Скопень М. М., к.е.н., доцент
Стародуб О. П., викладач-методист
Київський фаховий коледж
туризму та готельного господарства
м. Київ, Україна

DOI: https://doi.org/10.30525/978-9934-26-194-7-27

ОСОБЛИВОСТІ ШИФРУВАННЯ ТА ПРОГРАМУВАННЯ ОБМЕЖЕННЯ ДОСТУПУ У БЕЗДРОТОВИХ МЕРЕЖАХ

У відомих літературних джерелах достатньо добре розглянуто принципи організації та моделювання мереж [1; 2] конфігурування віртуальних мереж [3] та ін. Однак, аналіз видань свідчить про відсутність розкриття технології шифрування даних на базі протоколу WEP (Wired Equivalent Privacy) та програмування обмеження доступу до вузлів списком ACL (Access Control List) з декількома видами бездротових пристроїв при моделюванні мереж на платформі системи Cisco Packet Tracer. Саме ця технологія і пропонується авторами нижче для розгляду.

Припустимо, що в корпоративній мережі, яка структурована на основі бездротового роутера, точки доступу та центру обслуговування стільникового зв’язку, необхідно організувати шифрування та обмеження доступу.

В даному випадку технологія шифрування та програмування обмеження доступу буде складатися з наступних етапів:

– побудова топології мережі з декількома видами бездротових пристроїв (рис. 1);

– шифрування даних на WiFi роутері WRT300N та його вузлах;

– шифрування даних та програмування обмеження доступу, наприклад, до вузлів 192.168.1.3 і 192.168.1.4 на роутері 0;

– налаштування DNS (Domain name server), WEB – сервера;

– програмування функцій DHCP (Dynamic Host Configuration Protocol) і RIP (Routing Information Protocol) на роутері 1 та шифрування даних на точці доступу Access Point і її вузлів;

– налаштування обслуговування стільникового зв'язку.

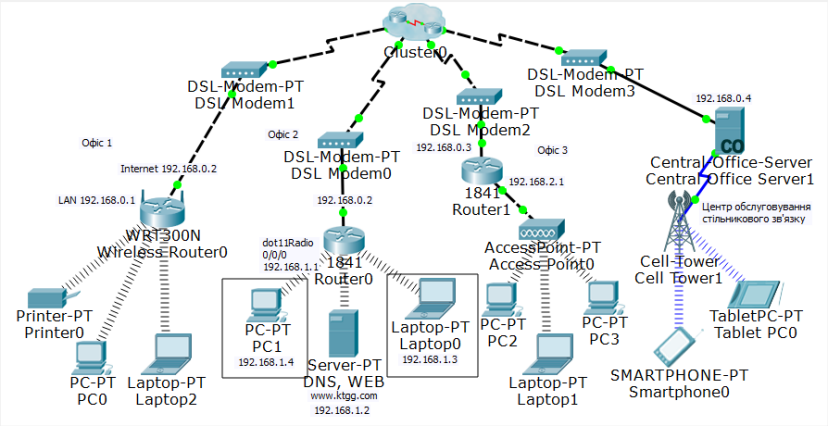

Рис. 1. Топологія мережі з декількома видами бездротових пристроїв

Шифрування даних на WiFi роутері WRT300N та його вузлах. Налаштування та шифрування здійснюється наступним чином. На вкладці Config / Internet встановлюється Default Gateway – 192.168.0.2, а DNS Server – 192.168.1.2. За умовчанням на вкладці Config / LAN буде IP-address 192.168.0.1, Subnet Mask – 255.255.255.0. Для шифрування даних активізується вкладка Config / Wireless0 і встановлюється: SSID – Office1, перемикач WEP та WEP Key – 0123456789. При цьому Encryption Type повинен бути 40/64-Bits (10 Hex digits). Для вузлів WiFi роутера фіксується режим DHCP, а для шифрування даних встановлюється (аналогічно як і на бездротовому роутері) SSID – *Office1*, перемикач WEP та WEP Key – *0123456789.*

Шифрування даних та програмування обмеження доступу до вузлів 192.168.1.3 і 192.168.1.4 на роутері 0. Спочатку роутер 0 вимикається і встановлюється модуль HWIC-AP-AG-B, який є точкою доступу, що підтримує однодіапазонні радіостанції 802.11b/g або дводіапазонні 802.11a/b/g. Статично задаються IP-адреси для шлюзів fa 0/0 – 192.168.0.2, та dot11Radio 0/0/0 – 192.168.1.1. Далі з використанням командного рядка CLI (Command Line Interface) програмується:

– *робота точки доступу з шифруванням*

```
Router>en
Router#conf t
Router(config)#dot11 ssid Office2
Router(config-ssid)#authentication open
Router(config-ssid)#guest-mode
Router(config-ssid)#exit
Router(config-if)#int dot11Radio 0/0/0
Router(config-if)#encryption mode wep mandatory
Router(config-if)#encryption key 1 size 40bit 0123456789
```

```
Router(config-if)#ssid Office2
Router(config-if)#do wr
```
– динамічна маршрутизація
```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#do wr
```
– та обмеження доступу вузлів 192.168.1.3, 192.168.1.4 до інших вузлів корпорації окрім DNS, WEB серверу
```
Router(config)#ip access-list standard Office2
Router(config-std-nacl)#deny host 192.168.1.3
Router(config-std-nacl)#deny host 192.168.1.4
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface Dot11Radio0/0/0
Router(config-if)#ip access-group Office2 in
Router(config-if)#do wr
```
Налаштування DNS, WEB – сервера. На вкладці Services послідовно активізуються служби DNS та WEB (режим HTTP) та виконується відповідне налаштування (рис. 2).

Програмування функцій DHCP і RIP на роутері 1 та шифрування даних на точці доступу Access Point і її вузлів. Статично задаються IP-адреси для шлюзів fa 0/0 – 192.168.0.3 та fa 0/1 – 192.168.2.1. Далі за допомогою командного рядка CLI програмується динамічна роздача вузлам IP-адрес і запускається протокол RIP для динамічної маршрутизації:
```
Router(config)#ip dhcp pool Nick
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.1.2
```

```
Router(dhcp-config)#do wr
Router(dhcp-config)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.2.0
Router(config-router)#do wr
```

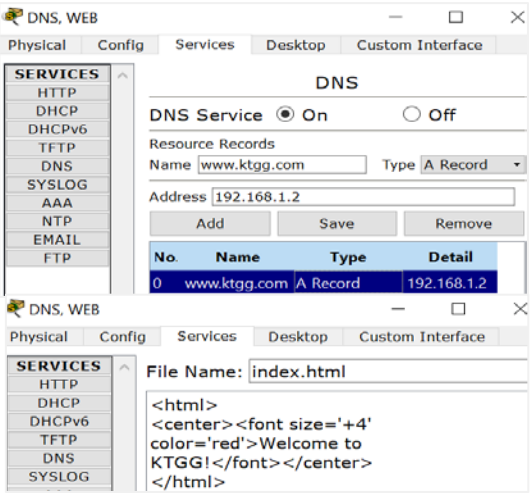

Рис. 2. Налаштування DNS, WEB- сервера

Для шифрування даних на бездротовій точці доступу Access Point відкриваються Config/ Port1, вводяться ідентифікатор (SSID) – *Office3* та код захисту (WEP Key): *0123456789*. На вузлах точки доступу вмикається режим DHCP і також встановлюються: SSID – *Office3* та WEP Key – *0123456789*.

Налаштування стільникового зв'язку. Тут, перш за все, конфігурується сервер на вкладці *Backbone Setting*, а саме встановлюються: Default Gateway – 192.168.0.2, IP-address – 192.168.0.4, Subnet Mask – 255.255.255.0, DNS Server –

192.168.1.2. При цьому на вкладці *Cell Tower* за умовчанням самостійно фіксується IP-адреса 172.16.1.1, яка для вузлів стільникового зв'язку служитиме за Default Gateway.

Після безпомилкового виконання налаштування топології мережі буде забезпечена успішна перевірка її працездатності.

Отже, запропонована технологію шифрування даних та програмування обмеження доступу до вузлів дозволяє вирішити питання підвищення якості вивчення побудови бездротових мереж. Представлену технологію можна рекомендувати для використання в навчальному процесі, а також моделювання мереж на стадії проектування.

Література:

1. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі : підручник для ВНЗ. Київ : САММІТ-Книга, 2010. 708 с.

2. Кулаков В.Г., Леохин Ю.Л. Моделирование компьютерных сетей в симуляторе Cisco Packet Tracer 6 : учебное пособие. Москва : Издательство МТИ, 2016. 175 с.

3. Скопень М.М., Будя О.П. Особливості моделювання та конфігурування віртуальних мереж з доступом до Інтернет засобами системи Cisco Packet Tracer / Механізми державного регулювання конкурентоспроможності національної економіки та міграційних процесів: матеріали Всеукраїнської науково-практичної конференції (13 березня 2021 року). Одеса : ОНУ імені І. І. Мечникова, 2021. С. 89–93.