

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ  
Федеральное государственное образовательное бюджетное учреждение  
высшего профессионального образования  
«Санкт-Петербургский государственный университет телекоммуникаций  
им. проф. М.А. Бонч-Бруевича»

---

# **Методические указания**

## **Эмулятор протоколов безопасности IEEE802.11**

Санкт-Петербург  
2015

## Содержание

ЭМУЛЯТОР ПРОТОКОЛОВ БЕЗОПАСНОСТИ ТОЧКИ ДОСТУПА СТАНДАРТА IEEE 802.11 .....	7
3.3. Принципы работы эмулятора.....	7
3.4. Структура эмулятора .....	9
3.4.1. Рабочий модуль.....	10
3.4.2. Модуль интерфейса управления Proxim Orinoco AP4000 .....	13
3.4.3. Модуль интерфейса управления NanoStation Loco m2 .....	15
3.5. Методические указания по работе с интерфейсом управления RADIUS-сервером .....	17
3.6. Методические указания по настройке режима работы «Беспроводной мост».....	24
3.7. Описание работы с эмулятором .....	28
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	33

# **ЭМУЛЯТОР ПРОТОКОЛОВ БЕЗОПАСНОСТИ ТОЧКИ ДОСТУПА СТАНДАРТА IEEE 802.11**

## **3.3. Принципы работы эмулятора**

Модернизируемое web-приложение представляет собой клиент-серверную архитектуру, в котором существует как серверная, так и клиентская часть исполнения программы. На клиентской стороне работают Javascript, HTML, CSS, а на серверной – PHP. Для исполнения PHP-скриптов необходимо наличие web-сервера с поддержкой PHP и MySQL и web-браузера со стороны пользователя (Рис. 9). Если код HTML реализует структуру страницы, CSS отвечает за оформление и размещение элементов на странице. А JavaScript предоставляет сценарный код, управляющий поведением этих элементов. При помощи исполняемых web-сервером PHP-скриптов определяется логика работы и реализуется функциональность эмулятора. Под логикой работы понимаются действия, необходимые для корректной и удобной работы пользователя с приложением, такие как обработка форм, хранение и манипуляция параметрами введенными пользователем и т.д.

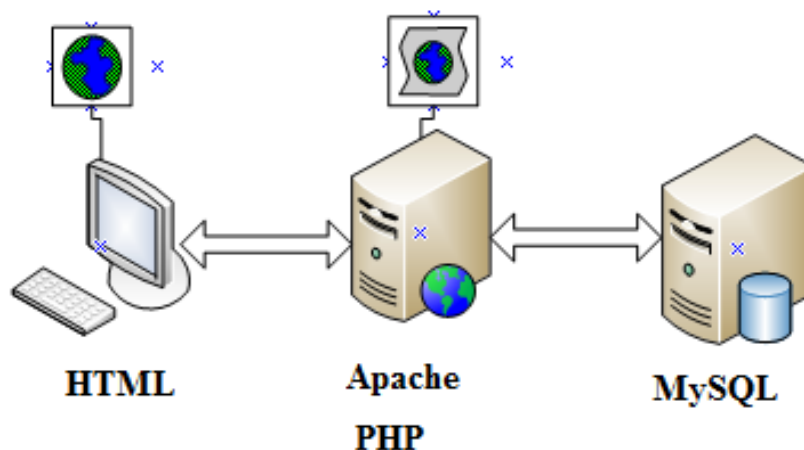


Рис. 9. Общая схема работы web-приложения

Обработка форм производится с помощью передачи пользовательских данных из HTML-формы в PHP-обработчик с помощью метода POST. Хранение пользовательских данных осуществляется при помощи использования механизма сессий PHP. Сессии необходимы, чтобы хранить сведения о пользователях при переходах между различными страницами. Преимуществом использования сессий является то, что данные сохраняются во временных файлах на сервере.

Протокол HTTP – это протокол "без сохранения состояния". Потому что данный протокол не обладает встроенным способом сохранения состояния между двумя транзакциями. Таким образом, когда пользователь открывает сначала одну страницу приложения, а затем переходит на другую страницу, то, основываясь только на средствах, предоставляемых протоколом HTTP, невозможно установить, что оба запроса относятся к одному пользователю. Точно также введенные пользователем данные в одну форму и следовательно переданные одному обработчику не будут доступны из другой формы или с другой страницы для другого обработчика. Таким образом необходим метод, при помощи которого было бы возможно отслеживать информацию о пользователе в течение одного сеанса связи с эмулятором.

Одним из таких методов является управление сеансами при помощи предназначенных для этого функций. Необходимо отметить, что сеанс представляет собой группу переменных, которые, в отличие от обычных переменных, сохраняются и после завершения выполнения PHP-сценария. Поддержка сессий позволяет сохранять данные между запросами в суперглобальном массиве `$_SESSION` [2]. Данные, введенные пользователем и записанные в массив `$_SESSION` можно использовать в течении сеанса работы на любой странице эмулятора.

### **3.4. Структура эмулятора**

Так как модернизируемый эмулятор является web-приложением, структуру его можно представить в виде четырех модулей (Рис. 10):

- Модуль интерфейсов управления точкой доступа Proxim Orinoco AP4000;
- Модуль интерфейсов управления точкой доступа NanoStation Loco m2;
- Рабочий модуль;
- Модуль интерфейса RADIUS-сервера.

Модульная структура web-приложения имеет ряд преимуществ. В результате разбиения структуры на модули получается четкое разделение функциональности эмулятора, это является важным фактором как с точки зрения разработчика, так и с точки зрения конечного пользователя. Пользователь, осуществляя работу с эмулятором, должен быть сконцентрирован на выполнении своих задач, а не на выяснении принципов работы эмулятора.



Рис. 10. Структура эмулятора

### 3.4.1. Рабочий модуль

Рабочий модуль состоит из нескольких компонентов:

1. Главное меню;
2. Страница ввода настроек точек доступа;
3. Страница ввода настроек клиента;

На странице главного меню (Рис.11) пользователь может проверить текущее состояние эмулятора. На ней видно, введены ли настройки точек доступа и беспроводного клиента, а также установлено ли соединение между клиентом и одной из беспроводных точек доступа, а также установлен или нет сетевой радио-мост. Также со страницы главного меню пользователь может перейти к интерфейсу модуля управления точкой доступа Proxim Orinoco AP4000 и Nanostation Loco m2.

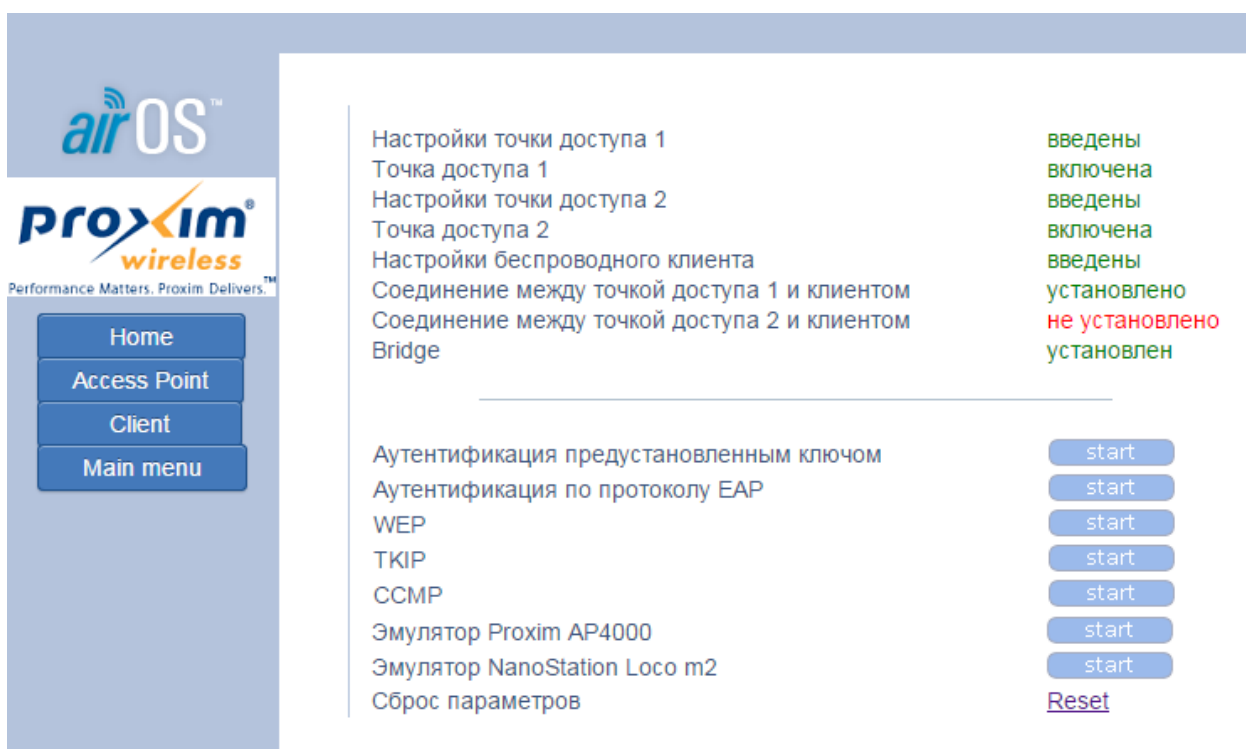


Рис. 11. Главное меню

Стоит отметить, что со страницы главного меню пользователь может вернуться на страницу “Home”, где находится различный теоретический материал и формы для регистрации и авторизации в системе. Отсюда же осуществляется переход к модулю эмуляции протоколов безопасности

Страница настроек точек доступа (Рис. 12) предназначена для проверки введенных в модуле интерфейсов управления точкой доступа Proxim Orinoco AP 4000 и NanoStation Loco m2 настроек точек доступа. При необходимости здесь возможно произвести корректировку настроек. Страница предназначена для упрощения работы с эмулятором, чтобы пользователю не приходилось каждый раз возвращаться в модули интерфейсов управления точками доступа.

airOS™

Proxim® wireless  
Performance Matters. Proxim Delivers.™

Home  
Access Point  
Client  
Main menu

Введите настройки точки доступа Ubiquiti Nano Station Loco m2

Настройки точки доступа

ip-address  
Маска 255.255.255.0  
SSID  
MAC-адрес  
Режим 802.11b only  
Канал 1

Настройки безопасности

Режим none  
Включить  
Выключить

Сохранить  
Далее

Рис. 12. Страница настроек точек доступа

Страница настроек клиента (Рис. 13) необходима для ввода настроек беспроводного клиента и подключения беспроводного клиента к одной из точек доступа.

Также со страницы настроек клиента производится подключение беспроводного клиента к точке доступа, как часть подготовительной работы для изучения работы RADIUS-сервера, режима работы «Bridge» и протоколов защиты точки доступа стандарта 802.11.

С данной страницы осуществляется переход к настройкам RADIUS-сервера. Оттуда осуществляет подробное изучение функциональных возможностей RADIUS-сервера.

Также в рамках модернизации эмулятора и изучения режима «Bridge», на страницу ввода настроек клиента была внедрена командная строка. Она предназначена для того, чтобы пользователь при помощи утилиты Ping в



любой момент мог проверить взаимосвязь между точками доступа, которые работают в режиме сетевого моста и RADIUS-сервером.

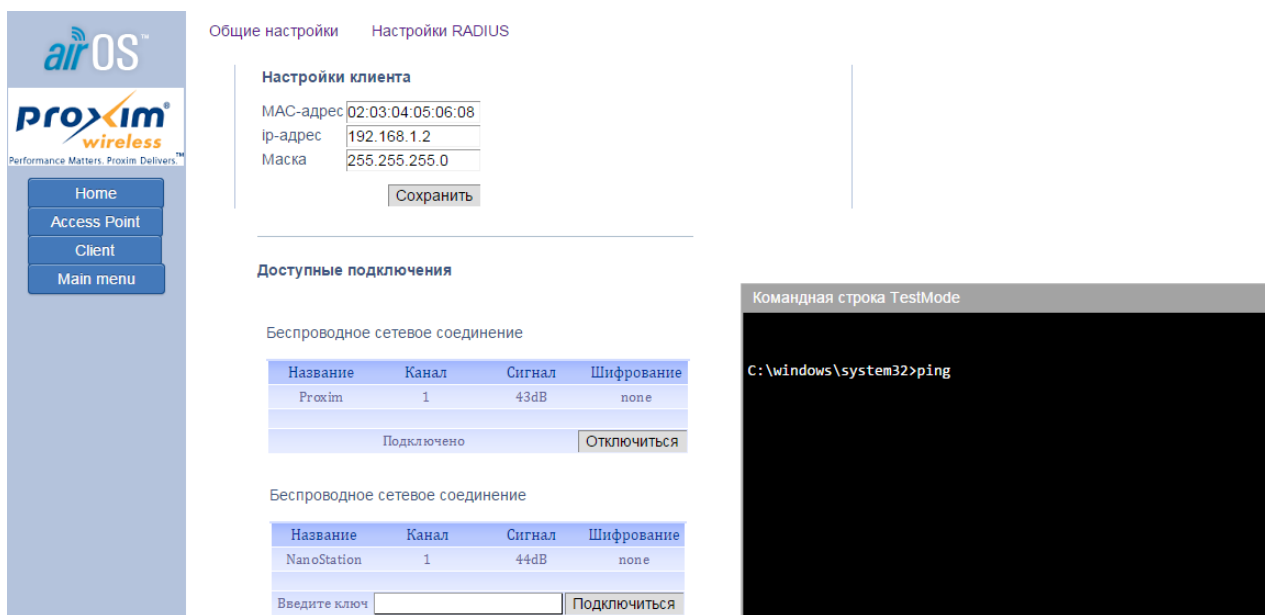


Рис. 13. Страница настроек клиента

### 3.4.2. Модуль интерфейса управления Proxim Orinoco AP4000

В качестве прототипа Web-интерфейса первой точки доступа был выбран Web-интерфейс беспроводной точки доступа Proxim Orinoco AP4000 (Рис. 14). Для этого в рамках модернизации эмулятора исходный код был переработан, а именно добавлены необходимые для осуществления поставленных целей элементы пользовательского интерфейса, а также их обработчики.



Рис. 14. Главная страница модуля интерфейсов управления точкой доступа

Модуль интерфейсов управления точкой доступа Proxim Orinoco AP4000 используется для ввода основных настроек точки доступа, таких как настройки LAN-интерфейса, настройки радиointерфейса и настройки безопасности. А также для ввода настроек RADIUS и ввода настроек WDS(Wireless Distribution System). Модуль позволяет сохранять введенные настройки. Такая функциональность является необходимой, поскольку введенные настройки используются в качестве параметров в модуле интерфейса RADIUS-сервера и при настройке сетевого радио-моста. Поскольку модуль позволяет сохранять введенные настройки, а также взаимодействует с пользователем посредством вывода сообщений об ошибках, он является превосходным инструментом обучения пользователей работе с web-интерфейсом точки доступа.

### 3.4.3. Модуль интерфейса управления NanoStation Loco m2

В рамках внедрения Web-интерфейса дополнительной точки доступа в разрабатываемое приложение был выбран прототип Web-интерфейса беспроводной точки доступа производства компании Ubiquiti NanoStation Loco m2 (Рис. 15). Компания Ubiquiti производит оборудование операторского класса, поэтому пользователям, обучающимся на эмуляторе будет крайне полезно ознакомиться и изучить web-интерфейс данной точки доступа. Web-интерфейс беспроводной точки доступа NanoStation Loco m2 является интуитивно-понятным и простым, но крайне функциональным. В ходе внедрения данного Web-интерфейса был переработан исходный код и добавлены необходимые для осуществления поставленных целей элементы пользовательского интерфейса, а также их обработчики.

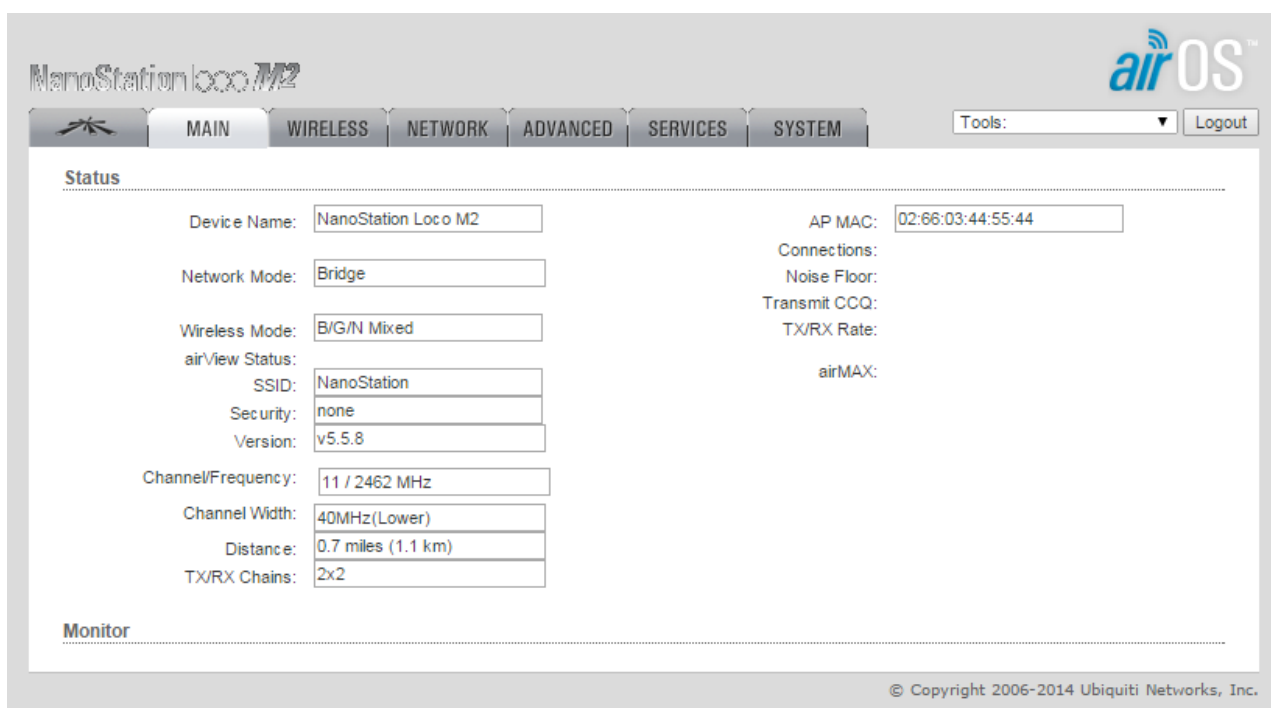


Рис.15 Web-интерфейс точки доступа Ubiquiti NanoStation Loco m2

Модуль интерфейсов управления точкой доступа NanoStation Loco m2 используется для ввода основных настроек точки доступа, таких как настройки беспроводной сети, настройки LAN-интерфейса, а также настроек безопасности. А также для ввода настроек RADIUS и ввода настроек WDS(Wireless Distribution System) для работы в режиме сетевого моста. Модуль позволяет осуществлять настройки с сохранением вводимых параметров. Такая функциональность является необходимой, поскольку введенные настройки используются в качестве параметров в модуле интерфейса настройки RADIUS-сервера. Поскольку модуль позволяет сохранять введенные настройки, а также взаимодействует с пользователем посредством вывода сообщений об ошибках, он является эффективным инструментом обучения пользователей работе с web-интерфейсом точки доступа.

### 3.5. Методические указания по работе с интерфейсом управления RADIUS-сервером

В рамках выполнения поставленной задачи был разработан интерфейс RADIUS-сервера. Схема взаимодействия точки доступа Proxim Orinoco AP 4000 и RADIUS-сервера представлена на рисунке 16.



Рис. 16 Схема взаимодействия точки доступа Proxim Orinoco AP 4000 и RADIUS-сервера

Далее будет описан подробный ход настройки RADIUS на интерфейсе разрабатываемого эмулятора.

В самом начале настройки для корректной работы RADIUS-сервера пользователю необходимо задать IP-address, Destination port и Shared в модуле интерфейса управления точкой доступа Proxim Orinoco AP4000 (Рис. 17.).

This page is used to edit the selected RADIUS Server Profile. A RADIUS server Profile consists of a Primary and a Secondary RADIUS server.

*Note: Changes to the RADIUS Server Profiles will not require a reboot of the device.*

*DNS is disabled. For configuring server names in the RADIUS profile, enable [DNS client](#) first.*

Server Profile Name		EAP Authentication
MAC Address Format Type (format/password)		DashDelimited/SS ▼
Accounting update interval (minutes)	0	
Accounting inactivity timer (minutes)	5	
Authorization lifetime (seconds)	0	

Server Parameter	Primary	Backup
Server Addressing Format	IP Address ▼	IP Address ▼
Server Name/IP Address	192.168.1.4	
Destination Port	1812	1812
Server VLAN ID (0-4094, untagged)	untagged	untagged
Shared Secret	testing222	*****
Response Time (seconds)	3	3
Maximum Retransmissions (0-4)	3	3
Server Status	Enable ▼	Disable ▼

save Cancel

Рис. 17 Настройки RADIUS в модуле интерфейсов управления точкой доступа Proxim Orinoco AP4000

После ввода настроек в модуле интерфейсов управления точкой доступа пользователь должен ввести настройки RADIUS на интерфейсе рабочего модуля (Рис. 18). Для правильного взаимодействия беспроводного клиента и RADIUS-сервера, настройки, введенные в модуле управления беспроводной точкой доступа и настройки на RADIUS-сервере должны совпадать. В случае несовпадения настроек в Лог командной строки выведется «нечитаемый» текст.

Рис. 18 Настройки RADIUS в рабочем модуле

Также в ходе настройки RADIUS пользователю необходимо отредактировать конфигурационные файлы RADIUS-сервера clients.conf (Рис. 19) и users.conf(Рис. 20). Для корректной работы RADIUS-сервера необходимо ввести общие настройки. Файл users.conf отвечает за параметры аутентификации и конфигурационную информацию для каждого пользователя, выступающего в роли беспроводного клиента. Файл clients.conf содержит описание клиента(NAS).

```

client{ 192.168.1.2
        secret      testing222
        shortname    mynetwork
        nastype      other
}

```

Рис.19 Файл Clients.conf

В конфигурационном файле clients.conf атрибут client содержит ip-адрес точки доступа (NAS - Network Authentication Server). Атрибуты secret и shortname являются обязательными, а поле nasype, которое определяет тип клиента, можно задать опционально.

```
user { 02:03:04:05:06:08
    Auth-Type      System
    User-Password   testing222
    Service-Type    Framed-User
    NAS-IP-Address  192.168.1.2
    Priority         15
}
```

Рис. 20 Файл Users.conf

В конфигурационном файле Users.conf атрибут User содержит Mac-адрес беспроводного клиента, при помощи которого пользователь подключается к точке доступа. В атрибуте Auth-Type осуществляется выбор метода аутентификации. Атрибут User-Password содержит пароль, при помощи которого пользователь подключается к беспроводной точке доступа. Атрибут Priority содержит уровень привилегий для данного пользователя.

Для работы с RADIUS-сервером в рабочем интерфейсе в настройках безопасности пользователю необходимо выбрать один из режимов аутентификации, использующий RADIUS, например WPA2-Enterprise (Рис. 21).



## Настройки безопасности

Режим

Сеть

WPA2-Enterprise ▼

none

WEP (RC4)

WPA-PSK (TKIP)

WPA-Enterprise (TKIP+802.1x)

WPA2 (CCMP)

WPA2-Enterprise (CCMP+802.1x)

Рис.21 Выбор режима безопасности

Затем пользователю необходимо запустить RADIUS-сервер, введя в командной строке команду «radiusd». В лог выводится сообщение о том, что RADIUS-сервер готов к работе. (Рис. 22)

```
Командная строка TestMode
-detailed-%Y%m%d.log"
detail: detailperm = 511
detail: dirperm = 493
detail: locking = no
Module: Instantiated detail (post_proxy_log)
detail: detailfile = "../var/log/radius/radacct/%{Client-IP-Address}/reply-detail-%Y%m%d.log"
detail: detailperm = 511
detail: dirperm = 493
detail: locking = no
Module: Instantiated detail (reply_log)
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.
```

Рис. 22 Лог командной строки

После ввода всех настроек пользователь должен подключиться к точке доступа, используя свой пароль (Рис. 23).

## Доступные подключения

### Беспроводное сетевое соединение

Название	Канал	Сигнал	Шифрование
Proxim	1	42dB	wpa2_802.1x
Введите ключ <input type="text"/>			
Подключиться			

Рис. 23 Подключение пользователя к беспроводной точке доступа.

Если не все настройки введены, не отредактированы файлы Users.conf и Clients.conf или RADIUS-сервер еще не запущен, то пользователь увидит диалоговое окно (Рис. 24).

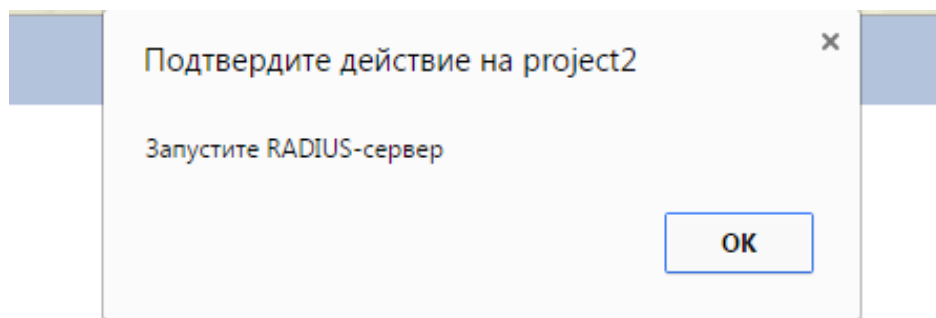


Рис. 24. Диалоговое окно

После попыток подключения к точке доступа в лог командной строки выводятся различные сообщения:

- Если настройки в модуле интерфейсов управления точкой доступа Proxim Orinoco AP4000 не совпадают с настройками, введенными в рабочем модуле – в Лог командной строки выводится «нечитаемый» текст.
- Если пароль, введенный пользователем, не совпадает с паролем, указанным в файле Users.conf – в лог выводится сообщение Pass\_fail, а от RADIUS сервера будет отправлено сообщение Access-Reject.

- Если пароль, указанный в рабочем модуле, не совпадает с паролем, указанным в конфигурационном файле Clients.conf – в лог выводится нечитаемый текст.
- Если все настройки введены правильно и пароль является верным – в лог выводится сообщение share\_secret\_ok. Пользователь будет успешно подключен к точке доступа, а от RADIUS-сервера будет отправлено сообщение Access-Accept.

При успешной настройке перед пользователем появляется диалоговое окно с сообщением, об успешной настройке RADIUS-сервера (Рис. 25)

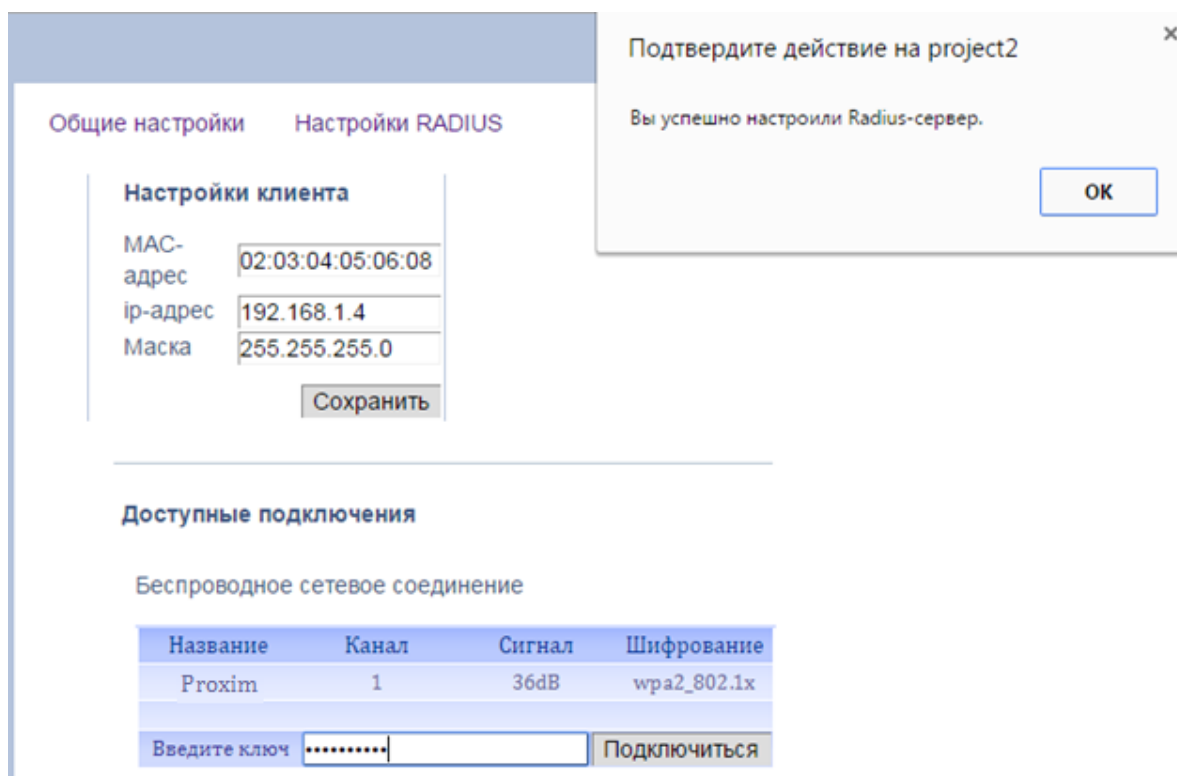


Рис. 25 Подключение к RADIUS

В Лог командной строки выводится сообщение о разрешении пользователю доступа к сетевым ресурсам (Рис.26).

#### Доступные подключения

Беспроводное сетевое соединение

Название	Канал	Сигнал	Шифрование
Proxim	1	46dB	wpa2_802.1x
Подключено			Отключиться

#### Командная строка TestMode

```
modcall[post-auth]: module "reply_log" returns ok for request 1
modcall: leaving group post-auth (returns ok) for request 1

Sending Access-Accept of id 2 to 192.168.1.2 port 1812

Finished request 1
Going to the next request
--- Walking the entire request list ---

secret_ok radius/output/shared-secret-ok.php
```

Рис.26 Подключение к RADIUS

### 3.6. Методические указания по настройке режима работы «Беспроводной мост»

В рамках модернизации эмулятора в Web-приложение был внедрен режим работы точки доступа, который называется «Bridge», или иначе – сетевой радио-мост. Для установления сетевого моста используется функция точки доступа, которая называется Wireless Distribution System(WDS).

WDS является технологией, позволяющей расширить зону покрытия беспроводной сети и объединить несколько WiFi точек доступа в единую сеть без необходимости наличия проводного соединения между ними.

На рисунке 27 представлена схема взаимодействия точки доступа Proxim Orinoco AP 4000, NanoStation Loco m2 с пользователем и беспроводным клиентом.



Рис.27 схема взаимодействия точки доступа Proxim Orinoco AP 4000 и NanoStation Loco m2

Ниже будет описан подробный ход настройки беспроводного радио-моста на основе модернизируемого эмулятора.

В начале настройки пользователю необходимо на интерфейсе управления беспроводной точкой доступа Proxim Orinoco AP4000 в разделе WDS (Рис. 28) задать Partner MAC address, то есть Mac-адрес точки доступа совместно с которой будет установлен беспроводной сетевой мост.

### WDS Security

WDS Security Mode	WEP ▼
Encryption Key 0	.....
<div>OK Cancel</div>	

### WDS partner access points

Port Index	1
Partner MAC Address	02:66:03:44:55:44
Status	Disable ▼
Port Index	2
Partner MAC Address	
Status	Disable ▼
Port Index	3
Partner MAC Address	
Status	Disable ▼
<div>Save Cancel</div>	

Рис. 28 WDS Proxim Orinoco AP4000

По такому же принципу необходимо ввести настройки на интерфейсе управления точкой доступа NanoStation Loco m2, которые находятся во вкладке Wireless, в поле WDS (Transparent Bridge Mode) (Рис. 29).

MAIN

WIRELESS

NETWORK

ADVANCED

S

Basic Wireless Settings

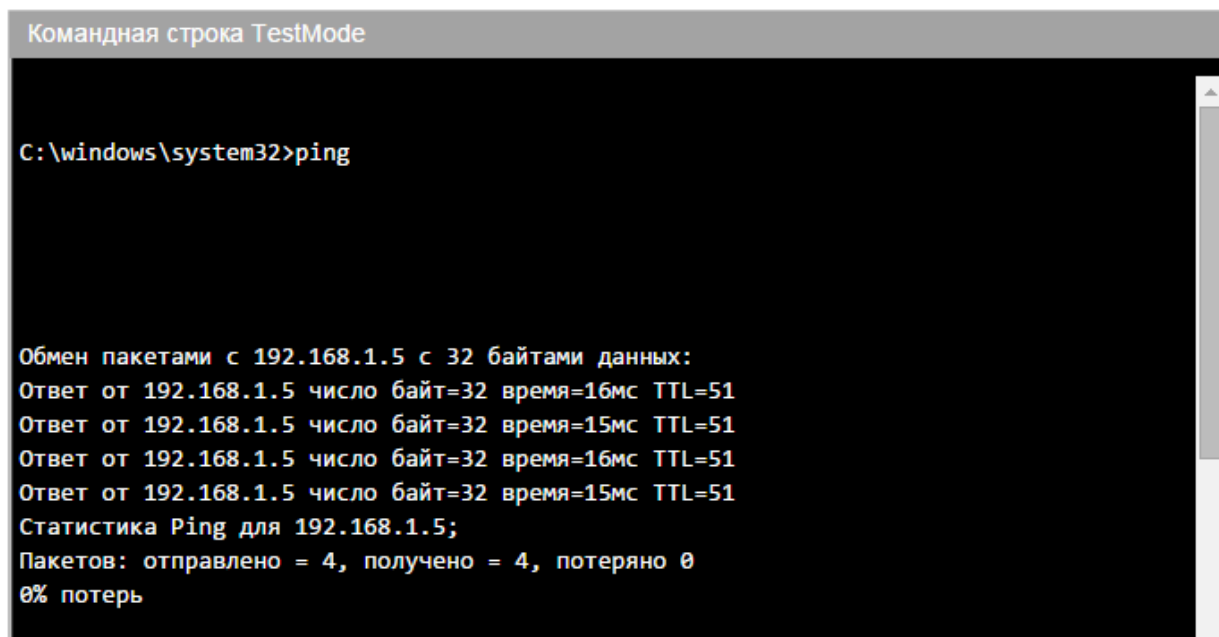
Wireless Mode: Access Point ▼

WDS (Transparent Bridge Mode): 02:03:04:05:06:08

Рис.29 WDS LocoNanoStation m2

В случае корректного ввода MAC адресов, сетевой радио-мост будет автоматически установлен. В главном меню пользователь сможет это

пронаблюдать. Для удобства проверки корректности ввода настроек в эмулятор была внедрена командная строка, где существует возможность при помощи утилиты Ping проверить идет ли обмен пакетами между точками доступа или нет. Если сетевой мост установлен в Лог командной строки выводится сообщение (Рис. 30).



```
Командная строка TestMode

C:\windows\system32>ping

Обмен пакетами с 192.168.1.5 с 32 байтами данных:
Ответ от 192.168.1.5 число байт=32 время=16мс TTL=51
Ответ от 192.168.1.5 число байт=32 время=15мс TTL=51
Ответ от 192.168.1.5 число байт=32 время=16мс TTL=51
Ответ от 192.168.1.5 число байт=32 время=15мс TTL=51
Статистика Ping для 192.168.1.5;
Пакетов: отправлено = 4, получено = 4, потеряно 0
0% потерь
```

Рис.30 Лог командной строки

А если настройки были введены некорректно , точки доступа не смогли подключиться друг к другу, то командная строка выведет сообщение о том, что между устройствами нет связи(Рис. 31 ).

A screenshot of a Windows command prompt window. The title bar at the top is grey and contains the text "Командная строка TestMode". The main area of the window is black with white text. The first line shows the command prompt "C:\windows\system32>ping". The second line shows an error message in Russian: "При проверке связи не удалось обнаружить узел 192.168.1.4. Проверьте имя узла и повторите попытку."

Рис. 31 Лог командной строки

### 3.7. Описание работы с эмулятором

Модернизируемое web-приложение является многопользовательским, а также имеет распределение ролей на студентов и преподавателей, работа с эмулятором начинается с регистрации пользователя (Рис. 32). При регистрации пользователю назначаются права, достаточные для использования эмулятора. Права, необходимые для контроля учетных записей имеет только администратор, которым является преподаватель. После авторизации пользователь на главной странице сможет увидеть свои учетные данные (Рис. 33).



The screenshot shows a web application titled "Эмулятор протоколов защиты точки доступа стандарта 802.11". It features a top header with a padlock icon and the title. The main content area is titled "Регистрация" (Registration). On the left, there is a "Меню" (Menu) sidebar with links: Главная (Home), Вход (Login), Регистрация (Registration), Демо (Demo), and About. On the right, there is a "Теория" (Theory) sidebar with links: Общие сведения (General information), Аутентификация (Authentication), Управление ключами (Key management), Инкапсуляция (Encapsulation), Radius, Режимы работы точки доступа (Access point operating modes), and Методические указания (Methodological instructions). The registration form itself contains input fields for: Имя (Name), Фамилия (Surname), Группа (Group), Пароль (Password), Повторите пароль (Repeat password), and login. A "Зарегистрироваться" (Register) button is located at the bottom of the form.

Рис. 32. Регистрация нового пользователя

The screenshot shows a confirmation message box with the following text: "Ваш логин: oleg", "Ваше имя: Олег", "Ваша фамилия: Юплин", "Группа: 123", and a blue link "Выход" (Exit).

Рис. 33 Учетные данные пользователя

Кроме основного предназначения эмулятора - ознакомление и изучение работы RADIUS-сервера, изучение режима работы беспроводной точки доступа «сетевой мост» и изучение протоколов безопасности, эмулятор также используется для обучения работе с интерфейсами реального оборудования. Поэтому прежде чем приступить к изучению вышеперечисленных компонентов в приложении предусмотрена предварительная настройка виртуальных точек доступа и беспроводного клиента. Это необходимо для понимания связи между введенными настройками и теми протоколами, которые предлагаются к изучению.

На рисунке 32 представлена схема отображения взаимосвязей web-страниц, начиная с главной страницы.

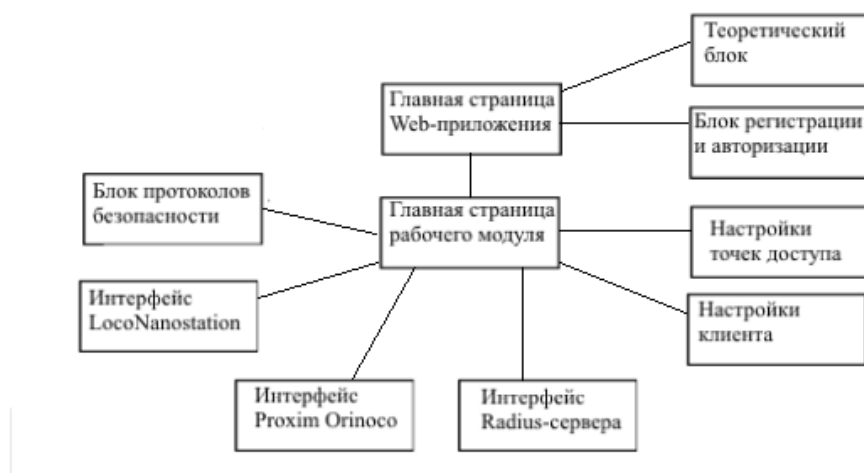


Рис. 32. Схема взаимосвязей web-страниц приложения

### **Предварительная настройка**

Конфигурирование точки доступа выполняется в модуле интерфейсов управления устройством Proxim Orinoco AP4000. Пользователю предлагается ввести настройки беспроводных Радиоинтерфейсов, настройки LAN-интерфейса и настройки безопасности (Рис. 35).



Рис. 35. Страница ввода настроек безопасности

Одной из приоритетных задач при разработке эмулятора являлось создание интерактивного и удобного пользовательского интерфейса, поэтому в ходе работы с настройками и их сохранения пользователь сопровождается подсказками и сообщениями об ошибках в случае их допущения. Далее необходимо ввести настройки беспроводного клиента в рабочем модуле. В качестве настроек вводятся IP-адрес и MAC-адрес устройства (Рис. 35).

Общие настройки      Настройки RADIUS

**Настройки клиента**

MAC-адрес

ip-адрес

Маска

Рис. 35. Форма ввода настроек клиента

После ввода настроек клиента следует перейти на главную страницу рабочего модуля. На главной странице рабочего модуля пользователь имеет возможность проверить правильность введенных настроек. Корректность настроек определяется не только с точки зрения существующих стандартов,

но и с точки зрения правильности построения локальной сети. Если какие-то настройки введены неверно, нет необходимости возвращаться в интерфейсы управления точкой доступа, так как их можно изменить в рабочем модуле на соответствующей странице.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. HTML, JavaScript, PHP и MySQL. Джентльменский набор Web-мастера / Прохоренок Н.А. – СПб.: БХВ-Петербург, 2012. - 912 с.
2. PHP и MySQL. Исчерпывающее руководство / Маклафлин Б. — СПб: Питер, 2013г. – 512 с.
3. RFC 2865. C. Rigney, S. Willens, A. Rubens, W. Simpson. Remote Authentication Dial In User Service (RADIUS) – IETF, June 2000. – 76 с.
4. Беспроводная сеть дома и в офисе / Денис Колисниченко - издательство БХВ-Петербург, 2009 г. – 480 с.
5. Беспроводная сеть за 5 минут. От выбора оборудования до устранения любых неполадок / Дж. Гайер, Э. Гайер, Дж. Кинг – издательство НТ Пресс, 2008 г. – 176 с.
6. Беспроводные сети / Ирина Иващук - Издательство LAP Lambert Academic Publishing, 2012 г. - 144 с.
7. Беспроводные сети Wi-Fi / Пролетарский А. В., Баскаков И. В., Чирков Д. Н. - БИНОМ. Лаборатория знаний, 2007 г. – 216 с.
8. Беспроводные технологии от последней мили до последнего дюйма / Михаил Немировский, Олег Шорин, Александр Бабин, Анатолий Сартаков – издательство Эко-Трендз, 2009 г. – 400 с.
9. Компьютерные сети / Таненбаум Э.С., Д. Уэзеролл – издательство Питер, 2015 г. - 960 с.
10. Компьютерные сети и сетевые технологии / Николай Кузьменко – издательство Наука и Техника, 2013 г. – 368 с,
11. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 / Ковалев Д., Ковцур М. / Первая миля. - 2014. - № 3 (42). С. 72-77.
12. Основы беспроводной передачи данных / Владимир Комашинский – Издательство Palmarium Academic Publishing, 2014г. – 296 с.

13. Основы компьютерных сетей. Учебное пособие / Олифер В.Г., Олифер Н.А. – СПб.: Питер. – 352 с.
14. Сети. Беспроводные технологии / Пол Беделл – издательство НТ Пресс, 2008 г. – 448 с.
15. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows / Джозеф Дэвис – издательство Эком, 2006 г. – 400 с.
16. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных / Елена Смирнова, Павел Козик – издательство БХВ-Петербург, 2012 г. – 272 с.
17. Энциклопедия WiMax. Путь к 4G / Вишневский В.М., Портной С.Л., Шахнович И.В. – издательство Техносфера, 2010. - 472 с.
18. Эффективный самоучитель по креативному WEB-дизайну. HTML, XHTML, CSS, JavaScript, PHP, ASP ActiveX / Крис Джамса, Конрад Кинг, Энди Андерсон – Москва, Торгово-издательский дом Diasoft, 2005 г. – 472 с.