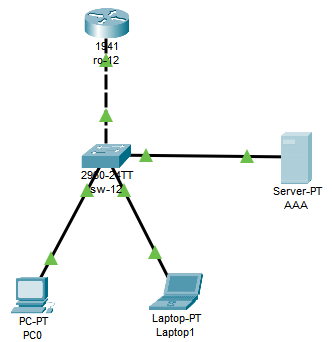
## Лабораторная работа №12. AAA

**AAA** (**A**uthentication, **A**uthorization, **A**ccounting) — общее название процессов, связанных с обеспечением защиты данных в информационных системах, включая обеспечение аутентификации, авторизации и аудита, но без обеспечения доступности данных (защиты от DOS-атак).

* Authentication (аутентификация) — сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю, сертификату, смарт-карте и т. д.
* Authorization (авторизация, проверка полномочий, проверка уровня доступа) — сопоставление учётной записи в системе (и персоны, прошедшей аутентификацию) и определённых полномочий (или запрета на доступ). В общем случае авторизация может быть «негативной» (пользователю А запрещён доступ к серверам компании).
* Accounting (учёт) — слежение за потреблением ресурсов (преимущественно сетевых) пользователем. В accounting включается также и запись фактов получения доступа к системе (англ. access logs).

Распространёнными сетевыми протоколами, реализующими AAA, являются:

* Radius (Remote Authentication in Dial-In User Service), разработан в 1997 г. и опубликован как RFC 2058 и RFC 2059. Существует несколько коммерческих и свободно распространяемых RADIUS-серверов.
* Diameter – сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола Radius, описан в RFC 6733, RFC 3589, RFC 4006.
* Tacacs+ (Terminal Access Controller Access Control System plus) – сеансовый протокол, результат дальнейшего усовершенствования протокола TACACS, предпринятого Cisco в 1993 г.



1. Расставим оборудование
   * Маршрутизатор Cisco 1941
   * Коммутатор Cisco 2960
   * Сервер
   * Несколько рабочих станций
2. Соединим оборудование
   * Соединим активное оборудование по гигабитным портам
   * Присоединим конечные устройства к коммутатору по портам FastEthernet.
3. Настройка сети (см. подробности в Приложении)
   * Спланируйте распределение статических и динамических IP-адресов
   * Настройка сервера
     + Настройте статический адрес сервера. Укажите шлюз по умолчанию и самого себя в качестве DNS-сервера
     + Настройте службу DNS и добавьте в неё 3 записи: ro-12, sw-12 и сам сервер aaa
   * Настройка маршрутизатора
     + Задайте имя
     + Задайте IP-адрес / маску на порту Gigabit Ethernet
   * Настройка коммутатора
     + Задайте имя
     + Задайте IP-адрес / маску на порту Vlan 1
   * Настройте службу DHCP на коммутаторе
     + Диапазон исключения
     + Сеть
     + Шлюз по умолчанию
     + DNS-сервер
   * Убедитесь, что рабочие станции получают корректные настройки IP\
   * Убедитесь, что пинги ходят по всей сети
     + По IP-адресам
     + По именам
4. Использование старой схемы авторизации
   * Добавьте локального пользователя username admin privilege 15 secret cisco
   * Подключите авторизацию в контекстах line console 0 и line vty 0 4 командой login local
   * Не сохраняйте настройки маршрутизатора
   * Убедитесь, что маршрутизатор требует авторизации при входе
     + На консоль
     + По telnet
   * Сбросьте маршрутизатор командой reload
5. Использование новой схемы авторизации
   * Подключите новую схему aaa new-model
   * Задайте авторизацию из локальной базы пользователей aaa authentication login default local
   * Добавьте локального пользователя username admin secret cisco
   * Убедитесь, что маршрутизатор требует авторизации при входе
     + На консоль
     + По telnet
6. Подключение внешнего сервера AAA
   * Настройте службу AAA на сервере
     + Включите
     + Добавьте маршрутизатор в качестве клиента AAA по протоколу Radius
     + Заведите пару пользователей с паролями
   * Удалите список источников авторизации на маршрутизаторе
   * Подключите использование сервера AAA и переход к локальной БД при сбое aaa authentication login default group radius local
   * Укажите Radius-сервер radius-server host 192.168.108.50 key qwerty
   * Убедитесь, что маршрутизатор требует авторизации при входе
     + На консоль
     + По telnet
   * Убедитесь, что для авторизации используется БД пользователей с сервера, но не локальная БД пользователей
   * Проверим работу авторизации при сбое сервера AAA
     + Временно отключите сервер от сети
     + Убедитесь, что авторизация на маршрутизаторе работает, но используется локальная БД пользователей
     + Восстановите подключение сервера
     + Проверьте работу авторизации на маршрутизаторе
7. Настройте авторизацию коммутатора
   * Аналогично настройке маршрутизатора
   * Убедитесь, что коммутатор требует авторизации при входе
     + На консоль
     + По telnet
   * Убедитесь, что для авторизации используется БД пользователей с сервера, но не локальная БД пользователей
8. Сохраните файл и отправьте его на оценку
   * Не забывайте про необходимость документирования сети

## Приложение

Настройки сетевого оборудования

hostname **ro-12**

aaa new-model

aaa authentication login default group radius local

username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

interface GigabitEthernet0/0

no shutdown

ip address 192.168.108.1 255.255.255.0

radius-server host 192.168.108.50 key qwerty

!

hostname **sw-12**

ip dhcp excluded-address 192.168.108.0 192.168.108.100

ip dhcp pool 12

network 192.168.108.0 255.255.255.0

default-router 192.168.108.1

dns-server 192.168.108.50

aaa new-model

aaa authentication login default group radius local

username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

interface Vlan1

no shutdown

ip address 192.168.108.10 255.255.255.0

radius-server host 192.168.108.50 key asdfg