

федеральное государственное автономное образовательное учреждение  
высшего образования  
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ОТЧЕТ**

по лабораторной работе №6

«Создание WLAN»

по дисциплине «Администрирование систем и сетей»

Вариант на оценку 5

Авторы: Кулаков Н. В.

Факультет: ПИиКТ

Группа: Р34312

Преподаватель: Афанасьев Д.Б.



**УНИВЕРСИТЕТ ИТМО**

Санкт-Петербург 2023

## Оглавление

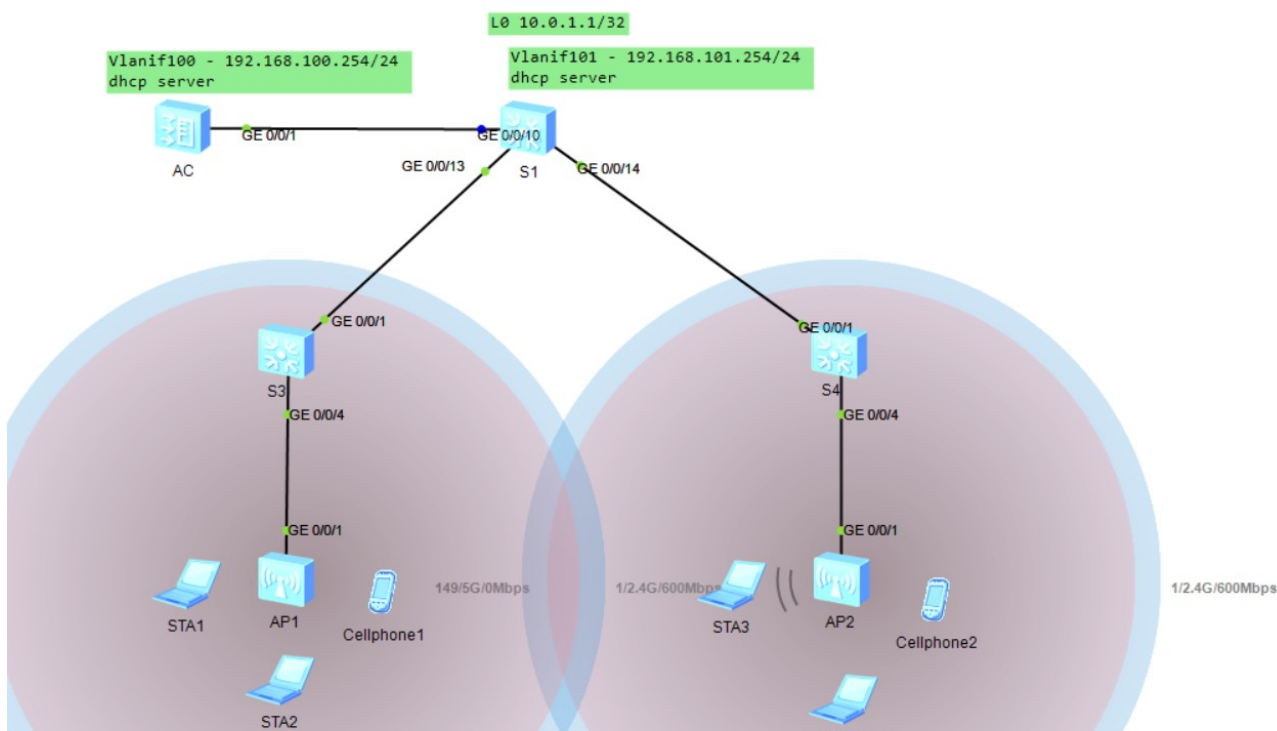
1. Лабораторная работа.....	3
1.1. Задачи.....	3
1.2. Топология.....	4
1.3. Настройка и диагностические команды.....	4
1.4. Конфигурации.....	8

# 1. Лабораторная работа

## 1.1. Задачи

- Настройка подключения к проводной сети.
- Настройка точек доступа и перевод их в режим онлайн
  - Создание групп точек доступа и добавление точек доступа с одинаковой конфигурацией в одну группу для унифицированной настройки.
  - Настройка системных параметров контроллера доступа, включая код страны и интерфейс-источник, используемый контроллером для связи с точками доступа.
  - Настройка режима аутентификации AP и импорт AP для выхода точек доступа в сеть.
- Настройка параметров сервисов WLAN и передача конфигурации точкам доступа, чтобы обеспечить доступ STA к WLAN.

## 1.2. Топология



## 1.3. Настройка и диагностические команды

Шаг 1.

Переименовать устройства, отключить ненужные порты на S1.

```
interface GigabitEthernet0/0/11
shutdown
#
interface GigabitEthernet0/0/12
shutdown
#
```

Шаг 2. Настроить так, чтобы S1 являлся DHCP-сервером для STA, а AC — DHCP-сервером для AP. Добавить соответствующие Vlanif 100 — AC, Vlanif 101 — S1.

```
[S1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
```

```
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
```

```
[AC]vlan batch 100 101
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[AC]interface GigabitEthernet 0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
```

```
[S3]vlan batch 100 101
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S3]interface GigabitEthernet 0/0/1
[S3-GigabitEthernet0/0/1]port link-type trunk
[S3-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]port link-type trunk
[S3-GigabitEthernet0/0/4]port trunk pvid vlan 100
[S3-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
```

```
[S4]vlan batch 100 101
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1] port link-type trunk
[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 101
[S4]interface GigabitEthernet0/0/4
[S4-GigabitEthernet0/0/4] port link-type trunk
[S4-GigabitEthernet0/0/4] port trunk pvid vlan 100
[S4-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 101
```

```
# AC
```

```
dhcp enable
```

```
#
```

```
ip pool ap
```

```
gateway-list 192.168.100.254
```

```
network 192.168.100.0 mask 255.255.255.0
```

```
#
```

```
interface Vlanif100
```

```
ip address 192.168.100.254 255.255.255.0
```

```
dhcp select global
#
return

# S1
interface LoopBack0
ip address 10.0.1.1 255.255.255.255
#
dhcp enable
#
ip pool sta
gateway-list 192.168.101.254
network 192.168.101.0 mask 255.255.255.0
#
interface Vlanif101
ip address 192.168.101.254 255.255.255.0
dhcp select global
#
```

### Шаг 3.

Настроить параметры точек доступа для выхода в сеть.

Создать AP группу ap-group1, добавить устройства в эту группу:

```
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain c
onfigurations of the radio and reset the AP. Continue?[Y/N]:y
```

Установить Vlanif100 как источник для установления CAPWAP туннелей:

```
capwap source interface vlanif100
```

Настройка режима аутентификации AP по MAC:

```
ap auth-mode mac-auth
```

Добавить AP в группу:

```
ap-id 0 ap-mac 00e0-fc8b-44b0
ap-name ap1
ap-group ap-group1
ap-id 1 ap-mac 00e0-fc9b-7640
ap-name ap2
ap-group ap-group1
```

Шаг 4.

Настроить параметры сервисов WLAN.

Создать профиль безопасности и настроить политику безопасности:

```
[AC-wlan-sec-prof-HCIA-WLAN]dis this
```

```
#
 security wpa-wpa2 psk pass-phrase %^%#\76\AcB2TWh5jn)+4jM/&7e;7g=f\(.cB0Axc~g4
%^%# aes
#
return
```

Создать SSID профиль:

```
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
Info: This operation may take a few seconds, please wait.done.
```

Настроить профиль VAP:

```
[AC]wlan
[AC-wlan-view]vap-profile name HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
```

Установить привязку VAP профиля к AP-шкам:

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

```
[AC]dis ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
```

Total AP information:

```
nor : normal [2]
```

```
-----
ID   MAC           Name Group   IP           Type           State STA Upti
me
-----
0    00e0-fc8b-44b0 ap1  ap-group1 192.168.100.88 AP2050DN      nor  1  7M:8
S
```

```
1      00e0-fc9b-7640 ap2  ap-group1 192.168.100.9  AP2050DN      nor  0  7M:1
2S
```

-----  
Total: 2

## Подключение с STA3:

STA>ipconfig

```
Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.101.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.101.254
Physical address.....: 54-89-98-AE-7E-7F
STA>ping 10.0.1.1
```

```
Ping 10.0.1.1: 32 data bytes, Press Ctrl_C to break
From 10.0.1.1: bytes=32 seq=1 ttl=255 time=203 ms
From 10.0.1.1: bytes=32 seq=2 ttl=255 time=140 ms
From 10.0.1.1: bytes=32 seq=3 ttl=255 time=156 ms
From 10.0.1.1: bytes=32 seq=4 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=5 ttl=255 time=266 ms
```

```
--- 10.0.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
 round-trip min/avg/max = 125/178/266 ms
```

## 1.4. Конфигурации

```
#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
 gateway-list 192.168.101.254
 network 192.168.101.0 mask 255.255.255.0
#
```



```
interface Vlanif101
  ip address 192.168.101.254 255.255.255.0
  dhcp select global
#
interface GigabitEthernet0/0/10
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/11
  shutdown
#
interface GigabitEthernet0/0/12
  shutdown
#
interface GigabitEthernet0/0/13
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/14
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
  ip address 10.0.1.1 255.255.255.255
#
user-interface con 0
  idle-timeout 0 0
user-interface vty 0 4
#
return

#
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool ap
  gateway-list 192.168.100.254
  network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif100
```

```
ip address 192.168.100.254 255.255.255.0
dhcp select global
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/8
undo negotiation auto
duplex half
#
capwap source interface vlanif100
#
wlan
traffic-profile name default
security-profile name default
security-profile name HCIA-WLAN
security wpa-wpa2 psk pass-phrase %^%#\76\AcB2TWh5jn)+4jM/&7e;7g=f\(:,cB0Axc~g4
%^%# aes
security-profile name default-wds
security-profile name default-mesh
ssid-profile name default
ssid-profile name HCIA-WLAN
ssid HCIA-WLAN
vap-profile name default
vap-profile name HCIA-WLAN
service-vlan vlan-id 101
ssid-profile HCIA-WLAN
security-profile HCIA-WLAN
wds-profile name default
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
```

```
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
  radio 0
    vap-profile HCIA-WLAN wlan 1
  radio 1
    vap-profile HCIA-WLAN wlan 1
  radio 2
    vap-profile HCIA-WLAN wlan 1
ap-id 0 type-id 69 ap-mac 00e0-fc8b-44b0 ap-sn 210235448310D524895A
  ap-name ap1
  ap-group ap-group1
ap-id 1 type-id 69 ap-mac 00e0-fc9b-7640 ap-sn 2102354483106408AE57
  ap-name ap2
  ap-group ap-group1
provision-ap
#
return

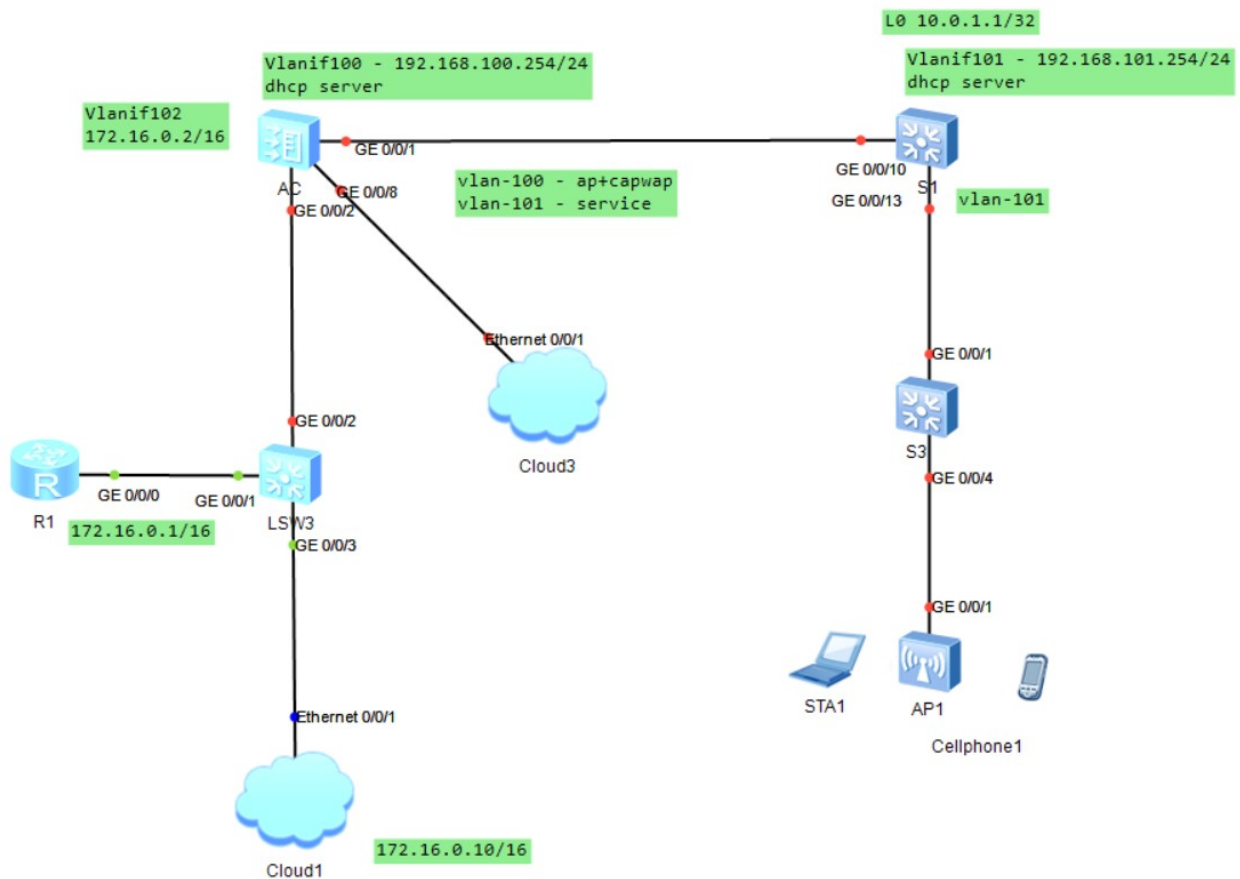
#
sysname S3
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
  port link-type trunk
  port trunk pvid vlan 100
  port trunk allow-pass vlan 100 to 101
#
user-interface con 0
  idle-timeout 0 0
user-interface vty 0 4
#
return

#
sysname S4
#
vlan batch 100 to 101
```

```
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
  port link-type trunk
  port trunk pvid vlan 100
  port trunk allow-pass vlan 100 to 101
#
user-interface con 0
  idle-timeout 0 0
user-interface vty 0 4
#
return
```

## 2. Дополнительное задание. WLAN authentication using RADIUS LDAP

### 2.1. Топология



## 2.2. Конфигурации

```
[V200R003C00]
#
 sysname R1
#
interface GigabitEthernet0/0/0
 ip address 172.16.0.1 255.255.0.0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.0.10
#
user-interface con 0
 authentication-mode password
 idle-timeout 0 0
user-interface vty 0 4
user-interface vty 16 20
#
return

#
 sysname AC
#
vlan batch 100 to 102
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name macportal_authen_profile
authentication-profile name radius-authentication-profile
 dot1x-access-profile radius-dot1x
 authentication-scheme radius-auth
 radius-server radius-vm
#
dhcp enable
#
radius-server template default
radius-server template radius-vm
 radius-server shared-key cipher %^%#bkW:,M@_b<)u3xDcb/e0G-[$Z%@7%#`H#p#k.TT9%^%
#
radius-server authentication 192.168.133.32 1812 weight 80
radius-server accounting 192.168.133.32 1813 weight 80
undo radius-server user-name domain-included
```

```
#
ip pool ap
 gateway-list 192.168.100.254
 network 192.168.100.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authentication-scheme radius
   authentication-mode radius
 authentication-scheme radius-auth
   authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 domain default
   authentication-scheme radius
   radius-server default
 domain default_admin
   authentication-scheme default
 local-user admin password irreversible-cipher $1a$q*jRUR'pK7$3JAS)Ivxj.~KTTD%SC
%EFEVf# 'WcFJ'q2pD}>Hz8$
 local-user admin privilege level 15
 local-user admin service-type http
#
interface Vlanif1
 ip address 192.168.0.4 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select global
#
interface Vlanif101
#
interface Vlanif102
 ip address 172.16.0.2 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 102
#
```

```
interface GigabitEthernet0/0/7
  undo negotiation auto
  duplex half
#
interface GigabitEthernet0/0/8
  port link-type access
  undo negotiation auto
  duplex half
#
interface NULL0
#
  info-center source AAA channel 0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.0.10
#
capwap source interface vlanif100
#
user-interface con 0
  authentication-mode password
  idle-timeout 0 0
user-interface vty 0 4
  protocol inbound all
user-interface vty 16 20
  protocol inbound all
#
wlan
  traffic-profile name default
  security-profile name default
  security-profile name default-wds
  security-profile name default-mesh
  security-profile name radius-security-profile
    security wpa2 dot1x aes
  ssid-profile name default
  ssid-profile name HCIA-WLAN
    ssid HCIA-WLAN
  vap-profile name HC
  vap-profile name default
  vap-profile name HCIA-WLAN
    service-vlan vlan-id 101
    ssid-profile HCIA-WLAN
    security-profile radius-security-profile
    authentication-profile radius-authentication-profile
  wds-profile name default
```

```
mesh-handover-profile name default
mesh-profile name default
regulatory-domain-profile name default
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
wireless-access-specification
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
    radio 0
        vap-profile HCIA-WLAN wlan 1
    radio 1
        vap-profile HCIA-WLAN wlan 1
    radio 2
        vap-profile HCIA-WLAN wlan 1
ap-id 1 type-id 69 ap-mac 00e0-fc9b-7640 ap-sn 2102354483106408AE57
    ap-name ap1
    ap-group ap-group1
provision-ap
#
dot1x-access-profile name dot1x_access_profile
dot1x-access-profile name radius-dot1x
    dot1x authentication-method pap
#
return

#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
    gateway-list 192.168.101.254
    network 192.168.101.0 mask 255.255.255.0
```



```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
user-interface con 0
 idle-timeout 0 0
user-interface vty 0 4
#
return

#
sysname S3
#
vlan batch 100 to 101
```

```

#
interface Vlanif1
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
  port link-type trunk
  port trunk pvid vlan 100
  port trunk allow-pass vlan 100 to 101
#
user-interface con 0
  idle-timeout 0 0
user-interface vty 0 4
#
return

```

No.	Port Type	Port Num	UDP Port	Port Open Status	Binding Info
1	Ethernet	1	64599	Internal	UDP
2	Ethernet	2	None	Public	Production -- IP: 172.16.0.10

#### Port Map Setting

Port Type:

Local Port Num:

Remote Port Num:

#### Port Mapping

No.	Local Port Num	Remote Port Num	Port Type
1	1	2	Ethernet
2	2	1	Ethernet

Рисунок 1: Cloud 1

No.	Port Type	Port Num	UDP Port	Port Open Status	Binding Info
1	Ethernet	1	3344	Internal	UDP
2	Ethernet	2	None	Public	Management -- IP: 192.168.0.10

#### Port Map Setting

Port Type:

Local Port Num:

Remote Port Num:

#### Port Mapping

No.	Local Port Num	Remote Port Num	Port Type
1	1	2	Ethernet
2	2	1	Ethernet

Рисунок 2: Cloud 3

## Интерфейсы на debian, где RADIUS:

```
allow-hotplug enp8s0
iface enp8s0 inet dhcp
```

```
auto enp9s0
iface enp9s0 inet static
    address 192.168.133.32
    netmask 255.255.255.0
    up ip route add 172.16.0.0/16 via 192.168.133.31 dev enp9s0
```

## Конфигурация RADIUS-сервера:

```
### clients.conf
```

```
client * {
    ipaddr = *
    secret = testing123
}
```

```
### mods-enabled:
```

```
root@debian:/etc/freeradius/3.0/mods-enabled# ls
```

always	detail.log	echo	files	mschap	preprocess	soh
utf8						
attr_filter	digest	exec	ldap	ntlm_auth	radutmp	
sradutmp						
chap	dynamic_clients	expiration	linelog	pap	realm	unix
detail	eap	expr	logintime	passwd	replicate	unpack

```
### mods-enabled/ldap:
```

```
ldap {
    server = 'ldaps://192.168.10.81'
    port = 3269
    base_dn = 'DC=cs,DC=ifmo,DC=ru'
    user {
        base_dn = "${..base_dn}"
        filter = "(samaccountname=%{%{Stripped-User-Name}:-{%{User-Name}}})"
    }
}
```

```
### sites-enabled:
```

```
root@debian:/etc/freeradius/3.0/sites-enabled# ls
```

```
default inner-tunnel
```

```
### sites-enabled/default:
```

```

authorize {
    -ldap
    if ((ok || updated) && User-Password) {
        update {
            control:Auth-Type := ldap
        }
    }
}

```

```

authenticate {
    Auth-Type LDAP {
        ldap
    }
}

```

## 2.3. Настройка окружения и проверки

Изначально была установлен RADIUS сервер на виртуальную машину в ОС Windows. Был использован NAT для подключения к ОС Windows для отправки трафика на LDAP, и также был использован NAT взаимодействия с ENSP. По своей глупости, я не понял, что оно оказывается работает, поэтому решил, что раз RADIUS сервер предварительно не настроенный не отвечает на посланные ему запросы, то это означает, что я что-то сделал не так (с точки зрения настройки связности). Оказалось, что я был не прав.

Также, пока виртуалка была в Windows, я заменил второй NAT на Loopback, однако внутри виртуалки он был в состоянии DOWN, поэтому я также, по глупости, посчитал, что оно не работает (хотя как потом выяснилось надо было просто настроить этот link, потому что он не является enp1s0, который настроен по дефолту), и изменить параметры на нем.

Далее я решил, что раз ничего не получается, попробую поставить RADIUS в докер на хост машину (linux), добавив его в docker bridge default сеть. Пока я до этого не догадывался, что есть такая штука как iptables, которая отбрасывает неподходящий трафик, а поскольку docker умный, и не дает заниматься такими

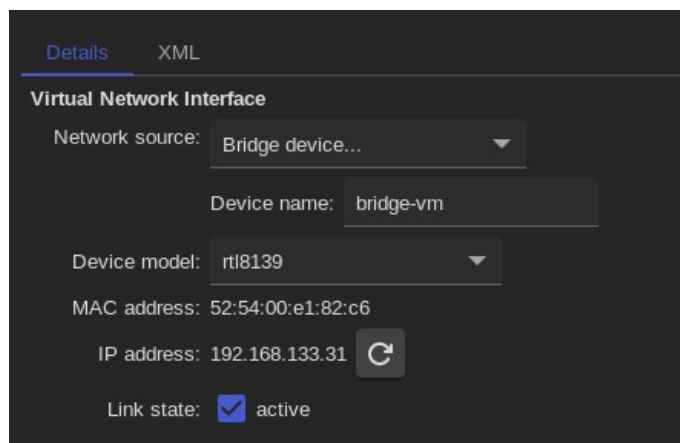
страшными манипуляциями между ним и хостовой виртуалкой с какими-то странными айпишниками, то iptables просто отбрасывали трафик (возможно на докеровском бридже, а возможно и дальше).

Поэтому я решил накатить вторую виртуалку на KVM. Поразбавившись, понял, что необходимо добавить их обоих в bridge сеть для обеспечения связности.

Реализовал следующим образом:

```
nikit@host ~ % ip link show | grep bridge-vm
12: bridge-vm: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
mode DEFAULT group default qlen 1000
37: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
bridge-vm state UNKNOWN mode DEFAULT group default qlen 1000
38: vnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
bridge-vm state UNKNOWN mode DEFAULT group default qlen 1000
```

vnet1, vnet2 — virtio интерфейсы, автоматически создаваемые libvirt.



Разницы между device model Hypervisor default (rtl8139) и virtio в данном случае нет, хотя в какой-то версии наблюдался баг, который обеспечивал связность между хостовой машиной и виртуалками, но не между виртуалками. У меня как раз была это ситуация, но проблема, как убедился, была не в типе устройств.

Наконец, как выяснилось после глупокого изучения данного вопроса, проблема была как раз в IP-адресах и настроенных iptables, который отбрасывал IP-пакеты со странными айпишниками (настроенными на виртуалках), поэтому при пересылке через bridge они отбрасывались. Выяснил это, потому что ARP

запросы между узлами приходили, и на них даже отвечали, а вот IP-пакеты (ICMP) были с no response.

Чтобы не менять настройку iptables, было принято решение отключить проверку на bridge с помощью команды:

```
su -c 'echo 0 > /proc/sys/net/bridge/bridge-nf-call-iptables'
```

Чтобы сделать перманентным:

```
su -c "echo 'net.bridge.bridge-nf-call-iptables = 0' > local.conf"
```

Таблица маршрутизации на Windows:

0.0.0.0	0.0.0.0	192.168.133.1	192.168.133.31	291
10.0.0.0	255.0.0.0	172.16.0.1	172.16.0.20	26
10.0.0.0	255.0.0.0	172.16.0.1	172.16.0.10	26
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
172.16.0.0	255.255.0.0	172.16.0.1	172.16.0.20	26
172.16.0.0	255.255.0.0	172.16.0.1	172.16.0.10	26
172.16.0.0	255.255.255.0	On-link	172.16.0.10	281
172.16.0.0	255.255.255.0	On-link	172.16.0.20	281
172.16.0.10	255.255.255.255	On-link	172.16.0.10	281
172.16.0.20	255.255.255.255	On-link	172.16.0.20	281
172.16.0.255	255.255.255.255	On-link	172.16.0.10	281
172.16.0.255	255.255.255.255	On-link	172.16.0.20	281
192.168.0.0	255.255.255.0	On-link	192.168.0.10	281
192.168.0.10	255.255.255.255	On-link	192.168.0.10	281
192.168.0.255	255.255.255.255	On-link	192.168.0.10	281
192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	On-link	192.168.56.1	281
192.168.133.0	255.255.255.0	On-link	192.168.133.31	291
192.168.133.31	255.255.255.255	On-link	192.168.133.31	291
192.168.133.255	255.255.255.255	On-link	192.168.133.31	291
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	192.168.56.1	281
224.0.0.0	240.0.0.0	On-link	192.168.133.31	291
224.0.0.0	240.0.0.0	On-link	172.16.0.20	281
224.0.0.0	240.0.0.0	On-link	172.16.0.10	281
224.0.0.0	240.0.0.0	On-link	192.168.0.10	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331

255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
255.255.255.255	255.255.255.255	On-link	192.168.133.31	291
255.255.255.255	255.255.255.255	On-link	172.16.0.20	281
255.255.255.255	255.255.255.255	On-link	172.16.0.10	281
255.255.255.255	255.255.255.255	On-link	192.168.0.10	281

Persistent Routes:

Network Address	Netmask	Gateway Address	Metric
10.0.0.0	255.0.0.0	172.16.0.1	1
172.16.0.0	255.255.0.0	172.16.0.1	1
0.0.0.0	0.0.0.0	192.168.133.1	Default
0.0.0.0	0.0.0.0	192.168.133.1	Default

На debian, где крутится RADIUS-сервер:

```
zubrailx@debian:~$ ip route
default via 192.168.122.1 dev enp8s0
172.16.0.0/16 via 192.168.133.31 dev enp9s0
192.168.122.0/24 dev enp8s0 proto kernel scope link src 192.168.122.89
192.168.133.0/24 dev enp9s0 proto kernel scope link src 192.168.133.32
```

192.168.122.89 — для связи с хостом через NAT, для получения доступа к сети

Проверка через ENSP связности с RADIUS-сервером:

```
<AC>ping 192.168.133.32
PING 192.168.133.32: 56 data bytes, press CTRL_C to break
  Reply from 192.168.133.32: bytes=56 Sequence=1 ttl=63 time=20 ms
  Reply from 192.168.133.32: bytes=56 Sequence=2 ttl=63 time=30 ms
  Reply from 192.168.133.32: bytes=56 Sequence=3 ttl=63 time=20 ms
  Reply from 192.168.133.32: bytes=56 Sequence=4 ttl=63 time=30 ms
  Reply from 192.168.133.32: bytes=56 Sequence=5 ttl=63 time=20 ms
```

И обратно:

```
zubrailx@debian:~$ ping 172.16.0.2
PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_seq=1 ttl=254 time=46.5 ms
64 bytes from 172.16.0.2: icmp_seq=2 ttl=254 time=22.3 ms
64 bytes from 172.16.0.2: icmp_seq=3 ttl=254 time=37.2 ms
64 bytes from 172.16.0.2: icmp_seq=4 ttl=254 time=44.1 ms
```

С интернетом RADIUS-сервер:

```
zubrailx@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=7.25 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=107 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=107 time=6.84 ms
```

В случае, когда не используется ITMO-Corp, используется openvpn:

```
nikit@host lab-6 % sudo openvpn students.ovpn
```

### Проверка связки RADIUS-ldap:

```
root@debian:/etc/freeradius/3.0/mods-enabled# radtest 's312563' 'fsafaadfa'
localhost -0 testing123
Sent Access-Request Id 83 from 0.0.0.0:39654 to 127.0.0.1:1812 length 77
    User-Name = "s312563"
    User-Password = "fsafaadfa"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "fsafaadfa"
Received Access-Reject Id 83 from 127.0.0.1:1812 to 127.0.0.1:39654 length 20
(0) -: Expected Access-Accept got Access-Reject
```

```
root@debian:/etc/freeradius/3.0/mods-enabled# radtest 's312563' '<real-
password>' localhost -0 testing123
Sent Access-Request Id 118 from 0.0.0.0:39286 to 127.0.0.1:1812 length 77
    User-Name = "s312563"
    User-Password = "<real-password>"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
    Message-Authenticator = 0x00
    Cleartext-Password = "<real-password>"
Received Access-Accept Id 118 from 127.0.0.1:1812 to 127.0.0.1:39286 length 20
```

### Проверка через ENSP:

```
[AC]test-aaa s312563 dfsafsaf radius-template radius-vm pap
[AC]
Info: Authentication fails due to incorrect name, password, shared key, and so o
```



```
n.Hello, s312563
[AC]test-aaa s312563 <real-password> radius-template radius-vm pap
[AC]
Info: Account test succeed.
```

## Проверка через беспроводное устройство:

```
<AC>debugging dot1x all
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.1-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulCmd=163.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.2-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulRet=0.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.3-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulCmd=167.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.4-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulRet=0.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.5-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulCmd=165.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.463.6-05:13 AC DOT1X/7/DEBUG:
[EAPOL-event] Rcv Vlan Add Port Evt. ulRet=0.
```

```
<AC>
```

```
Nov 25 2023 00:20:47.543.1-05:13 AC DOT1X/7/DEBUG:
[EAPOL-info] EAPOL Check Eap Packet entry
```

```
<AC>
```

```
Nov 25 2023 00:20:47.543.2-05:13 AC DOT1X/7/DEBUG:
[EAPOL-info] Get packet information.(MAC=0000-0000-0000, ucSlotNo=0,
ucPicNo=0,usPortNo=0, ucIsETrunkAccess=0, ulApAccessIfIndex=4294967295, ulIfIndex=15)
```

```
<AC>
```

Nov 25 2023 00:20:47.543.3-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Get packet information.(MAC=5489-98c1-1061,L2Type=1,QinqVlan=0,Vlan=6,  
Ip=0.0.0.0,EAPpktType=1,IFNAME=Wlan-Dbss0, Slot=0, PortIndex=0)

<AC>

Nov 25 2023 00:20:47.543.4-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] EAPOL Check Eap Packet. EAPOL\_IsDot1xEffectiveOnPort entry

<AC>

Nov 25 2023 00:20:47.543.5-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-stack] EAPOL Check Eap Packet. EAP packet:ulIfIndex=15,IF name:Wlan-Dbss0,  
MAC:5489-98c1-1061,vlan:101,CE-vlan:0.

<AC>

Nov 25 2023 00:20:47.543.6-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] EAPOL\_PacketEnqueue precess

<AC>

Nov 25 2023 00:20:47.543.7-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Get packet information.(MAC=0000-0000-0000, ucSlotNo=0,  
ucPicNo=0,usPortNo=0, ucIsETrunkAccess=0, ulApAccessIfIndex=4294967295, ulIfIndex=15)

<AC>

Nov 25 2023 00:20:47.543.8-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Get packet information.(MAC=5489-98c1-1061,L2Type=1,QinqVlan=0,Vlan=6,  
Ip=0.0.0.0,EAPpktType=1,IFNAME=Wlan-Dbss0, Slot=0, PortIndex=0)

<AC>

Nov 25 2023 00:20:47.543.9-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-stack] Packets enter eap module queue successfully.(ucPacketType=0,ulLay2Type=1)

<AC>

Nov 25 2023 00:20:47.543.10-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] EAPOL Check Eap Packet. Return

<AC>

Nov 25 2023 00:20:47.543.11-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Get packet information.(MAC=0000-0000-0000, ucSlotNo=0,  
ucPicNo=0,usPortNo=0, ucIsETrunkAccess=0, ulApAccessIfIndex=4294967295, ulIfIndex=15)

ex=15)

<AC>

Nov 25 2023 00:20:47.543.12-05:13 AC DOT1X/7/DEBUG:

[EAPOL-info] Get packet information.(MAC=5489-98c1-1061,L2Type=1,QinqVlan=0,Vlan=6,

Ip=0.0.0.0,EAPpktType=1,IFNAME=Wlan-Dbss0, Slot=0, PortIndex=0)

<AC>

Nov 25 2023 00:20:47.543.13-05:13 AC DOT1X/7/DEBUG:

[EAPOL-info] Received Eap packet.(MAC=5489-98c1-1061,CMIndex=4294967295)

<AC>

Nov 25 2023 00:20:47.543.14-05:13 AC DOT1X/7/DEBUG:

[EAPOL-info] Exist user receive the start packet.

<AC>

Nov 25 2023 00:20:47.543.1-05:13 AC DOT1X/7/DEBUG:

[EAPOL-info] Received start packet.(MAC=5489-98c1-1061, Index=1, CMIndex=4294967295)

<AC>

Nov 25 2023 00:20:47.543.2-05:13 AC DOT1X/7/DEBUG:

EAPOL packet: IN

ff ff ff ff ff ff 54 89 98 c1 10 61 81 00 00 65  
88 8e 01 01 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

<AC>

Nov 25 2023 00:20:47.543.3-05:13 AC DOT1X/7/DEBUG:

[EAPOL-info] Received EAPoL start packet.(MAC=5489-98c1-1061, Index=4294967295, CM Index=4294967295, MacMoveFlag=0)

<AC>

Nov 25 2023 00:20:47.543.4-05:13 AC DOT1X/7/DEBUG:

EAPOL packet: OUT

54 89 98 c1 10 61 00 e0 fc 8c 08 0a 81 00 00 60  
88 8e 01 00 00 05 01 03 00 05 01

<AC>

Nov 25 2023 00:20:47.543.5-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-packet] Send EAP packet to user successfully. (type:1, packet length:27,  
output interface:Wlan-Dbss0, VLAN:6, return:0)

<AC>

Nov 25 2023 00:20:47.543.6-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Send EAP\_request packet to user successfully.(Index=2)

<AC>

Nov 25 2023 00:20:47.543.7-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] EAPOL Dot1x User Associate Start, Received Wlan Timer Msg .(MAC=548  
9-98c1-1061,Index=2,CMIndex=4294967295)

<AC>

Nov 25 2023 00:20:47.543.8-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] EAPOL Dot1x User Associate Start, User is in authening status, wla  
n request start pkt will not be proc.

<AC>

Nov 25 2023 00:20:47.543.9-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] [EAPOL\_MsgSendWlanAssociateResult]

<AC>

Nov 25 2023 00:20:47.543.10-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-event] IPC message send to wlan. ulNodeId = 0, Ret = 0

<AC>

Nov 25 2023 00:21:17.543.1-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-timer] User response timeout.(Index:2) # STA не отвечает

<AC>

Nov 25 2023 00:21:17.543.2-05:13 AC DOT1X/7/DEBUG:  
EAPOL packet: OUT  
54 89 98 c1 10 61 00 e0 fc 8c 08 0a 81 00 00 60  
88 8e 01 00 00 05 01 03 00 05 01

<AC>

Nov 25 2023 00:21:17.543.3-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-packet] Send EAP packet to user successfully. (type:1, packet length:27,  
output interface:Wlan-Dbss0, VLAN:6, return:0)

<AC>

Nov 25 2023 00:21:17.543.4-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-info] Send EAP\_request packet to user successfully.(Index=2)

<AC>



Nov 25 2023 00:21:17.543.5-05:13 AC DOT1X/7/DEBUG:  
[EAPOL-event] Resend EAP\_request/identity.(Index=2,Ret=0)

<AC>

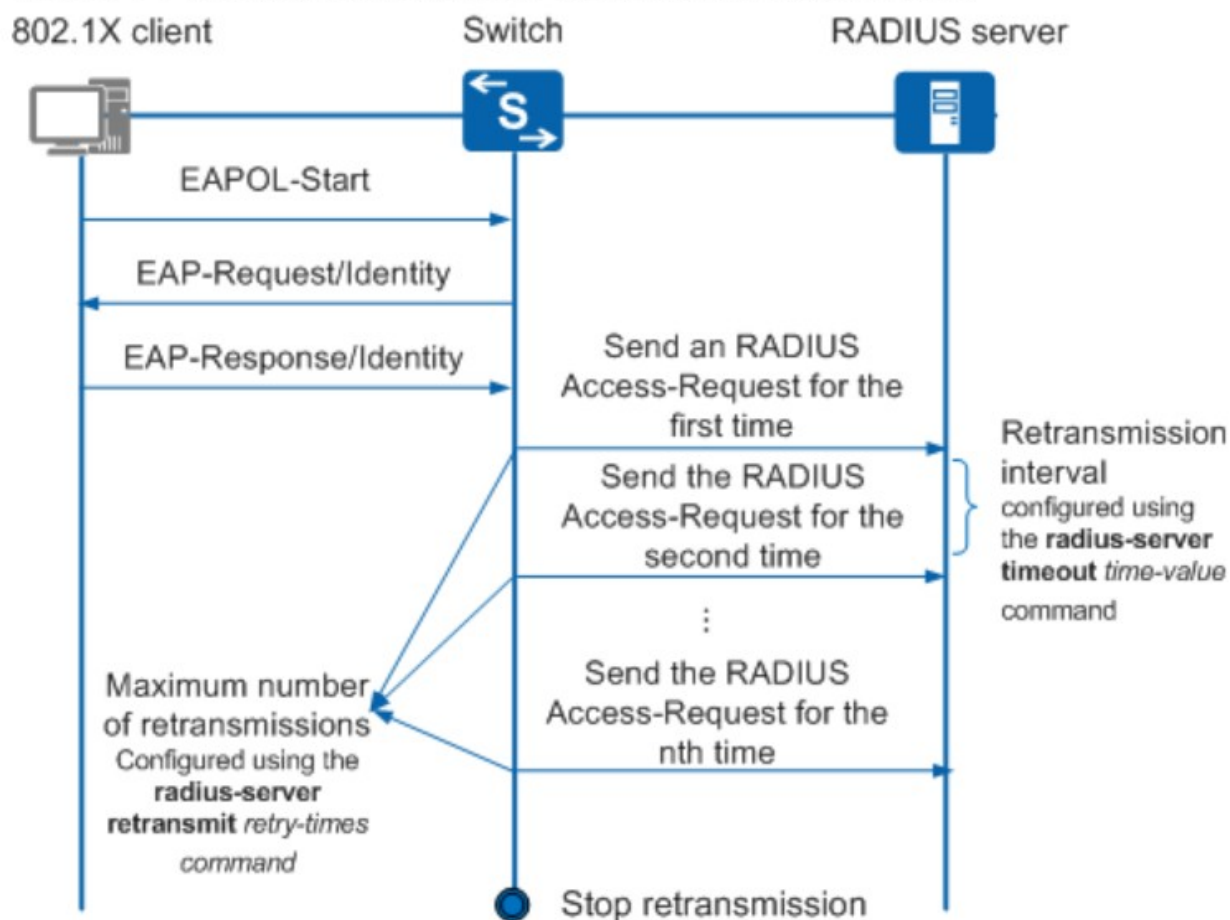
... ну и так далее, пока количество посылок не превысит лимит.

В общем, STA не отвечает на WPA2-Enterprise запросы, поэтому не устанавливается соединение.

При этом клиент сразу переходит в состояние obtaining-ip:

	SSID	Encryption	Status	VAP MAC	Channel	Radio Type
	HCIA-WLAN	WPA2 8021X	Obtaining ip...	00-E0-FC-9B-76-40	1	802.11bgn
	HCIA-WLAN	WPA2 8021X	Disconnected	00-E0-FC-9B-76-40	140	802.11bgn

**Figure 1-1** RADIUS authentication packet retransmission timer



Запросы на radius-сервер не отправляются, потому что не проходит это EAP-Request/EAP-Response.