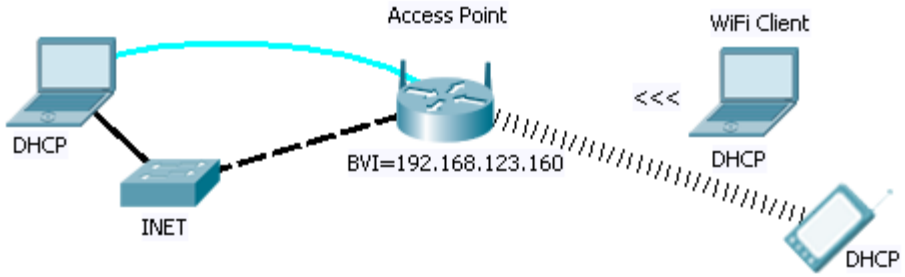
SIECI KOMPUTEROWE – LABORATORIUM 035

Tematyka:

Konfigurowanie sieci bezprzewodowych. Cisco IOS, Cisco Aironet 1200

Zadanie A: Podstawowa konfiguracja punktu dostępowego Cisco Aironet. Konfigurowanie SSID i WPA.

1. Należy przygotować do pracy Access Point (AP) Cisco Aironet 1200, łącząc go okablowaniem UTP w układzie PC-AP z podłączeniem do Internetu. Dodatkowo – można przygotować urządzenie mobilne mogące być klientem WiFi.



2. Logowanie do CLI: domyślne hasło to "Cisco" (z dużej litery). Konfiguracja (w tym także hasło) jest zapisywana w pliku flash:config.txt. Kasowanie ustawień do postaci fabrycznej sprowadza się do skasowania tego pliku. Domyślnie dostępny jest interfejs WWW. Dane logowania Cisco/Cisco (wyjątkowo - z dużej litery!).
3. W Cisco Aironet tworzony jest mostek BVI łączący porty bezprzewodowe i przewodowy (Fast Ethernet). Należy mu nadać adres IP. Protokół na nim uruchamia się dopiero po włączeniu interfejsów bezprzewodowego i FastEthernet. Gdy mostek jest aktywny - jego adres IP jest widoczny na zewnątrz (adres BVI 1 musimy skonfigurować, gdyż mostkowane interfejsy bezprzewodowy i WiFi nie mają adresów IP)
4. Domyślnie Access Point jest klientem DHCP. Udostępnia tą usługę asocjowanym klientom WiFi. Zdefiniowanie domyślnej bramy:
   Aironet(config)#ip default-gateway 192.168.123.254
   Adres domyślnej bramy dla klientów WiFi zostanie przekazany z DHCP. Jeśli jednak będzie potrzebny w IOS urządzenia AP, należy zdefiniować domyślna bramę także w AP.
5. Nazewnictwo interfejsów WiFi:
   - dot11radio 0 to Radio0-802.11B (moduł sprzętowy 802.11B 11Mbps)
   - dot11radio 1 to Radio0-802.11A (moduł sprzętowy 802.11G 54Mbps)
   Przy wyborze interfejsu WiFi należy sprawdzić, czy karta WiFi klienta będzie z nim kompatybilna. Niektóre (nowsze) karty WiFi laptopów czy PC mogą być skonfigurowane wyłącznie do obsługi standardu 802.11g lub 802.11n.

6. Należy skonfigurować SSID w AP (na razie bez przypisywania do interfejsu):
   Aironet(config)#dot11 ssid test

Aironet(config-ssid)#auth open
Aironet(config-ssid)#auth key wpa
Zdefiniowanie WPA preshare key:
Aironet(config-ssid)# wpa-psk ascii 12345678
W celu uruchomienia SSID broadcast należy włączyć dla guest-mode SSID (w innym wypadku SSID będzie niejawny i podawany przez klienta):
Aironet(config-ssid)# guest-mode
UWAGA!: Baza SSID i przypisania SSID do interfejsów muszą być uporządkowane. Nieścisłości (literówka, duplikat wpisu itp.) spowodują zawieszenie rozgłaszania SSID.

7. Należy skonfigurować wybrany interfejs radio.
Uwaga!: Należy ograniczyć zasięg radiowy instalacji doświadczalnej (np. nie montować anten), aby nie dopuścić do otwarcia sieci Laboratorium na zewnątrz w czasie eksperymentów z WiFi.
Aironet(config)#int dot11radio 0
Należy skonfigurować algorytm szyfrowania (dla WPA), np.:
Aironet (config-if)#encryption mode ciphers tkip
Przypisanie SSID do interfejsu:
Aironet (config-if)#ssid test
Gdzie *test* to nazwa SSID zdefiniowana wcześniej.
Uwaga: W konfiguracji SSID określamy użycie wybranych szyfrów. Przed przypisaniem takiego SSID do interfejsu szyfry te trzeba skonfigurować, co uczyniono poprzednią komendą. W innym przypadku przypisanie nie będzie możliwe.
Włączenie interfejsu WiFi:
Aironet (config-if)#no sh

8. Komendy opcjonalne dla interfejsu:
Aironet (config-if)#speed 11.0
gdzie11 to wymuszona prędkość AP (Mbps)
Aironet (config-if)#power local 30
gdzie *local* to antena AP (analogicznie *client* to spodziewana moc klienta), zaś *30* to wartość mocy (w przedziale 1-40 lub 1-50)
Aironet (config-if)#channel 10
gdzie *36* jest numerem kanału WiFi (w przypadku nie wybrania tej wartości AP poszuka najmniej obłożonego kanału)

9. Przydatne operacje diagnostyczne:

Sprawdzenie rozgłaszanego SSID:
Aironet #show dot11 bssid
Diagnostyka interfejsu WiFi:
Aironet #show dot11 statistics client-traffic
Aironet #show dot11 mac-authen filter-cache
Aironet #show dot11 associations
Aironet #show dot11 associations all
Diagnostyka interfejsów AP:
Aironet #show arp
Aironet #show ip int brie

Debugowanie:
Aironet #debug dot11 aaa manager keys
Aironet #debug dot11 aaa authenticator state-machine
Aironet #debug dot11 aaa authenticator process
Aironet #debug dot11 aaa dot11 process

Zadanie B: Konfigurowanie WEP-128

WEP jest rozwiązaniem przestarzałym i posiadającym luki w bezpieczeństwie. Nie należy go stosować w praktyce, a ćwiczenie ma tylko charakter poglądowy.
Przed przystąpieniem do konfigurowania należy przeładować urządzenia kasując ustawienia poprzednie.
Konfigurowanie WEP wymaga wybrania trybu autentyfikacji (wariant *open* = bez wysyłania *shared key* od klienta):

1. Należy skonfigurować SSID w AP (na razie bez przypisywania do interfejsu):
   Aironet(config)#dot11 ssid test
   Aironet(config-ssid)#auth open
   Aironet(config-ssid)# guest-mode
   Aironet(config-ssid)#exit

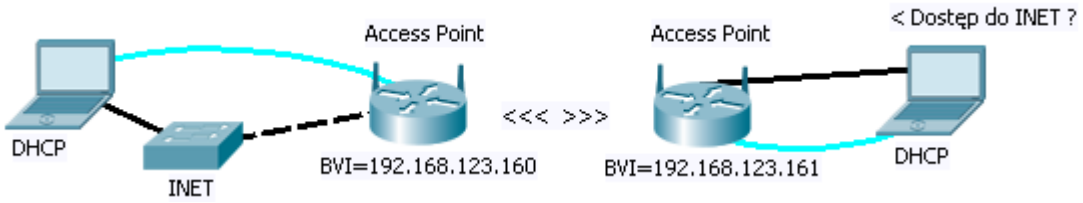
2. Należy skonfigurować wybrany interfejs bezprzewodowy.
   Aironet(config)#int dot11radio 0
   Aironet (config-if)#ssid test
   Gdzie *test* to nazwa SSID zdefiniowana wcześniej.
   Należy określić klucz algorytmu szyfrowania (dla WEP), np.:
   Aironet (config-if)#encryption key 3 size 128 09876543210987654321098765 transmit-key
   gdzie komenda *transmit-key* typuje klucz używany do wysyłania pakietów (indeks i treść podawana przez klienta AP musi być zgodna).

   Należy określić sam algorytm szyfrowania:
   Aironet (config-if)#encryption mode ciphers wep128
   Aironet (config-if)#broadcast-key change 200
   Aironet (config-if)#no sh

   Możliwe jest włączenie autentyfikacji *shared* (należy ją aktywować także w kliencie), jednak wówczas klucz jest wysyłany przez sieć - co jest niebezpieczne:
   Aironet(config)#dot11 ssid test
   Aironet(config-ssid)#auth shared
   Aironet(config-ssid)# guest-mode
   Aironet(config-ssid)#

Zadanie C: Mostki WiFi pomiędzy sieciami UTP (przewodowymi)

Aby stworzyć najprostszy mostek WiFi należy przygotować dwa AP, włączyć w nich interfejsy WiFi i skonfigurować te interfejsy odpowiednio do roli:
- root bridge - serwer mostka podłączony do sieci kablowej
- non-root bridge - klient mostka, który kończy tunel.
Ruch będzie przebiegał po trasie po trasie: INET (podłączony do Fast Ethernet 0 w root bridge) <-> root bridge <-> WiFi <-> non-root bridge <-> LAN (podłączony do Fast Ethernet 0 w non-root bridge).



Należy zbudować instalację według powyższego schematu.
Mostek jest niewidoczny w warstwie trzeciej (jednak obydwa BVI 1 w AP mają własne adresy IP).
Przed przystąpieniem do konfigurowania należy przeładować urządzenia kasując ustawienia poprzednie.
W obydwu AP mostka musimy zastosować ten sam SSID oraz zbieżny sposób autentyfikacji (np. open). Tryb guest mode AP nie jest konieczny.

1. Przygotuj konfigurację AP root:
   Aironet1(config)#dot11 ssid test
   Aironet1(config-ssid)#auth open
   Aironet1(config-ssid)#exit
   Aironet1(config)#int dot11radio 0
   Aironet1(config-if)#station-role root bridge
   Aironet1(config-if)#ssid test
2. Przygotuj konfigurację AP workgroup-bridge:
   Aironet2(config)#dot11 ssid test
   Aironet2(config-ssid)#auth open
   Aironet2(config-ssid)#guest-mode
   Aironet2(config-ssid)#exit
   Aironet2(config)#int dot11radio 0
   Aironet2(config-if)#station-role non-root bridge
   Aironet2(config-if)#ssid test
   Po zestawieniu połączenia (co w root bridge można to sprawdzić komendą *show dot11 associations all)* w obydwu AP pojawia sie nowy interfejs: Virtual-Dot11Radio0.

Gotowa konfiguracja urządzeń tworząca mostek nie zabezpieczony:

AP ROOT BRIDGE:

```
enable
conf t
dot11 ssid test
  auth open
exit

int dot11radio 0
  station-role root bridge
  ssid test
  no shut
```

AP CLIENT(NON ROOT):

```
enable
conf t
dot11 ssid test
  auth open
  guest-mode
exit
int dot11radio 0
  station-role non-root bridge
  ssid test
  no shut
```

3. Zabezpiecz mostek szyfrem. W tym celu po obydwu stronach w konfiguracji interfejsu zdefiniuj szyfr, a w konfiguracji SSID - klucz (uwaga: w przypadku WPA *preshare key* konfigurujemy po obydwu stronach mostka, gdyż połączenie ma nastąpić automatycznie.
4. Przykład korekt (należy konfigurować identycznie dla obydwu stron):

Aironet1(config)#int dot11radio 0
Aironet1(config-if)#encryption mode ciphers tkip
Aironet1(config-if))#exit
Aironet1(config)#dot11 ssid test
Aironet1(config-ssid)#auth key wpa
Aironet1(config-ssid)# wpa-psk ascii 12345678
Aironet1(config-ssid)#exit

Aironet2(config)#int dot11radio 0
Aironet2(config-if)#encryption mode ciphers tkip
Aironet1(config-if))#exit
Aironet2(config)#dot11 ssid test
Aironet2(config-ssid)#auth key wpa
Aironet2(config-ssid)# wpa-psk ascii 12345678
Aironet2(config-ssid)#exit

Gotowa konfiguracja urządzeń tworząca mostek szyfrowany:

AP ROOT BRIDGE:

```
enable
conf t
dot11 ssid test
  auth open
  auth key wpa
  wpa-psk ascii 12345678
exit
int dot11radio 0
  station-role root bridge
  encryption mode ciphers tkip
  ssid test
  no shut
exit
```

AP CLIENT(NON ROOT):

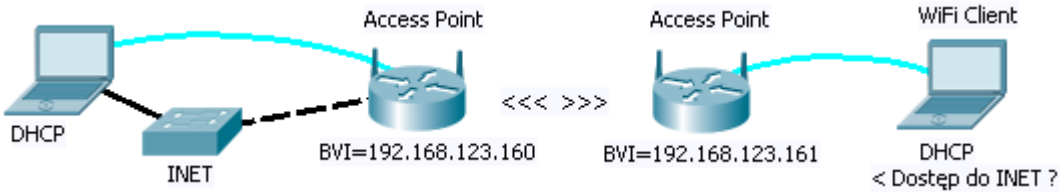
```
enable
conf t
dot11 ssid test
  auth open
  wpa-psk ascii 12345678
  auth key wpa
  guest-mode
exit
int dot11radio 0
  station-role non-root bridge
  encryption mode ciphers tkip
  ssid test
  no shut
exit
```

Sprawdzenie funkcjonowania szyfrowania w mostku:
Aironet 1#sh dot11 associations all
Aironet 1#sh dot11 associations all | *begin Key*
Uwaga: funkcje wyszukujące wzorce w tekście (np. widoczna *begin*) w Cisco IOS są domyślnie case-sensitive)

Zadanie D: Mostki WiFi z udostępnieniem AP.

Stworzenie mostka jednocześnie udostępniającego AP wymaga przekonfigurowania AP pełniącego rolę *non-root bridge* do roli *non-root wireless-clients* (mostek z jednoczesnym udostępnieniem ruchu klientom) oraz zdefiniowania dla nich opcji SSID: infrastructure.

Ruch będzie przebiegał po trasie po trasie: INET (podłączony do Fast Ethernet 0 w root bridge) <-> root bridge <-> WiFi <-> non-root wireless clients <-> WiFi



1. W AP root bridge należy wyłączyć SSID *guest mode*. W innym przypadku dwa AP (na potrzeby mostka i infrastructure AP) będą rozgłaszać ten sam SSID:
   Aironet1(config)#dot11 ssid test
   Aironet1(config-ssid)#no guest-mode
2. W AP *non-root wireless-clients* należy zmienić ustawienia SSID umożliwiając używanie go jako infrastructure. Zmiana trybu SSID na infrastructure:
   Aironet2(config)#dot11 ssid test
   Aironet2(config-ssid)#guest mode
   Aironet2(config-ssid)#infrastructure-ssid
   Uwaga: komenda *infrastructure-ssid* nie jest udostępniana przez auto-complete karetki IOS (trzeba ją wpisać ręcznie)
   Następnie należy zmienić tryb pracy interfejsu:
   Aironet2(config)#int dot11radio 0
   Aironet2(config-if)#station-role non-root wireless-clients
   Po dokonaniu zmian można łączyć się ze stacji klienckich. Należy sprawdzić status asocjacji w AP *non-root wireless-clients*, który powinien być zbliżony do następującego:

MAC Address	*IP address*	*Device*	*Name*	*Parent*	*State*
000e.d7b0.fb64	*128.0.0.23*	*bridge*	*ap*	*-*	*Assoc*
d0df.9a9d.c143	*128.0.0.21*	*unknown*	*-*	*self*	*Assoc*

   Gotowa konfiguracja urządzeń tworząca mostek szyfrowany z udostępnieniem Access Point:

AP ROOT BRIDGE:

```
enable
conf t
dot11 ssid test
  no guest-mode
  auth open
  auth key wpa
  wpa-psk ascii 12345678
exit
int dot11radio 0
  station-role root bridge
  encryption mode ciphers tkip
  ssid test
  no shut
exit
```

AP CLIENT(NON ROOT):

```
enable
dot11 ssid test
  guest-mode
  auth open
  wpa-psk ascii 12345678
  auth key wpa
  infrastructure-ssid
exit
int dot11radio 0
  station mode non-root wireless-clients
  encryption mode ciphers tkip
  ssid test
  no shut
exit
```

Zadanie E: Filtrowanie adresów MAC.

W celu uruchomienia filtrowania MAC w AP należy się posłużyć standardowymi listami ACL zdefiniowanymi w przedziale 700-799 (filtry dla Ethernet address).

1. Definiowanie listy ACL:
   Aironet(config)# access-list 701 permit D0DF.9A9D.C143
   Gdzie 701 do definiowany właśnie numer ACL. Przykład pokazuje poprawny sposób zapisania adresu MAC w komendzie.
   Weryfikacja:
   Aironet #show access-lists
   Bridge address access list 701
   permit d0df.9a9d.c143 0000.0000.0000 (1 match)
   Należy zdefiniować kolejno ACL dopuszczająca i wykluczającą (*permit*, *deny*) wybraną stację klienta WiFi.
2. Przypisanie ACL do interfejsu dot11:
   Aironet(config)#dot11 association mac-list 701
   gdzie 701 to numer listy ACL.
   Należy sprawdzić funkcjonowanie ACL w różnych konfiguracjach.