

// открытый практикум CyberED

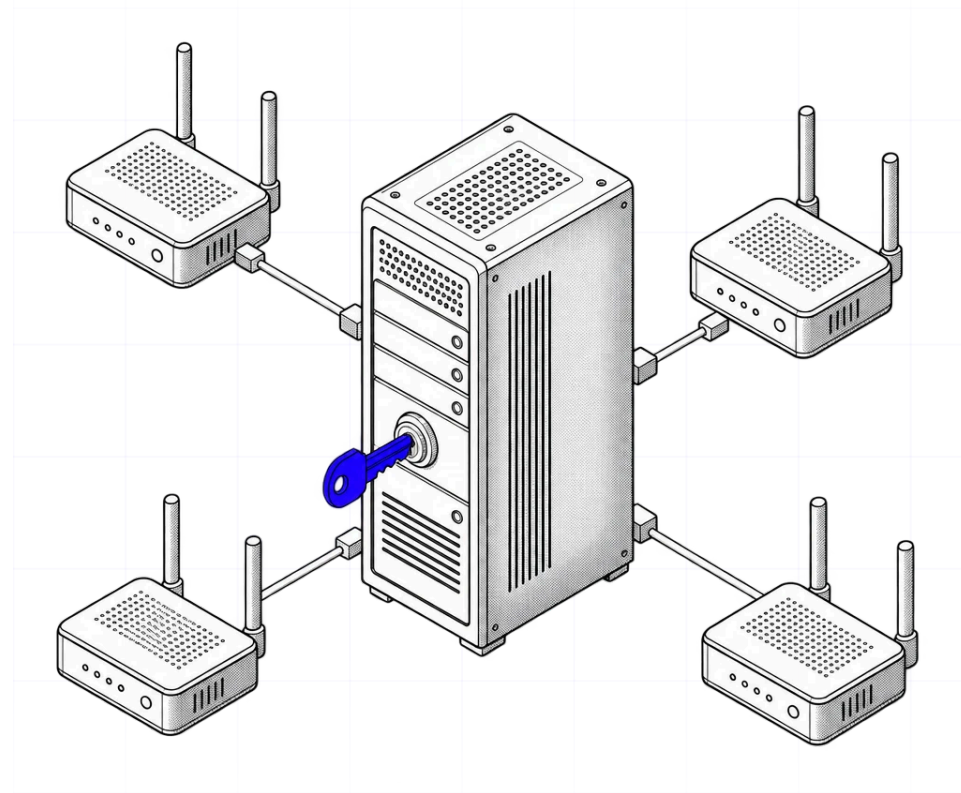
Безопасный доступ к сети компании

Централизованное управление доступом (AAA)
средствами протокола RADIUS на маршрутизаторах
Eltex

1 октября, четверг

19:00 МСК

онлайн





ШАБАЛИН АНДРЕЙ

- > 2011–2022 г.г.: тренер, инструктор академий Cisco, Huawei
- > 2022 — по н.в.: инструктор «Академия Eltex», «Астра Академия», «Альт Академия»
- > кандидат наук, доцент кафедры ИБ ТюмГУ



Тренируемся вместе

Группа VK: «Компьютерные сети и сетевая безопасность»

vk.com/utmn_network

МАТЕРИАЛЫ

- | | |
|----------------------|--|
| 1. Oracle VirtualBox | www.virtualbox.org/wiki/Downloads |
| 2. GNS3 | github.com/GNS3/gns3-gui/releases |
| 3. Образы и VM Eltex | eltex-co.ru/catalog/virtualnyi-servisnyi-marsrutizator-vesr/ |
| 4. Базовый софт | disk.360.yandex.ru/d/kf_wx_EvP6W_MQ |

Сервисные маршрутизаторы ESR

Наименование	Описание
vESR FREE	Опция программный сервисный маршрутизатор vESR FREE, 1 Mbit/s, 1024 RIB BGP, 1000 RIB OSPF, 1000 RIB RIP, 1000 RIB ISIS, 2 VPN

Особенности

- Running-config
- Candidate-config
- Commit
- Confirm
- Rollback
- Restore
- Save

Default Credentials

admin / password

FREE vESR_1.40.4: [disk.360.yandex.ru/d/AP9ipc7RmT7Bag](https://disk.yandex.ru/d/AP9ipc7RmT7Bag)



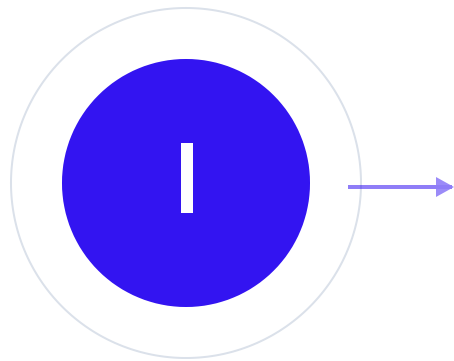
Теоретические сведения. SSH

SSH (Secure SHell):

- TCP 22 порт;
- v1 = 1995 год (Тату Юлөнен, Tatu Ylönen);
- v2 = 2006 год (RFC 4253): datatracker.ietf.org/doc/rfc4253/
- OpenSSH.

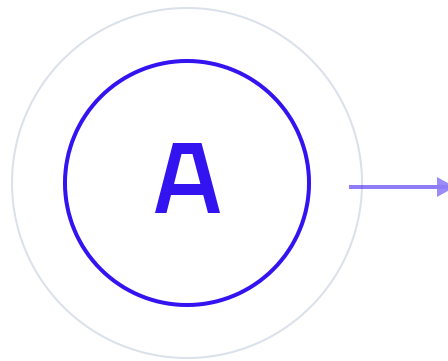


AAA. Теоретические сведения.



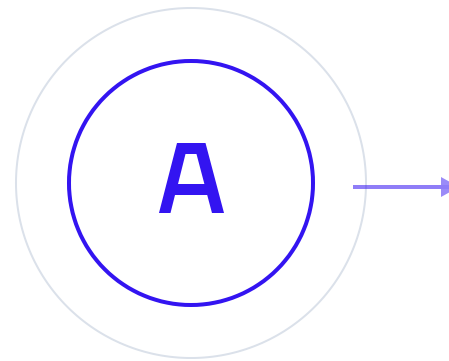
Identification

ввод идентифицирующей
информации (имя
пользователя)



Authentication

проверка идентифицирующей
информации (пароль)



Authorization

получение прав по
результатам успешной
аутентификации



Accounting

учёт событий (аудит)

AAA. Теоретические сведения.

Локальная база AAA:

- Учетные записи, пароли и права хранятся на самом устройстве.
- Трудно масштабируется.
- Небольшие сети.
- Учет не поддерживается.

Централизованная база AAA:

- Учетные данные создаются \ изменяются централизованно и доступны на всех сетевых устройствах.
- Крупные сети. Более простое обслуживание.
- Централизованный аудит.
- Может стать единой точкой отказа.



AUTHENTICATION



AUTHORIZATION



ACCOUNTING

ESR AAA:

Authentication	Local + Remote (Radius / Tacacs+ / LDAP)
Authorization	Privilege Levels + Remote (Radius / Tacacs+ (commands) / LDAP)
Accounting	(Radius / Tacacs+)

RADIUS vs TACACS+

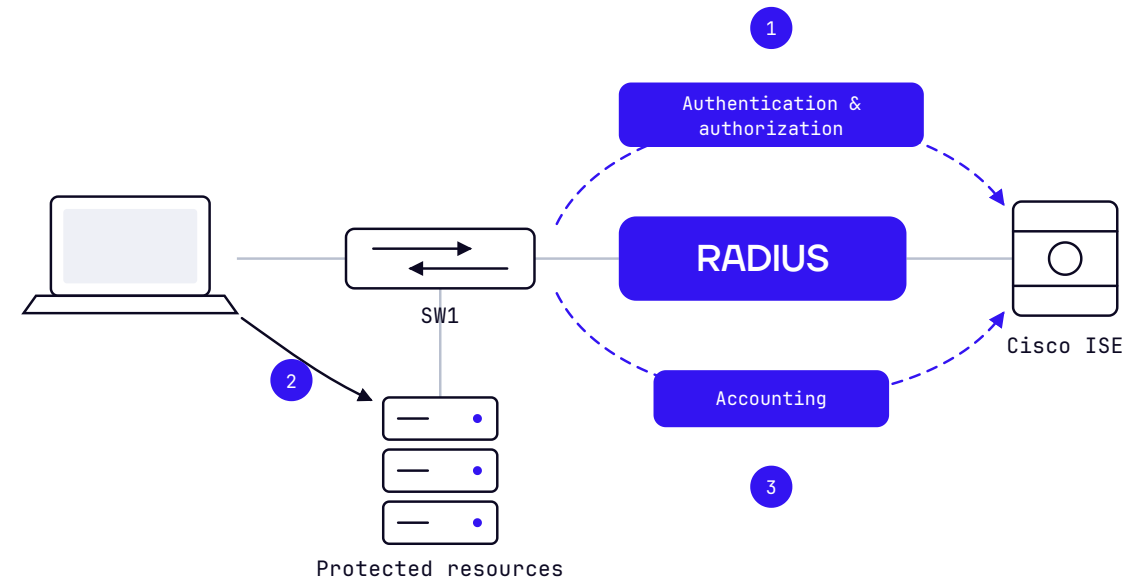
Feature	TACACS+	RADIUS
Authentication and Authorization	Separated	Combined
Accounting	Separated	Separated
Protocol	Cisco proprietary	Open standard
Transmission Protocol	TCP	UDP
Encryption	All AAA packets are encrypted	Only passwords are encrypted
Port Number	49	1812 — authentication and authorization, 1813 — accounting
Granular Control over Authorization	Yes, can specify the particular command	No external authorization of commands
Multiprotocol Support	Yes	No
Device Administration or Network Access	Device administration	Network access

Протоколы AAA

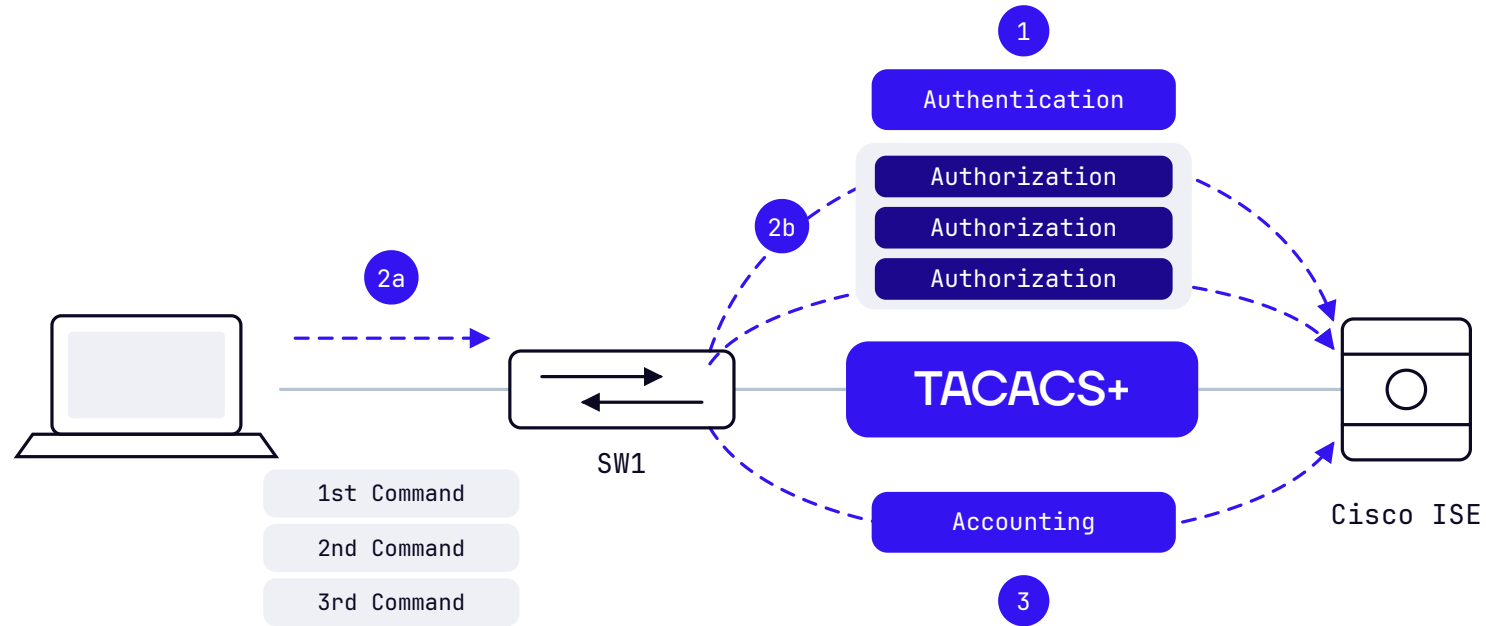
- | | |
|-------------|---|
| 1) RADIUS | Remote Authentication Dial In User Service —
RFC 2865 |
| 2) Diameter | RFC 6733 |
| 3) TACACS+ | Terminal Access Controller Access-Control
System Plus ⇒ Cisco — RFC 8907 |

AAA-server:

- **Network Policy Server (NPS)** ⇒ MS Windows Server.
- **freeradius:** freeradius.org
- **tac_plus:** [manpages.debian.org – tac_plus.8](https://manpages.debian.org/tac_plus.8)



TACACS+ NAC



// NAC – Network Access Control

Cisco ACS

Access Control Server

Cisco ISE

Identity Services Engine

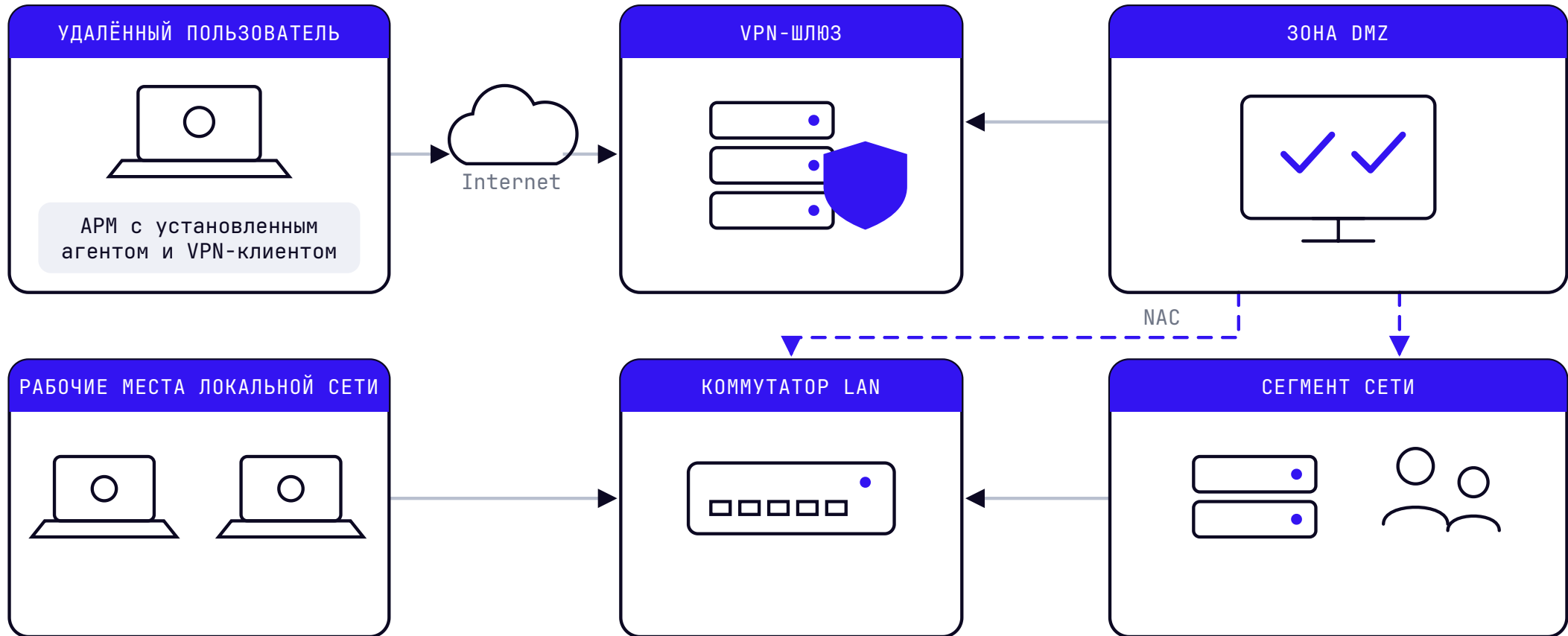
Huawei iMaster NCE-Campus

Agile Controller-Campus

Eltex NAICE

Network Access and Information Control Engine

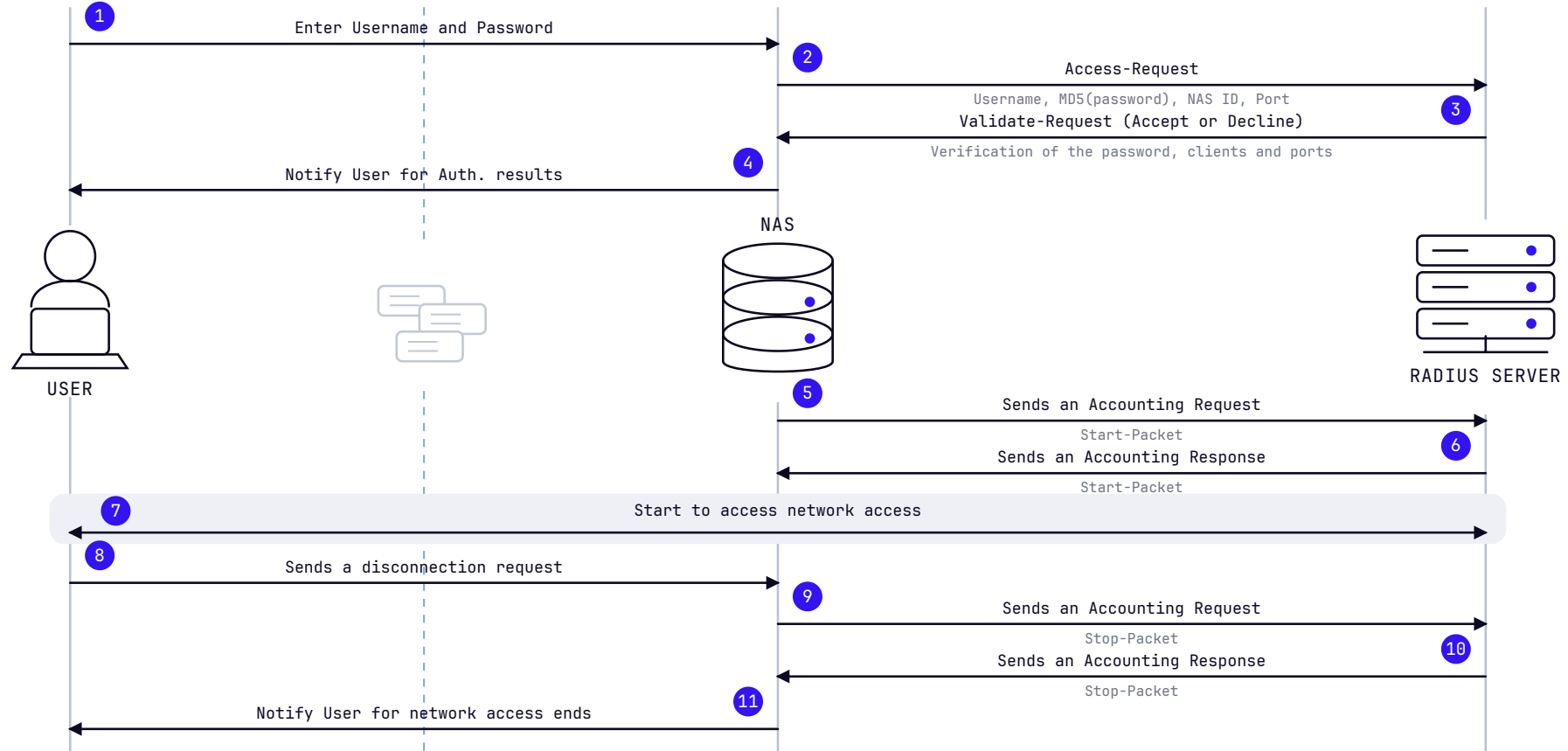
Функции систем контроля доступа (NAC)



Функции систем контроля доступа (NAC)

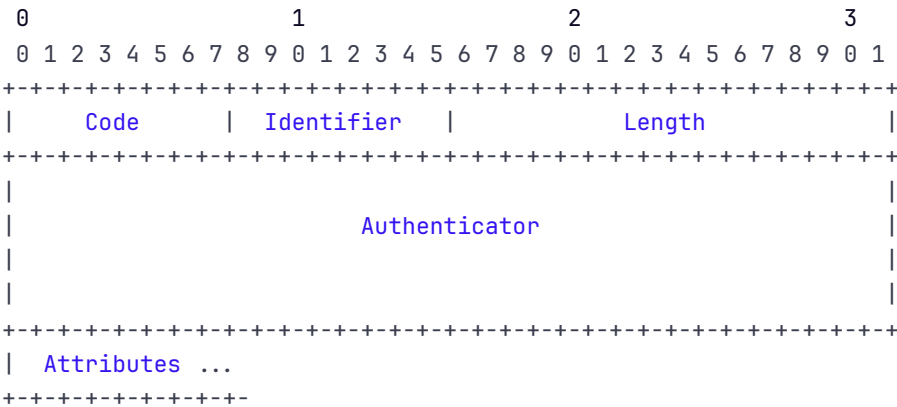
- > Контроль кабельных, беспроводных и удаленных (VPN) подключений.
- > Поддержка аутентификации по стандарту 802.1x (доступ в сеть по учетным данным, цифровым сертификатам, MAC-адресам).
- > Политики авторизации: загружаемые ACL, назначение VLAN, перенаправление на URL, поддержка RADIUS CoA и др.
- > Управление доступом к сетевому оборудованию с поддержкой протоколов TACACS+ и RADIUS.
- > Интеграция со службами каталогов: MS Active Directory, FreeIPA, OpenLDAP и т.д.
- > Профилирование подключаемых устройств и разграничение доступа на его основе.
- > Поддержка разных методов аутентификации.
- > Наличие встроенного центра управления сертификатами PKI (Public Key Infrastructure) или интеграция с имеющимися.
- > Создание гостевых порталов с возможностью саморегистрации пользователей по CMC и email.
- > Журналирование сессий подключения для выявления инцидентов ИБ и контроля корректности настройки политик доступа.
- > Проверка подключаемых устройств на соответствие политикам безопасности с помощью установленных агентов.

* NAS (Network Access Server) => router, switch, firewall



Radius. Теоретические сведения.

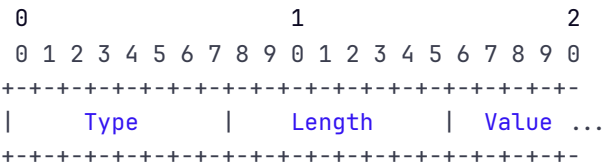
формат пакета



Code — один октет, задаёт тип пакета; пакет с недопустимым Code отбрасывается без ответа

1	Access-Request	11	Access-Challenge
2	Access-Accept	12	Status-Server (exp.)
3	Access-Reject	13	Status-Client (exp.)
4	Accounting-Request	255	Reserved
5	Accounting-Response		

формат атрибута



Значение атрибута — один из пяти типов данных; тип text является подмножеством типа string

text	1–253 octets, UTF-8 encoded 10646 characters; text of length zero (0) MUST NOT be sent.
string	1–253 octets of binary data (0–255 decimal); strings of length zero (0) MUST NOT be sent.
address	32 bit value, most significant octet first.
integer	32 bit unsigned value, most significant octet first.
time	32 bit unsigned value — seconds since 00:00:00 UTC, January 1, 1970.

Radius. Атрибуты

1	User-Name	16	Login-TCP-Port	31	Calling-Station-Id
2	User-Password	17	(unassigned)	32	NAS-Identifier
3	CHAP-Password	18	Reply-Message	33	Proxy-State
4	NAS-IP-Address	19	Callback-Number	34	Login-LAT-Service
5	NAS-Port	20	Callback-Id	35	Login-LAT-Node
6	Service-Type	21	(unassigned)	36	Login-LAT-Group
7	Framed-Protocol	22	Framed-Route	37	Framed-AppleTalk-Link
8	Framed-IP-Address	23	Framed-IPX-Network	38	Framed-AppleTalk-Network
9	Framed-IP-Netmask	24	State	39	Framed-AppleTalk-Zone
10	Framed-Routing	25	Class	40-59	(reserved for accounting)
11	Filter-Id	26	Vendor-Specific	60	CHAP-Challenge
12	Framed-MTU	27	Session-Timeout	61	NAS-Port-Type
13	Framed-Compression	28	Idle-Timeout	62	Port-Limit
14	Login-IP-Host	29	Termination-Action	63	Login-LAT-Port
15	Login-Service	30	Called-Station-Id		

Radius. Атрибуты

1. Стандартные атрибуты IETF (RFC-совместимые)

определены в RFC и поддерживаются всеми. Примеры:

ID	атрибут	назначение
1	User-Name	имя пользователя для аутентификации (например, andrey)
2	User-Password	пароль, передаётся в зашифрованном виде \ MD5
4	NAS-IP-Address	IP-адрес сетевого устройства, отправляющего запрос
6	Service-Type	тип услуги: Login-User — консоль, Framed-User — интернет
8	Framed-IP-Address	IP-адрес, который сервер выдаёт клиенту при авторизации
40	Acct-Status-Type	в пакетах учёта: начало (Start) или конец (Stop) сессии

2. Атрибуты, специфические для поставщика (VSA, Vendor-Specific Attributes)

проприетарные атрибуты, которые производители оборудования используют для передачи дополнительной информации. VSA инкапсулируются внутри стандартного атрибута с ID 26 (Vendor-Specific).

Пример: Cisco VSA для передачи уровня привилегий — Cisco-AVPair = "shell:priv-lvl=15"

Аутентификация

```
ESR1(config)# aaa authentication
```

- **login:** настройка списков методов аутентификации для первичного входа.
- **enable:** настройка списков методов аутентификации для доступа к более высоким уровням привилегий.
- **mode:** настройка режима работы со списками методов аутентификации.

По умолчанию включена аутентификация по локальной базе данных (`method list: Default`).

Режимы работы со списками методов аутентификации: `aaa authentication mode { break | chain }`

- **break:** при аутентификации будут использоваться последующие методы в случае недоступности более приоритетного;
- **chain:** при аутентификации будут использоваться последующие методы в случае получения отказа от более приоритетного.

Авторизация

1–4

базовый мониторинг функционала; запрет настройки

5–9

полный мониторинг, включая просмотр состояния функционала безопасности; запрет настройки

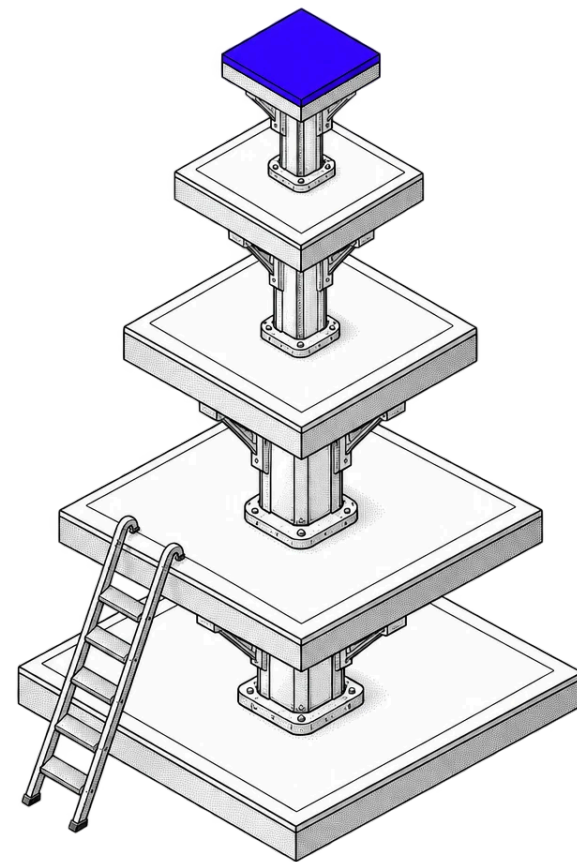
10–14

настройка большей части функционала, за исключением создания пользователей, перезагрузки устройства и загрузки ПО

15

доступ и настройка всех функций (нет ограничений)

У каждой команды есть требования к минимальному уровню привилегий пользователя



СПАСИБО ЗА ВНИМАНИЕ!
Практика...

Стенд остаётся у тебя

После эфира пришлём дистрибутивы, базовое программное обеспечение и учётные данные стенда — соберёшь тот же сценарий у себя и добавишь его в портфолио.



программа

«Инженер по ИБ»

старт потока

21 октября

// ЧЕМ ОТЛИЧАЕТСЯ ПРОГРАММА

Интенсив на 6 месяцев

вместо года — без тем, которые не влияют на найм

«3 в 1»

сети, Windows и Linux, средства защиты — одна траектория

Программа под рынок

разработана и обновляется по анализу спроса и вакансий

Стенды собираешь сам

сеть в GNS3, серверы на Linux и Windows, средства защиты

// ЧТО НОВОГО В ПОТОКЕ

ИБ 360

инженер · атакующий · защитник · AI-security — четыре ракурса на одну инфраструктуру

Все новые интенсивы уже внутри программы

ИИ-обучение с самого начала

Вебинары с Антоном Кузьминым

Технический директор Positive Technologies · ex-CTO Innostage

Подготовка к стажировкам и рабочий проект



Программа на сайте

new.cyber-ed.ru/inzhener-ib