ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

TELEKOMMUNIKATSIYA TARMOQLARIDA MARKAZLASHTIRILGAN KIRISHNI BOSHQARISHDA TACACS+ VA RADIUS TEXNOLOGIYALARINING QO'LLANILISHI VA XAVFSIZLIK SALOHIYATI

Alimatov Bekmurod Olimjon o'g'li
University of Management and Future Technologies
Kommunikatsiya va Raqamli Texnologiyalar Kafedrasi Magistranti.

https://doi.org/10.5281/zenodo.15429008

Annotatsiya. *Ushbu maqolada zamonaviy telekommunikatsiya tarmoqlarida markazlashtirilgan kirishni boshqarish tizimlarida TACACS+ va RADIUS protokollarining autentifikatsiya, avtorizatsiya va hisobga olish (AAA – Authentication, Authorization, Accounting) jarayonlaridagi o'rni yoritiladi. Protokollarning texnik xususiyatlari, ishlash prinsiplari, afzalliklari va kamchiliklari taqqoslanadi hamda ularning tarmoq xavfsizligini ta'minlashdagi salohiyati tahlil qilinadi.*

Kalit so'zlar: *AAA, autentifikatsiya, avtorizatsiya, hisobga olish, TACACS+, RADIUS, tarmoq xavfsizligi, markazlashtirilgan boshqaruv.*

ПРИМЕНЕНИЕ И ВОЗМОЖНОСТИ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ TACACS+ И RADIUS В ЦЕНТРАЛИЗОВАННОМ КОНТРОЛЕ ДОСТУПА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Аннотация. *На статье рассматривается роль протоколов TACACS+ и RADIUS в процессах аутентификации, авторизации и учета (AAA – Authentication, Authorization, Accounting) в централизованных системах контроля доступа в современных телекоммуникационных сетях. Сравниваются технические характеристики, принципы работы, преимущества и недостатки протоколов, анализируется их потенциал в обеспечении безопасности сети.*

Ключевые слова: *AAA, аутентификация, авторизация, учет, TACACS+, RADIUS, сетевая безопасность, централизованное управление.*

APPLICATION OF TACACS+ AND RADIUS TECHNOLOGIES IN CENTRALIZED ACCESS CONTROL IN TELECOMMUNICATION NETWORKS AND SECURITY CAPACITY

Abstract. *This article discusses the role of TACACS+ and RADIUS protocols in authentication, authorization, and accounting (AAA – Authentication, Authorization, Accounting) processes in centralized access control systems in modern telecommunication networks. The technical characteristics, operating principles, advantages and disadvantages of the protocols are compared, and their potential for ensuring network security is analyzed.*

Keywords: *AAA, authentication, authorization, accounting, TACACS+, RADIUS, network security, centralized management.*

KIRISH

Axborot texnologiyalarining jadal rivojlanishi natijasida korxonalar, tashkilotlar va xizmat ko'rsatuvchi provayderlar telekommunikatsiya tarmoqlarining xavfsizligi va ishonchliligini ta'minlashga tobora ko'proq e'tibor qaratmoqda.

Ayniqsa, yirik korporativ tarmoqlarda foydalanuvchilar va administratorlarning kirishlarini markazlashtirilgan tarzda boshqarish ehtiyoji yuzaga kelmoqda. Bu ehtiyojni qondirish uchun autentifikatsiya, avtorizatsiya va hisobga olish (AAA) tizimlari qo‘llaniladi.

AAA tizimlari orqali foydalanuvchi shaxsini aniqlash, unga ruxsat beriladigan resurslarni belgilash hamda uning faoliyatini doimiy nazorat qilish imkoniyati mavjud. Bunday markazlashtirilgan boshqaruvni amalga oshirish uchun esa RADIUS va TACACS+ protokollari eng ommabop va samarali yechimlardan hisoblanadi.

Mazkur maqolada aynan ushbu ikki protokolning texnik jihatlari, tarmoq xavfsizligidagi o‘rni, qo‘llanilishi va ularning o‘zaro farqlari chuqur tahlil qilinadi.

AAA MEXANIZMLARI: NAZARIY ASOSLAR

Telekommunikatsiya tarmoqlarining xavfsizligi foydalanuvchilarni tarmoq resurslariga cheklangan va nazoratli tarzda ulash orqali ta’minlanadi. Bu jarayonda autentifikatsiya, avtorizatsiya va hisobga olish (AAA) mexanizmlari asosiy rol o‘ynaydi:

- **Autentifikatsiya (Authentication)** — foydalanuvchining shaxsini aniqlash jarayoni bo‘lib, u ko‘pincha login va parol, biometrik ma’lumotlar, sertifikatlar yoki tokenlar orqali amalga oshiriladi. Bu bosqichda tizim foydalanuvchining kimligini tekshiradi.
- **Avtorizatsiya (Authorization)** — autentifikatsiyadan o‘tgan foydalanuvchiga qanday resurslardan, qanday darajada foydalanish mumkinligini aniqlash jarayoni. Bu ruxsat siyosatlari, rolga asoslangan kirish nazorati (RBAC) yoki maxsus siyosat dvijoklari orqali boshqariladi.
- **Hisobga olish (Accounting)** — foydalanuvchining tarmoqdagi harakatlarini qayd etish, ularga monitoring o‘rnatish va statistik ma’lumotlarni to‘plash jarayoni. Bu jarayon yordamida tarmoqdan foydalangan vaqt, resurslar, xizmatlar hajmi va boshqa parametrlar nazorat qilinadi.

AAA tizimlari xavfsizlik siyosatining asosiy qismi bo‘lib, ma’murlar uchun real vaqt rejimida kirishni boshqarish, huquqlarni sozlash, hamda foydalanuvchilarning harakatlarini tahlil qilish imkonini beradi.

TACACS+ TEXNOLOGIYASI

TACACS+ (Terminal Access Controller Access-Control System Plus) — bu Cisco tomonidan ishlab chiqilgan va xavfsiz tarmoq kirishini boshqarishga mo‘ljallangan protokol bo‘lib, u autentifikatsiya, avtorizatsiya va hisobga olish jarayonlarini alohida amalga oshirish imkoniyatiga ega. U TCP asosida ishlaydi va ma’lumotlarni to‘liq shifrlash bilan ajralib turadi.

Texnik xususiyatlari:

- **Transport protokoli**: TCP (odatda 49-port);
- **Shifrlash**: barcha AAA komponentlari (login, parol, ruxsatlar, loglar) shifrlanadi;
- **Moslik**: asosan Cisco qurilmalari bilan optimal ishlaydi;
- **Avtorizatsiya moslashuvi**: foydalanuvchilarga granular huquqlarni taqdim etish mumkin.

Afzalliklari:

- **Yuqori xavfsizlik**: barcha trafik to‘liq shifrlangan bo‘lib, ma’lumotlar sizib chiqish xavfi minimal darajaga tushiriladi;
- **Avtonom boshqaruv**: AAA komponentlarining alohida boshqarilishi ma’murlar uchun katta moslashuvchanlikni ta’minlaydi;
- **Detalizatsiyalangan audit**: foydalanuvchi harakatlarini chuqur tahlil qilish mumkin.

Kamchiliklari:

- **Mos keluvchanlik chegaralangan**: asosan Cisco tarmoq qurilmalari uchun mo‘ljallangan;
- **Murakkab sozlash**: boshqa protokollarga nisbatan sozlash va integratsiya qilish murakkabroq;
- **Qo‘shimcha infratuzilma zarurati**: alohida TACACS+ serverlarini tashkil etish talab qilinadi.

TACACS+ ayniqsa katta korporativ tarmoqlarda va xavfsizlik talablari yuqori bo‘lgan tizimlarda qo‘llaniladi.

RADIUS TEXNOLOGIYASI

RADIUS (Remote Authentication Dial-In User Service) — bu IETF (Internet Engineering Task Force) tomonidan standart sifatida ishlab chiqilgan va bugungi kunda ko‘plab tarmoq uskunalari tomonidan qo‘llab-quvvatlanadigan protokoldir. U ko‘p platformali muhitlarda foydalanuvchilarning tarmoqqa kirishini nazorat qilish uchun ishlatiladi.

Texnik xususiyatlari:

- **Transport protokoli**: UDP (1812 – autentifikatsiya, 1813 – hisobga olish);
- **Shifrlash**: faqat parollar shifrlanadi, boshqa ma’lumotlar ochiq ko‘rinishda yuboriladi;
- **Keng tarqalganlik**: ko‘plab OS, qurilma va platformalarda qo‘llab-quvvatlanadi;
- **Yengil va tez**: ishlash tezligi yuqori, resurslar kam talab qilinadi.

Afzalliklari:

- **Universallik**: har xil ishlab chiqaruvchilar tomonidan qo‘llaniladi, ochiq standartlarga asoslangan;
- **Sodda konfiguratsiya**: ma’murlar uchun oson sozlanadi va integratsiya qilinadi;
- **Tezkor ishlash**: yengil arxitekturasi tufayli yuqori samaradorlikka ega.

Kamchiliklari:

- **Xavfsizlik cheklovlari**: faqat parol shifrlanadi, qolgan trafik tahlil qilinishi mumkin;
- **AAA elementlarining birgalikda ishlashi**: avtorizatsiya va hisobga olish bosqichlari mustaqil emas;
- **Audit imkoniyatlari cheklangan**: harakatlar bo‘yicha batafsil hisobotlar yaratish qiyinroq.

RADIUS kichik va o‘rta darajadagi tarmoqlarda, Wi-Fi kirish nuqtalarida, VPN tizimlarida va ISP xizmatlarida keng qo‘llaniladi.

TACACS+ VA RADIUS TAQQOSLANISHI

TACACS+ va RADIUS protokollari har ikkisi ham AAA funksiyalarini bajarishga mo‘ljallangan bo‘lsa-da, ularning arxitekturasi, xavfsizlik darajasi, ishlash usuli va qo‘llanilish sohasi jihatidan sezilarli farqlari mavjud.

Ko‘rsatkich	TACACS+	RADIUS
Ishlash protokoli	TCP (port 49)	UDP (port 1812/1813 yoki 1645/1646)
Shifrlash darajasi	Barcha ma’lumotlar shifrlanadi	Faqat parol shifrlanadi
AAA	Har biri mustaqil ishlaydi	Avtorizatsiya va hisobga olish

Ko‘rsatkich	TACACS+	RADIUS
komponentlari		birgalikda
Tizimga moslashuv	Asosan Cisco qurilmalari	Turli ishlab chiqaruvchilarning qurilmalari
Moslashuvchanlik	Yuqori (detallangan siyosatlar)	O‘rtacha (asosiy ruxsatlar)
Audit va nazorat	Batafsil va moslashtirilgan	Cheklangan
Tarmoqdagi yuk	Nisbatan katta (TCP, to‘liq shifrlash tufayli)	Nisbatan kam (yengil UDP)
Qo‘llanish sohasi	Xavfsizlik muhim bo‘lgan yirik tarmoqlar	Wi-Fi, VPN, ISP, umumiy autentifikatsiya

Ushbu taqqoslashdan ko‘rinib turibdiki, TACACS+ xavfsizlik va nazorat darajasi yuqori bo‘lgan tizimlar uchun qulay, RADIUS esa ko‘proq umumiy foydalanish va platformalararo muvofiqlik uchun qulaylik yaratadi.

AMALIY QO‘LLANILISH VA TAVSIYALAR

TACACS+:

- **Qo‘llash sohasi**: korporativ tarmoqlar, bank tizimlari, davlat muassasalari, harbiy sohalar.
- **Afzalliklar**: har bir foydalanuvchining aniq huquqlarini sozlash, auditni batafsil yuritish, xavfsiz transport protokoli (TCP).
- **Tavsiya etiladi**, agar sizda quyidagilar mavjud bo‘lsa:
  - Cisco asosidagi tarmoq infratuzilmasi;
  - Maxfiy ma’lumotlar bilan ishlovchi tashkilot;
  - Markaziy boshqaruv va tahlil vositalari uchun ehtiyoj.

RADIUS:

- **Qo‘llash sohasi**: Internet-provayderlar, mehmonxona Wi-Fi tarmoqlari, universitet kampuslari, VPN xizmatlari.
- **Afzalliklar**: kengaytirilgan moslik, tez ishlash, oddiy sozlash, yengil tizim talablari.
- **Tavsiya etiladi**, agar:
  - Sizga tez va keng qamrovli autentifikatsiya kerak bo‘lsa;
  - Turli platformalarda (Linux, Windows, Mikrotik, Juniper) ishlovchi tarmoq mavjud bo‘lsa;
  - Kam resurs sarflovchi autentifikatsiya serveri zarur bo‘lsa.

Amaliy holatlar:

- **Wi-Fi kirish nuqtalarida**: RADIUS serverlar orqali mehmonlar va xodimlar uchun alohida autentifikatsiya siyosatlari joriy etiladi.
- **Tarmoq boshqaruvchilari uchun**: TACACS+ yordamida kim, qachon, qaysi qurilmaga qanday buyruq kiritganini batafsil loglarda qayd etish mumkin.

XULOSA

Telekommunikatsiya tarmoqlarida xavfsizlikni ta’minlash va foydalanuvchi kirishini markazlashtirilgan holda boshqarish zamonaviy infratuzilmalarning ajralmas qismiga aylangan.

Bu borada TACACS+ va RADIUS protokollari autentifikatsiya, avtorizatsiya va hisobga olish (AAA) mexanizmlarini amalga oshirishda asosiy vositalardan hisoblanadi.

- **TACACS+** — yuqori xavfsizlik, to‘liq shifrlash, kuchli audit tizimi va granular boshqaruv imkoniyatlari bilan ajralib turadi. Bu protokol katta, xavfsizlik darajasi yuqori bo‘lgan tashkilotlar uchun ideal tanlovdir.
- **RADIUS** esa ochiq standart, ko‘p platformali muvofiqlik, yengil arxitektura va keng qamrovli qo‘llanilishi bilan amaliyotda keng tarqalgan. Bu uni umumiy foydalanishdagi autentifikatsiya tizimlarida samarali qiladi.

Shunday qilib, qaysi protokolni tanlash tarmoqning tuzilishi, xavfsizlik darajasi va boshqaruv ehtiyojlariga bog‘liq. Ko‘p hollarda esa, **ikkala protokolni birgalikda** yoki bosqichma-bosqich joriy etish orqali tizimni yanada mukammallashtirish mumkin.

REFERENCES

1. Stallings, W. **Data and Computer Communications**. — 10th ed. — Pearson Education, 2013. — 888 p.
2. Radia Perlman, Charlie Kaufman, Mike Speciner. **Network Security: Private Communication in a Public World**. — 2nd ed. — Prentice Hall, 2002. — 752 p.
3. Cisco Systems. **Cisco Secure Access Control System (ACS) TACACS+ Configuration Guide**. — https://www.cisco.com
4. Rigney, C. **Remote Authentication Dial In User Service (RADIUS)**. — IETF RFC 2865, June 2000. — https://datatracker.ietf.org/doc/html/rfc2865
5. Cisco Systems. **TACACS+ Protocol Specification**. — https://www.cisco.com/c/en/us/about/security-center/tacacs-protocol.html
6. Behrouz A. Forouzan. **Data Communications and Networking**. — 5th ed. — McGraw-Hill, 2013. — 1264 p.
7. Tanenbaum A. S., Wetherall D. J. **Computer Networks**. — 5th ed. — Pearson Education, 2010. — 960 p.
8. Владимир Н. Егоров. **Безопасность компьютерных сетей**. — СПб.: Питер, 2018. — 448 с.
9. Марков Д.С., Соколов С.М. **Информационная безопасность компьютерных систем и сетей**. — М.: Академия, 2019. — 368 с.
10. Microsoft Learn. **Implementing RADIUS Authentication**. — https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top
11. Open Source Tool: **FreeRADIUS Project Documentation**. — https://freeradius.org
12. Кучкаров, Ш.Х., Турсунов А.А. **Telekommunikatsiya tizimlari va tarmoqlari**. — Toshkent: TDTTU, 2021. — 290 b.