

Instrukcja Obsługi
Bezprzewodowy Punkt Dostępu WL-5460AP



AP

Bridge

Client

WDS

WISP

Universal
Repeater2MB
Flash16MB
DRAM

Opis sygnalizacji LED











Dioda	Opis
Power	Dioda sygnalizuje że urządzenie jest włączone do zasilania
Status	Dioda zapala się na czerwono gdy system jest w fazie uruchamiania, następnie gaśnie i urządzenie jest gotowe do pracy
Link/Act	Dioda zapala się na zielono gdy moduł radiowy jest gotowy do pracy, dioda miga podczas bezprzewodowej transmisji danych
WEP/WPA	Dioda pali się na czerwono gdy transmisja bezprzewodowa jest zaszyfrowana
MAC Ctrl	Dioda pali się na czerwono gdy włączymy funkcje kontroli dostępu po adresach MAC urządzeń bezprzewodowych
Bridge/Repeater	Dioda pali się na czerwono gdy urządzenie działa w trybie Bridge (Most) lub Repeater
LAN1/LAN2	Dioda zapala się na zielono gdy port zostanie połączony z innym przewodowym urządzeniem sieciowym, dioda miga podczas przewodowej transmisji danych



Interfejs	Opis
AC 12V	Gniazdo zasilania, zasilacz zewnętrzny 12V, 0.8A
LAN1/LAN2	Porty Ethernet RJ-45, działają jak dwu portowy switch, w trybie GW (Router Bezprzewodowy) port LAN2 jest portem WAN a port LAN1 jest portem LAN
ANT	Gniazdo R-SMA (Reverse SMA) W modelu WI-5460AP można stosować dowolne anteny zakończone wtykiem R-SMA
Reset	Wciśnięcie przycisku reset na 1 sekundę wywoła Restart urządzenia. Wciśnięcie przycisku reset na 7 sekund wywoła przywrócenie ustawień fabrycznych. Trzymanie zwartego przycisku reset w chwili zasilania urządzenia wywoła wejście w tryb serwisowy (Dokładny opis na str.85)

Zastosowanie - Tryby Pracy

Tryb Pracy	Opis	Zastosowanie
AP (Access Point)	W tym trybie urządzenie rozsyła sygnał bezprzewodowy. Wszystkie inne urządzenia radiowe zgodne ze standardem IEEE 802.11b/g mogą podłączać się do tej stacji AP. Porty LAN1/2 działają jak dwuportowy switch	
Klient	Ten tryb służy do znajdowania sieci bezprzewodowych i do łączenia się z nimi. Ilość znalezionych sieci zależy m.in. od anteny jaką stosujemy.	
Most (Bridge)	W tym trybie możemy połączyć dwie niezależne sieci LAN znajdujące się np. w dwóch budynkach. Urządzenia radiowe będą komunikować się tylko ze sobą i nie będą widoczne dla innych urządzeń bezprzewodowych.	
WDS Repeater	Tryb służy do poszerzania zasięgu sieci bezprzewodowej. Połączenie może być ustanowione tylko z inną stacją obsługującą tryb WDS	
Universal Repeater	Ten tryb również służy do poszerzania sieci bezprzewodowej. Od trybu WDS Repeater różni się tym, że stacja do której się podłącza nie musi być w trybie WDS - wystarczy że działa np. jako AP lub WISP	
WISP	To tryb w którym urządzenie działa podobnie jak w trybie „Klient” ale pomiędzy interfejsem radiowym a interfejsem LAN zastosowano funkcje Routera. Umożliwia to rozdzielanie sygnału radiowego od usługodawcy bez potrzeby stosowania dodatkowego Routera.	
WISP + Universal Repeater	To tryb w którym urządzenie działa podobnie jak w trybie „Klient” ale pomiędzy interfejsem radiowym a interfejsem LAN zastosowano funkcje Routera. Umożliwia to rozdzielanie sygnału radiowego od usługodawcy bez potrzeby stosowania dodatkowego Routera. Dodatkowo za pomocą trybu „Universal Repeater” transmisja kierowana na porty LAN jest również rozsyłana bezprzewodowo.	
Tryb Gateway	W tym trybie WL-5460AP działa jak standardowy Router Bezprzewodowy. LAN1 pozostaje portem LAN natomiast LAN2 staje się portem WAN.	

Rozpoczynamy pracę z WL-5460AP

Przy pierwszym logowaniu do urządzenia, na karcie sieciowej w naszym komputerze musimy ustawić ręcznie adres IP. Fabryczny adres WL-5460AP to **192.168.100.252** dlatego my na karcie sieciowej ustawimy np. adres IP 192.168.100.100. Urządzenie WL-5460AP z komputerem łączymy za pomocą kabla Ethernet RJ-45. Kabel wpinamy do portu LAN1 lub do portu LAN2. Pierwsze logowanie może odbywać się również drogą bezprzewodową.



RJ-45

Aby nasz komputer mógł komunikować się z WL-5460AP oba urządzenia muszą być w tej samej klasie adresowej. Aby dopasować nasz komputer do klasy adresowej urządzenia bezprzewodowego proszę postępować według poniższej instrukcji:



Aby ustawić adres na karcie sieciowej klikamy na Start -> Panel Sterowania -> Połączenia Sieciowe

- Start

- Panel sterowania

- Połączenia sieciowe

- wybieramy Połączenie lokalne 2
Połączono
Intel(R) PRO/100 VE Network ...

- klikamy prawym przyciskiem myszki na połączenie lokalne i wybieramy Właściwości

- następnie klikamy na Protokół internetowy (TCP/IP) i wybieramy Właściwości

- ustawiamy Użyj następującego adresu IP:

Adres IP:	192 . 168 . 100 . 100
Maska podsieci:	255 . 255 . 255 . 0

- po zapisaniu ustawień otwieramy dowolną przeglądarkę internetową np. Internet Explorer i w pasku adresowym wpisujemy i zatwierdzamy Adres 192.168.100.252

- przy ustawieniach fabrycznych WL-5460AP nie wymaga logowania przy użyciu hasła. Od razu pojawi się strona



Jeśli po wykonaniu powyższych czynności strona konfiguracyjna nie otwiera się należy wcisnąć przycisk „reset” na urządzeniu WL-5460AP i przytrzymać go wciśniętego przez 7 sekund. Gdy zgaśnie czerwona dioda status należy otworzyć przeglądarkę i ponownie wpisać adres 192.168.100.252.

Czasem w komputerze jest dużo połączeń lokalnych i ważne jest aby podczas konfiguracji aktywne było tylko połączenie z WL-5460AP.

Przy połączeniu bezprzewodowym najpierw uruchamiamy program obsługujący kartę bezprzewodową. Za pomocą tego oprogramowania wyszukujemy dostępne sieci bezprzewodowe. WL-5460AP rozsyła nazwę „airlive”. Podłączamy się do stacji „airlive”. Następnie przechodzimy do konfiguracji bezprzewodowego połączenia sieciowego.

Konfiguracja trybów pracy

Tryb AP (Access Point)



Tryb AP jest domyślnym trybem urządzenia. Aby go uruchomić wystarczy włączyć urządzenie do zasilania i odczekać aż zgaśnie czerwona dioda „status” na panelu przednim WL-5460AP. Po uruchomieniu urządzenie rozsyła sygnał bezprzewodowo. Oba porty LAN1 i LAN2 w tym trybie są ze sobą połączone i stanowią dwu portowy switch.

Po podłączeniu kabla Ethernet (RJ-45) do któregośkolwiek z portów LAN urządzenie automatycznie zamienia sygnał z kabla na ramki radiowe. Aby uzyskać połączenie ze stacją AP należy uruchomić urządzenie klienckie np. kartę radiową USB i połączyć się z nią. Domyślna nazwa rozgłaszania WL-5460AP to „airlive”.

Aby uruchomić tryb Access Point:

1. W zakładce „Tryby Pracy” wybieramy tryb AP AP Konfiguracja Punkt Dostępu.
2. Do portu LAN1/LAN2 podłączamy kabel Ethernet RJ-45
3. W zakładce „konfiguracja” możemy zmieniać nazwę SSID, kanał pracy oraz inne ustawienia zaawansowane.

Tryb Client



W tym trybie WL-5460AP może łączyć się do innych urządzeń bezprzewodowych. **Wszystkie urządzenia w trybie Station Infrastructure podmieniają adresy MAC.** Oznacza to że, jeżeli do portów LAN mamy podłączone 3 urządzenia to do serwera dotrze tylko jeden adres MAC - adres interfejsu WLAN WL-5460AP. Jest to ważna informacja dla osób posiadających serwery autoryzacji po adresie MAC. W takim przypadku należy wykorzystać funkcje autoryzacji zaimplementowane w urządzeniu radiowym.

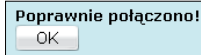
W przypadku gdy sieć do której chcemy się połączyć jest zabezpieczona kluczem WEP, WPA lub WPA2 musimy wybrać ten sam rodzaj klucza zanim dokonamy połączenia. (Jak ustawić klucz str. 14)

Aby uruchomić tryb Client:

1. Przeszujemy tryb pracy na Client Konfiguracja Stacja Odbiorcza / Ad-Hoc.
2. Klikamy „konfiguracja”
3. Wyszukujemy sieć radiową klikając: SSID: Skanowanie Sieci
4. Wybieramy sieć do której chcemy się połączyć

SSID	BSSID	Kanały	Typ	Szyfrowanie	Sygnal	Wybierz
ADW-4401	00:30:4f:60:da:e5	1 (B+G)	AP	no	87	<input type="radio"/>
default	00:30:4f:42:2c:75	11 (B+G)	AP	no	56	<input type="radio"/>
2	00:30:4f:37:24:6b	13 (B)	AP	no	18	<input type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	13	<input type="radio"/>

- Wybieramy sieć do której chcemy się podłączyć. Siła sygnału w zakładce „Sygnał” nie powinna być mniejsza niż 25. Mniejsza wartość może być przyczyną problemów z komunikacją. Po poprawnym połączeniu z wybraną siecią zobaczymy komunikat „Connect Sucesfull”
- Po poprawny połączeniu zobaczymy komunikat



Tryb Bridge



Jeśli chcemy połączyć osobne sieci lokalne np. dwa budynki to ten tryb jest najbardziej odpowiedni. Zapewni bezpieczne połączenie do którego inne stacje nie będą w stanie się podłączyć. Na takim linku uzyskamy też dużą wydajność i stabilność.

Aby uruchomić tryb Bridge:

- Wybieramy tryb pracy Bridge
- Oba skonfigurowane urządzenia należy ustawić na **różnych od siebie adresach IP** (np. stacja A 192.168.100.252 i stacja B 192.168.100.251. Zmiany dokonujemy w polu Adres IP: 192.168.100.252
- Oba urządzenia muszą pracować na takim samym kanale Numer Kanalu: 11
- Adresy MAC muszą być wpisane naprzemiennie

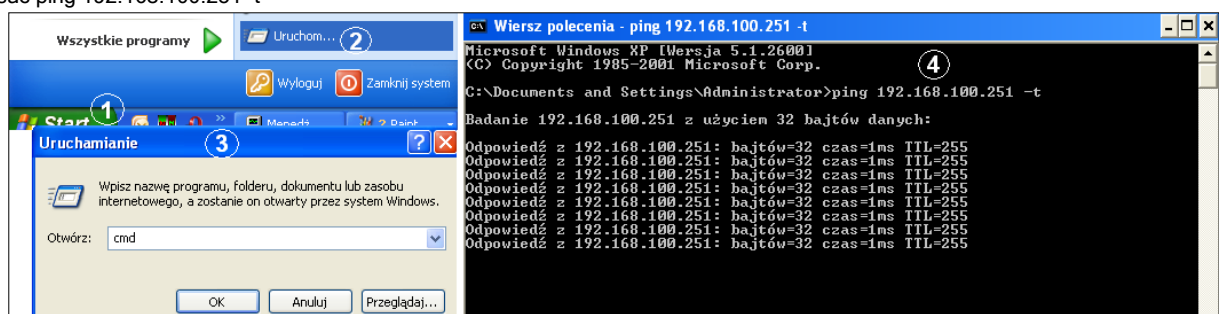
Podczas konfiguracji urządzenia A, wpisujemy w polu adres MAC urządzenia B.



Podczas konfiguracji urządzenia B wpisujemy adres MAC urządzenia A. W tym trybie adres MAC jest kluczem do poprawnej komunikacji. Połączenie pomiędzy urządzeniami zestawia się poprawnie po restarcie obu WL-5460AP.

Jak sprawdzić czy zestawione połączenie działa?

Uwzględniając że stacja A ma adres IP 192.168.100.252 a stacja B ma adres 192.168.100.251 ustawiamy adres na komputerze na karcie sieciowej 192.168.100.250. Teraz wszystkie urządzenia znajdują się w tej samej klasie adresowej i mogą poprawnie komunikować się ze sobą. Podłączamy komputer do portu LAN w stacji A i „pingujemy” na adres stacji B. W celu użycia komendy ping należy nacisnąć na pasku zadań „Start” -> uruchom - wpisać cmd -> wcisnąć enter -> w oknie poleceń wpisać ping 192.168.100.251 -t



Przy poprawnej konfiguracji otrzymamy odpowiedzi z adresu 192.168.100.251.

Tryb WDS Repeater



W tym trybie łączymy urządzenia tak samo jak w trybie Bridge. Dodatkowo stacja WDS Repeater będzie rozsyłała sygnał bezprzewodowo. Oznacza to że możemy podłączać klientów bezprzewodowych do połączenia typu Bridge. **WDS Repeater możemy połączyć tylko ze stacją obsługującą tryb pracy WDS.**

Aby uruchomić tryb Bridge:

1. Wybieramy tryb pracy WDS Repeater Konfiguracja WDS + AP.
2. Oba skonfigurowane urządzenia należy ustawić na **różnych od siebie adresach IP** (np. stacja A 192.168.100.252 i stacja B 192.168.100.251. Zmiany dokonujemy w polu Adres IP: 192.168.100.252
3. Oba urządzenia muszą pracować na takim samym kanale Numer Kanalu: 11
4. Adresy MAC muszą być wpisane naprzemiennie

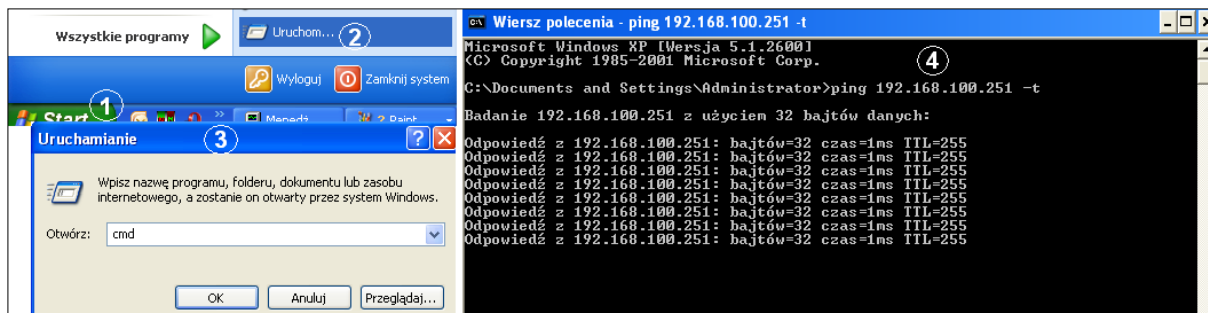
Podczas konfiguracji urządzenia A, wpisujemy w polu adres MAC urządzenia B.



Podczas konfiguracji urządzenia B wpisujemy adres MAC urządzenia A. W tym trybie adres MAC jest kluczem do poprawnej komunikacji. Połączenie pomiędzy urządzeniami zestawia się poprawnie po restarcie obu WL-5460AP.

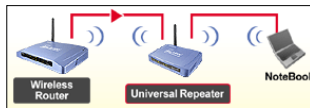
Jak sprawdzić czy zestawione połączenie działa?

Uwzględniając że stacja A ma adres IP 192.168.100.252 a stacja B ma adres 192.168.100.251 ustawiamy adres na komputerze na karcie sieciowej 192.168.100.250. Teraz wszystkie urządzenia znajdują się w tej samej klasie adresowej i mogą poprawnie komunikować się ze sobą. Podłączamy komputer do portu LAN w stacji A i „pingujemy” na adres stacji B. W celu użycia komendy ping należy nacisnąć na pasku zadań „Start” -> uruchom - wpisać cmd -> wcisnąć enter -> w oknie poleceń wpisać ping 192.168.100.251 -t



Przy poprawnej konfiguracji otrzymamy odpowiedzi z adresu 192.168.100.251.

Tryb Universal Repeater



W tym trybie użyjemy WL-5460AP w celu odebrania sygnału radiowego, wzmocnienia go i przesłania dalej. Jest to idealne rozwiązanie jeśli w miejscu instalacji sygnał od stacji nadawczej AP jest ledwie wystarczający. Wtedy ten słaby sygnał zostanie odebrany i wzmocniony. Stacja Universal Repeater na standardowej antenie 3dBi potrafi wzmocnić odebrany sygnał i rozesać go do 100 metrów przy pełnej widoczności optycznej. **Ograniczeniem jest obcięcie przepustowości linku radiowego o 50%.** W warunkach idealnych dwa urządzenia radiowe pracujące w standardzie IEEE 802.11g osiągają około 20Mbitów/s. W takim przypadku laptop na rysunku powyżej osiągnie około 10Mbitów przepustowości do urządzenia „Wireless Router”

Aby uruchomić tryb Universal Repeater:

1. Wybieramy tryb Universal Repeater
2. Wyszukujemy sieć radiową SSID:
3. Wybieramy sieć którą chcemy wzmocnić

SSID	BSSID	Kanały	Typ	Szyfrowanie	Sygnał	Wybierz
ADW-4401	00:30:4f60:da:e5	1 (B+G)	AP	no	87	<input checked="" type="radio"/>
default	00:30:4f42:2c:75	11 (B+G)	AP	no	56	<input type="radio"/>
2	00:30:4f37:24:6b	13 (B)	AP	no	18	<input type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	13	<input type="radio"/>

4. Konfigurujemy zabezpieczenia (str.14)
5. Po poprawny połączeniu zobaczymy komunikat
6. Numer kanału oraz nazwa SSID czyli parametry niezbędne do uzyskania połączenia zostaną pobrane automatycznie od stacji nadawczej.

Połączyliśmy się poprawnie do stacji nadającej. Rozgłaszamy sygnał ale o takiej samej nazwie. Aby rozróżnić którą sieć jest „nasza” a która to główna stacja nadająca możemy wpisać swoją nazwę np. zamiast ADW-4401 (2) do którego się łączymy możemy wpisać ADW-4401test (1).

Universal Konfiguracja Trybu Repeater

Nazwa:

Wyłącz Moduł Radiowy

Pasmo:

SSID: ①

Numer Kanału:

Separacja Klientów Radiowych:

SSID Interfejsu Wzmacniającego: ②

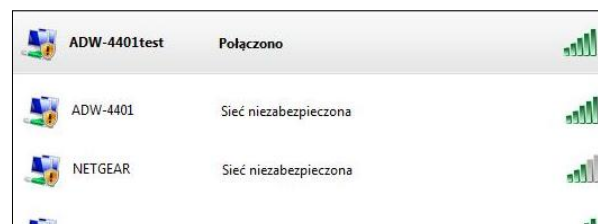
802.1d Spanning Tree:

Zabezpieczenia:

Ustawienia Zaawansowane:

Kontrola Dostępu:

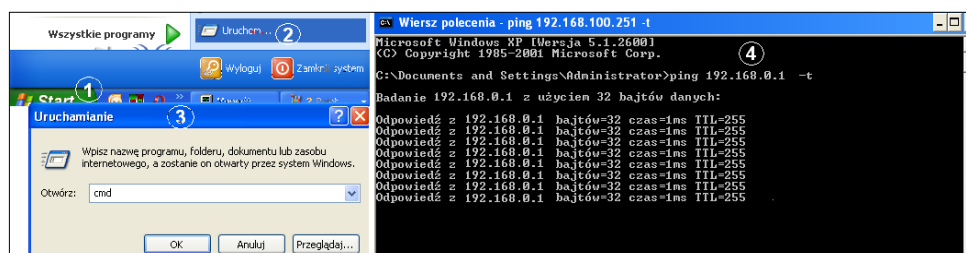
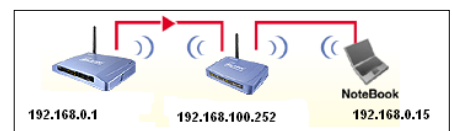
Efekt



W tym przykładzie „ADW-4401” to nazwa SSID stacji nadawczej AP lub WISP a nazwa „ADW-4401test” to nazwa rozsyłana z WL-5460AP Universal Repeater.

Jak sprawdzić czy tryb Universal Repeater działa poprawnie?

Na obrazu po prawej stronie widać przykład linku Universal Repeater. Laptop łączy się z WL-5460AP radiowo. Adres IP WL-5460AP służy tylko do zarządzania i nie ingeruje w sieć. Dlatego aby „zapingować” na adres 192.168.0.1 w celu sprawdzenia linku ustawiamy na laptopie tą samą klasę adresową jaką posiada urządzenie do którego się łączymy.



Tryb WISP



Tryb WISP służy do odbierania sygnału drogą radiową np. od sąsiada. Czym zatem różni się od trybu „Client”? Różnica jest dość istotna ponieważ WISP uruchamia również mechanizm NAT (Network Address Translation). Dla nas oznacza to tyle że jeżeli sąsiad „dał” nam tylko jeden adres IP np. 192.168.0.10 to

- używając trybu „client” moglibyśmy korzystać np. z Internetu tylko na jednym komputerze który to właśnie miałby adres 192.168.0.10, podłączając inny komputer i nadając mu adres 192.168.0.11 połączenie nie zadziała.

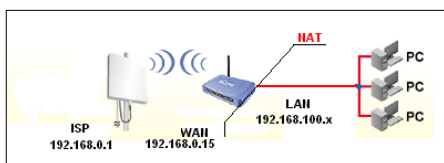
- tryb WISP natomiast potrzebuje tylko jeden adres IP i z tego adresu tworzy sobie podsieć oferując nam nową klasę adresową i 253 adresy IP do dyspozycji. Dodatkowo nasz sąsiad nie „widzi” od strony swojej sieci tego co dzieje się za NATem widzi tylko że używamy adres który nam przydzielił.

Aby uruchomić tryb WISP:

1. Wybieramy tryb WISP
2. Wyszukujemy sieć radiową SSID: airlive
3. Konfigurujemy zabezpieczenia (str. 14)
4. Po poprawnym połączeniu zobaczymy komunikat
5. Konfiguracja WAN
 - Musimy wiedzieć w „klient DHCP”. W od razu możemy WAN został był z innej klasy
 - W jaki sposób uzyskujemy adres IP jeżeli automatycznie to wybieramy opcję przypadku stałych adresów wybierzemy „Stale IP”. Przy opcji automatycznej uda się do zakładki Status-> System w celu sprawdzenia czy na interfejs przydzielony adres IP od usługodawcy. **Ważne aby adres na interfejsie WAN adresowej od adresu z interfejsu LAN.** Z definicji nie jest możliwe NATowanie adresu 192.168.100.xxx na klasę 192.168.100.xxx. Poprawna konfiguracja to np. WAN 192.168.0.1 a LAN np. 192.168.100.252.
6. Interfejs LAN od razu po włączeniu trybu WISP jest poprawnie skonfigurowany. Oznacza to że serwer DHCP odpowiedzialny za przydzielanie adresów jest włączony. Możemy podpinąć komputery do portów LAN1/LAN2 i korzystać z zasobów urządzenia do którego połączyliśmy się bezprzewodowo.

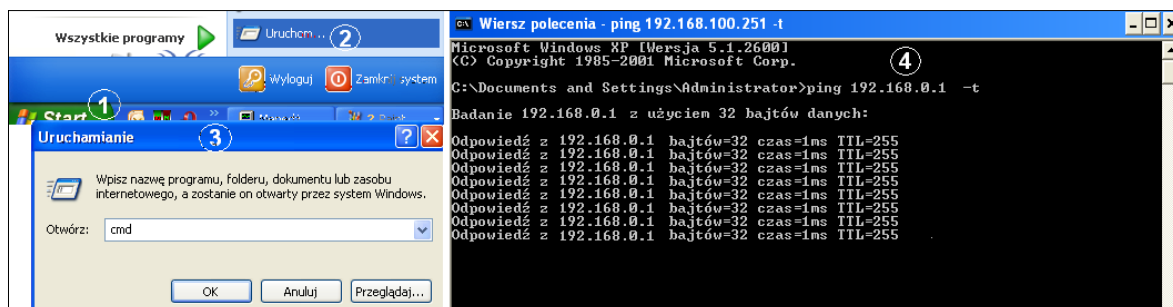
Jak sprawdzić czy WISP działa poprawnie?

Na przykładzie tego rysunku



Urządzenie ISP do którego połączyliśmy się bezprzewodowo posiada adres IP 192.168.0.1. WL-5460AP pobiera adres IP z serwera DHCP urządzenia ISP lub dostaje adres który wpisaliśmy ręcznie. Zakładamy że ten adres to 192.168.0.15. NAT rozdziela adres 192.168.0.15 na klasę adresową 192.168.100.x gdzie x oznacza adresy IP od 1-253. Oznacza to że komputery podpięte do portów LAN1/2 będą otrzymywały adresy IP 192.168.100.1,2,3-253.

Aby sprawdzić poprawność linku użyjemy komendy „ping” z komputera podłączonego do portu LAN



Tryb WISP + Universal Repeater



Tryb WISP + Repeater służy do odbierania sygnału drogą radiową np. od sąsiada. Czym zatem różni się od trybu „Client”? Różnica jest dość istotna ponieważ WISP uruchamia również mechanizm NAT (Network Address Translation). Dla nas oznacza to tyle że jeżeli sąsiad „da” nam tylko jeden adres IP np. 192.168.0.10 to

- używając trybu „client” moglibyśmy korzystać np. z Internetu tylko na jednym komputerze który to właśnie miałby adres 192.168.0.10, podłączając inny komputer i nadając mu adres 192.168.0.11 połączenie nie zadziałało.

- tryb WISP + Universal Repeater natomiast potrzebuje tylko jeden adres IP i z tego adresu tworzy sobie podsieć oferując nam nową klasę adresową i 253 adresy IP do dyspozycji. Dodatkowo nasz sąsiad nie „widzi” od strony swojej sieci tego co dzieje się za NATem widzi tylko że używamy adres który nam przydzielił. **Dodatkowo odebrany sygnał wzmacni i przekaże droga bezprzewodową.**

Aby uruchomić tryb WISP + Universal Repeater:

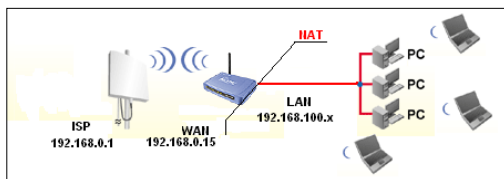
1. Wybieramy tryb WISP + Universal Repeater
2. Wyszukujemy sieć radiową
3. Konfigurujemy zabezpieczenia (jak?)
4. Po poprawnym połączeniu zobaczymy komunikat
5. Konfiguracja WAN

Musimy wiedzieć w „klient DHCP”. W od razu możemy WAN został **był z innej klasy** adresu 192.168.100.252 na klasę 192.168.100.252. Poprawna konfiguracja to np. WAN 192.168.0.1 a LAN 192.168.100.252.

jaki sposób uzyskujemy adres IP jeżeli automatycznie to wybieramy opcję przypadku stałych adresów wybierzemy „Stale IP”. Przy opcji automatycznej udać się do zakładki Status-> System w celu sprawdzenia czy na interfejs przydzielony adres IP od usługodawcy. **Ważne aby adres na interfejsie WAN adresowej od adresu z interfejsu LAN.** Z definicji nie jest możliwe NATowanie adresu 192.168.100.252 na klasę 192.168.100.252.
6. Interfejs LAN od razu po włączeniu trybu WISP jest poprawnie skonfigurowany. Oznacza to że serwer DHCP odpowiedzialny za przydzielanie adresów jest włączony. Możemy podpinąć komputery do portów LAN1/LAN2 i korzystać z zasobów urządzenia do którego połączyliśmy się bezprzewodowo.

Jak sprawdzić czy WISP działa poprawnie?

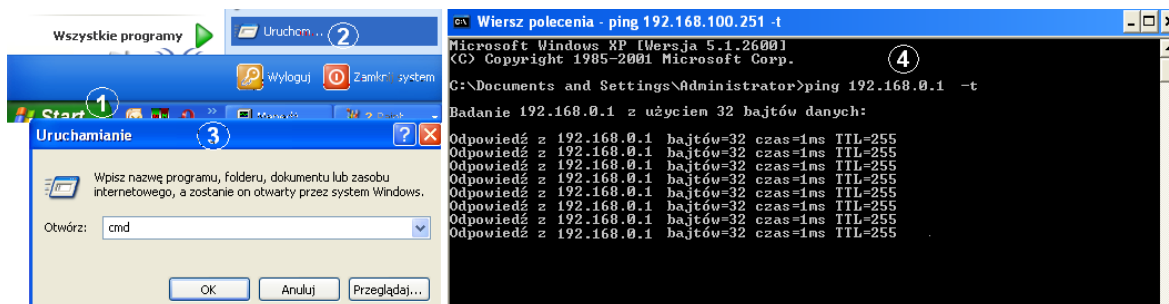
Na przykładzie tego rysunku



Urządzenie ISP do którego połączyliśmy się bezprzewodowo posiada adres IP 192.168.0.1. WL-5460AP pobiera adres IP z serwera DHCP urządzenia ISP lub dostaje adres który wpisaliśmy ręcznie. Zakładamy że ten adres to 192.168.0.15. NAT rozdziela adres 192.168.0.15 na klasę adresową 192.168.100.x gdzie x oznacza adresy IP od 1-253. Oznacza to że komputery podpięte do portów LAN1/2 będą otrzymywały adresy IP 192.168.100.1,2,3-253.

Jeżeli nie wiesz jaki adres IP posiada urządzenie ISP to sprawdź jaka bramę uzyskałeś lub wpisałeś na interfejsie WAN. Ta brama to adres na który należy „zapingować”.

Aby sprawdzić poprawność linku użyjemy komendy „ping” z komputera podłączonego do portu LAN



Tryb Gateway



W tym trybie WL-5460AP może odbierać sygnał kablowo i rozdzielać go stosując NAT. Sygnał rozdzielany jest zarówno dla klientów przewodowych jak i bezprzewodowych.

Takie rozwiązanie najczęściej stosuje się dla usług typu „DSL”.

Aby uruchomić tryb Gateway:

- Wybieramy tryb GW Gateway Konfiguracja WAN + LAN / AP.
- Do portu LAN2 wpinamy kabel od modemu (WAN)
- Do portu LAN1 wpinamy sieć lokalną (LAN)
- Konfiguracja WAN

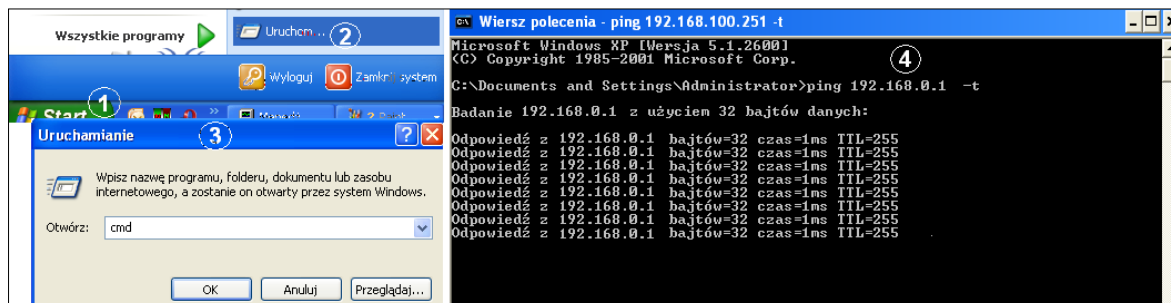
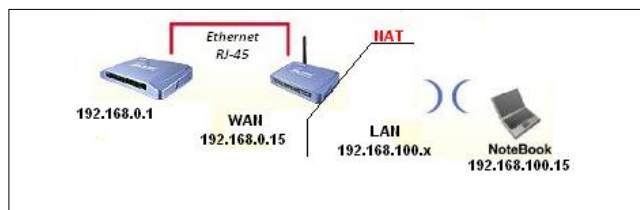
Klient DHCP
Stale IP
Klient DHCP
PPPoE
PPTP
L2TP

 Musimy wiedzieć w „klient DHCP”. W przypadku stałych adresów wybieramy „Stale IP”. Przy opcji automatycznej od razu możemy WAN zostać przydzielony adres IP od usługodawcy. **Ważne aby adres na interfejsie WAN adresowej od adresu z interfejsu LAN.** Z definicji nie jest możliwe NATowanie adresu 192.168.100.252 na klasę 192.168.100.252. Poprawna konfiguracja to np. WAN 192.168.0.1 a LAN 192.168.100.252.
- Interfejs LAN od razu po włączeniu trybu WISP jest poprawnie skonfigurowany. Oznacza to że serwer DHCP odpowiedzialny za przydzielanie adresów jest włączony. Możemy podpinąć komputery do portów LAN1/LAN2 i korzystać z zasobów urządzenia do którego połączyliśmy się bezprzewodowo.

Jak sprawdzić czy tryb Gateway działa poprawnie?

Jeśli pobieramy adres automatycznie to wystarczy po konfiguracji odwiedzić zakładkę Status -> System i tam w sekcji WAN zobaczyć czy zamiast zer pojawił się adres IP. Jeśli router otrzymał adres to wszystko powinno nam już działać. Jeżeli wcześniej na karcie sieciowej ustawialiśmy adres ręcznie aby móc zalogować się do WL-5460AP to należy pamiętać aby przestawić konfigurację z powrotem na „pobierz adres automatycznie”.

Jeśli adres ustawialiśmy ręcznie to najprostszą metodą jest „zapingowanie” na adres bramy którą wpisywaliśmy konfigurując interfejs WAN.



Opis Interfejsu WWW

W tym dziale omówimy wszystkie funkcje oprogramowania WL-5460AP.

Mode

Tryb AP

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G. 2.4 GHz (B)
2.4 GHz (G)
2.4 GHz (B+G) Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

SSID - identyfikator sieci składający się maksymalnie z 32 znaków. Wszystkie urządzenia pracujące w sieci aby się komunikować muszą mieć taką samą nazwę SSID. Identyfikator ten jest przesyłany w nagłówku ramki radiowej i pełni rolę hasła dostępowego przy próbie nawiązywania połączenia bezprzewodowego.

Site Survey - funkcja służy do skanowania dostępnych sieci bezprzewodowych. Po uruchomieniu ukazuje się tabela i znalezione sieci:

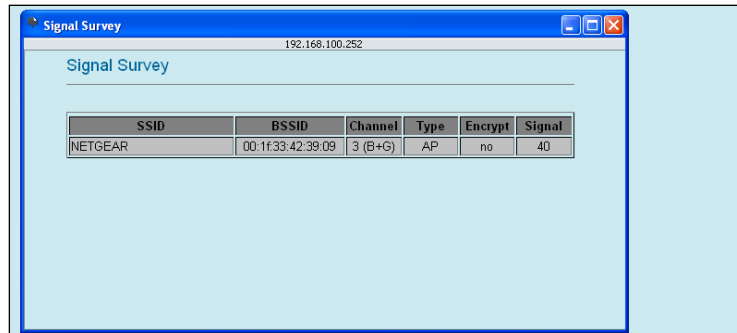
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
default	00:30:4f:42:2c:75	11 (B+G)	AP	no	64	<input type="radio"/>
ADW-4401	00:30:4f:60:da:e5	6 (B+G)	AP	no	64	<input type="radio"/>
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	43	<input checked="" type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	7	<input type="radio"/>
NO NAME	00:14:78:52:54:fe	6 (B+G)	AP	WEP	1	<input type="radio"/>

W tabelce znajdziemy:

- Nazwę **SSID** dostępnych sieci
- **BSSID** czyli numer identyfikacyjny odpowiadający adresowi MAC interfejsu bezprzewodowego
- **Channel**, tu znajdziemy informacje na jakim kanale i w jakim standardzie pracuje stacja nadawcza
- **Type** czyli tryb pracy stacji nadawczej
- **Encrypt** tu dowiemy się czy sieć jest zabezpieczona i jakiego klucza użyto do zabezpieczenia

- **Signal** to ważna informacja, oznacza siłę sygnału stacji nadającej. Do połączenia wymagana wartość minimalna nie powinna być mniejsza niż 25. Jest to minimum i taki link transmisja bezprzewodowa na takim linku często może być nie poprawna.
- **Select** czy pole które zaznaczamy aby wybrać daną sieć

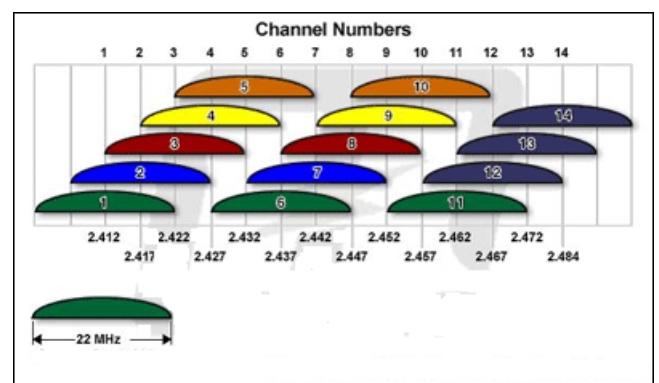
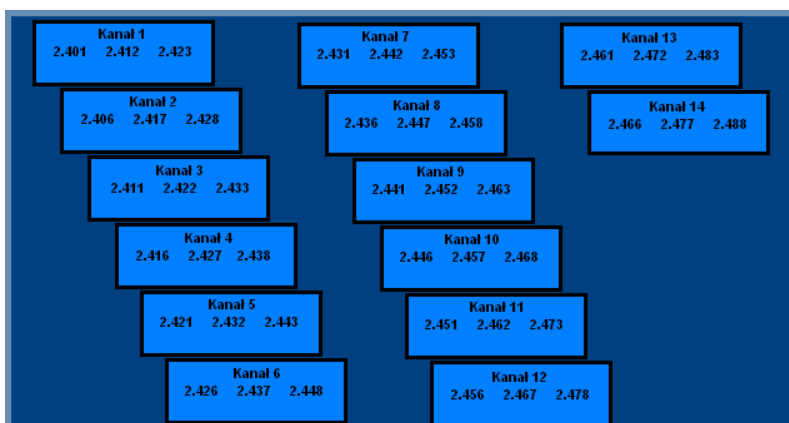
Signal Survey- to świetne rozwiązanie dynamicznego skanowania danej sieci. W polu „Select” wybieramy sieć, klikamy „Signal Survey”. Otworzy się osobne okienko w którym dynamicznie co 3 sekundy odświeża się informacja o sile sygnału stacji nadawczej. Bardzo przydatne narzędzie podczas zestawiania linku i konfiguracji anten.



Channel Number - tu wybieramy na jakim kanale ma pracować nasz nadajnik. Każdy kanał to określony zakres częstotliwości.

Numer Kanału	Dolna Częstotliwość Kanału w GHz	Środkowa Częstotliwość Kanału	Górna Częstotliwość Kanału w GHz
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488

Wszystkie kanały pokrywają się w pewnym stopniu częstotliwością. Oddzielone są np. kanały 1,7,13. Instalując sieci upewnijmy się jakie kanały są już używane. I użyjmy innych aby zredukować zakłócenia.



Ilość kanałów zależy od kodowania np.

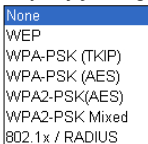
Region	Kodowanie	Ilość kanałów
USA	FCC	11
Europa	ETSI	13
Japonia	TELEC	14

Wireless Client Isolation - enabled (włącz), disabled (wyłącz). Funkcja izolacji klientów bezprzewodowych sprawia że użytkownicy nie będą wymieniać między sobą informacji. Użytkownicy nie będą mogli kopiować danych pomiędzy sobą w otoczeniu sieciowym dzięki temu można zwiększyć bezpieczeństwo danych w sieci oraz można skutecznie zwiększyć

wydajność urządzenia radiowego. Jeżeli klienci radiowi nie będą przysyłać między sobą danych, urządzenie radiowe nie będzie musiało ich przetwarzać. Funkcja dotyczy tylko klientów bezprzewodowych.

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze



Konfiguracja klucza WEP

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucza WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Wireless Security Setup

Encryption:

Pre-Shared Key Format:

Pre-Shared Key:

Group Key Life Time: sec

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Encryption:

Security:

Use 802.1x Authentication WEP 64bits WEP 128bits

Authentication RADIUS Server: Port IP address Password

Enable Accounting

Accounting RADIUS Server: Port IP address Password

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Inactivity Time: (101-60480000 10ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level:

Enable WatchDog

Watch Interval: (1-60 minutes)

Watch Host:

Ack time out: (0-255, 0:Auto adjustment, Unit: 4µsec)

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progu przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

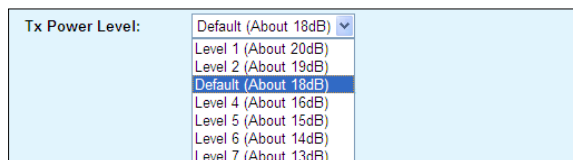
Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacja nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3



Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjęciem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

Access Control

Access Control używamy do blokowania lub dopuszczania adresów MAC. Wpisujemy adres MAC bez żadnych znaków np. 004f74301538 i wybieramy opcje Allow Listed lub Deny Listed:

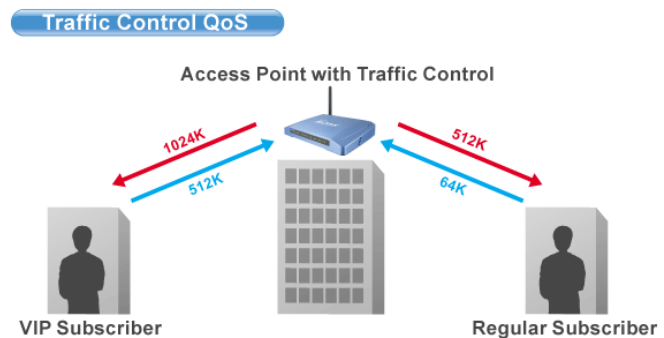
Allow Listed - dopuści wpisane adresy MAC ale odrzuci wszystkie pozostałe (niewpisane) adresy MAC

Deny Listed - dopuści wszystkie adresy MAC poza tymi wpisanymi przez nas.

Instrukcja Mechanizmu Traffic Control QoS

Czym jest Traffic Control QoS?

Traffic Control to świetne narzędzie do przydzielania pasma dla operatorów WISP (Wireless Internet Service Provider). Oznacza to, że operator może zagwarantować klientom zróżnicowany typ usług (Transferów danych) podobnie jak w usłudze ADSL. Zaawansowane oprogramowanie AirLive pozwala dedykować pasmo na podstawie adresów MAC lub IP.

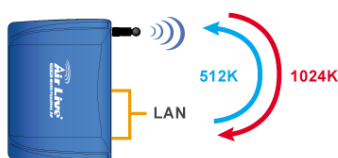


Co oferuje nam kontrola przydzielania pasma w oprogramowaniu (od E11) ?

Oprogramowanie e11 oferuje przydzielanie pasma maksymalnego "Maximum Data Rate". AirLive oferuje dwa poziomy mechanizmu przydzielania pasma.

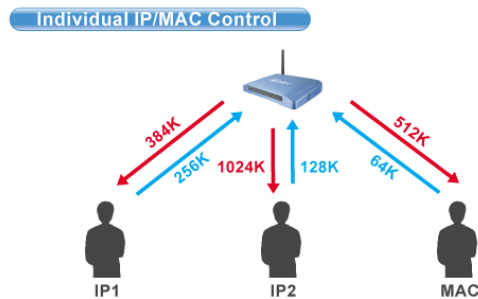
Interface Control (Kontrola Interfejsu)

Interface Traffic Control



Mechanizm QoS kontroluje prędkość transmisji danych na dwóch interfejsach WLAN i LAN. Dla obu interfejsów zasada działania QoS jest identyczna. Ten typ kontroli jest odpowiedni jeżeli urządzenie jest w trybie AP Klient lub WISP

Kontrola Indywidualna IP/MAC



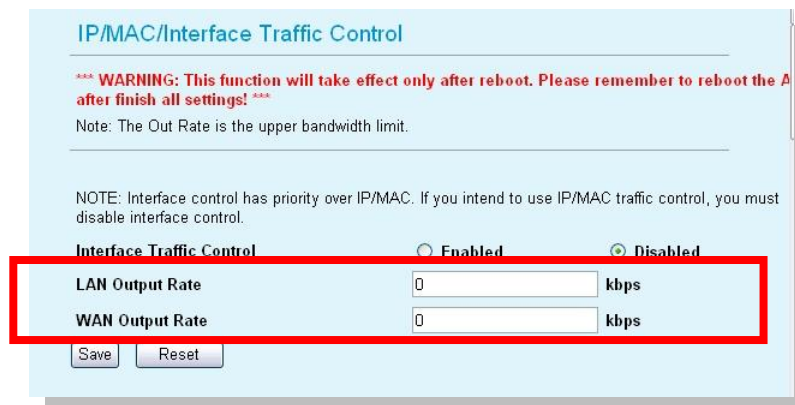
W AP możemy ustawić przydzielanie pasma dla konkretnego adresu IP lub MAC. Ten typ kontroli jest odpowiedni dla trybu AP lub Gateway.

Czym jest Output Rate?

“Output Rate” jest prędkością danych wychodzących z danego interfejsu. AP obsługuje 3 typy „Output Rate”

1. **LAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu LAN. W trybie Gateway prędkość wyjściowa LAN zawiera oba interfejsy LAN i WLAN.
2. **WLAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu Wireless LAN
3. **WAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu WAN. W trybie WISP, prędkość ruchu wyjściowego z interfejsu WAN zawiera również interfejs WLAN.

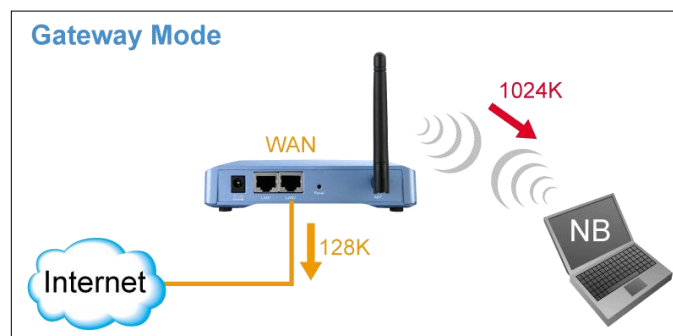
Oprogramowanie Web poinformuje cię, jakie są możliwości konfiguracji w zależności od wybranego trybu pracy są one różne.



Dla przykładu:

- AP jest w trybie Gateway Mode
- WAN Output Rate wynosi 128K
- LAN/WLAN Output Rate wynosi 1024K

W takim ustawieniu użytkownik z notbookiem osiągnie WYSYŁANIE na poziomie 128K i POBIERANIE na poziomie 1024K.



Konfiguracja Traffic Control QoS

Ze strony Mode Setting ,wybieramy "Traffic Control(QoS)" klikając na przycisk SETUP

AP Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

SSID:

Channel Number:

Wireless Client Isolation:

Security:

Advanced Settings:

Access Control:

Traffic Control (QoS):

Po kliknięciu na "setup" wyskoczy okienko z konfiguracją mechanizmu QoS. Opis poszczególnych sekcji "A", "B", "C", "D" znajduje się poniżej.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps **A**

WLAN Output Rate kbps

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

B

Note: Only the Wireless LAN side client IPs are supported.

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

C

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

D

"Interface Control" to kontrola interfejsu. Musisz wyłączyć "interface Traffic Control", jeżeli chcesz używać "IP/MAC Traffic Control"

Tu definiujemy reguły "Policy" dla konkretnych adresów "Individual IP/MAC Traffic Control". Raz utworzona reguła może być wybierana w opcji

Tu określamy przepustowość dla adresu IP. Możesz wpisać więcej niż jeden adres.

Tu określamy przepustowość dla adresu MAC. Możesz wpisać więcej niż jeden adres MAC.

A. Konfiguracja Interface Control:

***** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! *****

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

W tym ustawieniu kontrolowana jest ogólna przepustowość na każdym interfejsie. Dla przykładu jeżeli chcesz ograniczyć prędkość wychodzącą z LAN do 512K i prędkość wychodzącą z WLAN do 1024K. Powinieneś zrobić tak:

1. Włączyć "Interface Traffic Control"
2. Wpisać "512" w polu "LAN Output Rate"
3. Wpisać "1024" w polu "WLAN Output Rate"
4. Kliknąć na "Save"
5. Konieczny jest Reboot AP.

Przy takim ustawieniu komputer podpięty do LAN wysyła dane z prędkością 512 do komputera podpiętego do WLAN a komputer podpięty do WLAN wysyła z prędkością 1024 do komputera podpiętego do LAN.

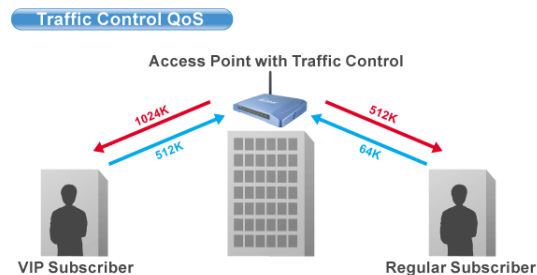


Ponieważ to ustawienie będziemy stosować głównie w trybie AP Klient, w ten sposób ograniczamy klientów podpiętych do LAN, aby nie obciążali nadmiernie stacji nadawczej AP wysyłanymi informacjami.

B. Definiowanie Reguł

Reguły określamy po to aby móc je później przyporządkować poszczególnym klientom. Dla przykładu jeżeli chcesz utworzyć dwie różne klasy usług dla dwóch klientów:

- Użytkownik VIP:
 - LAN Out Rate: 512 Kbps
 - WLAN Out Rate: 1024 Kbps
- Użytkownik Zwykły (Regular):
 - LAN Out Rate: 64 Kbps
 - WLAN Out Rate: 512 Kbps



Reguły można ustawić jako "VIP" i "Regular".

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Procedura utworzenia reguły "VIP" jest następująca:

1. Wpisz "VIP" w polu "PolicyName"
2. Wpisz "512" w polu "LAN Out Rate"
3. Wpisz "1024" w polu "WLAN Out Rate"
4. Wpisz "VIP Subscriber" w polu "Comment"
5. Kliknij na przycisk "Save".
6. Teraz reguła "VIP" ukaże się w "Current Policy Table"


Teraz reguła jest gotowa i można ją przyporządkować dla danego adresu IP lub MAC.

C. Przydzielanie pasma po adresie IP

Możesz określić maksymalną prędkość dla IP używając opcji „IP Control”.

Poniżej znajduje się procedura dla ustawień IP Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.

Note: Only the Wireless LAN side client IPs are supported. 

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
VIP	192.168.0.250	512 kbps	1024 kbps	Subscriber A

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	192.168.0.20	512	1024	Subscriber A	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Włącz IP Control
4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami IP na tym samym interfejsie, upewnij się że oba adresy IP są skonfigurowane w IP Traffic Control.*

D. Przydzielanie pasma po adresie MAC

Możesz określić maksymalną prędkość dla IP używając opcji MAC Control.

Poniżej znajduje się procedura dla ustawień MAC Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.
3. Włącz opcje MAC Control

Note: Only the Wireless LAN side client MACs are supported

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	004F60111111	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:4f:60:11:11:11	512	1024	VIP Subscriber	<input type="checkbox"/>

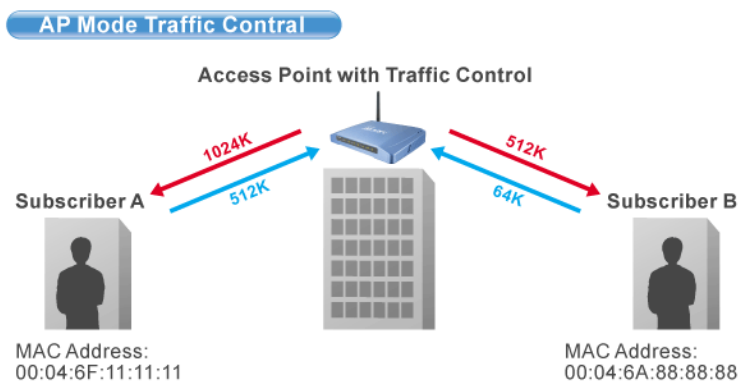
Delete Selected Delete all Reset

4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami MAC na tym samym interfejsie, upewnij się że oba adresy MAC są skonfigurowane w MAC Traffic Control.*

Przykłady zastosowania

Przykład: Kontrola Ruchu w trybie AP



Urządzenie AP jest zainstalowane na zewnątrz w celu udostępniania Internetu. Usługodawca WISP gwarantuje dwa różne typy usługi:

- **Usługa VIP :**
 - Wysłanie: 512 Kbps
 - Pobieranie: 1024 Kbps
- **Usługa Regular:**
 - Wysłanie: 64 Kbps
 - Pobieranie: 512 Kbps

Informacje o użytkownikach są następujące:

- Użytkownik A
 - Usługa VIP
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6F:11:11:11
- Użytkownik B
 - Usługa Regular
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6A:88:88:88

Konfiguracja Krok Po Kroku

1. Proszę wyłączyć "Interface Traffic Control"
2. Proszę dodać reguły "VIP" i "Regular" tak jak na rysunku poniżej

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Proszę włączyć "MAC Control"
4. Obie reguły powinny dodać się tak jak na rysunku poniżej

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	00:04:6f:11:11:11	512 kbps	1024 kbps	Subscriber A
Regular	00:4f:6a:88:88:88	64 kbps	512 kbps	Subscriber B

Save Reset

Current MAC control table:

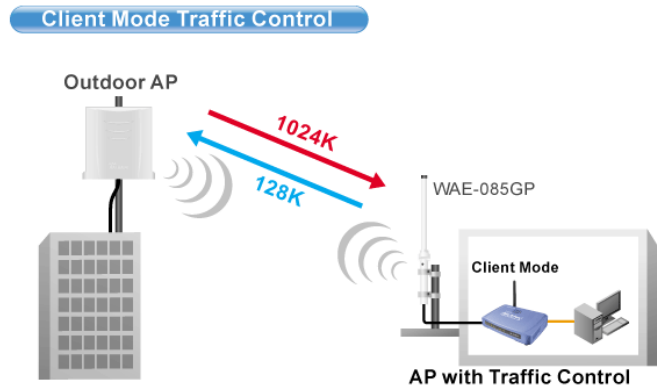
Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:04:6f:11:11:11	512	1024	Subscriber A	<input type="checkbox"/>
Regular	00:4f:6a:88:88:88	64	512	Subscriber B	<input type="checkbox"/>

Delete Selected Delete all Reset

5. Proszę zrobić Reboot AP

Przykład 2: Kontrola Ruchu w trybie Klient

Urządzenie pracuje jako klient w topologii usługodawcy WISP. Usługodawca chce ograniczyć pasmo pobierania do 1024K i wysyłania do 128K.



Konfiguracja Krok Po Kroku

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAN Output Rate	<input type="text" value="1024"/>	kbps
WLAN Output Rate	<input type="text" value="128"/>	kbps
<input type="button" value="Save"/>	<input type="button" value="Reset"/>	

1. Proszę włączyć "Interface Traffic Control"
2. Wpisać "1024" w polu "LAN Output Rate"
3. Wpisać "128" w polu "WLAN Output Rate"
4. Wcisnąć "Save"
5. Zrobić Reboot AP

Tryb AP Client

Client Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band: (dropdown)

Network Type: (dropdown)

SSID:

Channel Number: (dropdown)

Auto Mac Clone (Single Ethernet Client)

Manual MAC Clone Address:

Security:

Advanced Settings:

Traffic Control(QoS):

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G.

 Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

Network Type - typ sieci, możemy wybrać „Infrastrukture” jeśli urządzenie ma pracować jako klient bezprzewodowy np. gdy chcemy podłączyć się do stacji nadającej sygnał bezprzewodowy. Lub wybierzemy „AD-HOC” jeżeli nasz nadajnik ma połączyć się z innymi kartami sieciowymi pracującymi w trybie AD-HOC. Aby skonfigurować ten tryb wystarczy dostosować kanał i nazwę SSID do istniejącej sieci AD-HOC. Połączenie nastąpi automatycznie.

SSID - identyfikator sieci składający się maksymalnie z 32 znaków. Wszystkie urządzenia pracujące w sieci aby się komunikować muszą mieć taką samą nazwę SSID. Identyfikator ten jest przesyłany w nagłówku ramki radiowej i pełni rolę hasła dostępowego przy próbie nawiązywania połączenia bezprzewodowego.

Site Survey - funkcja służy do skanowania dostępnych sieci bezprzewodowych. Po uruchomieniu ukazuje się tabelka i znalezione sieci:

Wireless Site Survey

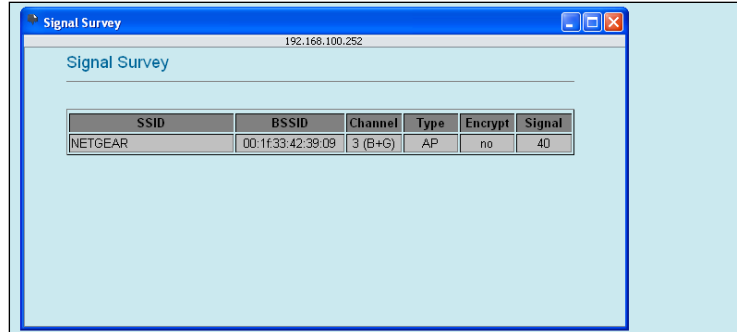
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
default	00:30:4f:42:2c:75	11 (B+G)	AP	no	64	<input type="radio"/>
ADW-4401	00:30:4f:60:da:e5	6 (B+G)	AP	no	64	<input type="radio"/>
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	43	<input checked="" type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	7	<input type="radio"/>
NO NAME	00:14:78:52:54:fe	6 (B+G)	AP	WEP	1	<input type="radio"/>

W tabelce znajdziemy:

- Nazwę **SSID** dostępnych sieci
- **BSSID** czyli numer identyfikacyjny odpowiadający adresowi MAC interfejsu bezprzewodowego
- **Channel**, tu znajdziemy informacje na jakim kanale i w jakim standardzie pracuje stacja nadawcza
- **Type** czyli tryb pracy stacji nadawczej
- **Encrypt** tu dowiemy się czy sieć jest zabezpieczona i jakiemu klucza użyto do zabezpieczenia

- **Signal** to ważna informacja, oznacza siłę sygnału stacji nadającej. Do połączenia wymagana wartość minimalna nie powinna być mniejsza niż 25. Jest to minimum i taki link transmisja bezprzewodowa na takim linku często może być nie poprawna.
- **Select** czy pole które zaznaczamy aby wybrać daną sieć

Signal Survey- to świetne rozwiązanie dynamicznego skanowania danej sieci. W polu „Select” wybieramy sieć, klikamy „Signal Survey”. Otworzy się osobne okienko w którym dynamicznie co 3 sekundy odświeża się informacja o sile sygnału stacji nadawczej. Bardzo przydatne narzędzie podczas zestawiania linku i konfiguracji anten.



SSID	BSSID	Channel	Type	Encrypt	Signal
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	40

Uwaga!

W trybie pracy AP Client aby uzyskać połączenie wystarczy przeskanować eter, wybrać sieć bezprzewodową i zatwierdzić ustawienia. Wszystkie niezbędne parametry do połączenia takie jak kanał i nazwa SSID zostaną automatycznie pobrane od sieci którą wybraliśmy.

Uwaga!

Nadajnik w trybie Infrastruktury podmienia we wszystkich ramkach adres MAC źródłowy na swój własny. Dlatego nie powinno się ustawiać urządzenia w trybie Infrastruktury po stronie serwerów. Mogą również występować problemy z DHCP oraz dostępem do serwerów z autoryzacją adresów MAC.

Auto MAC Clone - to opcja automatycznego zamieniania adresu MAC urządzenia WL-5460AP na adres MAC podłączonej do niego karty sieciowej. Funkcję tą wykorzystujemy gdy za WL-5460AP działa tylko jedno urządzenie. Po włączeniu tej opcji komunikację posiadał będzie tylko jeden komputer.

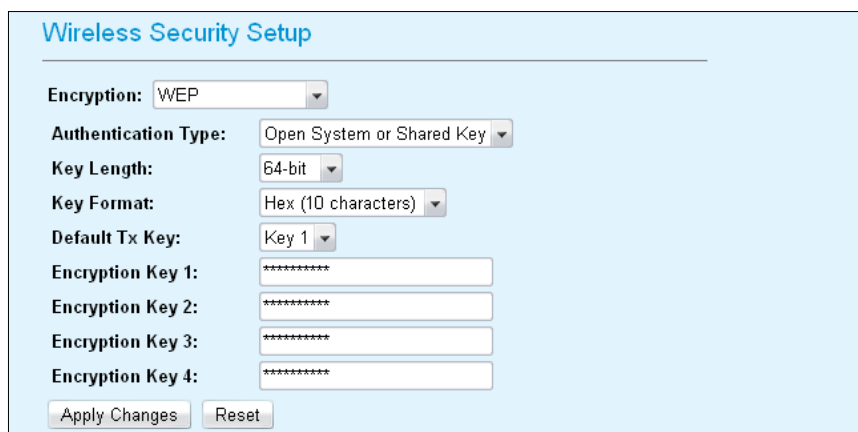
Manual MAC Clone - to opcja ręcznego wpisania adresu MAC. Po zatwierdzeniu ustawień wpisany adres MAC będzie adresem MAC WL-5460AP.

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP



Wireless Security Setup

Encryption: WEP

Authentication Type: Open System or Shared Key

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Apply Changes Reset

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/Radius

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Encryption:	802.1x / RADIUS		
Security:	WEP		
Use 802.1x Authentication:	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits		
Authentication RADIUS Server:	Port	IP address	Password
	1812		
<input type="checkbox"/> Enable Accounting			
Accounting RADIUS Server:	Port	IP address	Password
	0		
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>			

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings	
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Inactivity Time:	50000 (101-60480000 10ms)
Data Rate:	11M
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11g Protection:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Tx Power Level:	Level 1 (About 26dB)
<input type="checkbox"/> Enable WatchDog	
Watch Interval:	1 (1-60 minutes)
Watch Host:	0.0.0.0
Ack timeout:	0 (0-255, 0:Auto adjustment, Unit: 4µsec)
<input type="button" value="Set Default"/>	
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progu przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narazania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje.

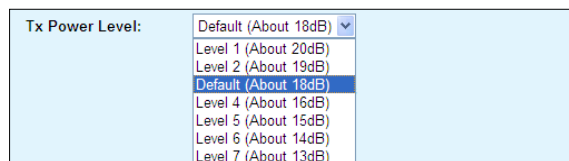
Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacji nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3



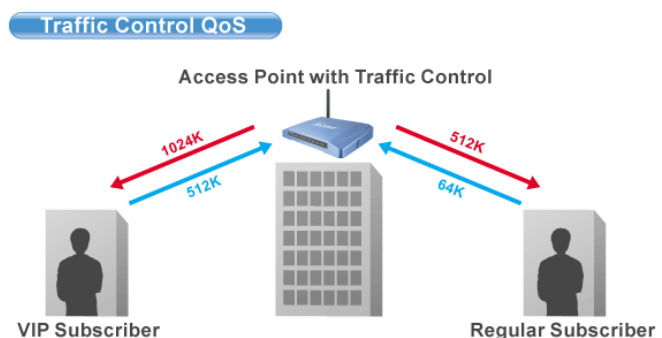
Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjęciem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższą wartością parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

Instrukcja Mechanizmu Traffic Control QoS

Czym jest Traffic Control QoS?

Traffic Control to świetne narzędzie do przydzielania pasma dla operatorów WISP (Wireless Internet Service Provider). Oznacza to, że operator może zagwarantować klientom zróżnicowany typ usług (Transferów danych) podobnie jak w usłudze ADSL. Zaawansowane oprogramowanie AirLive pozwala dedykować pasmo na podstawie adresów MAC lub IP.

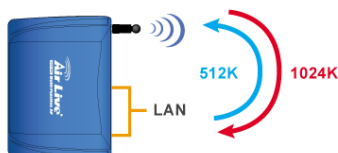


Co oferuje nam kontrola przydzielania pasma w oprogramowaniu (od E11) ?

Oprogramowanie e11 oferuje przydzielanie pasma maksymalnego "Maximum Data Rate". AirLive oferuje dwa poziomy mechanizmu przydzielania pasma.

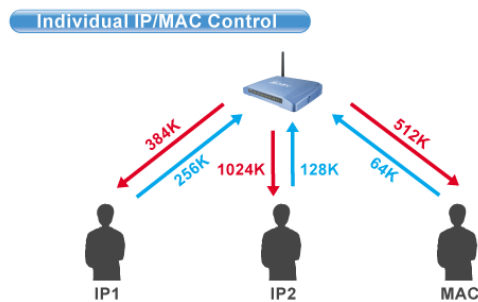
Interface Control (Kontrola Interfejsu)

Interface Traffic Control



Mechanizm QoS kontroluje prędkość transmisji danych na dwóch interfejsach WLAN i LAN. Dla obu interfejsów zasada działania QoS jest identyczna. Ten typ kontroli jest odpowiedni jeżeli urządzenie jest w trybie AP Klient lub WISP

Kontrola Indywidualna IP/MAC



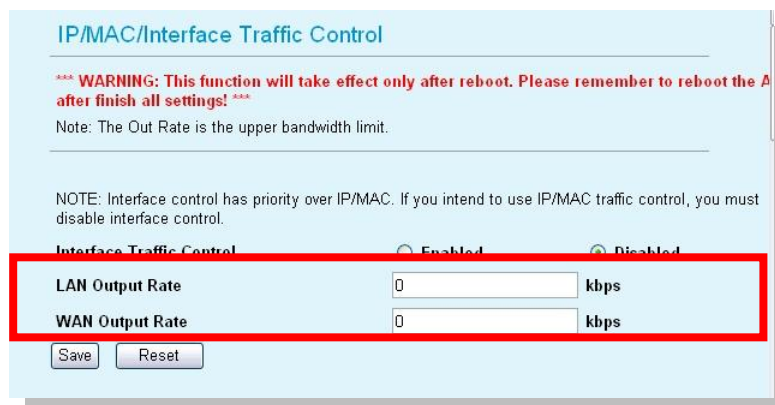
W AP możemy ustawić przydzielanie pasma dla konkretnego adresu IP lub MAC. Ten typ kontroli jest odpowiedni dla trybu AP lub Gateway.

Czym jest Output Rate?

“Output Rate” jest prędkością danych wychodzących z danego interfejsu. AP obsługuje 3 typy „Output Rate”

4. **LAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu LAN. W trybie Gateway prędkość wyjściowa LAN zawiera oba interfejsy LAN i WLAN.
5. **WLAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu Wireless LAN
6. **WAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu WAN. W trybie WISP, prędkość ruchu wyjściowego z interfejsu WAN zawiera również interfejs WLAN.

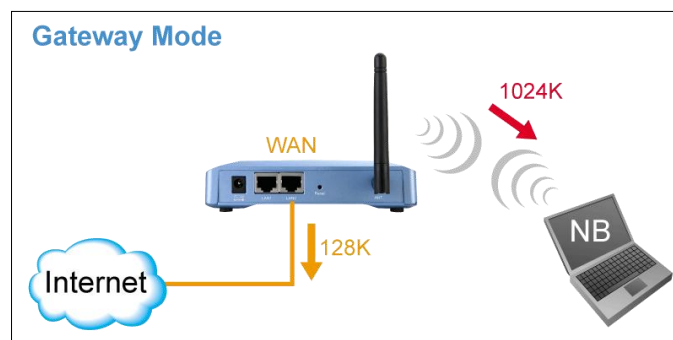
Oprogramowanie Web poinformuje cię, jakie są możliwości konfiguracji w zależności od wybranego trybu pracy są one różne.



Dla przykładu:

- AP jest w trybie Gateway Mode
- WAN Output Rate wynosi 128K
- LAN/WLAN Output Rate wynosi 1024K

W takim ustawieniu użytkownik z notbookiem osiągnie WYSYŁANIE na poziomie 128K i POBIERANIE na poziomie 1024K.



Konfiguracja Traffic Control QoS

Ze strony Mode Setting ,wybieramy "Traffic Control(QoS)" klikając na przycisk SETUP

AP Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

SSID:

Channel Number:

Wireless Client Isolation:

Security:

Advanced Settings:

Access Control:

Traffic Control (QoS):

Po kliknięciu na "setup" wyskoczy okienko z konfiguracją mechanizmu QoS. Opis poszczególnych sekcji "A", "B", "C", "D" znajduje się poniżej.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

A Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

B Policy Name LAN Out Rate WLAN Out Rate Comment

kbps kbps

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Note: Only the Wireless LAN side client IPs are supported.

C Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Note: Only the Wireless LAN side client MACs are supported.

D Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

"Interface Control" to kontrola interfejsu. Musisz wyłączyć "interface Traffic Control", jeżeli chcesz używać "IP/MAC Traffic Control"

Tu definiujemy reguły "Policy" dla konkretnych adresów "Individual IP/MAC Traffic Control". Raz utworzona reguła może być wybierana w opcji

Tu określamy przepustowość dla adresu IP. Możesz wpisać więcej niż jeden adres.

Tu określamy przepustowość dla adresu MAC. Możesz wpisać więcej niż jeden adres MAC.

A. Konfiguracja Interface Control:

***** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! *****

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

W tym ustawieniu kontrolowana jest ogólna przepustowość na każdym interfejsie. Dla przykładu jeżeli chcesz ograniczyć prędkość wychodzącą z LAN do 512K i prędkość wychodzącą z WLAN do 1024K. Powinieneś zrobić tak:

- Włączyć "Interface Traffic Control"
- Wpisać "512" w polu "LAN Output Rate"
- Wpisać "1024" w polu "WLAN Output Rate"
- Kliknąć na "Save"
- Konieczny jest Reboot AP.

Przy takim ustawieniu komputer podpięty do LAN wysyła dane z prędkością 512 do komputera podpiętego do WLAN a komputer podpięty do WLAN wysyła z prędkością 1024 do komputera podpiętego do LAN.

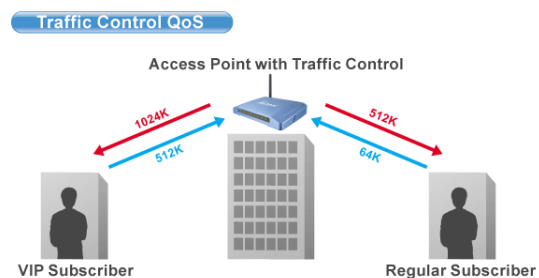


Ponieważ to ustawienie będziemy stosować głównie w trybie AP Klient, w ten sposób ograniczamy klientów podpiętych do LAN, aby nie obciążali nadmiernie stacji nadawczej AP wysyłanymi informacjami.

B. Definiowanie Reguł

Reguły określamy po to aby móc je później przyporządkować poszczególnym klientom. Dla przykładu jeżeli chcesz utworzyć dwie różne klasy usług dla dwóch klientów:

- Użytkownik VIP:
 - LAN Out Rate: 512 Kbps
 - WLAN Out Rate: 1024 Kbps
- Użytkownik Zwykły (Regular):
 - LAN Out Rate: 64 Kbps
 - WLAN Out Rate: 512 Kbps



Reguły można ustawić jako "VIP" i "Regular".

Policy Name **LAN Out Rate** kbps **WLAN Out Rate** kbps **Comment**

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Procedura utworzenia reguły "VIP" jest następująca:

- i. Wpisz "VIP" w polu "PolicyName"
- ii. Wpisz "512" w polu "LAN Out Rate"
- iii. Wpisz "1024" w polu "WLAN Out Rate"
- iv. Wpisz "VIP Subscriber" w polu "Comment"
- v. Kliknij na przycisk "Save".
- vi. Teraz reguła "VIP" ukaże się w "Current Policy Table"

Teraz reguła jest gotowa i można ją przyporządkować dla danego adresu IP lub MAC.

C. Przydzielanie pasma po adresie IP

Możesz określić maksymalną prędkość dla IP używając opcji „IP Control”.

Poniżej znajduje się procedura dla ustawień IP Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.

Note: Only the Wireless LAN side client IPs are supported. ←

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
VIP	192.168.0.250	512 kbps	1024 kbps	Subscriber A

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	192.168.0.20	512	1024	Subscriber A	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Włącz IP Control
4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami IP na tym samym interfejsie, upewnij się że oba adresy IP są skonfigurowane w IP Traffic Control.*

D. Przydzielanie pasma po adresie MAC

Możesz określić maksymalną prędkość dla IP używając opcji MAC Control.

Poniżej znajduje się procedura dla ustawień MAC Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.
3. Włącz opcje MAC Control

Note: Only the Wireless LAN side client MACs are supported

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	004F60111111	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:4f:60:11:11:11	512	1024	VIP Subscriber	<input type="checkbox"/>

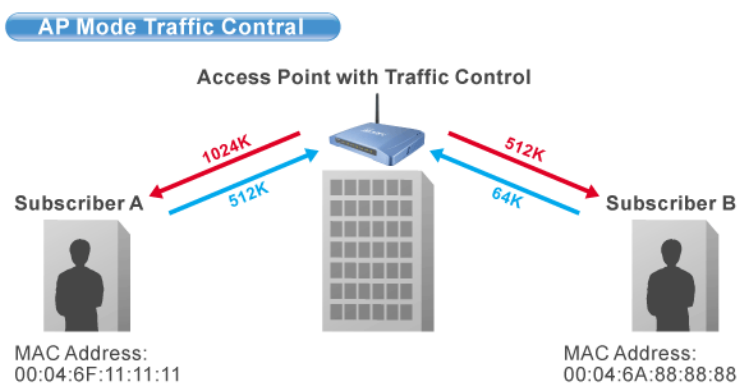
Delete Selected Delete all Reset

4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami MAC na tym samym interfejsie, upewnij się że oba adresy MAC są skonfigurowane w MAC Traffic Control.*

Przykłady zastosowania

Przykład: Kontrola Ruchu w trybie AP



Urządzenie AP jest zainstalowane na zewnątrz w celu udostępniania Internetu. Usługodawca WISP gwarantuje dwa różne typy usługi:

- **Usługa VIP :**
 - Wysłanie: 512 Kbps
 - Pobieranie: 1024 Kbps
- **Usługa Regular:**
 - Wysłanie: 64 Kbps
 - Pobieranie: 512 Kbps

Informacje o użytkownikach są następujące:

- Użytkownik A
 - Usługa VIP
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6F:11:11:11
- Użytkownik B
 - Usługa Regular
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6A:88:88:88

Konfiguracja Krok Po Kroku

1. Proszę wyłączyć "Interface Traffic Control"
2. Proszę dodać reguły "VIP" i "Regular" tak jak na rysunku poniżej

The screenshot shows a configuration page for traffic control. At the top, there are input fields for 'Policy Name' (VIP), 'LAN Out Rate' (512 kbps), 'WLAN Out Rate' (1024 kbps), and 'Comment' (VIP Subscriber). Below these are 'Save' and 'Reset' buttons. Underneath is a table titled 'Current Policy Table' with columns for Policy Name, LAN Rate (Kbps), WLAN Rate (Kbps), Comment, and Select. The table lists two policies: VIP (512, 1024, VIP Subscriber) and Regular (64, 512, Regular Subscriber). At the bottom are 'Delete Selected', 'Delete all', and 'Reset' buttons.

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

3. Proszę włączyć "MAC Control"
4. Obie reguły powinny dodać się tak jak na rysunku poniżej

The screenshot shows a configuration page for MAC control. At the top, there is a note: "Note: Only the Wireless LAN side client MACs are supported." Below this is a checkbox labeled 'Enable MAC control' which is checked. There are input fields for 'Policy Name' (with a dropdown arrow), 'MAC' (00:04:6f:11:11:11), 'LAN Out Rate' (512 kbps), 'WLAN Out Rate' (1024 kbps), and 'Comment' (Subscriber A). Below these are 'Save' and 'Reset' buttons. Underneath is a table titled 'Current MAC control table' with columns for Policy Name, MAC Addr, LAN Rate (Kbps), WLAN Rate (Kbps), Comment, and Select. The table lists two policies: VIP (00:04:6f:11:11:11, 512, 1024, Subscriber A) and Regular (00:4f6a:88:88:88, 64, 512, Subscriber B). At the bottom are 'Delete Selected', 'Delete all', and 'Reset' buttons.

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

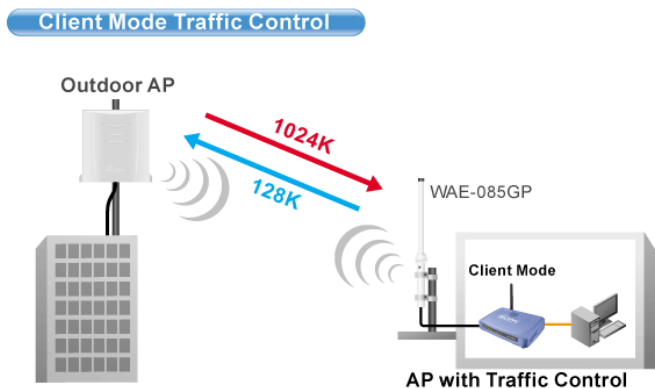
Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	00:04:6f:11:11:11	512 kbps	1024 kbps	Subscriber A

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:04:6f:11:11:11	512	1024	Subscriber A	<input type="checkbox"/>
Regular	00:4f6a:88:88:88	64	512	Subscriber B	<input type="checkbox"/>

5. Proszę zrobić Reboot AP

Przykład 2: Kontrola Ruchu w trybie Klient

Urządzenie pracuje jako klient w topologii usługodawcy WISP. Usługodawca chce ograniczyć pasmo pobierania do 1024K i wysyłania do 128K.



Konfiguracja Krok Po Kroku

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAN Output Rate	<input type="text" value="1024"/>	kbps
WLAN Output Rate	<input type="text" value="128"/>	kbps
<input type="button" value="Save"/>	<input type="button" value="Reset"/>	

1. Proszę włączyć "Interface Traffic Control"
2. Wpisać "1024" w polu "LAN Output Rate"
3. Wpisać "128" w polu "WLAN Output Rate"
4. Wcisnąć "Save"
5. Zrobić Reboot AP

Tryb Bridge

Bridge Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

Channel Number:

802.1d Spanning Tree:

WDS Security:

Advanced Settings:

AP MAC Address:

Comment:

AP MAC List:

MAC Address	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="button" value="Delete Selected"/>
		<input type="button" value="Delete All"/>
		<input type="button" value="Reset"/>

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

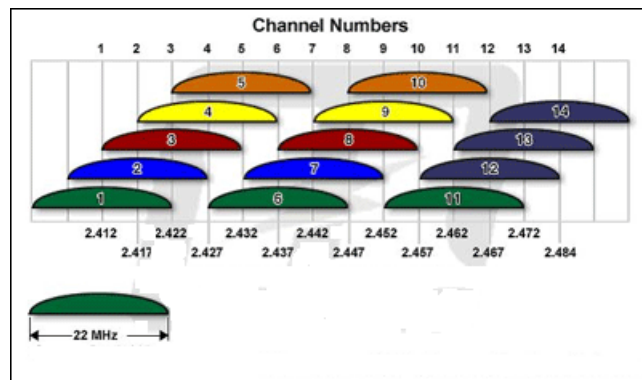
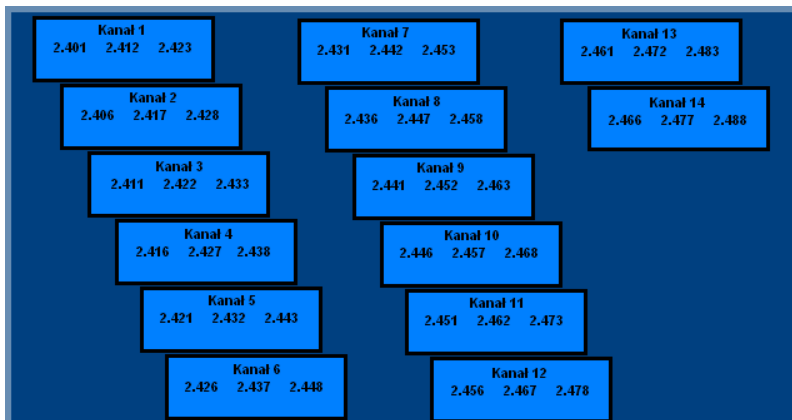
Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G. Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

Channel Number - tu wybieramy na jakim kanale ma pracować nasz nadajnik. Każdy kanał to określony zakres częstotliwości.

Numer Kanalu	Dolna Częstotliwość Kanalu w GHz	Środkowa Częstotliwość Kanalu	Górna Częstotliwość Kanalu w GHz
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488

Wszystkie kanały pokrywają się w pewnym stopniu częstotliwością. Oddzielone są np. kanały 1,7,13. Instalując sieci upewnijmy się jakie kanały są już używane. I użyjmy innych aby zredukować zakłócenia.



Ilość kanałów zależy od kodowania np.

Region	Kodowanie	Ilość kanałów
USA	FCC	11
Europa	ETSI	13
Japonia	TELEC	14

802.1d Spanning Tree - podczas łączenia wielu stacji w trybie WDS może dojść do sytuacji rozłączania stacji i braku możliwości przyłączenia nowych. Aby zapobiec takim problemom należy włączyć (Enable) mechanizm Spanning Tree. Linki pomiędzy urządzeniami nie będą się zapęllać i sieć będzie działa poprawnie.

WDS Security - W trybie WDS dostępne szyfrowania to :

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Wireless Security Setup

Encryption: WPA-PSK (AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Group Key Life Time: 86400 sec

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację przewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Encryption: 802.1x / RADIUS

Security: WEP

Use 802.1x Authentication WEP 64bits WEP 128bits

Authentication RADIUS Server: Port 1812 IP address Password

Enable Accounting

Accounting RADIUS Server: Port 0 IP address Password

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Inactivity Time: 50000 (101-60480000 10ms)

Data Rate: 11M

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level: Level 1 (About 26dB)

Enable WatchDog

Watch Interval: 1 (1-60 minutes)

Watch Host: 0.0.0.0

Ack timeout: 0 (0-255, 0:Auto adjustment, Unit: 4µsec)

Set Default

Apply Changes Reset

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszenia wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progów przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacja nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjęciem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

Tryb WDS Repeater

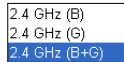
The screenshot shows the 'WLAN Access Point' configuration page for 'WDS Repeater Mode Settings'. The interface includes a navigation bar with 'Mode', 'Status', 'TCP/IP', 'Reboot', and 'Other' tabs. The main settings area contains the following fields and controls:

- Alias Name:** Text input field containing 'Wireless_AP'.
- Disable Wireless LAN Interface**
- Band:** Dropdown menu set to '2.4 GHz (B+G)'.
- SSID:** Text input field containing 'airlive'.
- Channel Number:** Dropdown menu set to '11'.
- Wireless Client Isolation:** Dropdown menu set to 'Disabled'.
- 802.1d Spanning Tree:** Dropdown menu set to 'Disabled'.
- Security:** 'Setup' button.
- WDS Security:** 'Setup' button.
- Advanced Settings:** 'Setup' button.
- Access Control:** 'Setup' button.

At the bottom of the settings area are 'Apply Changes' and 'Reset' buttons. Below this is a section for 'AP MAC Address' with a text input field and a 'Site Survey' button. A 'Comment' text input field is also present, with 'Add MAC Address', 'Reset', and 'Show Statistics' buttons below it. At the very bottom is an 'AP MAC List' table with columns for 'MAC Address', 'Comment', and 'Select', and buttons for 'Delete Selected', 'Delete All', and 'Reset'.

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

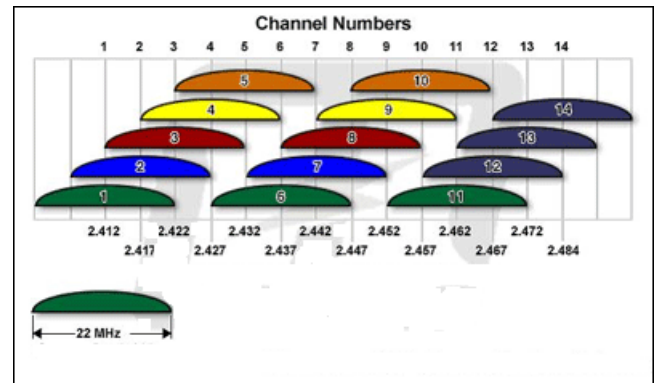
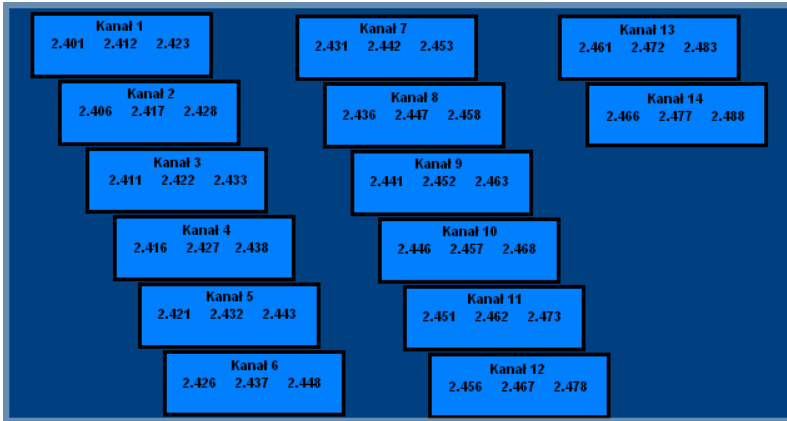
Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G.  Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

Channel Number - tu wybieramy na jakim kanale ma pracować nasz nadajnik. Każdy kanał to określony zakres częstotliwości.

Numer Kanału	Dolna Częstotliwość Kanału w GHz	Środkowa Częstotliwość Kanału	Górna Częstotliwość Kanału w GHz
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488

Wszystkie kanały pokrywają się w pewnym stopniu częstotliwością. Oddzielone są np. kanały 1,7,13. Instalując sieci upewnijmy się jakie kanały są już używane. I użyjmy innych aby zredukować zakłócenia.



Ilość kanałów zależy od kodowania np.

Region	Kodowanie	Ilość kanałów
USA	FCC	11
Europa	ETSI	13
Japonia	TELEC	14

Wireless Client Isolation - enabled (włącz), disabled (wyłącz). Funkcja izolacji klientów bezprzewodowych sprawia że użytkownicy nie będą wymieniać między sobą informacji. Użytkownicy nie będą mogli kopiować danych pomiędzy sobą w otoczeniu sieciowym dzięki temu można zwiększyć bezpieczeństwo danych w sieci oraz można skutecznie zwiększyć wydajność urządzenia radiowego. Jeżeli klienci radiowi nie będą przysyłać między sobą danych, urządzenie radiowe nie będzie musiało ich przetwarzać. Funkcja dotyczy tylko klientów bezprzewodowych.

802.1d Spanning Tree - podczas łączenia wielu stacji w trybie WDS może dojść do sytuacji rozłączania stacji i braku możliwości przyłączania nowych. Aby zapobiec takim problemom należy włączyć (Enable) mechanizm Spanning Tree. Linki pomiędzy urządzeniami nie będą się zapętlać i sieć będzie działa poprawnie.

Security - w trybie WDS Repeater możemy użyć osobnego szyfrowania sygnału SSID i osobnego szyfrowania połączenia WDS.

WDS Security - W trybie WDS dostępne szyfrowania to :

WDS Security Setup

Encryption:

WEP Key Format:

WEP Key:

Pre-Shared Key Format:

Pre-Shared Key:

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP

The screenshot shows the 'Wireless Security Setup' page with the following settings:

- Encryption: WEP
- Authentication Type: Open System or Shared Key
- Key Length: 64-bit
- Key Format: Hex (10 characters)
- Default Tx Key: Key 1
- Encryption Key 1: [Redacted]
- Encryption Key 2: [Redacted]
- Encryption Key 3: [Redacted]
- Encryption Key 4: [Redacted]

Buttons: Apply Changes, Reset

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

The screenshot shows the 'Wireless Security Setup' page with the following settings:

- Encryption: WPA-PSK (AES)
- Pre-Shared Key Format: Passphrase
- Pre-Shared Key: [Redacted]
- Group Key Life Time: 86400 sec

Buttons: Apply Changes, Reset

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

7. Wybieramy rodzaj klucza WPA lub WPA2
8. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
9. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
10. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progu przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość

odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okrasie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacja nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjąłem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

Access Control

Wireless Access Control

Wireless Access Control Mode: ▼

MAC Address:

Current Access Control List:

MAC Address	Comment	Select

Access Control używamy do blokowania lub dopuszczania adresów MAC. Wpisujemy adres MAC bez żadnych znaków np. 004f74301538 i wybieramy opcje Allow Listed lub Deny Listed:

Allow Listed - dopuści wpisane adresy MAC ale odrzuci wszystkie pozostałe (niewpisane) adresy MAC

Deny Listed - dopuści wszystkie adresy MAC poza tymi wpisanymi przez nas.

Tryb Universal Repeater

Air Live
www.airlive.com

WLAN Access Point

Mode | Status | TCP/IP | Reboot | Other

Universal Repeater Mode Settings

This page is used to setup different wireless mode.

Alias Name:

Disable Wireless LAN Interface

Band: ▼

SSID:

Channel Number: ▼

Wireless Client Isolation: ▼

SSID of Extended Interface:

802.1d Spanning Tree: ▼

Security:

Advanced Settings:

Access Control:

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

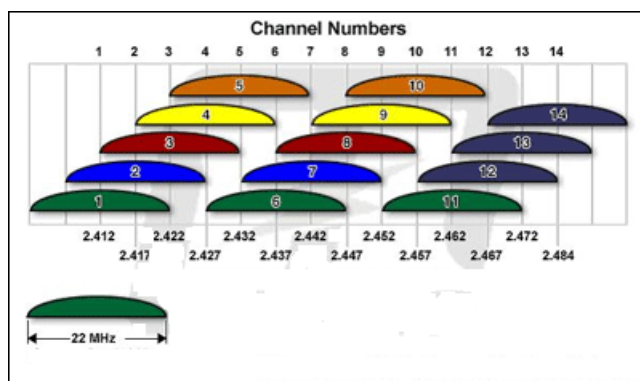
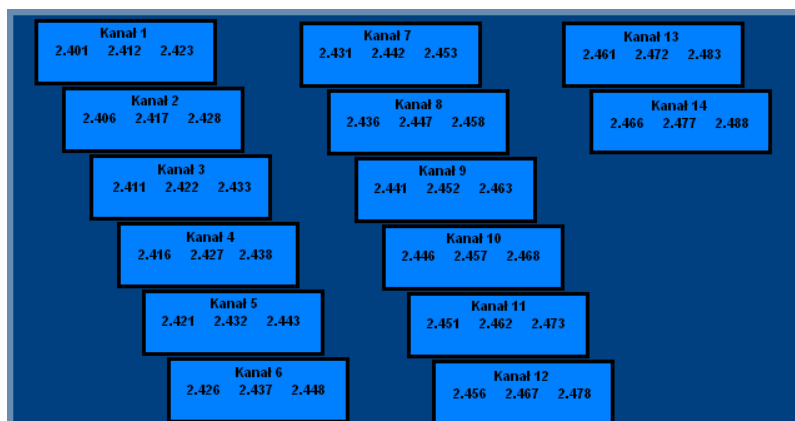
SSID - tu wpisujemy własną nazwę. Tak będzie nazywała się nasza domowa sieć bezprzewodowa.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G. Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

Channel Number - tu wybieramy na jakim kanale ma pracować nasz nadajnik. Każdy kanał to określony zakres częstotliwości.

Numer Kanału	Dolna Częstotliwość Kanału w GHz	Środkowa Częstotliwość Kanału	Górna Częstotliwość Kanału w GHz
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488

Wszystkie kanały pokrywają się w pewnym stopniu częstotliwością. Oddzielone są np. kanały 1,7,13. Instalując sieci upewnijmy się jakie kanały są już używane. I użyjmy innych aby zredukować zakłócenia.



Ilość kanałów zależy od kodowania np.

Region	Kodowanie	Ilość kanałów
USA	FCC	11
Europa	ETSI	13
Japonia	TELEC	14

Wireless Client Isolation - enabled (włącz), disabled (wyłącz). Funkcja izolacji klientów bezprzewodowych sprawia że użytkownicy nie będą wymieniać między sobą informacji. Użytkownicy nie będą mogli kopiować danych pomiędzy sobą w otoczeniu sieciowym dzięki temu można zwiększyć bezpieczeństwo danych w sieci oraz można skutecznie zwiększyć wydajność urządzenia radiowego. Jeżeli klienci radiowi nie będą przysyłać między sobą danych, urządzenie radiowe nie będzie musiało ich przetwarzać. Funkcja dotyczy tylko klientów bezprzewodowych.

SSID of Extended Interface - tu musi być nazwa SSID sieci do której się łączy WL-5460AP

802.1d Spanning Tree - podczas łączenia wielu stacji w trybie WDS może dojść do sytuacji rozłączania stacji i braku możliwości przyłączenia nowych. Aby zapobiec takim problemom należy włączyć (Enable) mechanizm Spanning Tree. Linki pomiędzy urządzeniami nie będą się zapętlać i sieć będzie działa poprawnie.

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP

Wireless Security Setup

Encryption:

Authentication Type:

Key Length:

Key Format:

Default Tx Key:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie.

Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

7. Wybieramy rodzaj klucza WPA lub WPA2
8. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
9. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
10. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Inactivity Time: (101-60480000 10ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level:

Enable WatchDog

Watch Interval: (1-60 minutes)

Watch Host:

Ack timeout: (0-255, 0:Auto adjustment, Unit: 4µsec)

Fragment Treshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progu przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Treshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzono jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacja nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjąłem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

Access Control

Wireless Access Control

Wireless Access Control Mode: ▼

MAC Address:

Current Access Control List:

MAC Address	Comment	Select

Access Control używamy do blokowania lub dopuszczania adresów MAC. Wpisujemy adres MAC bez żadnych znaków np. 004f74301538 i wybieramy opcje Allow Listed lub Deny Listed:

Allow Listed - dopuści wpisane adresy MAC ale odrzuci wszystkie pozostałe (niewpisane) adresy MAC

Deny Listed - dopuści wszystkie adresy MAC poza tymi wpisanymi przez nas.

Tryb WISP

WISP Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

SSID:

Security:

Advanced Settings:

Wan Port:

Virtual Server:

Special Application:

DMZ:

Remote Management:

Dynamic DNS:

Traffic Control(QoS):

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G.

 Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

SSID - identyfikator sieci składający się maksymalnie z 32 znaków. Wszystkie urządzenia pracujące w sieci aby się komunikować muszą mieć taką samą nazwę SSID. Identyfikator ten jest przesyłany w nagłówku ramki radiowej i pełni rolę hasła dostępowego przy próbie nawiązywania połączenia bezprzewodowego.

Site Survey - funkcja służy do skanowania dostępnych sieci bezprzewodowych. Po uruchomieniu ukazuje się tabelka i znalezione sieci:

Wireless Site Survey

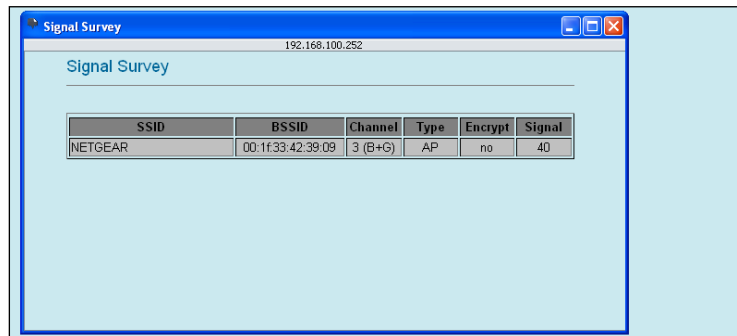
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
default	00:30:4f:42:2c:75	11 (B+G)	AP	no	64	<input type="radio"/>
ADW-4401	00:30:4f:60:da:e5	6 (B+G)	AP	no	64	<input type="radio"/>
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	43	<input checked="" type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	7	<input type="radio"/>
NO NAME	00:14:78:52:54:fe	6 (B+G)	AP	WEP	1	<input type="radio"/>

W tabelce znajdziemy:

- Nazwę **SSID** dostępnych sieci
- **BSSID** czyli numer identyfikacyjny odpowiadający adresowi MAC interfejsu bezprzewodowego
- **Channel**, tu znajdziemy informacje na jakim kanale i w jakim standardzie pracuje stacja nadawcza

- **Type** czyli tryb pracy stacji nadawczej
- **Encrypt** tu dowiemy się czy sieć jest zabezpieczona i jakiego klucza użyto do zabezpieczenia
- **Signal** to ważna informacja, oznacza siłę sygnału stacji nadającej. Do połączenia wymagana wartość minimalna nie powinna być mniejsza niż 25. Jest to minimum i taki link transmisja bezprzewodowa na takim linku często może być nie poprawna.
- **Select** czy pole które zaznaczamy aby wybrać daną sieć

Signal Survey- to świetne rozwiązanie dynamicznego skanowania danej sieci. W polu „Select” wybieramy sieć, klikamy „Signal Survey”. Otworzy się osobne okienko w którym dynamicznie co 3 sekundy odświeża się informacja o sile sygnału stacji nadawczej. Bardzo przydatne narzędzie podczas zestawiania linku i konfiguracji anten.



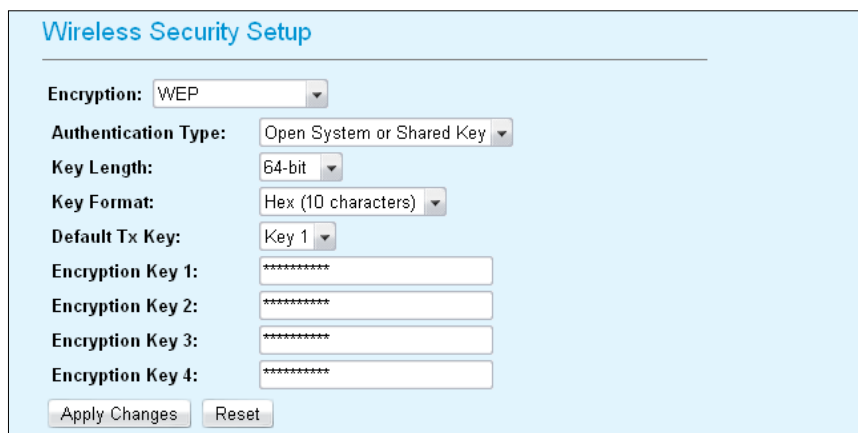
SSID	BSSID	Channel	Type	Encrypt	Signal
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	40

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP



Wireless Security Setup

Encryption: WEP

Authentication Type: Open System or Shared Key

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Apply Changes Reset

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.
- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.
- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Inactivity Time: (101-60480000 10ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level:

Enable WatchDog

Watch Interval: (1-60 minutes)

Watch Host:

Ack timeout: (0-255, 0:Auto adjustment, Unit: 4µsec)

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progów przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacja nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjąłem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

WAN Port - W trybie (Wireless Internet Service Provider) urządzenie ma funkcjonalność routera dlatego do poprawnego działania wymagana jest konfiguracja portu WAN.

WAN Port Configuration

WAN Access Type: DHCP Client ▼

Check DHCP server alive by ping per 30 seconds

TTL: Disable ▼

TTL Value: 255 (1-255)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

Respond to WAN Ping

Enable UPnP

Enable IPsec pass through on VPN connection

Enable PPTP pass through on VPN connection

Enable L2TP pass through on VPN connection

Save Reset

WAN Access Type - to rodzaj połączenia interfejsu WAN. Adres możemy:

- pobierać automatycznie „DHCP Client”
- ustawić ręcznie „Static IP”
- uzyskać połączenie za pomocą nazwy i loginu przez połączenie „PPPoE”
- uzyskać połączenie po VPN „PPTP”
- uzyskać połączenie po VPN „L2TP”

Check DHCP Server alive.. - zaznaczamy opcje dla stałego podtrzymywania połączenia WAN

TTL - to czas życia pakietu w sieci. Często administrator ustawia wartość tego parametru na TTL=1 a wtedy taki pakiet nie może być przesłany przez router. Jest to równoznaczne z brakiem możliwości rozdzielania takiego sygnału na kilka komputerów. WI-5460AP oferuje możliwość zaawansowanej konfiguracji tego parametru:

- Disable pozostawia wartość TTL bez zmian
- Increase zwiększa TTL o wartość podaną w polu TTL Value
- Decrease zmniejsza TTL o wartość podaną w polu TTL Value
- Equal ustawia nową wartość parametru TTL na wartość podaną w polu TTL Value

Attain DNS Automatically - oznacza automatyczne pobieranie adresów DNS
Set DNS Manually - daje możliwość ręcznego wpisania 3 adresów DNS
Clone MAC Address - umożliwia ręczną zmianę adresu MAC interfejsu WAN

- Responding to WAN ping (włącz / wyłącz odpowiadanie na pakiety ICMP na interfejsie WAN)
- Enable UPnP (włącz / wyłącz automatyczne rozpoznawanie urządzeń w sieci)
- Enable IPsec passthrough (włącz / wyłącz przesyłanie pakietów VPN IPsec)
- Enable PPTP passthrough (włącz / wyłącz przesyłanie pakietów VPN PPTP)
- Enable L2TP passthrough (włącz / wyłącz przesyłanie pakietów VPN L2TP)

Virtual Server - opcja pozwala na przekierowanie portów. Ponieważ WL-5460AP w trybie WISP używa mechanizm NAT porty są widoczne dla zewnętrznych aplikacji. Jeżeli chcemy dostać się po danym porcie przez WLAN/WAN do LAN musimy zrobić dla tego portu tak zwane przekierowanie.

Na przykład używamy WL-5460AP w trybie WISP działa nam Internet i kupiliśmy kamerę IP. Kamera IP działa na porcie 80 tak samo jak przeglądarka internetowa. Podłączyliśmy kamerę do naszej sieci i ustawiliśmy jej adres lokalny w tej samej klasie adresowej co LAN WL-5460AP. Nasza kamera ma adres IP 192.168.100.200. Aby móc oglądać obraz jaki rejestruje kamera ze świata zrobimy następujące przekierowanie:

UWAGA!

Dla poprawnego działania przekierowania niezbędne jest wpisanie w kamerze bramy (którą jest adres IP LAN WL-5460AP).

UWAGA!

Ważne aby sprawdzać poprawność konfiguracji z innej sieci zewnętrznej, zapytanie musi przyjść na port WAN urządzenia WL-5460AP. Wpisywanie adresu zewnętrznego będąc w sieci LAN nie ma najmniejszego sensu.

UWAGA!

Porty użyte raz w Virtual Server nie mogą być przekierowane na inny adres IP. Oznacza to że dany port może być przekierowany tylko raz !

UWAGA!

Nie można jednocześnie używać funkcji Virtual Server i DMZ

W podanym przykładzie użyliśmy portu 80 który jest bardzo często używany. Tym samym uniemożliwiliśmy sobie możliwość zarządzania naszym urządzeniem ze świata. Aby ominąć ten problem w kamerze (lub innym urządzeniu) musimy znaleźć opcję „second port” i zmusić kamerę do pracy dodatkowo na innym porcie. Lub zmienić port do zarządzania w WL-5460AP w zakładce Remote Management.

Enable Virtual Servers - włącza mechanizm przekierowania portów

Servers - możemy wybrać najczęściej wybierane usługi wtedy porty wkleją się automatycznie. Do wyboru mamy Web, FTP, E-mail (POP3), E-mail (SMTP), DNS, Telnet. Lub wybrać „New” i samemu określić porty.

Local Address IP- tu wpisujemy adres IP jaki posiada nasze urządzenie (komputer, kamera IP itd..)

Protocol - do wyboru mamy TCP lub UDP. Aplikacje wykorzystują transmisję bezpieczną TCP lub nie wymagającą potwierżeń transmisję UDP. Jeżeli nie wiemy lub nie jesteśmy pewni jaki typ transmisji wybrać zaznaczamy opcję „Both” (UDP i TCP)

Port Range - oznacza zakres portów. Wpisujemy zakres np. 90-120 lub jeden port 80-80.

Opis - daje nam możliwość opisanie dodawanej reguły.

Special Application - niektóre aplikacje wymagają stałego dostępu do portów. W takim przypadku musimy określić porty źródłowe i docelowe. Aplikacja w porozumieniu z urządzeniem WL-5460AP będzie realizowała połączenie niezależnie od adresu lub adresów IP z naszej sieci lokalnej.

Special Applications

Name	Incoming Type	Incoming Start Port	Incoming End Port	Trigger Type	Trigger Start Port	Trigger End Port	Enable
Quick Time 4	UDP	6970	6999	UDP	554	554	<input checked="" type="checkbox"/>
Dialpad	UDP	51200	51201	UDP	7175	7175	<input type="checkbox"/>
Paltalk	UDP	2090	2091	UDP	8200	8700	<input type="checkbox"/>
Battle.net	TCP	6112	6119	TCP	6112	6112	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>

Save Reset

DMZ - to najszybszy i najprostszy sposób na przekierowanie portów. Aplikacja otwiera wszystkie porty ale tylko dla jednego adresu IP. Wystarczy włączyć (enable DMZ) i wpisać adres IP urządzenia na które mają być otwarte wszystkie porty np. na komputer lub na kamerę IP.

DMZ

Enable DMZ

DMZ Host IP Address:

Save Reset

Remote Management - czyli zarządzanie zdalne (ze świata). Opcję należy włączyć i ustawić port po którym będzie odbywała się komunikacja. Port 80 jest portem domyślnym i nie ma potrzeby aby go wpisywać. Jednak gdy użyjemy np. portu 8080 to będąc w innej lokalizacji chcąc zalogować się do WL-5460AP wpisujemy **83.15.125.48:8080** gdzie adres IP 83.15.125.48 jest adresem interfejsy WAN urządzenia WL-5460AP.

Remote Management

Enable Web Server Access via WAN

Port Number:

Save Reset

Dynamic DNS Setting - w przypadku gdy twój adres IP zmienia się co jakiś czas lub gdy po prostu chcesz zamienić swój adres na nazwę domenową możesz skorzystać z funkcjonalności mechanizmu DDNS. Należy zarejestrować swoją nazwę domenową (host.dyndns) w serwisie DDNS www.dyndns.com. Następnie do urządzenia WL-5460AP wpisujemy dane:

- Domain Name czyli nazwę naszej domeny
- User Name czyli nazwę użytkownika

- Password czyli hasło użytkownika

W polu „Result” pojawi się status czy nasza nazwa domenowa została pomyślnie zarejestrowana.

Dynamic DNS Setting

Enable DDNS

Service Provider: DynDNS

Domain Name: host.dyndns.org

User Name/Email:

Password/Key:

Result:

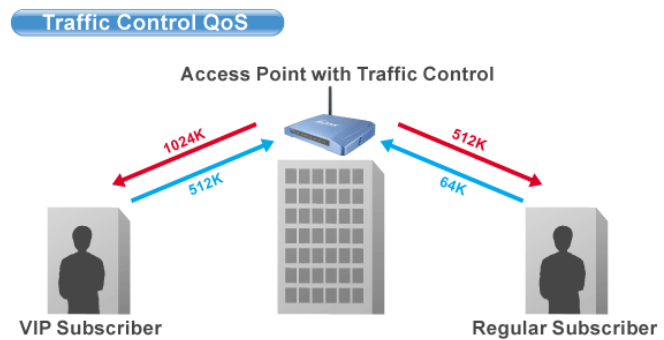
Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#).
For DynDNS, you can create your DynDNS account [here](#).

Update Reset

Instrukcja Mechanizmu Traffic Control QoS

Czym jest Traffic Control QoS?

Traffic Control to świetne narzędzie do przydzielania pasma dla operatorów WISP (Wireless Internet Service Provider). Oznacza to, że operator może zagwarantować klientom zróżnicowany typ usług (Transferów danych) podobnie jak w usłudze ADSL. Zaawansowane oprogramowanie AirLive pozwala dedykować pasmo na podstawie adresów MAC lub IP.

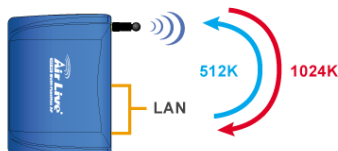


Co oferuje nam kontrola przydzielania pasma w oprogramowaniu (od E11) ?

Oprogramowanie e11 oferuje przydzielanie pasma maksymalnego “Maximum Data Rate”. AirLive oferuje dwa poziomy mechanizmu przydzielania pasma.

Interface Control (Kontrola Interfejsu)

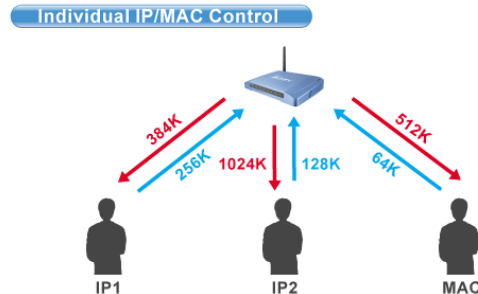
Interface Traffic Control



Mechanizm QoS kontroluje prędkość transmisji danych na dwóch interfejsach WLAN i LAN. Dla obu interfejsów zasada działania QoS jest identyczna. Ten typ kontroli jest odpowiedni jeżeli urządzenie jest w trybie AP Klient lub WISP

Kontrola Indywidualna IP/MAC

W AP możemy ustawić przydzielanie pasma dla konkretnego adresu IP lub MAC. Ten typ kontroli jest odpowiedni dla trybu AP lub Gateway.

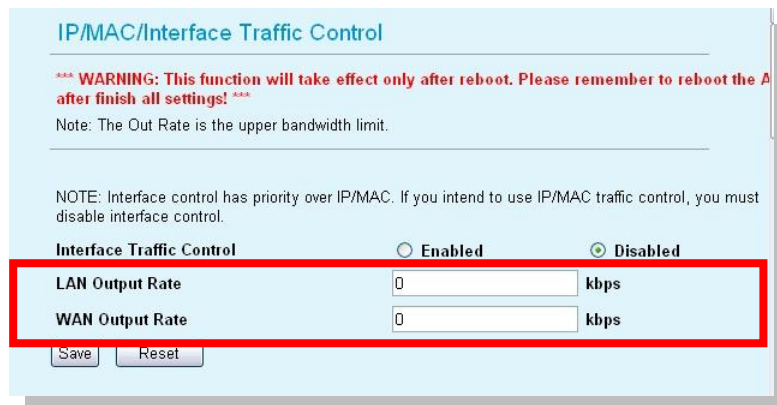


Czym jest Output Rate?

“Output Rate” jest prędkością danych wychodzących z danego interfejsu. AP obsługuje 3 typy „Output Rate”

8. **LAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu LAN. W trybie Gateway prędkość wyjściowa LAN zawiera oba interfejsy LAN i WLAN.
9. **WLAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu Wireless LAN
10. **WAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu WAN. W trybie WISP, prędkość ruchu wyjściowego z interfejsu WAN zawiera również interfejs WLAN.

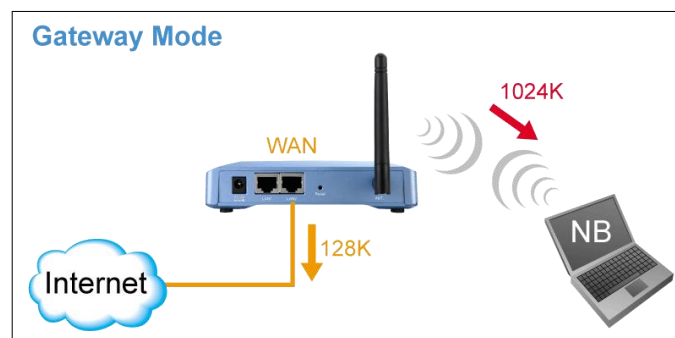
Oprogramowanie Web poinformuje cię, jakie są możliwości konfiguracji w zależności od wybranego trybu pracy są one różne.



Dla przykładu:

- a. AP jest w trybie Gateway Mode
- b. WAN Output Rate wynosi 128K
- c. LAN/WLAN Output Rate wynosi 1024K

W takim ustawieniu użytkownik z notbookiem osiągnie WYSYŁANIE na poziomie 128K i POBIERANIE na poziomie 1024K.



Konfiguracja Traffic Control QoS

Ze strony Mode Setting ,wybieramy "Traffic Control(QoS)" klikając na przycisk SETUP

The screenshot shows the 'AP Mode Settings' interface. At the bottom, the 'Traffic Control (QoS)' section is highlighted with a red box, and the 'Setup' button next to it is also highlighted. Other visible fields include 'Alias Name: Wireless_AP', 'Band: 2.4 GHz (B+G)', 'SSID: airlive', and 'Channel Number: 11'.

Po kliknięciu na "setup" wyskoczy okienko z konfiguracją mechanizmu QoS. Opis poszczególnych sekcji "A", "B", "C", "D" znajduje się poniżej.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate: 0 kbps **A**

WLAN Output Rate: 0 kbps

Save Reset

"Interface Control" to kontrola interfejsu. Musisz wyłączyć "interface Traffic Control", jeżeli chcesz używać "IP/MAC Traffic Control"

Policy Name LAN Out Rate WLAN Out Rate Comment

Save Reset

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select

Delete Selected Delete all Reset **B**

Tu definiujemy reguły "Policy" dla konkretnych adresów "Individual IP/MAC Traffic Control". Raz utworzona reguła może być wybierana w opcji

Note: Only the Wireless LAN side client IPs are supported.

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment

Save Reset **C**

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select

Delete Selected Delete all Reset

Tu określamy przepustowość dla adresu IP. Możesz wpisać więcej niż jeden adres.

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment

Save Reset **D**

Tu określamy przepustowość dla adresu MAC. Możesz wpisać więcej niż jeden adres MAC.

A. Konfiguracja Interface Control:

***** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! *****

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

W tym ustawieniu kontrolowana jest ogólna przepustowość na każdym interfejsie. Dla przykładu jeżeli chcesz ograniczyć prędkość wychodzącą z LAN do 512K i prędkość wychodzącą z WLAN do 1024K. Powinieneś zrobić tak:

- Włączyć "Interface Traffic Control"
- Wpisać "512" w polu "LAN Output Rate"
- Wpisać "1024" w polu "WLAN Output Rate"
- Kliknąć na "Save"
- Konieczny jest Reboot AP.

Przy takim ustawieniu komputer podpięty do LAN wysyła dane z prędkością 512 do komputera podpiętego do WLAN a komputer podpięty do WLAN wysyła z prędkością 1024 do komputera podpiętego do LAN.

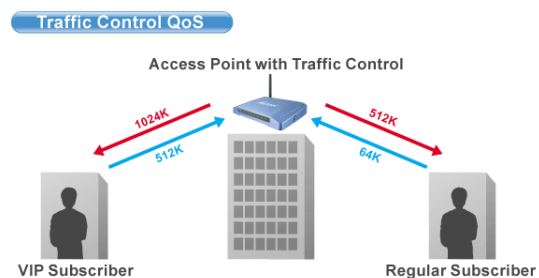


Ponieważ to ustawienie będziemy stosować głównie w trybie AP Klient, w ten sposób ograniczamy klientów podpiętych do LAN, aby nie obciążali nadmiernie stacji nadawczej AP wysyłanymi informacjami.

B. Definiowanie Reguł

Reguły określamy po to aby móc je później przyporządkować poszczególnym klientom. Dla przykładu jeżeli chcesz utworzyć dwie różne klasy usług dla dwóch klientów:

- Użytkownik VIP:
 - LAN Out Rate: 512 Kbps
 - WLAN Out Rate: 1024 Kbps
- Użytkownik Zwykły (Regular):
 - LAN Out Rate: 64 Kbps
 - WLAN Out Rate: 512 Kbps



Reguły można ustawić jako "VIP" i "Regular".

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Procedura utworzenia reguły "VIP" jest następująca:

- i. Wpisz "VIP" w polu "PolicyName"
- ii. Wpisz "512" w polu "LAN Out Rate"
- iii. Wpisz "1024" w polu "WLAN Out Rate"
- iv. Wpisz "VIP Subscriber" w polu "Comment"
- v. Kliknij na przycisk "Save".
- vi. Teraz reguła "VIP" ukaże się w "Current Policy Table"


Teraz reguła jest gotowa i można ją przyporządkować dla danego adresu IP lub MAC.

C. Przydzielanie pasma po adresie IP

Możesz określić maksymalną prędkość dla IP używając opcji „IP Control”.

Poniżej znajduje się procedura dla ustawień IP Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.

Note: Only the Wireless LAN side client IPs are supported. 

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
VIP	192.168.0.250	512 kbps	1024 kbps	Subscriber A

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	192.168.0.20	512	1024	Subscriber A	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Włącz IP Control
4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami IP na tym samym interfejsie, upewnij się że oba adresy IP są skonfigurowane w IP Traffic Control.*

D. Przydzielanie pasma po adresie MAC

Możesz określić maksymalną prędkość dla IP używając opcji MAC Control.

Poniżej znajduje się procedura dla ustawień MAC Traffic Control

5. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
6. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.
7. Włącz opcje MAC Control

Note: Only the Wireless LAN side client MACs are supported

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	004F60111111	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:4f:60:11:11:11	512	1024	VIP Subscriber	<input type="checkbox"/>

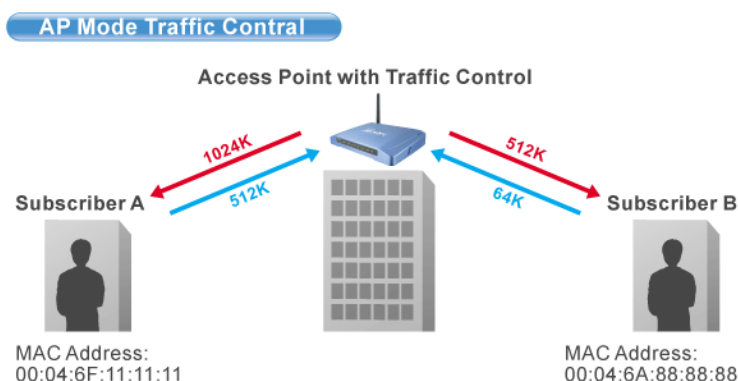
Delete Selected Delete all Reset

8. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
9. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednia wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
10. Wciśnij "Save" aby zapisać
11. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami MAC na tym samym interfejsie, upewnij się że oba adresy MAC są skonfigurowane w MAC Traffic Control.*

Przykłady zastosowania

Przykład: Kontrola Ruchu w trybie AP



Urządzenie AP jest zainstalowane na zewnątrz w celu udostępniania Internetu. Usługodawca WISP gwarantuje dwa różne typy usługi:

- **Usługa VIP :**
 - Wysłanie: 512 Kbps
 - Pobieranie: 1024 Kbps
- **Usługa Regular:**
 - Wysłanie: 64 Kbps
 - Pobieranie: 512 Kbps

Informacje o użytkownikach są następujące:

- Użytkownik A
 - Usługa VIP
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6F:11:11:11
- Użytkownik B
 - Usługa Regular
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6A:88:88:88

Konfiguracja Krok Po Kroku

12. Proszę wyłączyć "Interface Traffic Control"
13. Proszę dodać reguły "VIP" i "Regular" tak jak na rysunku poniżej

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Delete Selected Delete all Reset

14. Proszę włączyć "MAC Control"
15. Obie reguły powinny dodać się tak jak na rysunku poniżej

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	00:04:6f:11:11:11	512 kbps	1024 kbps	Subscriber A
Regular	00:4f:6a:88:88:88	64 kbps	512 kbps	Subscriber B

Save Reset

Current MAC control table:

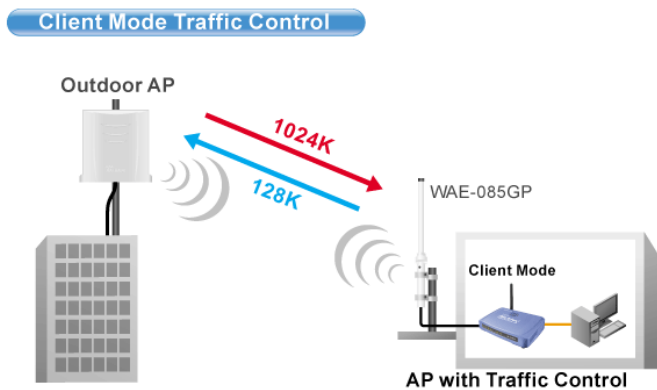
Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:04:6f:11:11:11	512	1024	Subscriber A	<input type="checkbox"/>
Regular	00:4f:6a:88:88:88	64	512	Subscriber B	<input type="checkbox"/>

Delete Selected Delete all Reset

16. Proszę zrobić Reboot AP

Przykład 2: Kontrola Ruchu w trybie Klient

Urządzenie pracuje jako klient w topologii usługodawcy WISP. Usługodawca chce ograniczyć pasmo pobierania do 1024K i wysyłania do 128K.



Konfiguracja Krok Po Kroku

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAN Output Rate	<input type="text" value="1024"/>	kbps
WLAN Output Rate	<input type="text" value="128"/>	kbps
<input type="button" value="Save"/>	<input type="button" value="Reset"/>	

1. Proszę włączyć "Interface Traffic Control"
2. Wpisać "1024" w polu "LAN Output Rate"
3. Wpisać "128" w polu "WLAN Output Rate"
4. Wcisnąć "Save"
5. Zrobić Reboot AP

Tryb WISP+Repeater

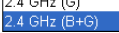
The screenshot shows the configuration page for the AirLive WLAN Access Point in WISP + Universal Repeater Mode. The page title is "WISP + Universal Repeater Mode Settings". The interface includes a navigation menu with "Mode", "Status", "TCP/IP", "Reboot", and "Other". A sidebar on the left contains the AirLive logo and a note: "This page is used to setup different wireless mode." The main configuration area includes the following fields and options:

- Alias Name:** Wireless_AP
- Disable Wireless LAN Interface**
- Band:** 2.4 GHz (B+G)
- SSID:** airlive (with a "Site Survey" button)
- SSID of Extended Interface:** (empty field)
- Enable Encryption On:** Both WAN and WLAN side
- Security:** Setup
- Advanced Settings:** Setup
- Access Control:** Setup
- Wan Port:** Setup
- Virtual Server:** Setup
- Special Application:** Setup
- DMZ:** Setup
- Remote Management:** Setup
- Dynamic DNS:** Setup
- Traffic Control(QoS):** Setup

At the bottom of the configuration area are "Apply Changes" and "Reset" buttons.

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

Band - standard radiowy. Do wyboru mamy standard B, G lub B+G.  Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

SSID - identyfikator sieci składający się maksymalnie z 32 znaków. Wszystkie urządzenia pracujące w sieci aby się komunikować muszą mieć taką samą nazwę SSID. Identyfikator ten jest przesyłany w nagłówku ramki radiowej i pełni rolę hasła dostępowego przy próbie nawiązywania połączenia bezprzewodowego.

Site Survey - funkcja służy do skanowania dostępnych sieci bezprzewodowych. Po uruchomieniu ukazuje się tabela i znalezione sieci:

Wireless Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
default	00:30:4f:42:2c:75	11 (B+G)	AP	no	64	<input type="radio"/>
ADW-4401	00:30:4f:60:da:e5	6 (B+G)	AP	no	64	<input type="radio"/>
NETGEAR	00:1f:33:42:39:09	3 (B+G)	AP	no	43	<input checked="" type="radio"/>
Filemon	00:1d:7e:b2:dc:7e	11 (B+G)	AP	WPA2-PSK	7	<input type="radio"/>
NO NAME	00:14:78:52:54:fe	6 (B+G)	AP	WEP	1	<input type="radio"/>

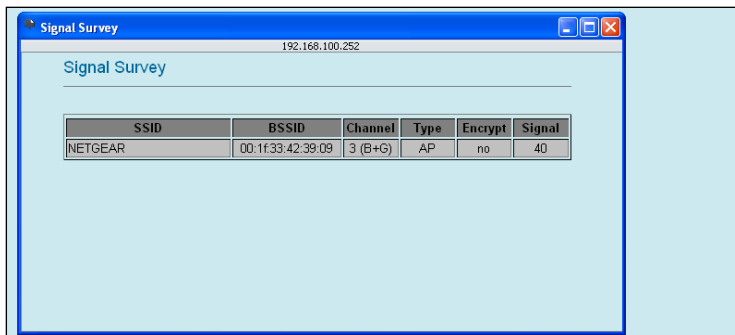
Refresh Signal Survey

W tabelce znajdziemy:

- Nazwę **SSID** dostępnych sieci
- **BSSID** czyli numer identyfikacyjny odpowiadający adresowi MAC interfejsu bezprzewodowego
- **Channel**, tu znajdziemy informacje na jakim kanale i w jakim standardzie pracuje stacja nadawcza
- **Type** czyli tryb pracy stacji nadawczej
- **Encrypt** tu dowiemy się czy sieć jest zabezpieczona i jakiego klucza użyto do zabezpieczenia

- **Signal** to ważna informacja, oznacza siłę sygnału stacji nadającej. Do połączenia wymagana wartość minimalna nie powinna być mniejsza niż 25. Jest to minimum i taki link transmisja bezprzewodowa na takim linku często może być nie poprawna.
- **Select** czy pole które zaznaczamy aby wybrać daną sieć

Signal Survey - to świetne rozwiązanie dynamicznego skanowania danej sieci. W polu „Select” wybieramy sieć, klikamy „Signal Survey”. Otworzy się osobne okienko w którym dynamicznie co 3 sekundy odświeża się informacja o sile sygnału stacji nadawczej. Bardzo przydatne narzędzie podczas zestawiania linku i konfiguracji anten.



SSID	BSSID	Channel	Type	Encrypt	Signal
NETGEAR	00:1F:33:42:39:09	3 (B+G)	AP	no	40

SSID of extended Interface - w przypadku gdy odbieramy sygnał bezprzewodowo i rozsyłamy go dalej po domu w formie bezprzewodowej, fajnie by było nazwać „naszą” sieć po swojemu. I tak w polu SSID pozostawiamy nazwę usługodawcy do którego jesteśmy podłączeni a polu SSID of extended Interface wpisujemy naszą własną nazwę SSID.

Enable Encryption on - czyli włącz szyfrowanie na interfejsie:

- **Both WAN and WLAN side** - ustawione szyfrowanie będzie działało dla obu interfejsów: WAN (połączenie z usługodawcą) i WLAN (nasza sieć domowa). I będzie identyczne dla obu interfejsów.

- **WLAN side only** - tylko na interfejsie WLAN (nasza sieć domowa).

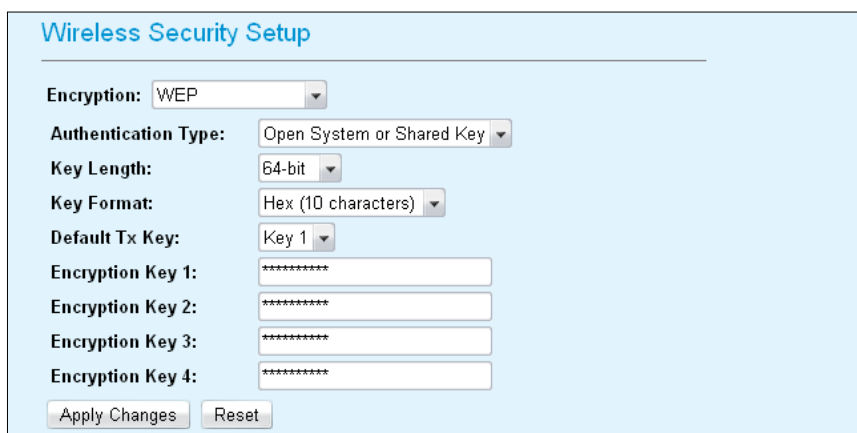
- **WAN side only** - tylko na interfejsie WAN (połączenie z usługodawcą)

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP



Wireless Security Setup

Encryption: WEP

Authentication Type: Open System or Shared Key

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Apply Changes Reset

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucza WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/Radius

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Inactivity Time: (101-60480000 10ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level:

Enable WatchDog

Watch Interval: (1-60 minutes)

Watch Host:

Ack timeout: (0-255, 0:Auto adjustment, Unit: 4µsec)

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progów przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacji nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjęcie ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

WAN Port - W trybie (Wireless Internet Service Provider) urządzenie ma funkcjonalność routera dlatego do poprawnego działania wymagana jest konfiguracja portu WAN.

WAN Port Configuration

WAN Access Type: DHCP Client ▼

Check DHCP server alive by ping per 30 seconds

TTL: Disable ▼

TTL Value: 255 (1-255)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

Respond to WAN Ping
 Enable UPnP
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Save Reset

WAN Access Type - to rodzaj połączenia interfejsu WAN. Adres możemy:

- pobierać automatycznie „DHCP Client”
- ustawić ręcznie „Static IP”
- uzyskać połączenie za pomocą nazwy i loginu przez połączenie „PPPoE”
- uzyskać połączenie po VPN „PPTP”
- uzyskać połączenie po VPN „L2TP”

Check DHCP Server alive.. - zaznaczamy opcje dla stałego podtrzymywania połączenia WAN

TTL - to czas życia pakietu w sieci. Często administrator ustawia wartość tego parametru na TTL=1 a wtedy taki pakiet nie może być przesłany przez router. Jest to równoznaczne z brakiem możliwości rozdzielania takiego sygnału na kilka komputerów. WI-5460AP oferuje możliwość zaawansowanej konfiguracji tego parametru:

- Disable pozostawia wartość TTL bez zmian
- Increase zwiększa TTL o wartość podaną w polu TTL Value

- Decrease zmniejsza TTL o wartość podaną w polu TTL Value
- Equal ustawia nową wartość parametru TTL na wartość podaną w polu TTL Value

Attain DNS Automatically - oznacza automatyczne pobieranie adresów DNS

Set DNS Manually - daje możliwość ręcznego wpisania 3 adresów DNS

Clone MAC Address - umożliwia ręczną zmianę adresu MAC interfejsu WAN

- Responding to WAN ping (włącz / wyłącz) odpowiadać na pakiety ICMP na interfejsie WAN)
- Enable UPnP (włącz / wyłącz) automatyczne rozpoznawanie urządzeń w sieci)
- Enable IPSec passthrough (włącz / wyłącz) przesyłanie pakietów VPN IPSec)
- Enable PPTP passthrough (włącz / wyłącz) przesyłanie pakietów VPN PPTP)
- Enable L2TP passthrough (włącz / wyłącz) przesyłanie pakietów VPN L2TP)

Virtual Server - opcja pozwala na przekierowanie portów. Ponieważ WL-5460AP w trybie WISP używa mechanizm NAT porty są widoczne dla zewnętrznych aplikacji. Jeżeli chcemy dostać się po danym porcie przez WLAN/WAN do LAN musimy zrobić dla tego portu tak zwane przekierowanie.

Na przykład używamy WL-5460AP w trybie WISP działa nam Internet i kupiliśmy kamerę IP. Kamera IP działa na porcie 80 tak samo jak przeglądarka internetowa. Podłączyliśmy kamerę do naszej sieci i ustawiliśmy jej adres lokalny w tej samej klasie adresowej co LAN WL-5460AP. Nasza kamera ma adres IP 192.168.100.200. Aby móc oglądać obraz jaki rejestruje kamera ze świata zrobimy następujące przekierowanie:

UWAGA!

Dla poprawnego działania przekierowania niezbędne jest wpisanie w kamerze bramy (którą jest adres IP LAN WL-5460AP).

UWAGA!

Ważne aby sprawdzać poprawność konfiguracji z innej sieci zewnętrznej, zapytanie musi przyjść na port WAN urządzenia WL-5460AP. Wpisywanie adresu zewnętrznego będąc w sieci LAN nie ma najmniejszego sensu.

UWAGA!

Porty użyte raz w Virtual Server nie mogą być przekierowane na inny adres IP. Oznacza to że dany port może być przekierowany tylko raz!

UWAGA!

Nie można jednocześnie używać funkcji Virtual Server i DMZ

W podanym przykładzie użyliśmy portu 80 który jest bardzo często używany. Tym samym uniemożliwiliśmy sobie możliwość zarządzania naszym urządzeniem ze świata. Aby ominąć ten problem w kamerze (lub innym urządzeniu) musimy znaleźć opcję „second port” i zmusić kamerę do pracy dodatkowo na innym porcie. Lub zmienić port do zarządzania w WL-5460AP w zakładce Remote Management.

Enable Virtual Servers - włącza mechanizm przekierowania portów

Servers - możemy wybrać najczęściej wybierane usługi wtedy porty wkleją się automatycznie. Do wyboru mamy Web, FTP, E-mail (POP3), E-mail (SMTP), DNS, Telnet. Lub wybrać „New” i samemu określić porty.

Local Address IP- tu wpisujemy adres IP jaki posiada nasze urządzenie (komputer, kamera IP itd..)

Protocol - do wyboru mamy TCP lub UDP. Aplikacje wykorzystują transmisję bezpieczną TCP lub nie wymagającą potwierżeń transmisję UDP. Jeżeli nie wiemy lub nie jesteśmy pewni jaki typ transmisji wybrać zaznaczamy opcję „Both” (UDP i TCP)

Port Range - oznacza zakres portów. Wpisujemy zakres np. 90-120 lub jeden port 80-80.

Opis - daje nam możliwość opisanie dodawanej reguły.

Special Application - niektóre aplikacje wymagają stałego dostępu do portów. W takim przypadku musimy określić porty źródłowe i docelowe. Aplikacja w porozumieniu z urządzeniem WL-5460AP będzie realizowała połączenie niezależnie od adresu lub adresów IP z naszej sieci lokalnej.

Special Applications

Name	Incoming Type	Incoming Start Port	Incoming End Port	Trigger Type	Trigger Start Port	Trigger End Port	Enable
Quick Time 4	UDP	6970	6999	UDP	554	554	<input checked="" type="checkbox"/>
Dialpad	UDP	51200	51201	UDP	7175	7175	<input type="checkbox"/>
Paltalk	UDP	2090	2091	UDP	8200	8700	<input type="checkbox"/>
Battle.net	TCP	6112	6119	TCP	6112	6112	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>

Save Reset

DMZ - to najszybszy i najprostszy sposób na przekierowanie portów. Aplikacja otwiera wszystkie porty ale tylko dla jednego adresu IP. Wystarczy włączyć (enable DMZ) i wpisać adres IP urządzenia na które mają być otwarte wszystkie porty np. na komputer lub na kamerę IP.

DMZ

Enable DMZ

DMZ Host IP Address:

Save Reset

Remote Management - czyli zarządzanie zdalne (ze świata). Opcje należy włączyć i ustawić port po którym będzie odbywała się komunikacja. Port 80 jest portem domyślnym i nie ma potrzeby aby go wpisywać. Jednak gdy użyjemy np. portu 8080 to będąc w innej lokalizacji chcąc zalogować się do WL-5460AP wpisujemy **83.15.125.48:8080** gdzie adres IP 83.15.125.48 jest adresem interfejsy WAN urządzenia WL-5460AP.

Remote Management

Enable Web Server Access via WAN

Port Number:

Save Reset

Dynamic DNS Setting - w przypadku gdy twój adres IP zmienia się co jakiś czas lub gdy po prostu chcesz zamienić swój adres na nazwę domenową możesz skorzystać z funkcjonalności mechanizmu DDNS. Należy zarejestrować swoją nazwę domenową (host.dyndns) w serwisie DDNS www.dyndns.com. Następnie do urządzenia WL-5460AP wpisujemy dane:

- Domain Name czyli nazwę naszej domeny
- User Name czyli nazwę użytkownika
- Password czyli hasło użytkownika

W polu „Result” pojawi się status czy nasza nazwa domenowa została pomyślnie zarejestrowana.

Dynamic DNS Setting

Enable DDNS

Service Provider: DynDNS

Domain Name:

User Name/Email:

Password/Key:

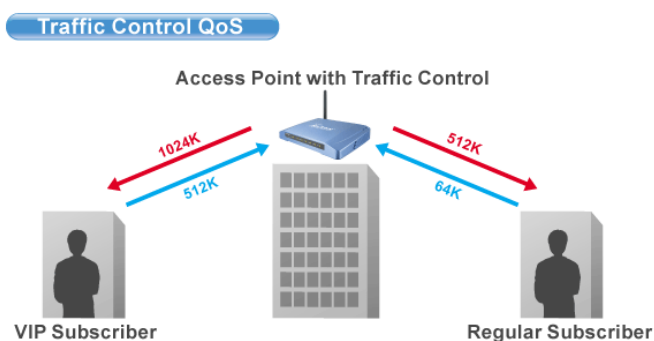
Result:

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#).
For DynDNS, you can create your DynDNS account [here](#).

Instrukcja Mechanizmu Traffic Control QoS

Czym jest Traffic Control QoS?

Traffic Control to świetne narzędzie do przydzielania pasma dla operatorów WISP (Wireless Internet Service Provider). Oznacza to, że operator może zagwarantować klientom zróżnicowany typ usług (Transferów danych) podobnie jak w usłudze ADSL. Zaawansowane oprogramowanie AirLive pozwala dedykować pasmo na podstawie adresów MAC lub IP.

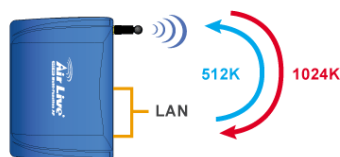


Co oferuje nam kontrola przydzielania pasma w oprogramowaniu (od E11) ?

Oprogramowanie e11 oferuje przydzielanie pasma maksymalnego "Maximum Data Rate". AirLive oferuje dwa poziomy mechanizmu przydzielania pasma.

Interface Control (Kontrola Interfejsu)

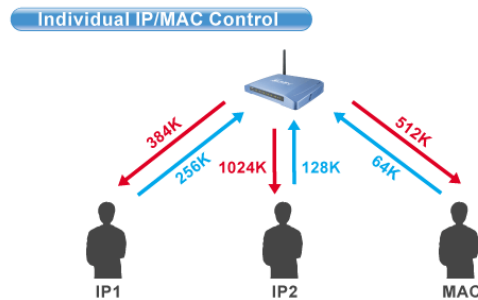
Interface Traffic Control



Mechanizm QoS kontroluje prędkość transmisji danych na dwóch interfejsach WLAN i LAN. Dla obu interfejsów zasada działania QoS jest identyczna. Ten typ kontroli jest odpowiedni jeżeli urządzenie jest w trybie AP Klient lub WISP

Kontrola Indywidualna IP/MAC

W AP możemy ustawić przydzielanie pasma dla konkretnego adresu IP lub MAC. Ten typ kontroli jest odpowiedni dla trybu AP lub Gateway.



Czym jest Output Rate?

“Output Rate” jest prędkością danych wychodzących z danego interfejsu. AP obsługuje 3 typy „Output Rate”

1. **LAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu LAN. W trybie Gateway prędkość wyjściowa LAN zawiera oba interfejsy LAN i WLAN.
2. **WLAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu Wireless LAN
3. **WAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu WAN. W trybie WISP, prędkość ruchu wyjściowego z interfejsu WAN zawiera również interfejs WLAN.

Oprogramowanie Web poinformuje cię, jakie są możliwości konfiguracji w zależności od wybranego trybu pracy są one różne.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

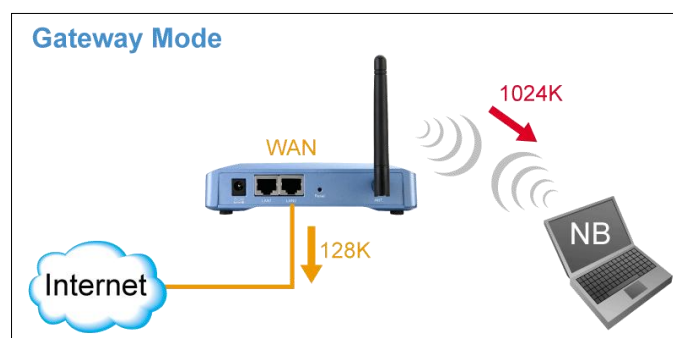
Interface Traffic Control Enabled Disabled

LAN Output Rate	<input style="width: 100%;" type="text" value="0"/>	kbps
WAN Output Rate	<input style="width: 100%;" type="text" value="0"/>	kbps

Dla przykładu:

- a. AP jest w trybie Gateway Mode
- b. WAN Output Rate wynosi 128K
- c. LAN/WLAN Output Rate wynosi 1024K

W takim ustawieniu użytkownik z notebookiem osiągnie WYSYŁANIE na poziomie 128K i POBIERANIE na poziomie 1024K.



Konfiguracja Traffic Control QoS

Ze strony Mode Setting ,wybieramy "Traffic Control(QoS)" klikając na przycisk SETUP

Po kliknięciu na "setup" wyskoczy okienko z konfiguracją mechanizmu QoS. Opis poszczególnych sekcji "A", "B", "C", "D" znajduje się poniżej.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

A

"Interface Control" to kontrola interfejsu. Musisz wyłączyć "interface Traffic Control", jeżeli chcesz używać "IP/MAC Traffic Control"

Policy Name LAN Out Rate kbps WLAN Out Rate kbps Comment

Save Reset

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Delete Selected Delete all Reset

B

Tu definiujemy reguły "Policy" dla konkretnych adresów "Individual IP/MAC Traffic Control". Raz utworzona reguła może być wybierana w opcji

Note: Only the Wireless LAN side client IPs are supported.

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Delete Selected Delete all Reset

C

Tu określamy przepustowość dla adresu IP. Możesz wpisać więcej niż jeden adres.

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

D

Tu określamy przepustowość dla adresu MAC. Możesz wpisać więcej niż jeden adres MAC.

A. Konfiguracja Interface Control:

***** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! *****

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

W tym ustawieniu kontrolowana jest ogólna przepustowość na każdym interfejsie. Dla przykładu jeżeli chcesz ograniczyć prędkość wychodzącą z LAN do 512K i prędkość wychodzącą z WLAN do 1024K. Powinieneś zrobić tak:

- Włączyć "Interface Traffic Control"
- Wpisać "512" w polu "LAN Output Rate"
- Wpisać "1024" w polu "WLAN Output Rate"
- Kliknąć na "Save"
- Konieczny jest Reboot AP.

Przy takim ustawieniu komputer podpięty do LAN wysyła dane z prędkością 512 do komputera podpiętego do WLAN a komputer podpięty do WLAN wysyła z prędkością 1024 do komputera podpiętego do LAN.

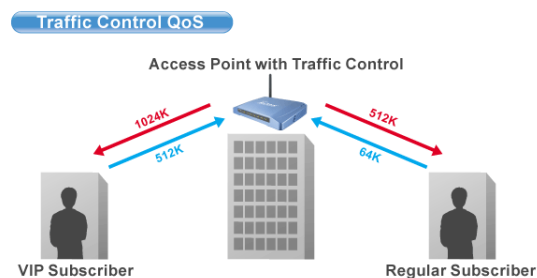


Ponieważ to ustawienie będziemy stosować głównie w trybie AP Klient, w ten sposób ograniczamy klientów podpiętych do LAN, aby nie obciążali nadmiernie stacji nadawczej AP wysyłanymi informacjami.

B. Definiowanie Reguł

Reguły określamy po to aby móc je później przyporządkować poszczególnym klientom. Dla przykładu jeżeli chcesz utworzyć dwie różne klasy usług dla dwóch klientów:

- Użytkownik VIP:
 - LAN Out Rate: 512 Kbps
 - WLAN Out Rate: 1024 Kbps
- Użytkownik Zwykły (Regular):
 - LAN Out Rate: 64 Kbps
 - WLAN Out Rate: 512 Kbps



Reguły można ustawić jako "VIP" i "Regular".

Policy Name **LAN Out Rate** kbps **WLAN Out Rate** kbps **Comment**

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Procedura utworzenia reguły "VIP" jest następująca:

1. Wpisz "VIP" w polu "PolicyName"
2. Wpisz "512" w polu "LAN Out Rate"
3. Wpisz "1024" w polu "WLAN Out Rate"
4. Wpisz "VIP Subscriber" w polu "Comment"
5. Kliknij na przycisk "Save".
6. Teraz reguła "VIP" ukaże się w "Current Policy Table"

Teraz reguła jest gotowa i można ją przyporządkować dla danego adresu IP lub MAC.

C. Przydzielanie pasma po adresie IP

Możesz określić maksymalną prędkość dla IP używając opcji „IP Control”.

Poniżej znajduje się procedura dla ustawień IP Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.

Note: Only the Wireless LAN side client IPs are supported. ←

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
VIP	192.168.0.250	512 kbps	1024 kbps	Subscriber A

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	192.168.0.20	512	1024	Subscriber A	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Włącz IP Control
4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami IP na tym samym interfejsie, upewnij się że oba adresy IP są skonfigurowane w IP Traffic Control.*

D. Przydzielanie pasma po adresie MAC

Możesz określić maksymalną prędkość dla IP używając opcji MAC Control.

Poniżej znajduje się procedura dla ustawień MAC Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.
3. Włącz opcje MAC Control

Note: Only the Wireless LAN side client MACs are supported. **Please check this part to find out what IP addresses are supported. It varies between each mode**

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	004F60111111	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:4f:60:11:11:11	512	1024	VIP Subscriber	<input type="checkbox"/>

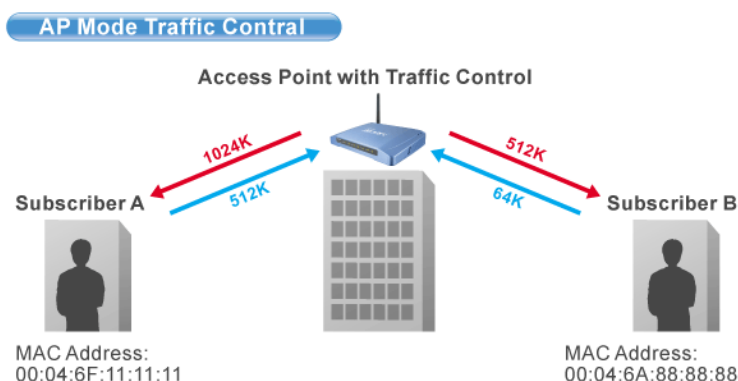
Delete Selected Delete all Reset

4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami MAC na tym samym interfejsie, upewnij się że oba adresy MAC są skonfigurowane w MAC Traffic Control.*

Przykłady zastosowania

Przykład: Kontrola Ruchu w trybie AP



Urządzenie AP jest zainstalowane na zewnątrz w celu udostępniania Internetu. Usługodawca WISP gwarantuje dwa różne typy usługi:

- **Usługa VIP :**
 - Wysłanie: 512 Kbps
 - Pobieranie: 1024 Kbps
- **Usługa Regular:**
 - Wysłanie: 64 Kbps
 - Pobieranie: 512 Kbps

Informacje o użytkownikach są następujące:

- Użytkownik A
 - Usługa VIP
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6F:11:11:11
- Użytkownik B
 - Usługa Regular
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6A:88:88:88

Konfiguracja Krok Po Kroku

1. Proszę wyłączyć "Interface Traffic Control"
2. Proszę dodać reguły "VIP" i "Regular" tak jak na rysunku poniżej

The screenshot shows a configuration page for traffic control. At the top, there are input fields for 'Policy Name', 'LAN Out Rate', 'WLAN Out Rate', and 'Comment'. The 'Policy Name' is set to 'VIP', 'LAN Out Rate' is 512 kbps, and 'WLAN Out Rate' is 1024 kbps. Below these fields are 'Save' and 'Reset' buttons. Underneath is a table titled 'Current Policy Table' with columns for Policy Name, LAN Rate (Kbps), WLAN Rate (Kbps), Comment, and Select. The table contains two rows: 'VIP' with 512 LAN and 1024 WLAN rates, and 'Regular' with 64 LAN and 512 WLAN rates. At the bottom of the table are 'Delete Selected', 'Delete all', and 'Reset' buttons.

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

3. Proszę włączyć "MAC Control"
4. Obie reguły powinny dodać się tak jak na rysunku poniżej

The screenshot shows a configuration page for MAC control. At the top, there is a note: 'Note: Only the Wireless LAN side client MACs are supported.' Below this is a checkbox labeled 'Enable MAC control' which is checked. There are input fields for 'Policy Name', 'MAC', 'LAN Out Rate', 'WLAN Out Rate', and 'Comment'. The 'Policy Name' is set to 'VIP', 'LAN Out Rate' is 512 kbps, and 'WLAN Out Rate' is 1024 kbps. Below these fields are 'Save' and 'Reset' buttons. Underneath is a table titled 'Current MAC control table' with columns for Policy Name, MAC Addr, LAN Rate (Kbps), WLAN Rate (Kbps), Comment, and Select. The table contains two rows: 'VIP' with MAC address 00:04:6f:11:11:11, and 'Regular' with MAC address 00:4f:6a:88:88:88. At the bottom of the table are 'Delete Selected', 'Delete all', and 'Reset' buttons.

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

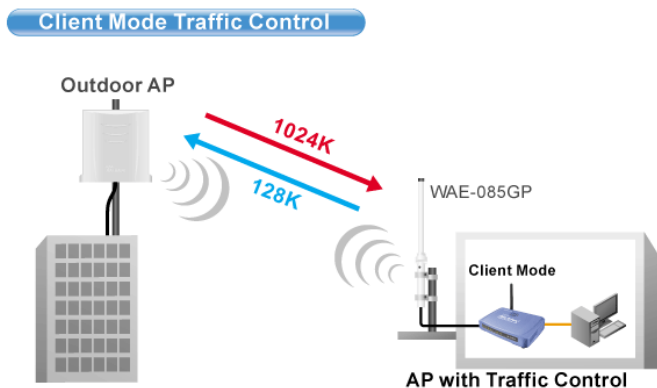
Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	00:04:6f:11:11:11	512 kbps	1024 kbps	

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:04:6f:11:11:11	512	1024	Subscriber A	<input type="checkbox"/>
Regular	00:4f:6a:88:88:88	64	512	Subscriber B	<input type="checkbox"/>

5. Proszę zrobić Reboot AP

Przykład 2: Kontrola Ruchu w trybie Klient

Urządzenie pracuje jako klient w topologii usługodawcy WISP. Usługodawca chce ograniczyć pasmo pobierania do 1024K i wysyłania do 128K.



Konfiguracja Krok Po Kroku

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAN Output Rate	<input type="text" value="1024"/>	kbps
WLAN Output Rate	<input type="text" value="128"/>	kbps
<input type="button" value="Save"/>	<input type="button" value="Reset"/>	

6. Proszę włączyć "Interface Traffic Control"
7. Wpisać "1024" w polu "LAN Output Rate"
8. Wpisać "128" w polu "WLAN Output Rate"
9. Wcisnąć "Save"
10. Zrobić Reboot AP

Tryb GW

WLAN Access Point

Mode | Status | TCP/IP | Reboot | Other

Gateway Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

SSID:

Channel Number:

Wireless Client Isolation:

Security:

Advanced Settings:

Access Control:

Wan Port:

Virtual Server:

Special Application:

DMZ:

Remote Management:

Dynamic DNS:

Ping:

DoS Setting:

Diagnostics:

URL Filtering:

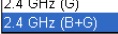
MAC Filtering:

IP Filtering:

Traffic Control(QoS):

Alias Name - to nasza własna nazwa urządzenia. Nadajemy ją aby móc zidentyfikować urządzenie przez interfejs WWW.

Disable Wireless LAN Interface - gdy zaznaczymy to pole moduł radiowy zostanie wyłączony i urządzenie nie będzie rozgłaszać sygnału bezprzewodowego. Nikt nie podłączy się radiowo do urządzenia.

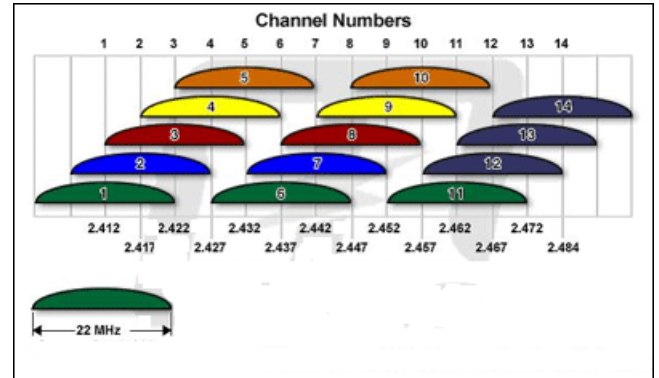
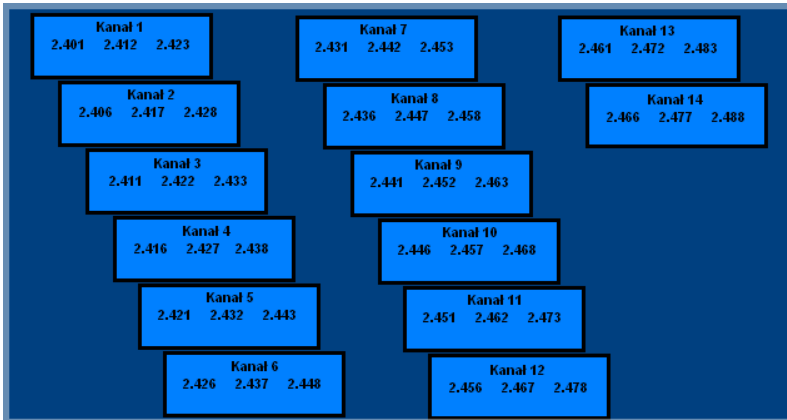
Band - standard radiowy. Do wyboru mamy standard B, G lub B+G.  Jeżeli ustawimy tylko standard B do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie B. Jeżeli ustawimy tylko standard G do urządzenia będą mogły podłączyć się tylko urządzenia pracujące w standardzie G. Przy ustawieniu B+G do urządzenia będą mogły podłączyć się urządzenia pracujące w obu standardach B i G.

SSID - identyfikator sieci składający się maksymalnie z 32 znaków. Wszystkie urządzenia pracujące w sieci aby się komunikować muszą mieć taką samą nazwę SSID. Identyfikator ten jest przesyłany w nagłówku ramki radiowej i pełni rolę hasła dostępowego przy próbie nawiązywania połączenia bezprzewodowego.

Channel Number - tu wybieramy na jakim kanale ma pracować nasz nadajnik. Każdy kanał to określony zakres częstotliwości.

Numer Kanału	Dolna Częstotliwość Kanału w GHz	Środkowa Częstotliwość Kanału	Górna Częstotliwość Kanału w GHz
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488

Wszystkie kanały pokrywają się w pewnym stopniu częstotliwością. Oddzielone są np. kanały 1,7,13. Instalując sieci upewnijmy się jakie kanały są już używane. I użyjmy innych aby zredukować zakłócenia.



Ilość kanałów zależy od kodowania np.

Region	Kodowanie	Ilość kanałów
USA	FCC	11
Europa	ETSI	13
Japonia	TELEC	14

Wireless Client Isolation - enabled (włącz), disabled (wyłącz). Funkcja izolacji klientów bezprzewodowych sprawia że użytkownicy nie będą wymieniać między sobą informacji. Użytkownicy nie będą mogli kopiować danych pomiędzy sobą w otoczeniu sieciowym dzięki temu można zwiększyć bezpieczeństwo danych w sieci oraz można skutecznie zwiększyć wydajność urządzenia radiowego. Jeżeli klienci radiowi nie będą przysyłać między sobą danych, urządzenie radiowe nie będzie musiało ich przetwarzać. Funkcja dotyczy tylko klientów bezprzewodowych.

Security - w tej zakładce wybieramy rodzaj klucza którym będzie kodowana transmisja danych. Zabezpieczone urządzenia mogą się komunikować tylko wtedy gdy używają takiego samego klucza przy zachowaniu zgodności kodów.

Do wyboru mamy następujące klucze

- None
- WEP
- WPA-PSK (TKIP)
- WPA-PSK (AES)
- WPA2-PSK(AES)
- WPA2-PSK Mixed
- 802.1x / RADIUS

Konfiguracja klucza WEP

Wireless Security Setup

Encryption:

Authentication Type:

Key Length:

Key Format:

Default Tx Key:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

- **Authentication Type** czyli typ autoryzacji. **Open System** przy pierwszej wymianie ramek radiowych klucz WEP nie jest użyty i praktycznie każde urządzenie może się podłączyć do naszego nadajnika ale nie oznacza to że będą one ze sobą współpracowały ponieważ do tego wymagana jest zgodność kluczy. Zatem gdy stacja obca nie szyfruje transmisji lub szyfruje ją innym kluczem po procesie autoryzacji i przyłączenia zostanie odrzucona. Przy autoryzacji typu **Shared Key** następuje czterostopniowy proces autentykacji kluczem WEP po którym następuje połączenie. Wbrew pozorom ten typ autoryzacji jest gorszym zabezpieczeniem ponieważ istnieje możliwość podsłuchania ramek radiowych w których podczas czterostopniowego procesu autentykacji jest przesyłana treść klucza WEP.

Jeżeli już decydujemy się na ten typ klucza wybierzmy opcje Open System.

- **Key Length** to długość klucza. Klucz może być 64 lub 128 bitowy. Dłuższy klucz jest trudniejszy do złamania.

- **Key Format** to forma klucza. Może być to **ASCII** z obsługą 127 znaków. Wymaga wpisania 5 znaków. Lub **HEX** z obsługą znaków 0-9 i A-Z. Wymaga wpisania 10 znaków.

- **Default Tx Key** w tym polu wybieramy którego klucza będziemy używać. Możemy wprowadzić cztery klucze WEP.

- **Encryption Key 1,2,3,4** w tych polach wpisujemy klucze. Wystarczy wypełnić jedno pole np. Key 1 i upewnić się że Key 1 jest ustawiony w polu Default Tx Key.

Aby ustawić szyfrowanie WEP:

Jeśli już zdecydujemy się na klucz WEP który jest kluczem prostym do złamania ale za to obsługiwany przez wszystkie urządzenia radiowe to:

1. Wybieramy Open System
2. Długość klucza najlepiej 128bit
3. HEX lub ASCII wybieramy dowolnie
4. Zostawiamy Key 1
5. W polu pierwszym wpisujemy dowolną treść klucza, ilość znaków i typ znaków zależy od ustawienia HEX czy ASCII
6. Zatwierdzamy ustawienia i pamiętamy o wprowadzeniu identycznych ustawień w drugim urządzeniu.

Konfiguracja klucza WPA, WPA2

Konfiguracja kluczy WPA, WPA2 oraz WPA Mixed jest identyczna. Są to klucze bardziej zaawansowane niż klucz WEP. Wykorzystują szyfrowanie TKIP oraz AES. Najbardziej zaawansowane szyfrowanie to WPA2(AES).

Aby ustawić szyfrowanie WPA,WPA2

1. Wybieramy rodzaj klucza WPA lub WPA2
2. W polu **Pre-Shared Key Format** wybieramy formę klucza. "Passphrase" oznacza frazę i minimum 8 znaków a HEX oznacza 64 znaki od 0-9 i od A-F. W tym polu wpisujemy nasz klucz.
3. Parametr **Group Key Life Time** to czas po którym klucz dynamicznie ulega zmianie. Im krótszy czas tym zabezpieczenie jest lepsze.
4. Zapisujemy ustawienia. Pamiętajmy o powtórzeniu tej czynności w drugim urządzeniu z którym nawiązujemy komunikację bezprzewodową.

Konfiguracja 802.1x/RADIUS

Jeżeli posiadamy w sieci serwer Radius możemy wybrać ten typ autoryzacji. Wystarczy wybrać rodzaj klucza, wpisać adres IP serwera Radius oraz hasło do serwera Radius. Urządzenia które nie przejdą autoryzacji na serwerze Radius nie zostaną dołączone do sieci.

Advanced Settings w tej zakładce znajdują się funkcje zaawansowane.

Wireless Advanced Settings

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Inactivity Time: (101-60480000 10ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Tx Power Level:

Enable WatchDog

Watch Interval: (1-60 minutes)

Watch Host:

Ack timeout: (0-255, 0:Auto adjustment, Unit: 4µsec)

Fragment Threshold to próg fragmentacji ramek. Mechanizm służy do polepszania wydajności w warunkach dużego ruchu sieciowego. Jeżeli karta sieciowa podłączona do WL-5460AP często przesyła duże pliki można użyć fragmentacji w celu rozdzielenia ramek na mniejsze. W warunkach gdzie nie występują interferencje maksymalna wartość progów przekłada się na szybkość transmisji. Jednak wszystko zależy od środowiska w jakim pracuje dana sieć bezprzewodowa. Gdy ramki wymagają retransmisji z powodu zakłóceń dobrze aby retransmitowane były mniejsze ilości danych.

RTS Threshold to mechanizm który zapobiega kolizjom ramek radiowych. W sytuacji gdy dwa odbiorniki nie obejmują się zasięgiem ale w ich zasięgu jest nadajnik może często dochodzić do kolizji ramek radiowych. W takim przypadku oba odbiorniki muszą retransmitować ramki. Stacje odbiorcze nie są w stanie informować się o nadawaniu ponieważ nie obejmują się zasięgiem i nie mogą się ze sobą komunikować. Na takich stacjach klienckich powinniśmy włączyć mechanizm RTS. Po tej czynności stacja wyśle do nadajnika ramkę RTS co oznacza chęć rozpoczęcia transmisji. Następnie nadajnik wyśle do wszystkich urządzeń radiowych ramkę CTS z informacją synchronizującą dalszą transmisję radiową. Dzięki temu wszystkie urządzenia radiowe wiedzą kiedy mogą nadawać bez narażania ramek na kolizję. Każda ramka większa niż wartość RTS będzie poprzedzona tego typu procedurą. W sieci gdzie jest duża ilość odbiorników widzących nadajnik ale nie widzących się nawzajem zmniejszenie parametry RTS może poprawić wydajność.

Beacon Interval to czas pomiędzy transmisją ramek Beacon. Ramki Beacon służą do synchronizacji urządzeń radiowych. Im mniejszy parametr Beacon Interval tym krótszy czas logowania się nowych stacji radiowych. Zwiększenie tego parametru to oszczędność zużycia energii urządzeń przebywających w stanie uśpienia.

Inactivity Time

Data Rate to prędkość transmisji. Zaleca się aby ta wartość ustawiona była na „Auto”. Wraz ze zmianą prędkości transmisji, zmienia się również czułość urządzenia. Podczas automatycznego ustawienia prędkości urządzenie samo dostosuje się do istniejących warunków i wybiera optymalną prędkość. Często gdy istotna jest stabilność połączenia a nie jej wydajność ustawia się minimalną prędkość, wtedy czułość urządzenia jest największa. Rozwiązanie to sprawdza się w środowisku niskich interferencji. Im urządzenia są czulsze tym więcej zakłóceń odbierają co może wpłynąć na ich gorszą pracę.

Preamble Type czyli typ preambuły. Do wyboru mamy preambułę długą (LONG) oraz krótką (SHORT). Preambuła to pole w nagłówku ramki radiowej. Kiedyś urządzenia używały tylko preambuły długiej w późniejszym okresie wprowadzoną jej krótszą wersję co znacznie skróciło czas jej przetwarzania przez urządzenia radiowe. Preambułę długą pozostawiono aby zachować kompatybilność ze starszymi urządzeniami. W praktyce rzadko się przydaje. Ponieważ urządzenia z ustawioną krótką preambułą potrafią odczytać istotny fragment z preambuły długiej można stosować je jednocześnie w sieciach.

Broadcast SSID to identyfikator sieci radiowej składający się maksymalnie z 32 znaków. Przesyłany jest w nagłówkach pakietów i pełni rolę hasła dostępowego. Aby urządzenia mogły się komunikować muszą mieć taką samą nazwę SSID.

IAPP to protokół odpowiadający za roaming. Po włączeniu go na stacji nadawczych urządzenia radiowe mogą przemieszczać się pomiędzy tymi stacjami nadawczymi bez utraty połączenia. Protokół odpowiada za przekazywanie informacji pomiędzy stacjami nadawczymi.

802.11g Protection to funkcja dzięki której nasze urządzenie będzie kompatybilne z modulacją CCK standardu 802.11b i nie będzie przez niego zakłócanie. W środowisku gdzie nie występują stacje zgodne ze standardem 802.11b nie należy włączać tej opcji ponieważ obniży to wydajność naszego urządzenia.

Tx Power Level to regulacja mocy nadajnika dostępna w 7 poziomach. Poziom 1 (Level 1) oznacza największą moc nadajnika. Standardowo moc ustawiona jest na poziomie 3

Tx Power Level:	Default (About 18dB) ▼
	Level 1 (About 20dB)
	Level 2 (About 19dB)
	Default (About 18dB)
	Level 4 (About 16dB)
	Level 5 (About 15dB)
	Level 6 (About 14dB)
	Level 7 (About 13dB)

Enable Watchdog to opcja samoczynnego restartowania nadajnika w określonych warunkach. Mechanizm działa na zasadzie wysyłania pakietów ICMP. W ten sposób sprawdza tak jakby samo siebie czy nadal działa poprawnie. Jeżeli urządzenie po nadaniu pakietów ICMP nie otrzyma pakietów zwrotnych, automatycznie wykona restart. W celu poprawnej konfiguracji należy ustawić interwał czasowy (1-60 minut) wysyłania pakietów ICMP oraz podać adres IP urządzenia do którego te pakiety będą wysyłane.

ACK Timeout parametr określa limit czasu oczekiwania na potwierdzenie ACK (przyjąłem ramkę możesz transmitować następną). Jeżeli zestawiliśmy połączenie na długim dystansie należy zwiększyć parametr ACK Timeout. Inaczej nadajnik po długim czasie oczekiwania wykona retransmisję pakietu. Najwyższa wartość parametru to 255. Każda jednostka to równowartość 4 mikrosekund. Parametr równy wartości 0 oznacza automatyczne dostosowanie ACK Timeout.

WAN Port - W trybie (Wireless Internet Service Provider) urządzenie ma funkcjonalność routera dlatego do poprawnego działania wymagana jest konfiguracja portu WAN.

WAN Port Configuration

WAN Access Type: DHCP Client ▼

Check DHCP server alive by ping per 30 seconds

TTL: Disable ▼

TTL Value: 255 (1-255)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

Respond to WAN Ping
 Enable UPnP
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Save Reset

WAN Access Type - to rodzaj połączenia interfejsu WAN. Adres możemy:

- pobierać automatycznie „DHCP Client”
- ustawić ręcznie „Static IP”
- uzyskać połączenie za pomocą nazwy i loginu przez połączenie „PPPoE”
- uzyskać połączenie po VPN „PPTP”
- uzyskać połączenie po VPN „L2TP”

Check DHCP Server alive.. - zaznaczamy opcje dla stałego podtrzymywania połączenia WAN

TTL - to czas życia pakietu w sieci. Często administrator ustawia wartość tego parametru na TTL=1 a wtedy taki pakiet nie może być przesłany przez router. Jest to równoznaczne z brakiem możliwości rozdzielania takiego sygnału na kilka komputerów. WI-5460AP oferuje możliwość zaawansowanej konfiguracji tego parametru:

- Disable pozostawia wartość TTL bez zmian
- Increase zwiększa TTL o wartość podaną w polu TTL Value

- Decrease zmniejsza TTL o wartość podaną w polu TTL Value
- Equal ustawia nową wartość parametru TTL na wartość podaną w polu TTL Value

Attain DNS Automatically - oznacza automatyczne pobieranie adresów DNS

Set DNS Manually - daje możliwość ręcznego wpisania 3 adresów DNS

Clone MAC Address - umożliwia ręczną zmianę adresu MAC interfejsu WAN

- Responding to WAN ping (włącz / wyłącz odpowiadanie na pakiety ICMP na interfejsie WAN)
- Enable UPnP (włącz / wyłącz automatyczne rozpoznawanie urządzeń w sieci)
- Enable IPSec passthrough (włącz / wyłącz przesyłanie pakietów VPN IPSec)
- Enable PPTP passthrough (włącz / wyłącz przesyłanie pakietów VPN PPTP)
- Enable L2TP passthrough (włącz / wyłącz przesyłanie pakietów VPN L2TP)

Virtual Server - opcja pozwala na przekierowanie portów. Ponieważ WL-5460AP w trybie WISP używa mechanizm NAT porty są widoczne dla zewnętrznych aplikacji. Jeżeli chcemy dostać się po danym porcie przez WLAN/WAN do LAN musimy zrobić dla tego portu tak zwane przekierowanie.

Na przykład używamy WL-5460AP w trybie WISP działa nam Internet i kupiliśmy kamerę IP. Kamera IP działa na porcie 80 tak samo jak przeglądarka internetowa. Podłączyliśmy kamerę do naszej sieci i ustawiliśmy jej adres lokalny w tej samej klasie adresowej co LAN WL-5460AP. Nasza kamera ma adres IP 192.168.100.200. Aby móc oglądać obraz jaki rejestruje kamera ze świata zrobimy następujące przekierowanie:

UWAGA!

Dla poprawnego działania przekierowania niezbędne jest wpisanie w kamerze bramy (którą jest adres IP LAN WL-5460AP).

UWAGA!

Ważne aby sprawdzać poprawność konfiguracji z innej sieci zewnętrznej, zapytanie musi przyjść na port WAN urządzenia WL-5460AP. Wpisywanie adresu zewnętrznego będąc w sieci LAN nie ma najmniejszego sensu.

UWAGA!

Porty użyte raz w Virtual Server nie mogą być przekierowane na inny adres IP. Oznacza to że dany port może być przekierowany tylko raz!

UWAGA!

Nie można jednocześnie używać funkcji Virtual Server i DMZ

W podanym przykładzie użyliśmy portu 80 który jest bardzo często używany. Tym samym uniemożliwiliśmy sobie możliwość zarządzania naszym urządzeniem ze świata. Aby ominąć ten problem w kamerze (lub innym urządzeniu) musimy znaleźć opcję „second port” i zmusić kamerę do pracy dodatkowo na innym porcie. Lub zmienić port do zarządzania w WL-5460AP w zakładce Remote Management.

Enable Virtual Servers - włącza mechanizm przekierowania portów

Servers - możemy wybrać najczęściej wybierane usługi wtedy porty wkleją się automatycznie. Do wyboru mamy Web, FTP, E-mail (POP3), E-mail (SMTP), DNS, Telnet. Lub wybrać „New” i samemu określić porty.

Local Address IP- tu wpisujemy adres IP jaki posiada nasze urządzenie (komputer, kamera IP itd..)

Protocol - do wyboru mamy TCP lub UDP. Aplikacje wykorzystują transmisję bezpieczną TCP lub nie wymagającą potwierżeń transmisję UDP. Jeżeli nie wiemy lub nie jesteśmy pewni jaki typ transmisji wybrać zaznaczamy opcję „Both” (UDP i TCP)

Port Range - oznacza zakres portów. Wpisujemy zakres np. 90-120 lub jeden port 80-80.

Opis - daje nam możliwość opisanie dodawanej reguły.

Special Application - niektóre aplikacje wymagają stałego dostępu do portów. W takim przypadku musimy określić porty źródłowe i docelowe. Aplikacja w porozumieniu z urządzeniem WL-5460AP będzie realizowała połączenie niezależnie od adresu lub adresów IP z naszej sieci lokalnej.

Special Applications

Name	Incoming Type	Incoming Start Port	Incoming End Port	Trigger Type	Trigger Start Port	Trigger End Port	Enable
Quick Time 4	UDP	6970	6999	UDP	554	554	<input checked="" type="checkbox"/>
Dialpad	UDP	51200	51201	UDP	7175	7175	<input type="checkbox"/>
Paltalk	UDP	2090	2091	UDP	8200	8700	<input type="checkbox"/>
Battle.net	TCP	6112	6119	TCP	6112	6112	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>

Save Reset

DMZ - to najszybszy i najprostszy sposób na przekierowanie portów. Aplikacja otwiera wszystkie porty ale tylko dla jednego adresu IP. Wystarczy włączyć (enable DMZ) i wpisać adres IP urządzenia na które mają być otwarte wszystkie porty np. na komputer lub na kamerę IP.

DMZ

Enable DMZ

DMZ Host IP Address:

Save Reset

Remote Management - czyli zarządzanie zdalne (ze świata). Opcje należy włączyć i ustawić port po którym będzie odbywała się komunikacja. Port 80 jest portem domyślnym i nie ma potrzeby aby go wpisywać. Jednak gdy użyjemy np. portu 8080 to będąc w innej lokalizacji chcąc zalogować się do WL-5460AP wpisujemy **83.15.125.48:8080** gdzie adres IP 83.15.125.48 jest adresem interfejsy WAN urządzenia WL-5460AP.

Remote Management

Enable Web Server Access via WAN

Port Number:

Save Reset

Dynamic DNS Setting - w przypadku gdy twój adres IP zmienia się co jakiś czas lub gdy po prostu chcesz zamienić swój adres na nazwę domenową możesz skorzystać z funkcjonalności mechanizmu DDNS. Należy zarejestrować swoją nazwę domenową (host.dyndns) w serwisie DDNS www.dyndns.com. Następnie do urządzenia WL-5460AP wpisujemy dane:

- Domain Name czyli nazwę naszej domeny
- User Name czyli nazwę użytkownika
- Password czyli hasło użytkownika

W polu „Result” pojawi się status czy nasza nazwa domenowa została pomyślnie zarejestrowana.

Dynamic DNS Setting

Enable DDNS

Service Provider:

Domain Name:

User Name/Email:

Password/Key:

Result:

Note:
 For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#).
 For DynDNS, you can create your DynDNS account [here](#).

Ping - umożliwia wysłanie pakietów ICMP z poziomu urządzenia WL-5460AP. Narzędzie przydatne w celu diagnostyki sieci.

Ping Toolkit

IP Address / Host Name

Response PING 213.180.138.148 (213.180.138.148): 56 data bytes

DoS Settings - to narzędzie chroniące naszą sieć przed atakami hakerskimi które mogą negatywnie wpływać na pracę naszego urządzenia.

Denial of Service

Enable DoS Prevention

<input type="checkbox"/> Whole System Flood: SYN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> TCP/UDP PortScan	<input type="text" value="Low"/>	Sensitivity
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		
<input type="checkbox"/> TCP Scan		
<input type="checkbox"/> TCP SynWithData		
<input type="checkbox"/> UDP Bomb		
<input type="checkbox"/> UDP EchoChargen		

Enable Source IP Blocking Block time (sec)

Mechanizm daje nam możliwość filtrowania ilości pakietów po znacznikach zawartych w ramkach oraz odrzucanie pakietów charakterystycznych dla ataków hakerskich.

Diagnostics - to narzędzie do sprawdzania pod jakim adresem ukrywa się dana nazwa URL.

Network Diagnostics - DNS Lookup

Domain name/URL:

Address: 172.16.2.9
 Name: www.onet.pl
 Address: 213.180.138.148

URL Filtering - pozwala blokować strony www. Wystarczy wpisać nazwę strony aby nie wyświetlała się ona na komputerach sieci LAN i WLAN.

URL Filtering

Enable URL Filtering

URL Address:

Current Filter Table:

URL Address	Select
www.redtube.pl	<input type="checkbox"/>

MAC Filtering - pozwala blokować adresy MAC. Użytkownik o adresie MAC który jest wpisany do tablicy nie zostanie dopuszczony do zasobów WL-5460AP. Adresy MAC wpisujemy w formie: 004f74301538 .

MAC Filtering

Enable MAC Filtering

MAC Address:

Description:

Current Filter Table:

MAC Address	Description	Select
00:4f:74:30:15:38	Użytkownik 1	<input type="checkbox"/>

IP Filtering - pozwala blokować adresy IP. Użytkownik o adresie IP który jest wpisany do tablicy nie zostanie dopuszczony do zasobów WL-5460AP. Adresy IP wpisujemy w formie: 192.168.100.5 . Adresy muszą być z tej samej podsieci co interfejs LAN.

IP Filtering

Enable IP Filtering

Local IP Address:

Protocol:

Description:

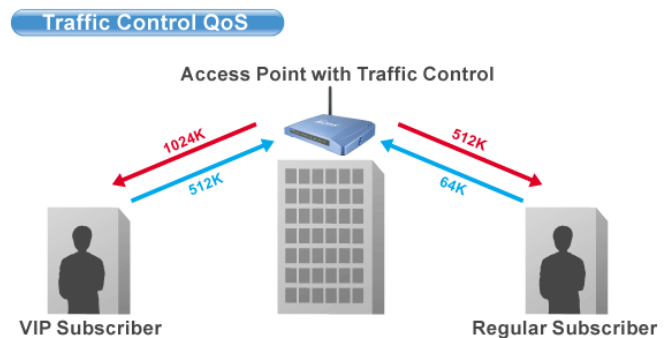
Current Filter Table:

Local IP Address	Protocol	Description	Select
192.168.100.5	TCP+UDP	Użytkownik 1	<input type="checkbox"/>

Instrukcja Mechanizmu Traffic Control QoS

Czym jest Traffic Control QoS?

Traffic Control to świetne narzędzie do przydzielania pasma dla operatorów WISP (Wireless Internet Service Provider). Oznacza to, że operator może zagwarantować klientom zróżnicowany typ usług (Transferów danych) podobnie jak w usłudze ADSL. Zaawansowane oprogramowanie AirLive pozwala dedykować pasmo na podstawie adresów MAC lub IP.

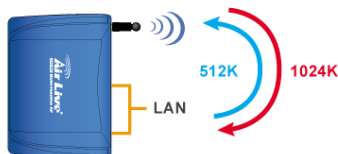


Co oferuje nam kontrola przydzielania pasma w oprogramowaniu (od E11) ?

Oprogramowanie e11 oferuje przydzielanie pasma maksymalnego "Maximum Data Rate". AirLive oferuje dwa poziomy mechanizmu przydzielania pasma.

Interface Control (Kontrola Interfejsu)

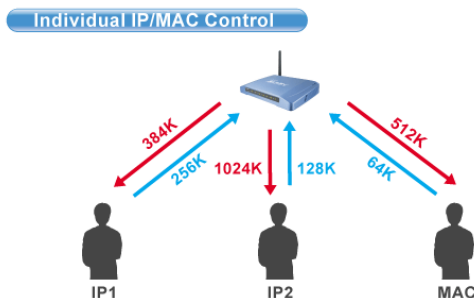
Interface Traffic Control



Mechanizm QoS kontroluje prędkość transmisji danych na dwóch interfejsach WLAN i LAN. Dla obu interfejsów zasada działania QoS jest identyczna. Ten typ kontroli jest odpowiedni jeżeli urządzenie jest w trybie AP Klient lub WISP

Kontrola Indywidualna IP/MAC

W AP możemy ustawić przydzielanie pasma dla konkretnego adresu IP lub MAC. Ten typ kontroli jest odpowiedni dla trybu AP lub Gateway.



Czym jest Output Rate?

“Output Rate” jest prędkością danych wychodzących z danego interfejsu. AP obsługuje 3 typy „Output Rate”

1. **LAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu LAN. W trybie Gateway prędkość wyjściowa LAN zawiera oba interfejsy LAN i WLAN.
2. **WLAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu Wireless LAN
3. **WAN Output Rate:** To jest prędkość ruchu wyjściowego z interfejsu WAN. W trybie WISP, prędkość ruchu wyjściowego z interfejsu WAN zawiera również interfejs WLAN.

Oprogramowanie Web poinformuje cię, jakie są możliwości konfiguracji w zależności od wybranego trybu pracy są one różne.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

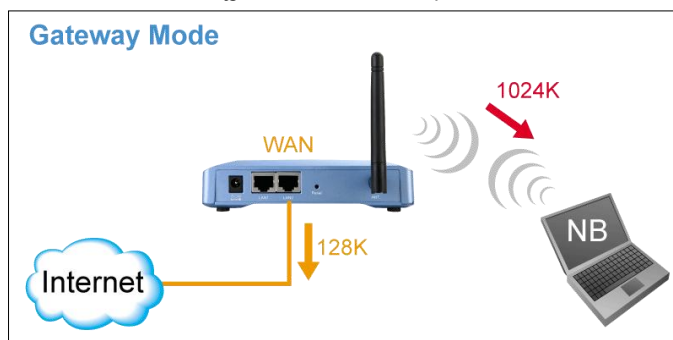
LAN Output Rate kbps

WAN Output Rate kbps

Dla przykładu:

- a. AP jest w trybie Gateway Mode
- b. WAN Output Rate wynosi 128K
- c. LAN/WLAN Output Rate wynosi 1024K

W takim ustawieniu użytkownik z notbookiem osiągnie WYSYŁANIE na poziomie 128K i POBIERANIE na poziomie 1024K.



Konfiguracja Traffic Control QoS

Ze strony Mode Setting ,wybieramy "Traffic Control(QoS)" klikając na przycisk SETUP

AP Mode Settings

Alias Name:

Disable Wireless LAN Interface

Band:

SSID:

Channel Number:

Wireless Client Isolation:

Security:

Advanced Settings:

Access Control:

Traffic Control (QoS):

Po kliknięciu na "setup" wyskoczy okienko z konfiguracją mechanizmu QoS. Opis poszczególnych sekcji "A", "B", "C", "D" znajduje się poniżej.

IP/MAC/Interface Traffic Control

*** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! ***

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

A Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

B Policy Name LAN Out Rate WLAN Out Rate Comment

kbps kbps

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Note: Only the Wireless LAN side client IPs are supported.

C Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Note: Only the Wireless LAN side client MACs are supported.

D Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
<input type="text"/>	<input type="text"/>	<input type="text"/> kbps	<input type="text"/> kbps	<input type="text"/>

"Interface Control" to kontrola interfejsu. Musisz wyłączyć "interface Traffic Control", jeżeli chcesz używać "IP/MAC Traffic Control"

Tu definiujemy reguły "Policy" dla konkretnych adresów "Individual IP/MAC Traffic Control". Raz utworzona reguła może być wybierana w opcji

Tu określamy przepustowość dla adresu IP. Możesz wpisać więcej niż jeden adres.

Tu określamy przepustowość dla adresu MAC. Możesz wpisać więcej niż jeden adres MAC.

A. Konfiguracja Interface Control:

***** WARNING: This function will take effect only after reboot. Please remember to reboot the AP after finish all settings! *****

Note: The Out Rate is the upper bandwidth limit.

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control Enabled Disabled

LAN Output Rate kbps

WLAN Output Rate kbps

W tym ustawieniu kontrolowana jest ogólna przepustowość na każdym interfejsie. Dla przykładu jeżeli chcesz ograniczyć prędkość wychodzącą z LAN do 512K i prędkość wychodzącą z WLAN do 1024K. Powinieneś zrobić tak:

- Włączyć "Interface Traffic Control"
- Wpisać "512" w polu "LAN Output Rate"
- Wpisać "1024" w polu "WLAN Output Rate"
- Kliknąć na "Save"
- Konieczny jest Reboot AP.

Przy takim ustawieniu komputer podpięty do LAN wysyła dane z prędkością 512 do komputera podpiętego do WLAN a komputer podpięty do WLAN wysyła z prędkością 1024 do komputera podpiętego do LAN.

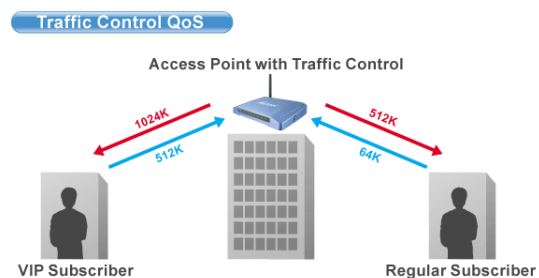


Ponieważ to ustawienie będziemy stosować głównie w trybie AP Klient, w ten sposób ograniczamy klientów podpiętych do LAN, aby nie obciążali nadmiernie stacji nadawczej AP wysyłanymi informacjami.

B. Definiowanie Reguł

Reguły określamy po to aby móc je później przyporządkować poszczególnym klientom. Dla przykładu jeżeli chcesz utworzyć dwie różne klasy usług dla dwóch klientów:

- Użytkownik VIP:
 - LAN Out Rate: 512 Kbps
 - WLAN Out Rate: 1024 Kbps
- Użytkownik Zwykły (Regular):
 - LAN Out Rate: 64 Kbps
 - WLAN Out Rate: 512 Kbps



Reguły można ustawić jako "VIP" i "Regular".

Policy Name **LAN Out Rate** kbps **WLAN Out Rate** kbps **Comment**

Current Policy Table:

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

Procedura utworzenia reguły "VIP" jest następująca:

1. Wpisz "VIP" w polu "PolicyName"
2. Wpisz "512" w polu "LAN Out Rate"
3. Wpisz "1024" w polu "WLAN Out Rate"
4. Wpisz "VIP Subscriber" w polu "Comment"
5. Kliknij na przycisk "Save".
6. Teraz reguła "VIP" ukaże się w "Current Policy Table"


Teraz reguła jest gotowa i można ją przyporządkować dla danego adresu IP lub MAC.

C. Przydzielanie pasma po adresie IP

Możesz określić maksymalną prędkość dla IP używając opcji „IP Control”.

Poniżej znajduje się procedura dla ustawień IP Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.

Note: Only the Wireless LAN side client IPs are supported. 

Enable IP control

Policy Name	IP	LAN Out Rate	WLAN Out Rate	Comment
VIP	192.168.0.250	512 kbps	1024 kbps	Subscriber A

Save Reset

Current IP control table:

Policy Name	IP Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	192.168.0.20	512	1024	Subscriber A	<input type="checkbox"/>

Delete Selected Delete all Reset

3. Włącz IP Control
4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami IP na tym samym interfejsie, upewnij się że oba adresy IP są skonfigurowane w IP Traffic Control.*

D. Przydzielanie pasma po adresie MAC

Możesz określić maksymalną prędkość dla IP używając opcji MAC Control.

Poniżej znajduje się procedura dla ustawień MAC Traffic Control

1. Upewnij się, że opcja "Interface Traffic Control" jest wyłączona
2. Sprawdź komunikat i upewnij się, jakiego typu adresy są obsługiwane. W zależności od trybu te komunikaty będą się różniły.
3. Włącz opcje MAC Control

Note: Only the Wireless LAN side client MACs are supported ←

Enable MAC control

Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	004F60111111	512 kbps	1024 kbps	VIP Subscriber

Save Reset

Current MAC control table:

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:4f:60:11:11:11	512	1024	VIP Subscriber	<input type="checkbox"/>

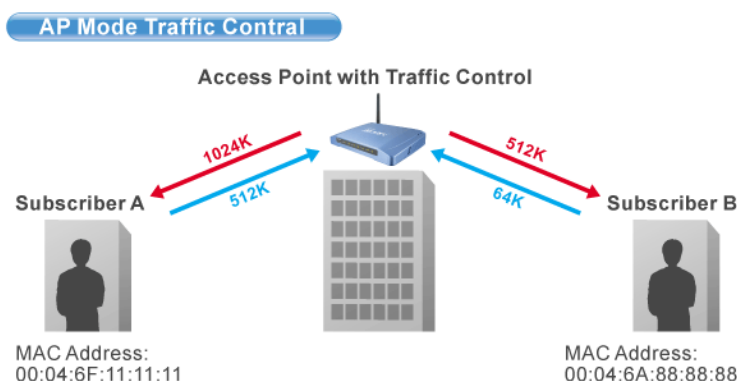
Delete Selected Delete all Reset

4. Jeżeli masz już zdefiniowane reguły wybierz jedną z nich. Prędkość "Out Rates" zostanie automatycznie zaimportowana z reguły. W przypadku importu reguły nie ma możliwości edycji wartości prędkości.
5. Jeżeli chcesz zdefiniować nową prędkość, proszę nie wybierać żadnej reguły. Teraz możesz wprowadzić odpowiednią wartość dla "LAN", "WLAN", lub "WAN" Out Rates.
6. Wciśnij "Save" aby zapisać
7. Zrób Reboot twojego AP.

**Jeżeli chcesz ustawić ograniczenie prędkości pomiędzy adresami MAC na tym samym interfejsie, upewnij się że oba adresy MAC są skonfigurowane w MAC Traffic Control.*

Przykłady zastosowania

Przykład: Kontrola Ruchu w trybie AP



Urządzenie AP jest zainstalowane na zewnątrz w celu udostępniania Internetu. Usługodawca WISP gwarantuje dwa różne typy usługi:

- **Usługa VIP :**
 - Wysłanie: 512 Kbps
 - Pobieranie: 1024 Kbps
- **Usługa Regular:**
 - Wysłanie: 64 Kbps
 - Pobieranie: 512 Kbps

Informacje o użytkownikach są następujące:

- Użytkownik A
 - Usługa VIP
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6F:11:11:11
- Użytkownik B
 - Usługa Regular
 - MAC Adres komputera PC lub klienta Bezprzewodowego: 00:04:6A:88:88:88

Konfiguracja Krok Po Kroku

1. Proszę wyłączyć "Interface Traffic Control"
2. Proszę dodać reguły "VIP" i "Regular" tak jak na rysunku poniżej

Policy Name	LAN Out Rate	WLAN Out Rate	Comment
VIP	512 kbps	1024 kbps	VIP Subscriber

Policy Name	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	512	1024	VIP Subscriber	<input type="checkbox"/>
Regular	64	512	Regular Subscriber	<input type="checkbox"/>

3. Proszę włączyć "MAC Control"
4. Obie reguły powinny dodać się tak jak na rysunku poniżej

Note: Only the Wireless LAN side client MACs are supported.

Enable MAC control

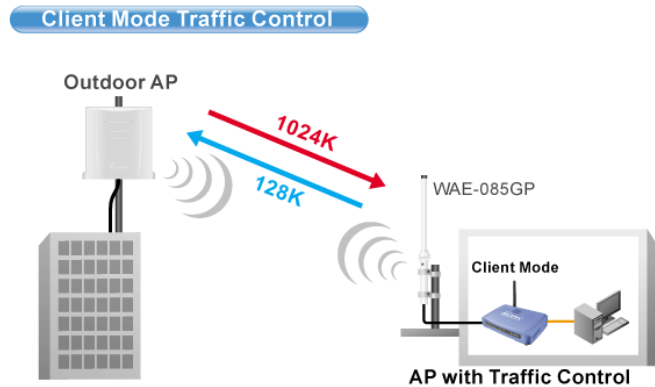
Policy Name	MAC	LAN Out Rate	WLAN Out Rate	Comment
VIP	00:04:6f:11:11:11	512 kbps	1024 kbps	Subscriber A
Regular	00:4f:6a:88:88:88	64 kbps	512 kbps	Subscriber B

Policy Name	MAC Addr	LAN Rate (Kbps)	WLAN Rate (Kbps)	Comment	Select
VIP	00:04:6f:11:11:11	512	1024	Subscriber A	<input type="checkbox"/>
Regular	00:4f:6a:88:88:88	64	512	Subscriber B	<input type="checkbox"/>

5. Proszę zrobić Reboot AP

Przykład 2: Kontrola Ruchu w trybie Klient

Urządzenie pracuje jako klient w topologii usługodawcy WISP. Usługodawca chce ograniczyć pasmo pobierania do 1024K i wysyłania do 128K.



Konfiguracja Krok Po Kroku

NOTE: Interface control has priority over IP/MAC. If you intend to use IP/MAC traffic control, you must disable interface control.

Interface Traffic Control	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAN Output Rate	<input type="text" value="1024"/>	kbps
WLAN Output Rate	<input type="text" value="128"/>	kbps
<input type="button" value="Save"/>	<input type="button" value="Reset"/>	

1. Proszę włączyć "Interface Traffic Control"
2. Wpisać "1024" w polu "LAN Output Rate"
3. Wpisać "128" w polu "WLAN Output Rate"
4. Wcisnąć "Save"
5. Zrobić Reboot AP

Status

System - w tej zakładce znajdują się ważne podstawowe informacje takie jak wersja oprogramowania oraz status interfejsów WL-5460AP.

The screenshot shows the 'System Data' page of the Air Live WLAN Access Point. The page is divided into three main sections: System, Wireless, LAN Configuration, and Internet Configuration. Each section lists various parameters and their values.

System Data

System

- Uptime: 0day:2h:0m:57s
- Firmware Version: 5470AP_e17_eu_b2

Wireless

- Mode: AP
- Physical Address: 00:4f:62:23:4b:48
- Band: 2.4 GHz (B+G)
- SSID: airlive
- Channel Number: 11
- Encryption: Disabled
- Associated Clients: 0
- BSSID: 00:4f:62:23:4b:48

LAN Configuration

- Connection Method: Fixed IP
- Physical Address: 00:4f:62:23:4b:48
- IP Address: 192.168.100.252
- Network Mask: 255.255.255.0
- DHCP Server: OFF
- DHCP Start IP Address: 192.168.100.100
- DHCP Finish IP Address: 192.168.100.200

Internet Configuration

- Connection Method: DHCP
- Physical Address: 00:4f:62:23:4b:49
- IP Address: 192.168.1.42
- Network Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Refresh

Przyciskiem „Refresh” możemy odświeżyć status. Funkcja przydatna podczas próby pozyskania połączenia.

Statistics - w tej zakładce uzyskamy informacje o ilości wysłanych (sent) i odebranych (receive) pakietów na danym interfejsie urządzenia WL-5460AP.

The screenshot shows the 'Statistics' page of the Air Live WLAN Access Point. The page displays a table with network statistics for Wireless LAN, Ethernet LAN, and Ethernet WAN. Each interface has two rows: Sent Packets and Received Packets.

Statistics

Wireless LAN	Sent Packets	213
	Received Packets	434
Ethernet LAN	Sent Packets	1451
	Received Packets	22529
Ethernet WAN	Sent Packets	782
	Received Packets	9587

Refresh

Active Clients - w tej zakładce uzyskamy informacje o podłączonych klientach bezprzewodowych.

WLAN Access Point

Mode | Status | TCP/IP | Reboot | Other

System / Statistics / Active Clients

Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Signal
00:1c:bf:20:7b:cc	6	80	54	yes	25

Refresh

MAC Address - adres fizyczny podłączonego urządzenia radiowego

Tx Packet - ilość wysłanych pakietów

Rx Packet - ilość odebranych pakietów

Tx Rate - prędkość połączenia

Power Saving - urządzenie obsługuje tryb oszczędzania energii

Signal - poziom siły sygnału. Wartość optymalna to minimum 25

Przycisk „Refresh” odświeży informacje.

TCP/IP

WLAN Access Point

Mode | Status | TCP/IP | Reboot | Other

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc...

IP Address: 192.168.100.252

Subnet Mask: 255.255.255.0

DHCP: Server Server IP: 0.0.0.0

DHCP Client Range: 192.168.100.100 - 192.168.100.200 Show Client

DHCP Leased Time: 86400 (sec 86400sec is a day.)

Clone MAC Address: 000000000000

Disable Ping

Port Number: 80

Apply Changes Reset

IP Address - adres IP urządzenia WL-5460AP

Subnet Mask - maska podsieci

DHCP - możliwe ustawienia to:

- Disable oznacza że urządzenie nie przydziela i nie pobiera adresów IP
- Client oznacza że urządzenie samo pobierze sobie adres od innego serwera DHCP
- Server oznacza że urządzenie będzie przydzielało adresy IP innym urządzeniom w sieci

DHCP Client Range - oznacza zakres z jakiego WL-5460AP będzie przydzielało adresy IP. Możemy ustawić np. 192.168.100.100 do 192.168.100.105 i tylko 5 komputerów w naszej sieci dostanie adresy IP.

Show Client - opcja umożliwia uzyskanie informacji jaki adres IP dla danego MAC zaferował serwer DHCP

DHCP Leased Time - to czas dzierżawy adresu IP od serwera DHCP. Po tym czasie dany adres MAC ponownie poprosi o przydzielenie adresu IP. Domyślnie czas dzierżawy ustawiony jest na 1 dzień.

Clone MAC Address - umożliwia ręczną zmianę adresu MAC interfejsu LAN

Disable Ping - załączenie opcji umożliwi odrzucanie pakietów ICMP

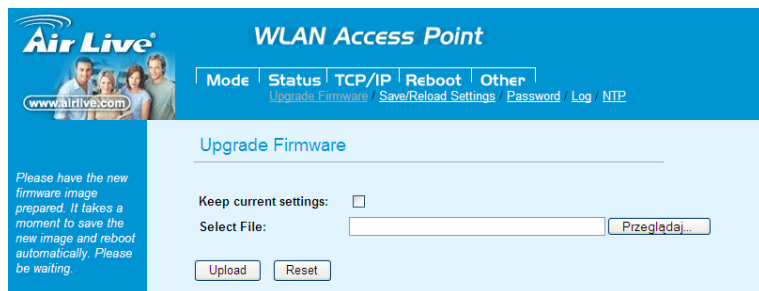
Port Number - opcja pozwala na zmianę portu którego używamy do zarządzania urządzeniem WL-5460AP od strony lokalnej LAN.

Reboot

Reboot oznacza restart urządzenia równoznaczny z wyłączeniem zasilania. Zmiana niektórych parametrów w WL-5460AP wymaga restartu. Dopiero po nim wprowadzone zmiany zaczynają działać. Wcisnięcie i natychmiastowe puszczenie przycisku „reset” na tylnym panelu WL-5460AP również wywołuje restart urządzenia.

Other

Firmware Upgrade - to funkcja która umożliwia nam aktualizację oprogramowania.



Aby zaktualizować oprogramowanie należy kliknąć na „Przełączaj” i wskazać rozpakowany plik xxxx.bin.

Keep current settings - jeśli zaznaczymy to pole oprogramowanie zaktualizuje się i zachowa wszystkie poprzednie ustawienia konfiguracyjne.

Klikamy „Upload” ..Urządzenie samo wykona restart i po około minucie będzie gotowe do pracy. Znakiem rozpoznawczym gotowości urządzenia do pracy jest ustanie aktywności diody „Status”.

Save/Reload Settings - pozwala na zapisywanie i wgrywanie pliku z konfiguracją urządzenia.

Save Settings to File - pozwala zapisać plik konfiguracyjny na dysku

Load Settings from File - pozwala wgrać zapisany plik konfiguracyjny

Reset Settings to Default - to opcja która pozwala przywrócić ustawienia fabryczne.

Password - umożliwia zmianę hasła dostępu do panelu zarządzania WL-5460AP. Login to zawsze „admin”.

New Password - tu wpisz nowe hasło

Confirmed Password - tu wpisz ponownie hasło w celu potwierdzenia zgodności znaków

Po zatwierdzeniu wyskoczy okienko logowania. Użyj loginu „admin” i swojego nowego hasła aby ponownie zalogować się do urządzenia.

Log - tu znajdziemy wszystkie informacje systemowe

System Log

This page can be used to set remote log server and show the system log.

Enable Log

System all Wireless only

```

0day 00:00:41 (none) kern.info klogd: br0: topology change detected,
propagating
0day 00:00:41 (none) kern.info klogd: br0: port 1(eth0) entering learning state
0day 00:00:41 (none) kern.info klogd: br0: port 1(eth0) entering forwarding
state
0day 00:00:41 (none) kern.info klogd: br0: topology change detected,
propagating
0day 00:00:51 (none) kern.warn klogd: eth1:phy is 8201
0day 00:00:53 (none) kern.info udhcpd: udhcp client (v0.9.9-pre) started
0day 00:01:00 (none) kern.debug udhcpd: Sending select for 192.168.1.42...
0day 00:01:00 (none) kern.info udhcpd: Lease of 192.168.1.42 obtained, lease
time 86400
  
```

Enable Log - załącza mechanizm sczytywania informacji systemowych

System All - pokazuje wszystkie informacje systemowe

Wireless only - pokazuje tylko informacje systemowe dotyczące modułu bezprzewodowego

„Refresh” odświeża stronę. „Clear” czyści wszystkie dotychczasowe informacje systemowe. Po restarcie urządzenia wszystkie informacje systemowe są zapisywane od nowa.

NTP - sieciowy protokół odpowiadający za synchronizację czasu.

Time Zone Setting

Current Time: Year 2000 Month 1 Day 1 Hr 0 Min 19 Sec 30

Enable NTP client update

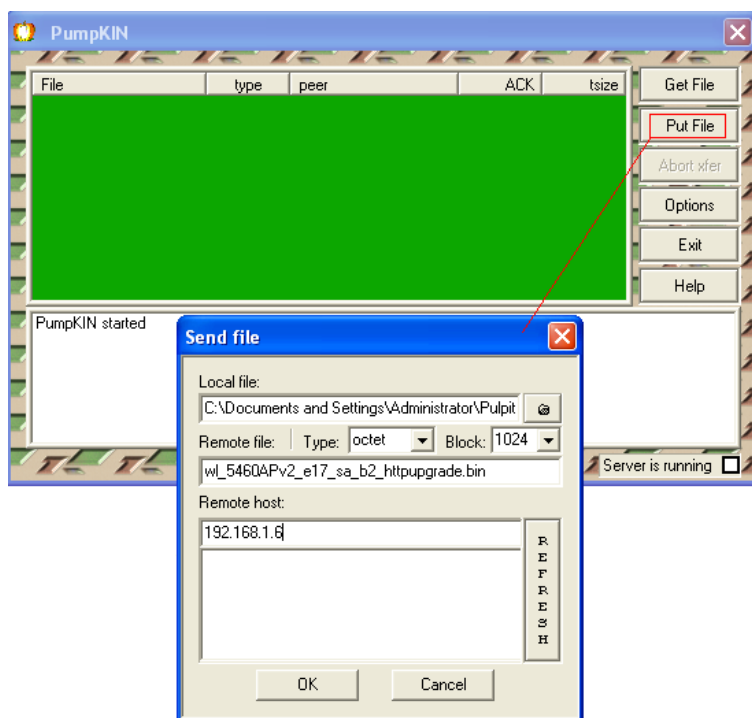
Time Zone Select: (GMT+08:00)Taipei

NTP server: 192.5.41.41 - North America (Manual IP Setting)

Czas możemy ustawić ręcznie poprzez opcję „Current Time”. Lub ustawić serwer NTP (Enable NTP client update) z którego czas będzie pobierany automatycznie.

Tryb Serwisowy

Jeżeli WL-5460AP uległo uszkodzeniu możemy sami spróbować naprawić urządzenie. Zanim włączymy zasilanie wciskamy przycisk „Reset” na tylnym panelu. Gdy reset jest zwarty wpinamy zasilanie. Po 3 sekundach puuszczamy przycisk „Reset”. Po tej czynności urządzenie znajduje się w trybie serwisowym na adresie 192.168.1.6. Na karcie sieciowej w komputerze ustawiamy ręcznie adres IP np. 192.168.1.100. Uruchamiamy program TFTP (np. Klever Pumpkin <http://kin.klever.net/pumpkin/binaries>) i wrzucamy na adres 192.168.1.6 standardowe oprogramowanie. Po około 2 minutach urządzenie samo uruchomi się i będzie gotowe do pracy.



5. Specyfikacja Techniczna

Opis	AP, Bridge(Most),Klient, Universal Repeater Obsługa Trybu WISP Klient Router Obsługa Trybu WISP + Repeater Odkręcana Antenka, 2 porty LAN 802.1x, WPA, WPA2, Zarządzanie Web 4 - Stopniowa Regulacja Mocy Mechanizm Watchdog (ICMP) Separacja Klientów Radiowych ACK Timeout DHCP Relay Ochrona Stacji 802.11g				
Specyfikacja Sprzętowa	LAN 2 x 10/100Mbps Pamięć: 2MB Flash, 16MB SDRAM				
Antena	Odkręcana Antenka 2dBi Możliwość instalacji anteny zewnętrznej Typ złącza R-SMA (Reverse SMA)				
Zakres Częstotliwości	USA (FCC) 11 Kanałów: 2.412GHz~2.462GHz Europa (ETSI) 13 Kanałów: 2.412GHz~2.483GHz Japonia (TELEC) 14 Kanałów: 2.412GHz~2.483GHz				
Czułość Rx@25°C	IEEE 802.11b	Min (dBm)	1Mbps	-91	
			2Mbps	-90	
			5Mbps	-90	
			11Mbps	-86	
	IEEE 802.11g	Min (dBm)	6Mbps	-87	
			9Mbps	-87	
			12Mbps	-86	
			18Mbps	-84	
			24Mbps	-82	
			36Mbps	-78	
			48Mbps	-73	
			54Mbps	-70	
	Rodzaje Modulacji	11g Prostokątne Podział Multipleksowania Częstotliwości (64QAM, 16QAM, QPSK, BPSK) 11b Kierunkowe Sekwencje Rozpiętości Spektrum (CCK, DQPSK, DBPSK) Wielkość Transmisji: 54, 48, 36, 24, 18, 11, 5.5, 2, 1 Mbps			
	Moc Wyjściowa	18dBm Regulacja w czterech poziomach			
Tryb WISP	Obsługa Autoryzacji ISP: DHCP, PPTP, L2TP, PPPoE Funkcja Klienta Bezprzewodowego jako WAN				
Zabezpieczenia	64/128bit WEP Obsługa WPA/WPA2-PSK Obsługa Radius 802.1x Obsługa WPA w trybie AP/WDS				
Konfiguracja	Zarządzanie Web WDS (Bridge, Klient, Repeater) Ukrywanie ESSID Obsługa 802.1x Kontrola Dostępu Adresów MAC Tablica Adresów MAC Separacja Klientów Radiowych Ustawiane SSID, Kanały, Próg RTS, Fragmentowanie Progu				
Zasilanie	DC 12V				
Zgodność EMI	FCC, CE				
Waga	180g				
Wymiary	135 x 100 x 26 mm				