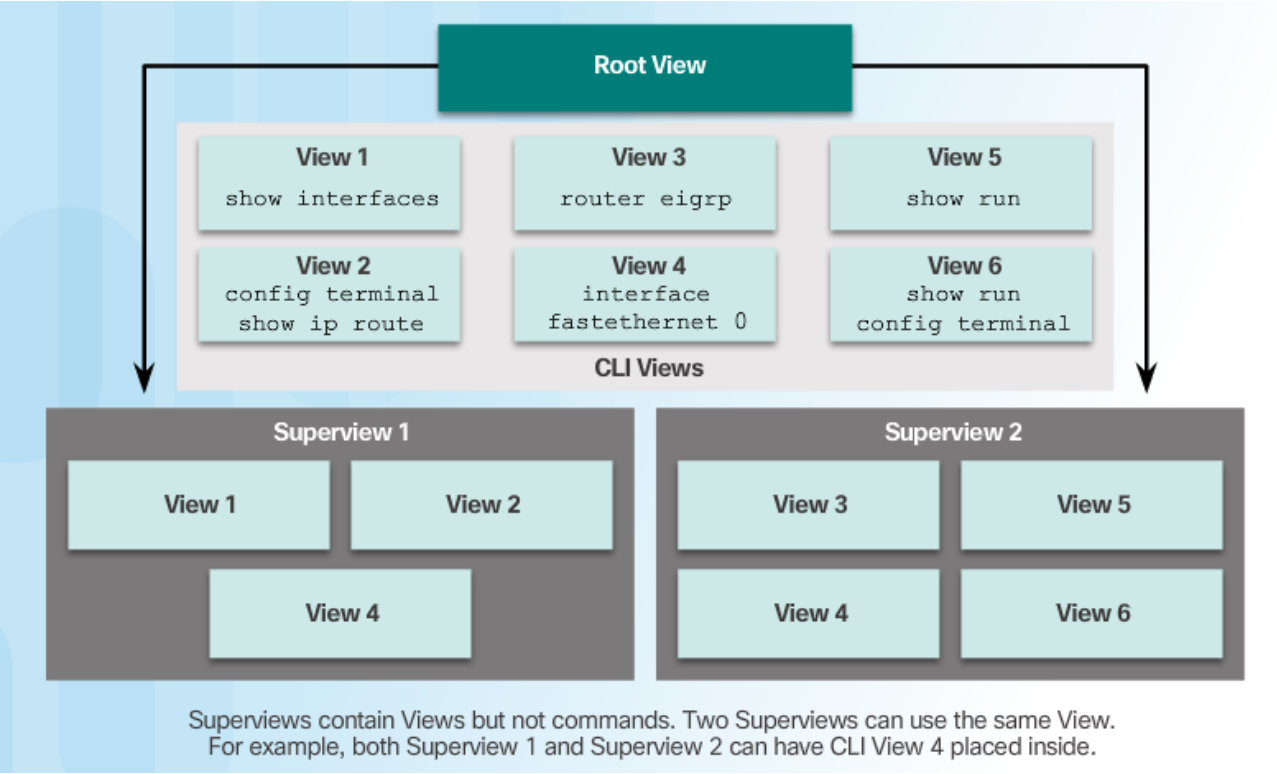
Privilege Levels - príklad

- Privilege Levels
  - 16 úrovní (0–15), kde 15 = plný prístup
  - Príkazy možno priradiť k úrovniam:

```
! Level 5 and SUPPORT user configuration
! Add the ping cmd to the level 5
R1(config)# privilege exec level 5 ping
! 1) Assign a pass for accessing level 5 - one method
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
! Or 2) Create an user and assign him to the level 5 with a password - second method
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt secret cisco5

! Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt secret cisco10

! Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret cisco123
```

Riešenia na základe rolí - Role-Based CLI / GUI

- Role-Based prístup
  - Poskytuje jemnejšiu kontrolu než **Privilege Levels**
  - Koncept **„view“** = zoznam povolených príkazov pre rolu
    - Root view – práva ako level 15; správa ostatných view
    - CLI views – konkrétne zoznamy príkazov (napr. show only, WAN ops)
    - Superviews – „kontajnery“ z viacerých CLI views pre skupiny používateľov
  - Jeden používateľ = jedna (alebo viac) priradených **view**
  - Vhodné pre operátorov NOC/SOC, špecializované tím



- Nepotrebuje AAA server (lokálne na zariadení)
- **Bez dedenia** – povolené je len to, čo je explicitne v view
- Best practice
  - Doplnok, pre enterprise kombinovať s TACACS+ command authorization

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad

```
R1(config)# aaa new-model
R1(config)# exit

R1# enable view
Password: <priv-level-15-pass / enable secret>

R1# conf t

! Create a CLI view
R1(config)# parser view SHOWVIEW
! Secure access
R1(config-view)# secret cisco
! Add commands
R1(config-view)# commands exec include show version
R1(config-view)# commands exec include show interfaces
R1(config-view)# commands exec include show ip interface
brief
R1(config-view)# commands exec include show parser view
R1(config-view)# exit

R1(config)# parser view VERIFYVIEW
R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit

R1(config)# parser view REBOOTVIEW
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
```

```
! Verify
R1# sh parser view all
No view is active ! Currently in Privilege Level
Context

! View must be active
R1# enable view SHOWVIEW
Password: cisco

R1# show parser view
Current view is 'SHOWVIEW'

R1# sh parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
-------(*) represent superview-------

R1# show ?
…
  interfaces  Interface status and configuration
  ip          IP information
  parser      Display parser information
  version     System hardware and software status

R1# show run | begin view
parser view SHOWVIEW
 secret 5 $1$C3gn$NTq088ymZY4VlfwvpmiuZ.
 commands exec include all show
…
! Delete view
No parser view SHOWVIEW
```

Príklad superview

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
Password: <priv-level-15-pass>

R1# conf t

R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit


R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit

R1(config)# parser view JR-ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view REBOOTVIEW
R1(config-view)# end
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Overenie

```
R1# sh parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 REBOOT
 VERIFYVIEW
 REBOTVIEW
 TEMP
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------

R1# show run | begin view

parser view SHOWVIEW
 secret 5 $1$C3gn$NTq088ymZY4VlfwvpmiuZ.
 commands exec include show
…
```

```
R1# show parser view
Current view is 'root'

R1#enable view JR-ADMIN
Password:

R1#sh parser view
Current view is 'JR-ADMIN'
R1# ?
Exec commands:
  do-exec  Mode-independent "do-exec" prefix support
  enable   Turn on privileged commands
  exit     Exit from the EXEC
  ping     Send echo messages
  reload   Halt and perform a cold restart
  show     Show running system information
R1#show ?
  bootflash:  display information about bootflash: file
system
  disk0:      display information about disk0: file system
  disk1:      display information about disk1: file system
  flash:      display information about flash: file system
  parser      Display parser information
  slot0:      display information about slot0: file system
  slot1:      display information about slot1: file system
```

Server-based AAA autorizácia

- Authentication (overenie identity)
  - Potvrdzuje, že zariadenie alebo používateľ je legitímny
  - Samotná autentifikácia neurčuje, aké príkazy môžeš vykonať
- Authorization (autorizácia)
  - Povoľuje alebo zakazuje overeným používateľom prístup k oblastiam/službám/príkazom v sieti
- **TACACS+ vs. RADIUS**
  - **TACACS+**
    - **Oddeľuje autentifikáciu od autorizácie**
    - **Pre každú autorizáciu vytvára nové TCP spojenie (TCP/49)**
  - RADIUS
    - Neoddeľuje autentifikáciu od autorizácie (pre user access stačí, na per-command kontrolu nie)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Konfigurácia AAA autorizácie – jednotlivé kroky

- 1) Definujte zoznam autorizácie – zoznam autorizačných serverov pre jednotlivé služby

```
Router(config)# aaa authorization {commands | config-commands | configuration | exec
  | network | reverse-access} {default | LIST-NAME} method1 [method2 ...]
```

  - commands: Server musí vrátiť povolenie na použitie akéhokoľvek príkazu zariadenia na akejkoľvek úrovni oprávnenia
  - config-commands: Server musí vrátiť povolenie na použitie akéhokoľvek konfiguračného príkazu zariadenia
  - configuration: Server musí vrátiť povolenie na vstup do konfiguračného režimu zariadenia
  - exec: Server musí vrátiť povolenie pre používateľa na spustenie EXEC relácie zariadenia.Server môže tiež vrátiť úroveň oprávnenia používateľa, aby mohol byť okamžite presunutý do privilegovaného EXEC (enable) režimu bez zadania príkazu „enable“
  - network: Server musí vrátiť povolenie na použitie sieťových služieb (SLIP, PPP, ARAP)
  - reverse-access: Server musí vrátiť povolenie pre používateľa na prístup k reverse Telnet relácii na zariadení.

- 2) Aktivujte podporu pre nový AAA:

```
Router(config)# aaa new-model
```

- 3) Aplikujte autorizačné metódy na linku a overte

```
Router(config-line)# authorization {commands level | exec | reverse-access} {default
  | LIST-NAME}
```

  - Network: Pre sieťové služby, ako je PPP
  - Exec: Pre spustenie exec (shell)
  - Commands level: Pre exec (shell) príkazy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Konfigurácia autorizácie – najjednoduchšie

```
username JR-ADMIN algorithm-type scrypt secret G33dP@ssw4rd
username ADMIN algorithm-type scrypt secret T4t1lBr5t@lP@ssw4rdWrtYU!H3LL&:-)
!
aaa new-model
!
! Use a default schema, case sensitive for running EXEC
aaa authorization exec default local-case
!
! Use own DB name with tacacs+
! tacacs server SERVER-T1
!        address ipv4 192.168.1.100
!        key TACACS-pa55w0rd

! aaa authorization network AUTHOR_NET_T+L group tacacs+ local
!
! Apply for example for vty line
line vty 0 15
  authorization exec default
```

- Note:
  - An administrator must create a user with full access rights before authorization is enabled,
  - do it immediately locks the administrator out of the system in the moment the aaa authorization command is entered

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Účtovanie (Accounting) na sieťových zariadeniach (s Cisco IOS/IOS XE)

Accounting (Cisco IOS)

1. Aktivácia AAA: aaa new-model
2. Definuj čo sa bude zaznamenávať (**method-lists)** a čo to spustí **(trigger)** pre accounting
   - Kategórie pre účtovanie v IOS/IOS XE:
     - **Network -** PPP/VPN, dialer, dot1x/WLAN
     - **System** - globálne udalosti zariadenia
     - **exec** - spustenie/ukončenie shellu
     - **commands <level>** - účtovanie vykonaných príkazov (user + príkaz) – *TACACS+*
     - **Connection** - odchádzajúce spojenia (SSH, Telnet, dialer)
   - Režim záznamu / triggers
     - **start-stop** (odporúčaný) alebo **stop-only**; **interim-update** pre dlhé relácie
3. Priraď accounting metódy (method-lists) a over

- Transport a ciele
  - **TACACS+** (TCP/49) alebo **RADIUS** (UDP/1813)
- Best practice
  - Centralizácia do SIEM, NTP/UTC, fallback na lokál + OOB
- Bez TACACS+ príkazov
  - **archive log config** → zmeny configu do syslogu

Konfigurácia accouting

```
username JR-ADMIN algorithm-type scrypt secret G33dP@ssw4rd
username ADMIN algorithm-type scrypt secret T4t1lBr5t@lP@ssw4rdWrtYU!H3LL&:-)
!
aaa new-model
!
aaa authentication login default local-case
aaa authorization exec default local-case
aaa authorization network AUTHOR_NET_T+L group tacacs+ local
!
! Define accounting
aaa accouting exec default start-stop local-case
aaa accouting network default start-stop group tacacs+
! apply
line vty 0 15
  authentication login default
  authorization exec default
  accouting exec default
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

KIS príklad

- Departmental network
  - Tacacs+ server on ubuntu
    - **TACACS_STUDENTS_READ_ONLY_PRIV_LEVEL1**
      - Allows

```
cmd = show {
        permit "cdp.*"
        permit "lldp.*"
        permit "protocols.*"
        permit "ip.*"
        permit "ipv6.*"
        permit "mac address-table.*"
        permit "spanning.*"
        permit "interface.*"
        permit "vtp status"
        permit "etherchannel.*"
        permit "snmp.*"
        permit "clock"
        permit "run int.*"
        permit "ntp.*"
        permit "running-config"
        permit "access-list.*"
        permit "show vpc.*"
        deny .*
```

  - AD for authentication
    - **Student user group TACACS_STUDENTS_READ_ONLY_PRIV_LEVEL1**
  - Set of cisco switches

```
aaa new-model
tacacs server TACACS-KIS1
        address ipv4 192.168.XY.XY_1
        single-connection
        key PASSWORD
!
radius server RADIUS-ON-DC
        address ipv4 192.168.XY.XY_2
        key PASSWORD
aaa authentication login KIS_AUTENT group tacacs+ group radius local
aaa authorization config-commands
aaa authorization exec KIS_AUTOR group tacacs+ group radius local
aaa authorization commands 15 KIS_AUTOR_CMDS group tacacs+ local
aaa authorization commands 1 KIS_AUTOR_CMDS group tacacs+ local
aaa accounting commands 15 KIS_ACNT_CMDS start-stop group tacacs+
aaa accounting commands 1 KIS_ACNT_CMDS start-stop group tacacs+
!
line vty 0 4
 authorization commands 1 KIS_AUTOR_CMDS
 authorization commands 15 KIS_AUTOR_CMDS
 authorization exec KIS_AUTOR
 accounting commands 1 KIS_ACNT_CMDS
 accounting commands 15 KIS_ACNT_CMDS
 logging synchronous
 login authentication KIS_AUTENT
 length 0
 transport input ssh
line vty 5 15
 authorization commands 1 KIS_AUTOR_CMDS
 authorization commands 15 KIS_AUTOR_CMDS
 authorization exec KIS_AUTOR
 accounting commands 1 KIS_ACNT_CMDS
 accounting commands 15 KIS_ACNT_CMDS
 logging synchronous
 login authentication KIS_AUTENT
 transport input ssh
!
end
```


Financované Európskou úniou NextGenerationEU

Troubleshooting Server-Based AAA Authentication

AAA debugging

```
debug aaa authentication

no debug aaa authentication
```

```
Router# debug aaa authentication
…
…
 6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
 6:50:20: TAC+: send AUTHEN/CONT packet
 6:50:20: TAC+ (50996740): received authen response status = PASS
 6:50:20: AAA/AUTHEN (50996740): status = PASS
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AAA debugging (cont.)

```
R1# debug radius ?
  accounting       RADIUS accounting packets only
  authentication   RADIUS authentication packets only
  brief            Only I/O transactions are recorded
  elog             RADIUS event logging
  failover         Packets sent upon fail-over
  retransmit       Retransmission of packets
  verbose          Include non essential RADIUS debugs
  <cr>
```

```
R1# debug tacacs ?
  accounting       TACACS+ protocol accounting
  authentication   TACACS+ protocol authentication
  authorization    TACACS+ protocol authorization
  events           TACACS+ protocol events
  packet           TACACS+ packets
  <cr>
```

Debugging TACACS+ and RADIUS (Cont.)

AAA Server-Based Authentication Success

```
R1# debug tacacs
TACACS access control debugging is on
R1#

14:00:09: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.1.101 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.1.101 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.1.101 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

AAA Server-Based Authentication Failure

```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

debug radius

```
login as: palo
Keyboard-interactive authentication prompts
from server:
| Password:
End of keyboard-interactive prompts from
server

sw-Test#
```

```
sw-Test#
07:24:55: RADIUS/ENCODE(00000018): ask "Password: "
07:24:55: RADIUS/ENCODE(00000018): send packet; GET_PASSWORD

sw-Test#
07:25:18: RADIUS/ENCODE(00000018):Orig. component type = Exec
07:25:18: RADIUS:  AAA Unsupported Attr: interface         [210] 4
07:25:18: RADIUS:   74 74                  [ tt]
07:25:18: RADIUS/ENCODE(00000018): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
07:25:18: RADIUS(00000018): Config NAS IP: 0.0.0.0
07:25:18: RADIUS(00000018): Config NAS IPv6: ::
07:25:18: RADIUS/ENCODE(00000018): acct_session_id: 9
07:25:18: RADIUS(00000018): sending
07:25:18: RADIUS/ENCOD
sw-Test#E: Best Local IP-Address 192.168.255.50 for Radius-Server
192.168.10.2
07:25:18: RADIUS(00000018): Send Access-Request to 192.168.10.2:1645 id
1645/15, len 68
07:25:18: RADIUS:  authenticator A5 EC 7A 6B AB BE 6E 15 - B9 49 63 81 BE 02
37 CE
07:25:18: RADIUS:  User-Name           [1]   6   "palo"
07:25:18: RADIUS:  User-Password       [2]   18  *
07:25:18: RADIUS:  NAS-Port            [5]   6   2
07:25:18: RADIUS:  NAS-Port-Id         [87]  6   "tty2"
07:25:18: RADIUS:  NAS-
sw-Test#Port-Type       [61]  6   Virtual                    [5]
07:25:18: RADIUS:  NAS-IP-Address      [4]   6   192.168.255.50
07:25:18: RADIUS(00000018): Sending a IPv4 Radius Packet
07:25:18: RADIUS(00000018): Started 5 sec timeout
07:25:18: RADIUS: Received from id 1645/15 192.168.10.2:1645, Access-Accept,
len 109
07:25:18: RADIUS:  authenticator 10 69 9C CD 51 A2 CE 3F - 7B C9 60 0F 6F 20
F4 7D
07:25:18: RADIUS:  Idle-Timeout        [28]  6   600
07:25:18: RADIUS:  Po
sw-Test#rt-Limit          [62]  6   1
07:25:18: RADIUS:  Service-Type        [6]   6   Callback Framed
[4]
07:25:18: RADIUS:  Class               [25]  46
07:25:18: RADIUS:   E1 AD 0B ED 00 00 01 37 00 01 02 00 C0 A8 0A 02 00 00 00
00 FD 50 BC FF D7 7D FF 3E 01 DA 6A ED EB 3D CD 4C 00 00 00 00 00 00 00 31
[ 7P}>j=L1]
07:25:18: RADIUS:  Vendor, Cisco       [26]  25
07:25:18: RADIUS:   Cisco AVpair       [1]   19  "shell:priv-lvl=15"
07:25:18: RADIUS(00000018): Received from id 1645/15
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

debug tacacs

```
login as: palo
Keyboard-interactive authentication prompts
from server:
|
| Password:
| 80090308: LdapErr: DSID-0C090449, comment:
AcceptSecurityContext error, data
> 52e, v3839 (463)
| Password incorrect.
End of keyboard-interactive prompts from
server
Access denied
Keyboard-interactive authentication prompts
from server:
|
| Password:
```

```
07:40:55: TPLUS: Queuing AAA Authentication request 29 for processing
07:40:55: TPLUS(0000001D) login timer started 1020 sec timeout
07:40:55: TPLUS: processing authentication start request id 29
07:40:55: TPLUS: Authentication start packet created for 29(palo)
07:40:55: TPLUS: Using server 192.168.XY.XY
07:40:55: TPLUS(0000001D)/0/NB_WAIT/C0CEC: Started 5 sec timeout
07:40:55: TPLUS(0000001D): wrote 42 bytes after server UP.
07:40:55: TPLUS(0000001D)/0/NB_WAIT: wrote entire 42 bytes request
07:
sw-Test#40:55: TPLUS: Would block while reading pak header
07:40:55: TPLUS(0000001D)/0/READ: read entire 12 header bytes (expect 17
bytes)
07:40:55: TPLUS(0000001D)/0/READ: read entire 29 bytes response
07:40:55: TPLUS(0000001D)/0/C0CEC: Processing the reply packet
07:40:55: TPLUS: Received authen response status GET_PASSWORD (8)



07:41:25: TPLUS: Queuing AAA Authentication request 29 for processing
07:41:25: TPLUS(0000001D) login timer started 1020 sec timeout
07:41:25: TPLUS: processing authentication continue request id 29
07:41:25: TPLUS: Authentication continue packet generated for 29
07:41:25: TPLUS(0000001D)/0/WRITE/C0CEC: Started 5 sec timeout
07:41:25: TPLUS(0000001D)/0/WRITE: wrote entire 26 bytes request
07:41:25: TPLUS(0000001D)/0/READ: read entire 12 header bytes (expect 120
bytes)
07:41:25: TPLUS(0000001D)/0/R
sw-Test#EAD: read entire 132 bytes response
07:41:25: TPLUS(0000001D)/0/C0CEC: Processing the reply packet
07:41:25: TPLUS: Received authen response status FAIL (3)
07:41:27: TPLUS: Queuing AAA Authentication request 29 for processing
07:41:27: TPLUS(0000001D) login timer started 1020 sec timeout
07:41:27: TPLUS: processing authentication start request id 29
07:41:27: TPLUS: Authentication start packet created for 29(palo)
07:41:27: TPLUS: Using server 192.168.XY.XY
07:41:27: TPLUS(0000001D)/0/IDLE/C0CEC:
sw-Test# got immediate connect on new 0
07:41:27: TPLUS(0000001D)/0/WRITE/C0CEC: Started 5 sec timeout
07:41:27: TPLUS(0000001D)/0/WRITE: wrote entire 42 bytes request
07:41:27: TPLUS(0000001D)/0/READ: read entire 12 header bytes (expect 17
bytes)
07:41:27: TPLUS(0000001D)/0/READ: read entire 29 bytes response
07:41:27: TPLUS(0000001D)/0/C0CEC: Processing the reply packet
07:41:27: TPLUS: Received authen response status GET_PASSWORD (8)
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

debug tacacs

```
login as: test
Keyboard-interactive authentication prompts
from server:
|
| Password:
End of keyboard-interactive prompts from
server

sw-Test>
sw-Test>ena
sw-Test#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
sw-Test(config)#



## len auth vas pusti dnu, ale nasledne
## v EXEC mozte zadat co chcete.
## treba authorization
```

```
08:03:44: TPLUS: Queuing AAA Authentication request 37 for processing
08:03:44: TPLUS(00000025) login timer started 1020 sec timeout
08:03:44: TPLUS: processing authentication start request id 37
08:03:44: TPLUS: Authentication start packet created for 37()
08:03:44: TPLUS: Using server 192.168.XT.XT
08:03:44: TPLUS(00000025)/0/IDLE/402D24: got immediate connect on new 0
08:03:44: TPLUS(00000025)/0/WRITE/402D24: Started 5 sec timeout
08:03:44: TPLUS(00000025)/0/WRITE: wrote entire 29 bytes reques

User Access Verification

Username: admt
08:03:44: TPLUS(00000025)/0/READ: read entire 12 header bytes (expect 43
bytes)
08:03:44: TPLUS(00000025)/0/READ: read entire 55 bytes response
08:03:44: TPLUS(00000025)/0/402D24: Processing the reply packet
08:03:44: TPLUS: Received authen response status GET_USER (7)


08:04:43: TPLUS: Queuing AAA Authentication request 38 for processing
08:04:43: TPLUS(00000026) login timer started 1020 sec timeout
08:04:43: TPLUS: processing authentication continue request id 38
08:04:43: TPLUS: Authentication continue packet generated for 38
08:04:43: TPLUS(00000026)/0/WRITE/402D24: Started 5 sec timeout
08:04:43: TPLUS(00000026)/0/WRITE: wrote entire 22 bytes request
08:04:43: TPLUS(00000026)/0/READ: read entire 12 header bytes (expect 16
bytes)
08:04:43: TPLUS(00000026)/0/READ: read entire 28 bytes response
08:04:43: TPLUS(00000026)/0/402D24: Processing the reply packet
08:04:43: TPLUS: Received authen response status GET_PASSWORD (8)


sw-Test>
08:05:19: TPLUS: Queuing AAA Authentication request 38 for processing
08:05:19: TPLUS(00000026) login timer started 1020 sec timeout
08:05:19: TPLUS: processing authentication continue request id 38
08:05:19: TPLUS: Authentication continue packet generated for 38
08:05:19: TPLUS(00000026)/0/WRITE/402D24: Started 5 sec timeout
08:05:19: TPLUS(00000026)/0/WRITE: wrote entire 26 bytes request
08:05:19: TPLUS(00000026)/0/READ: read entire 12 header bytes (expect 6
bytes)
08:05:19: TPLUS(00000026)/0/RE
sw-Test>AD: read entire 18 bytes response
08:05:19: TPLUS(00000026)/0/402D24: Processing the reply packet
08:05:19: TPLUS: Received authen response status PASS (2)
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE