
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Меня хорошо видно && слышно?

Ставьте +, если все хорошо
Напишите в чат, если есть проблемы

AAA

Кулиничев Алексей
Администратор Сетей
Santchous42@yandex.ru

Правила вебинара

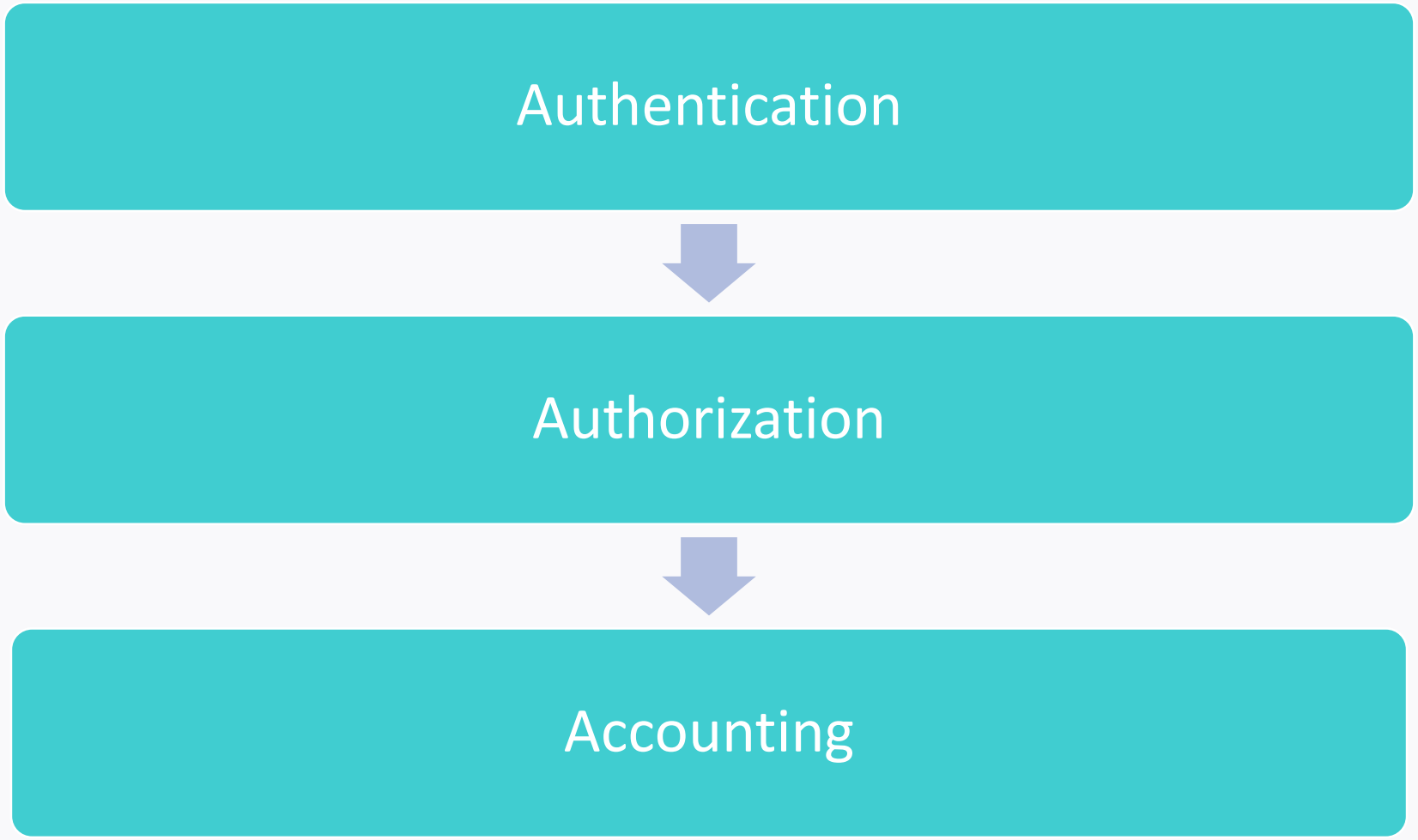
Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара



1 Authentication

Authentication

Виды аутентификации:

- Односторонняя
- Двусторонняя

Authentication

Элементы системы аутентификации:

- субъект, который проходит процедуру
- характеристика субъекта — отличительная черта
- хозяин системы аутентификации, несущий ответственность и контролирующий её работу
- механизм аутентификации, то есть принцип работы системы
- механизм управления доступом, предоставляющий определённые права доступа субъекту

Authentication

Элемент аутентификации	Пещера 40 разбойников	Регистрация в системе
Субъект	Человек, знающий пароль	Пользователь
Характеристика	Пароль "Сим-Сим, откройся!"	Тайный пароль
Хозяин системы	40 разбойников	Предприятие
Механизм аутентификации	Волшебное устройство, реагирующее на слова	ПО, проверяющее пароль
Механизм управления доступом	Механизм, отодвигающий камень от входа в пещеру	Процесс регистрации

Authentication

Authentication

Аутентификация в систему:

- Password Authentication Protocol, PAP (связка логин-пароль)
- Карта доступа (USB с сертификатом, SSO)
- Биометрия (голос, отпечаток пальца/ладони/радужки глаза)

Аутентификация в сети:

- Secure SNMP с использованием цифровой подписи
- Cookie сессии
- Kerberos Tickets
- Сертификаты X.509

Identification

Процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор

Вариант идентификации	Факторы аутентификации	Результат идентификации (идентификатор)
Идентификация пользователя	Логин/пароль	Логин
Идентификация по банковской карте	микропроцессорная банковская карта, ПИН-код	Учетный номер карты (PAN) - считывается с банковской карты
Идентификация по банковской карте с биоверификацией	микропроцессорная банковская карта, биометрический фактор (отпечаток пальца)	Учетный номер карты (PAN) - считывается с банковской карты
Идентификация товара по штрих-коду	штрих-код	Учетный номер товара

2 Authorization

Authorization

Авторизации – процесс предоставление прав доступа к каким-либо ресурсам или системам.
Есть несколько видов авторизации которые делятся на:

1. Дискреционное управление доступом(DAC)
2. Мандатное управление доступом(MAC)
3. Управление доступом на основе ролей(RBAC)
4. Другие типы управления доступом(CBAC, LBAC, ABAC и др.)

Authorization

Дискреционное управление доступом(DAC) –

Доступ предоставляется явно указанным субъектам, пользователям или группам пользователей.

Эта система имеет одного выделенного служебного субъекта – суперпользователя, имеющего право устанавливать права доступа для любых субъектов.

Authorization

Мандатное управление доступом(MAC)

Разделение информации по степени секретности, а пользователей по уровню доступа к этой информации.
Главное преимущество ограничение прав владельца объекта.

Поддерживается операционными системами Ubuntu, SUSE, FreeBSD

Может применяться вместе с дискреционным контролем доступа

Authorization

Управление доступом на основе ролей(RBAC)

Доступ сформирован с учетом специфики применения политик доступа, на основе роли объекта в каждый момент времени.
Похож на мандатный способ управления доступа, но обладает более гибкими настройками.
Часто используется для управления пользовательскими правами доступа в пределах системы или приложения.

- Microsoft Active Directory
- SELinux
- PostgreSQL

3 Accounting

Accounting

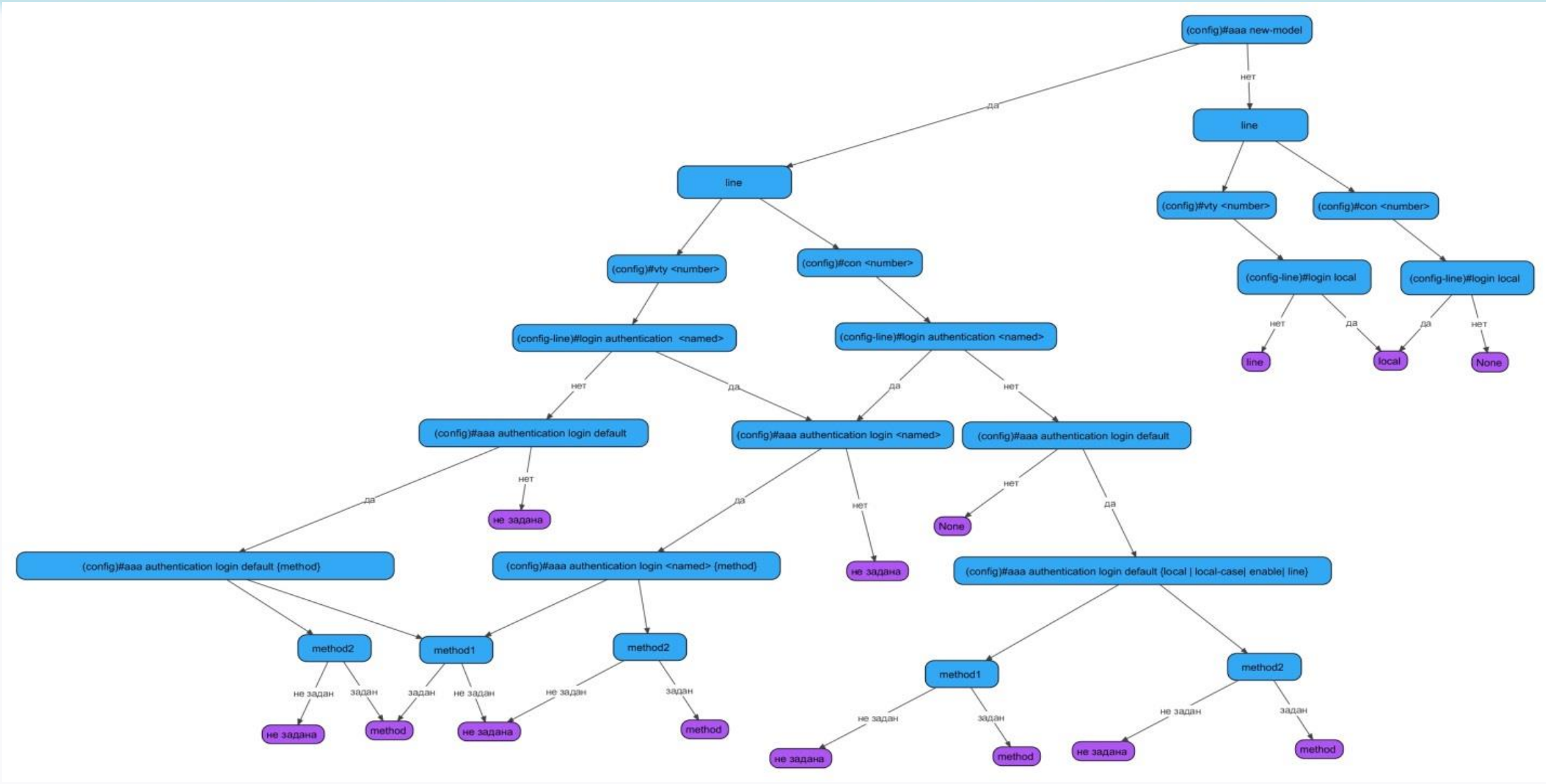
Функция учета AAA позволяет отслеживать сервисы, к которым пользователи получают доступ, а также потребляемый объем сетевых ресурсов.

Дополнительно можно отслеживать действия пользователей на оборудовании

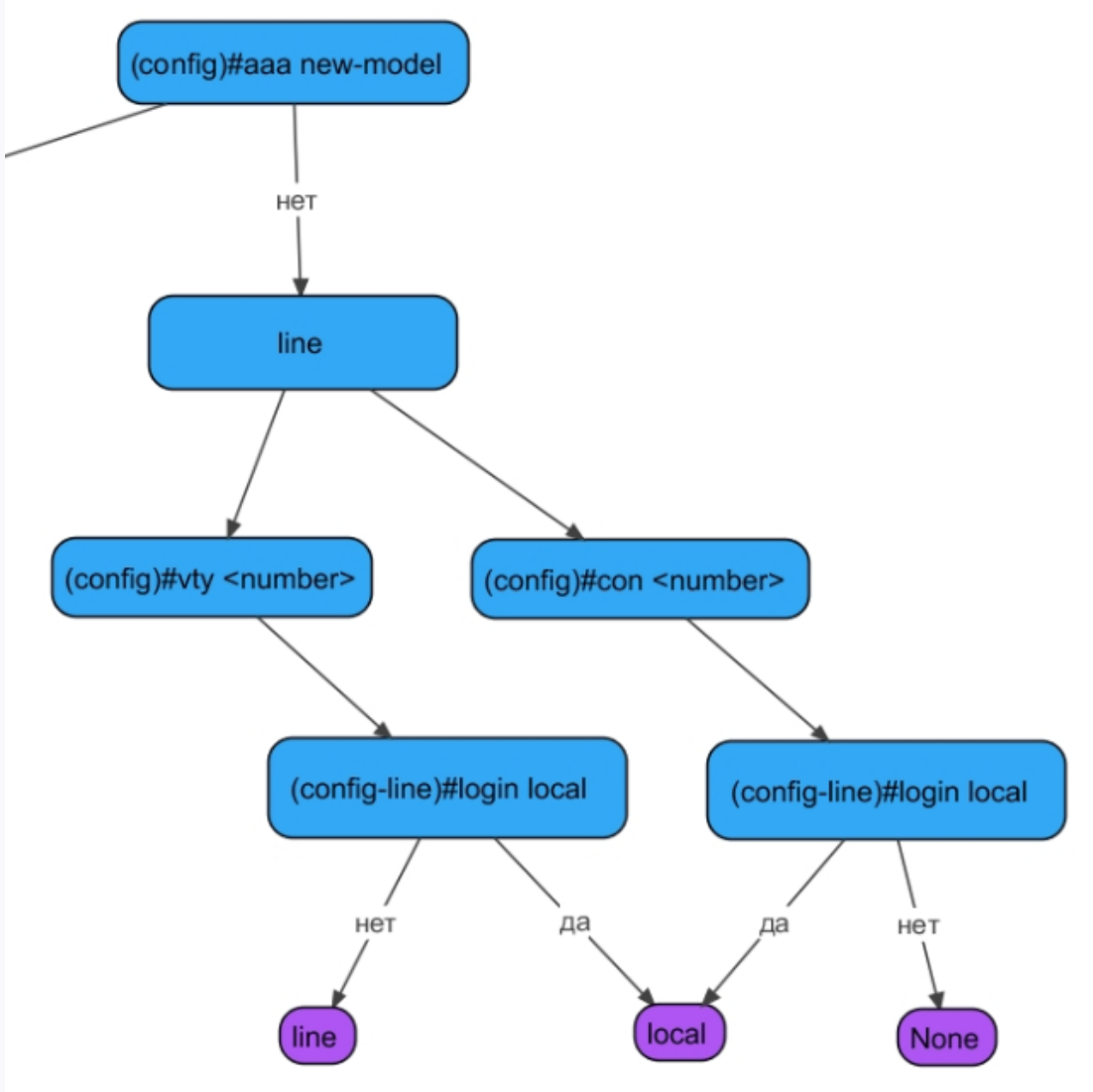
4

AAA в cisco

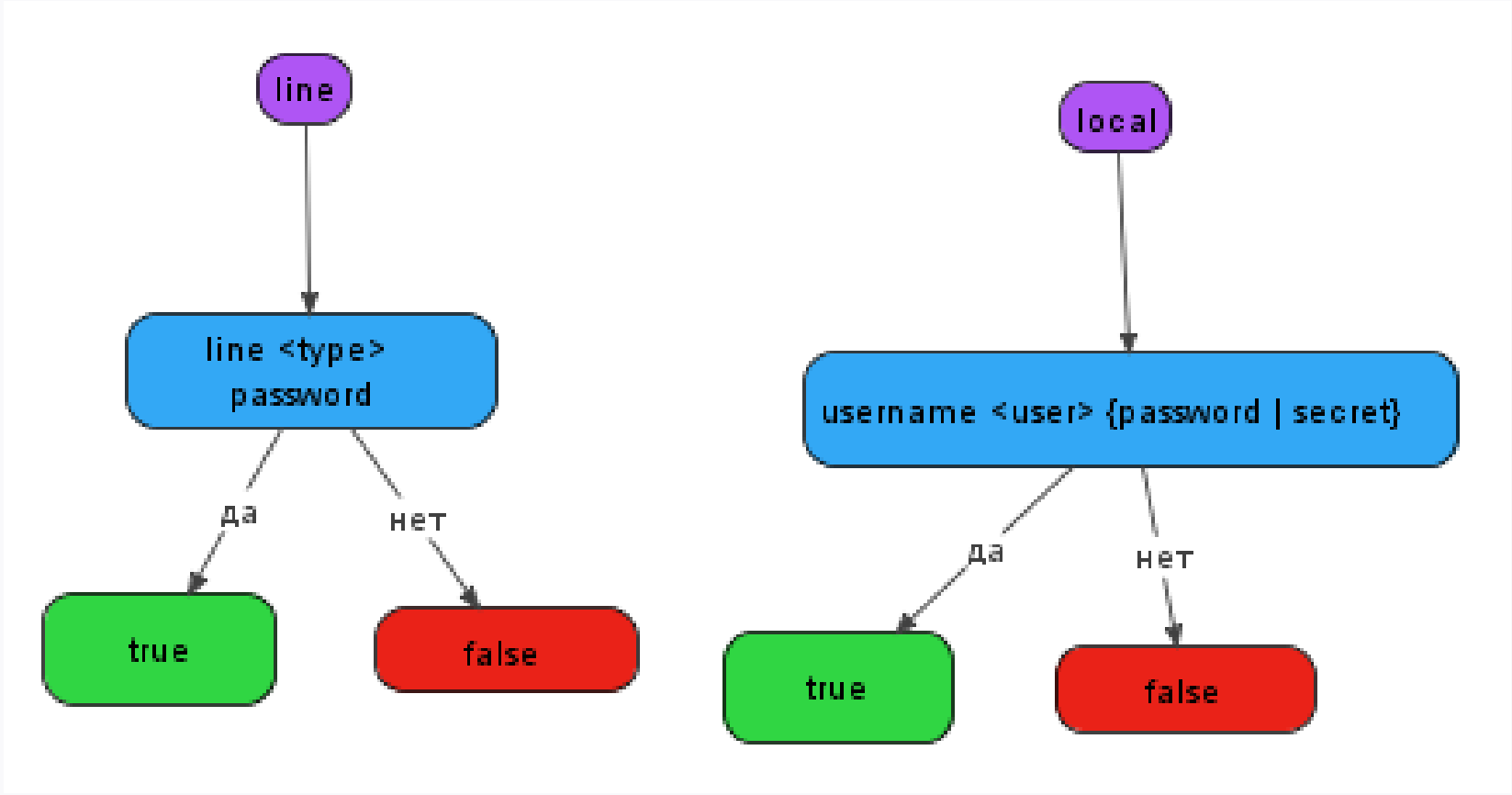
AAA


(config)#aaa new-model
да
нет
line
(config)#vty <number>
(config)#con <number>
(config-line)#login local
(config-line)#login local
нет
да
да
нет
line
local
None
line
(config)#vty <number>
(config)#con <number>
(config-line)#login authentication <named>
(config-line)#login authentication <named>
нет
да
да
нет
(config)#aaa authentication login default
(config)#aaa authentication login <named>
(config)#aaa authentication login default
да
нет
нет
да
нет
да
не задана
None
(config)#aaa authentication login default {method}
(config)#aaa authentication login <named> {method}
не задана
(config)#aaa authentication login default {local | local-case| enable| line}
method2
method1
method2
method1
method2
не задан
задан
задан
не задан
не задан
задан
не задан
задан
не задан
задан
не задана
method
не задана
method
не задана
method
не задана
method

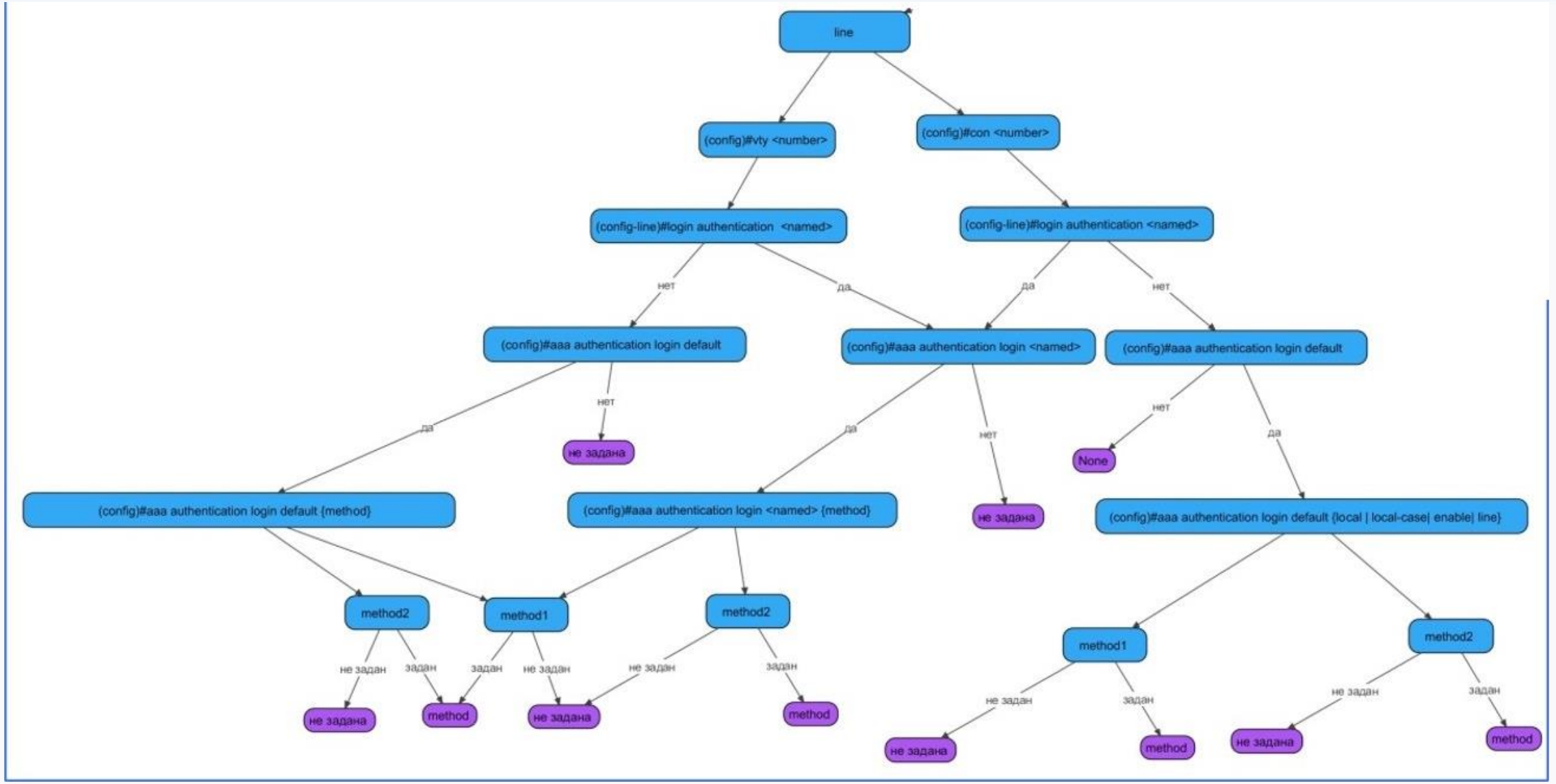
AAA


(config)#aaa new-model
нет
line
(config)#vty <number>
(config)#con <number>
(config-line)#login local
(config-line)#login local
нет
да
да
нет
line
local
None

AAA


line
line <type>
password
да
нет
true
false
local
username <user> {password | secret}
да
нет
true
false

AAA


line
(config)#vty <number>
(config)#con <number>
(config-line)#login authentication <named>
(config-line)#login authentication <named>
нет
да
да
нет
(config)#aaa authentication login default
(config)#aaa authentication login <named>
(config)#aaa authentication login default
нет
да
нет
не задана
да
нет
None
да
(config)#aaa authentication login default {method}
(config)#aaa authentication login <named> {method}
не задана
(config)#aaa authentication login default {local | local-case| enable} line}
method2
method1
method2
method1
method2
не задан
задан
задан
не задан
не задан
задан
не задан
задан
не задан
задан
не задана
method
не задана
method
не задана
method
не задана
method

AAA

```
(config)# ip domain name otus.ru
(config)# crypto key generate rsa
(config)# service password-encryption
(config)# username user privilege 15 {password | secret} Pa$$w0rd
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# logging local
(config-line)# exec-timeout 60 0
```

AAA

Настройка AAA

AAA в cisco позволяет гибко насорить доступ на оборудование.
Включается командой
aaa new-model – по умолчанию отключено.

Далее необходимо выбрать метод аутентификации – сформировать определенный список – default или со своим названием.

Можно создать несколько списков и повести каждый на свою линию – aux; vty; con, etc

AAA

(config)#aaa new-model

(config)#aaa authentication login {default | list-name} method1 [method2…]

(config)#line {vty | aux | con…} line-numbers

(config-line)#login authentication {default | list-name}

AAA

- Local — база данных логинов и паролей храниться на самом сетевом устройстве. Требует username {password | secret}
- Local-case — тот же самый метод, что и local, но чувствительный к регистру при вводе логина
- Enable — для аутентификации требуется enable{password | secret}
- Line — для аутентификации требуется пароль line

AAA

- None — аутентификация не требуется, доступ к устройству предоставляется без ввода логина и пароля

- Group {tacacs+ | radius} — подключение серверов с установленным Tacacs+ или RADIUS для расширения возможностей конфигурации aaa

- Group {group-name} — позволяет настроить группу серверов с установленным Tacacs+ или RADIUS или настроить частный сервер группы.

AAA

(config)#aaa authentication login default group servradius1

(config)#radius-server host 192.168.1.1
(config)#radius-server host 192.168.1.2
(config)#radius-server host 192.168.1.3

(config)#aaa group server radius servradius1
(config-sg-radius)#server 192.168.1.1
(config-sg-radius)#server 192.168.1.2
(config-sg-radius)#server 192.168.1.3

AAA

```
aaa authentication login default group radius local

radius server radius-01
 address ipv4 172.23.132.54 auth-port 1812 acct-port 1813
 key 7 123

radius server radius-02
 address ipv4 172.23.4.70 auth-port 1812 acct-port 1813
 key 7 321
```

AAA

Авторизация включается:

aaa authorization exec default group {radius | tacacs+} if-authenticated

При использовании только этой команды, нет необходимости вводить enable пароль.

AAA

aaa authorization config-commands

- для каждой конфиг-команды (в режиме conf t) проверяется разрешение для ввода команды на сервере, например, можно разрешить пользователю только изменять description на интерфейсах

aaa authorization commands 15 default group TAC_PLUS local

- для каждой команды в режиме enable, проверяется разрешение на сервере

AAA

Accounting формирует сообщение и отправляет его на NAS (Network Access Server) – tacacs+ (radius?)

несколько методов сбора статистики при помощи accounting:

- EXEC accounting - сохраняет информацию о каждом сеансе на маршрутизаторе, при этом записывается информация о имени пользователя, дате, времени, и IP адресе;
- System accounting - этот метод сохраняет информацию о системных событиях маршрутизатора, таких как перезагрузки системы, выключение питания и т.д.;

AAA

- Command accounting - сохраняет информацию о командах вводимых в EXEC или Shell сессиях. Записывается информация о том какая команда выполнялась, кто запускал эту команду, когда она запускалась, и с каким уровнем привилегий

- Connection accounting - записывает информацию о исходящих соединениях сделанных с маршрутизатора, таких как telnet, SSH

- Network accounting - сохраняет информацию о PPP, SLIP, и ARAP сессиях

AAA

3 типа логирования:

- start-stop - позволяет настроить маршрутизатор посылать лог сообщения, когда сервис запускается и останавливается

- stop-only - этот параметр заставит маршрутизатор создать сообщение только при окончании работы сервиса. Для EXEC accounting этот параметр создаст запись о том когда пользователь закончил работу с маршрутизатором

AAA

3 типа логирования:

- wait-start - этот параметр откладывает запуск сервиса до тех пор, пока с сервера NAS не будет получено подтверждение о том что лог сообщение об этом событии получено. Этот параметр применяют для особо важных действий, когда каждое соединение и команда выполненная на маршрутизаторе должна быть обязательно записана. Если NAS сервер не пошлет уведомление о том что лог запись была успешно создана, маршрутизатор не запустит этот сервис или не будет выполнять данную команду

AAA

Рекомендации по настройке AAA Accounting:

1. EXEC start-stop – Этот метод позволит определить когда кто то подключался к маршрутизатору.

2. System stop-only – Для системных событий достаточно этого типа

3. Command stop-only – Команды как правило выполняются в коротком промежутке времени, и этот параметр позволит избежать дублирования сообщений о каждой выполненной команде

4. Connection start-stop – Учет времени начала и конца исходящих соединений с маршрутизатора, позволит иметь полную статистику

5. Network start-stop – Для облегчения разбора лог сообщений, также следует использовать параметр start-stop

AAA

(config)#aaa accounting exec default start-stop group radius
(config)#aaa accounting system default stop-only group radius
(config)#aaa accounting connection default start-stop group radius
(config)#aaa accounting network default start-stop group radius

Указываем, какого уровня команды будут логироваться на NAS сервер
(config)#aaa accounting commands 1 default stop-only group radius
(config)#aaa accounting commands 15 default stop-only group radius

Логирование неудачных попыток входа на устройство:
aaa accounting send stop-record authentication failure

AAA

(config)#aaa accounting exec default start-stop group radius
(config)#aaa accounting system default stop-only group radius
(config)#aaa accounting connection default start-stop group radius
(config)#aaa accounting network default start-stop group radius

Указываем, какого уровня команды будут логироваться на NAS сервер
(config)#aaa accounting commands 1 default stop-only group radius
(config)#aaa accounting commands 15 default stop-only group radius

Логирование неудачных попыток входа на устройство:
aaa accounting send stop-record authentication failure

AAA

Логирование удачных и не удачных попыток входа без aaa accounting:

login on-failure log
login on-success log

Jun 14 11:03:13.070: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: user] [Source: 172.16.20.250] [localport: 22] at 14:03:13 MSK Fri Jun 21 2020

5

AAA без tacacs+

Без tacacs+

Создать пользователя с паролем и указать уровень привилегий:
username {user} privilege {level} secret [encryption-type] {password}

Указать уровень привилегий:
privilege mode [all] level {level} {command}

В качестве AAA используется модель:
aaa authentication login default local

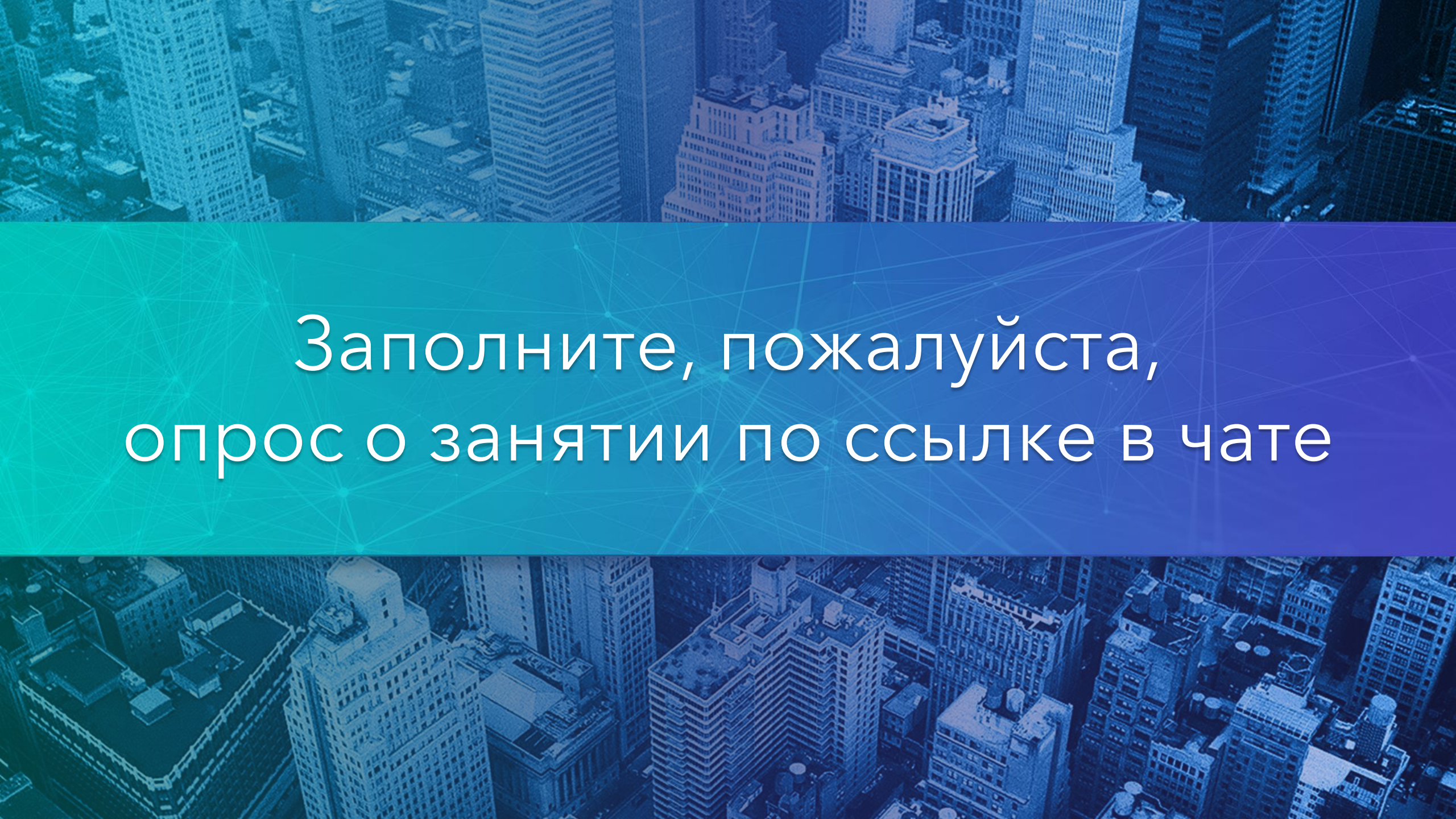
Без tacacs+

(config)#username user1 privilege 3 secret 0 us1pass

(config)#privilege exec level 3 configure terminal
(config)#privilege configure level 3 interface GigabitEthernet1/0/2
(config)#privilege interface level 3 switchport access vlan

Задаем пароль для 3 уровня доступа:
(config)#enable secret level 3 0 lv3pass

Чтобы зайти в привилегии 3 уровня:
>enable 3


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

До новых встреч!
Приходите на следующие занятия

Кулиничев Алексей
Администратор Сетей
Santchous42@yandex.ru