

Technologie sieciowe 2

Autor:

Tymon Tobolski (181037)

Jacek Wieczorek (181043)

Prowadzący:

Dr inż. Arkadiusz Grzybowski

Wydział Elektroniki

III rok

Pn TN 11.15 - 13.00

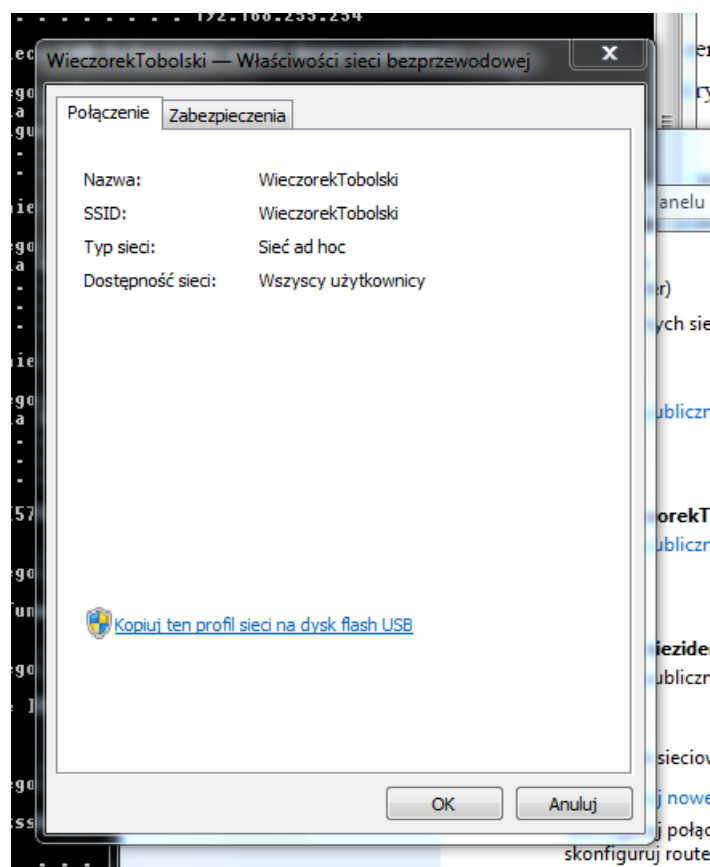
15 stycznia 2012

1 Cel laboratorium

Celem laboratorium było zapoznanie się z podstawowymi problemami związanymi z budową bezprzewodowej sieci LAN pracującej w standardzie IEEE 802.11 b/g/n.

2 Konfiguracja sieci typu ad hoc

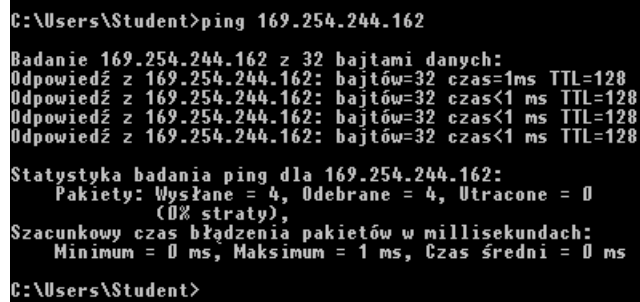
Konfiguracja sieci ad hoc w systemie Windows 7 jest intuicyjna i nie stanowi żadnego problemu.



Rysunek 1: Skonfigurowana sieć typu ad hoc

Rysunek 1 przedstawia podstawową konfigurację sieci bezprzewodowej typu ad hoc, której nadaliśmy nazwę *WieczorekTobolski* oraz takie samo SSID.

W celu weryfikacji poprawności połączenia, wykonana została komenda ping:



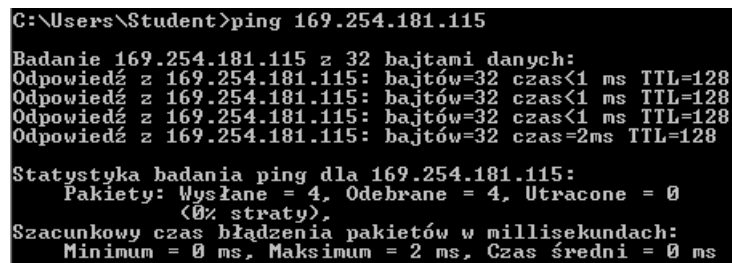
```
C:\Users\Student>ping 169.254.244.162

Badanie 169.254.244.162 z 32 bajtami danych:
Odpowiedź z 169.254.244.162: bajtów=32 czas=1ms TTL=128
Odpowiedź z 169.254.244.162: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 169.254.244.162: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 169.254.244.162: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 169.254.244.162:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
              (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 0 ms, Maksimum = 1 ms, Czas średni = 0 ms

C:\Users\Student>
```

Rysunek 2: Komenda ping do użytkownika Tymon Tobolski



```
C:\Users\Student>ping 169.254.181.115

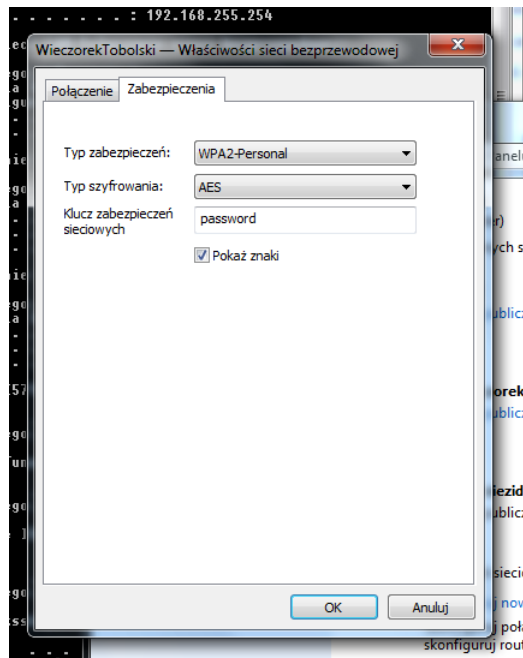
Badanie 169.254.181.115 z 32 bajtami danych:
Odpowiedź z 169.254.181.115: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 169.254.181.115: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 169.254.181.115: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 169.254.181.115: bajtów=32 czas=2ms TTL=128

Statystyka badania ping dla 169.254.181.115:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
              (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 0 ms, Maksimum = 2 ms, Czas średni = 0 ms
```

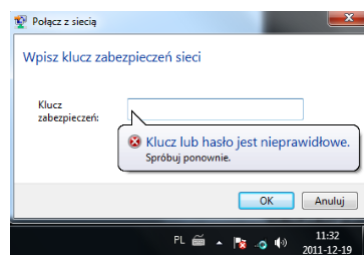
Rysunek 3: Komenda ping do użytkownika Jacek Wieczorek

Rysunki 2 i 3 przedstawiają pomyślne wykonanie komendy ping, weryfikujące połączenie pomiędzy dwoma użytkownikami.

W celu zabezpieczenia sieci ad hoc przed nieporządanym dostępem, ustawione zostało hasło:



Rysunek 4: Zabezpieczona sieć typu ad hoc



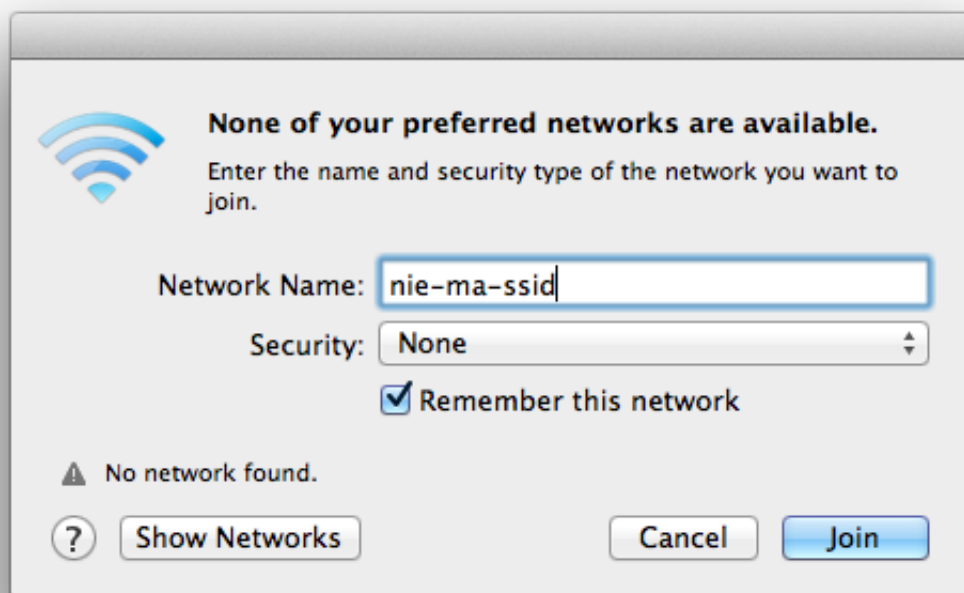
Rysunek 5: Źle wprowadzone hasło

Na Rysunku 4 przedstawiona została konfiguracja zabezpieczenia sieci hasłem dostępu, natomiast Rysunek 5 przedstawia próbę uzyskania nieautoryzowanego dostępu do sieci, która zakończyła się niepowodzeniem.

3 Sieć typu infrastrukturalnego

Konfiguracja podstawowych parametrów sieci bezprzewodowej w routerze Linksys WRT 150 jest prosta i intuicyjna. Wystarczy połączyć się z urządzeniem za pomocą kabla ethernetowego i ustawić podstawowe parametry, lub skorzystać z ustawień predefiniowanych.

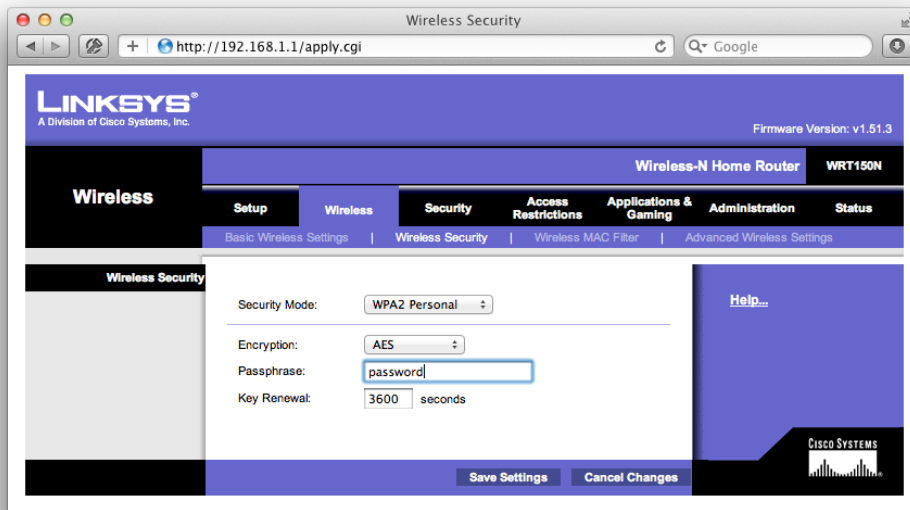
W celu połączenia się z siecią bezprzewodową należy podać prawidłową nazwę SSID.



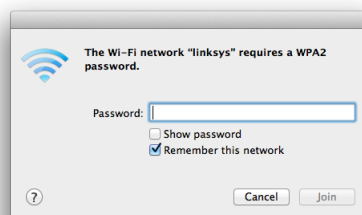
Rysunek 6: Nieprawidłowa nazwa SSID

Na Rysunku 6 przedstawiona została sytuacja, w której podano złe SSID, co uniemożliwiło połączenie z siecią. W celu weryfikacji połączenia pomiędzy komputerami, podobnie jak w poprzednim zadaniu, użyto komendy ping, której wynik w obu przypadkach był pozytywny.

Kolejnym etapem konfiguracji infrastrukturalnej sieci bezprzewodowej było zabezpieczenie jej hasłem dostępowym (Rysunek 7).



Rysunek 7: Konfiguracja zabezpieczenia sieci bezprzewodowej



Rysunek 8: Wymagane podanie hasła podczas próby podłączenia się do sieci

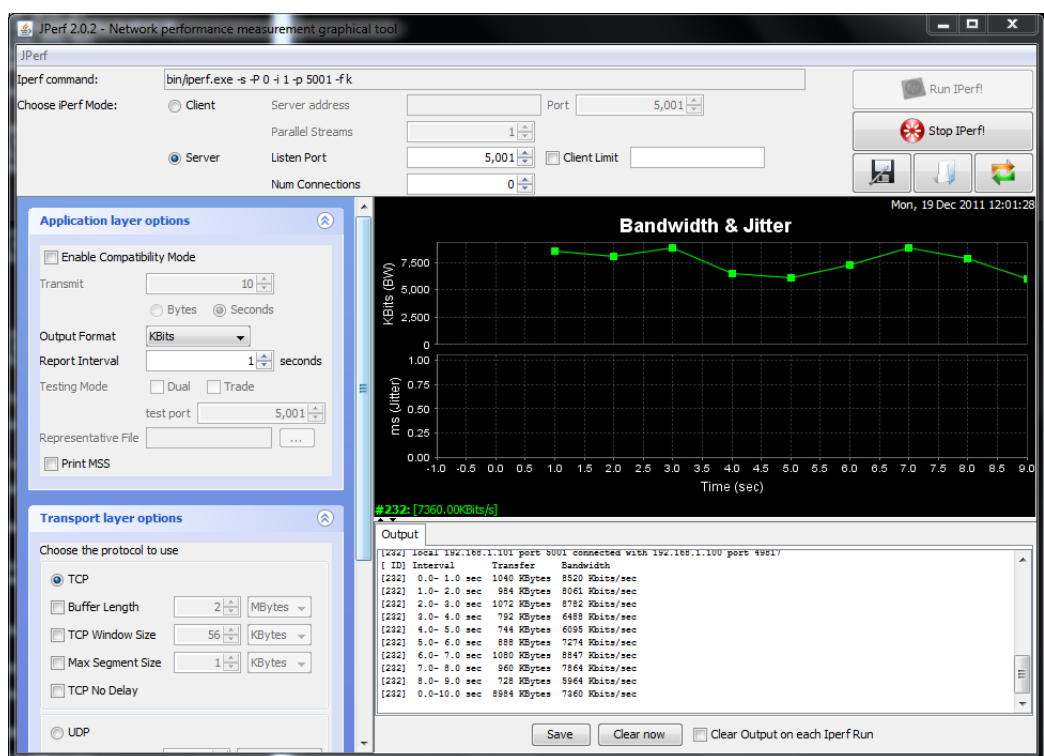
Rysunek 9 przedstawia sytuację, podczas której użytkownik próbował nawiązać połączenie z siecią bezprzewodową podając błędne hasło.



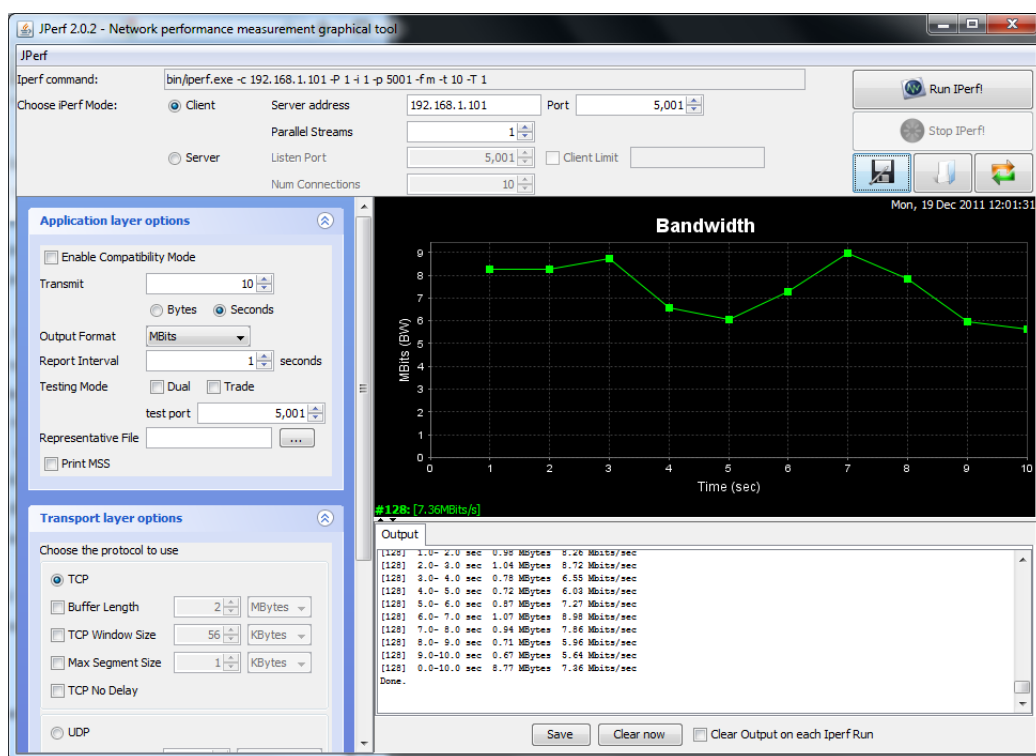
Rysunek 9: Próba nieautoryzowanego dostępu do sieci

Ostatnia część zadania polegała na zbadaniu wydajności połączenia za pomocą punktu dostępowego z wykorzystaniem programu Jperf, dla różnych rozmiarów przesyłanych danych, a także dla różnych warunków:

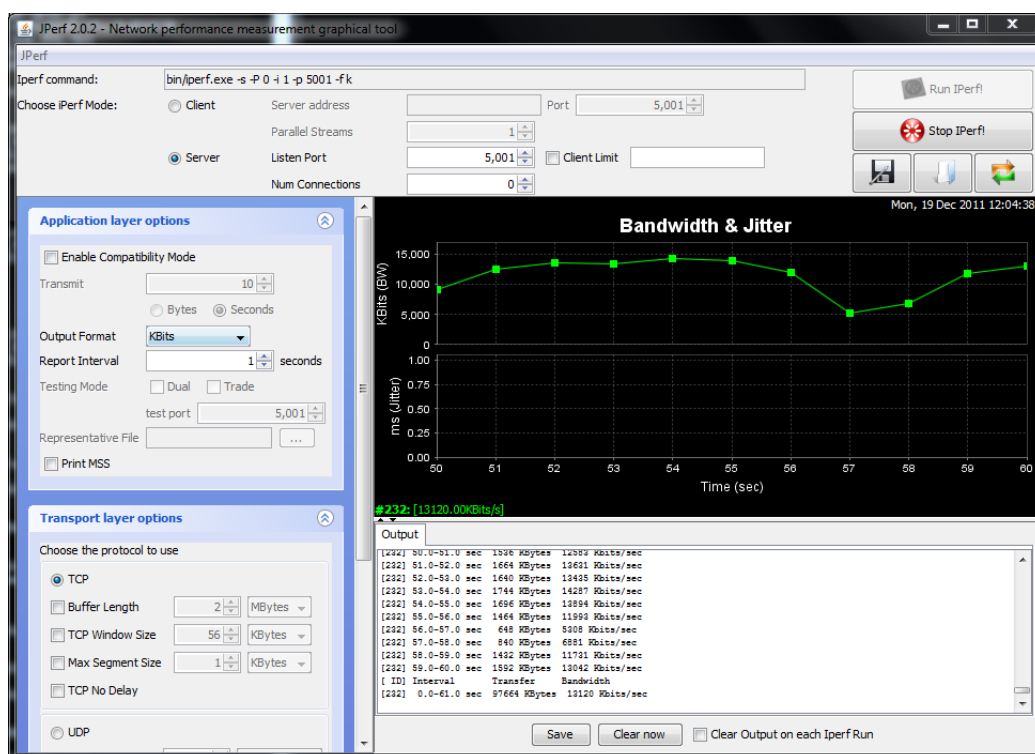
- połączenie szyfrowane i nieszyfrowane
- z przysłoniętą i odkrytą anteną punktu dostępowego



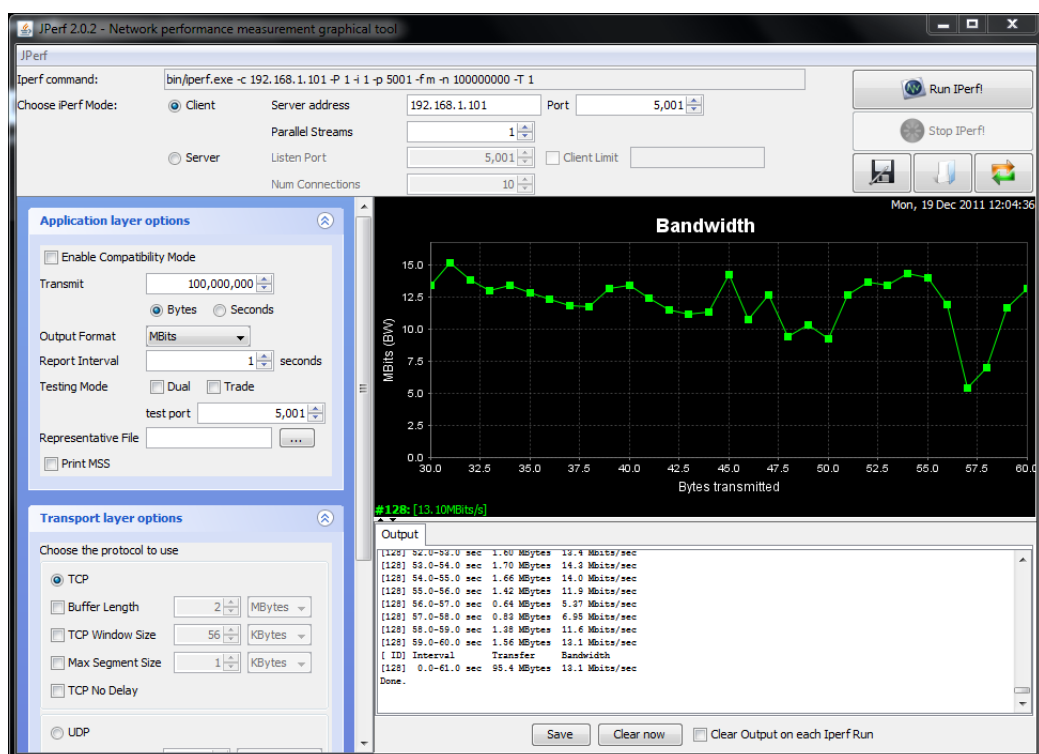
Rysunek 10: Połączenie nieszyfrowane - odbiorca



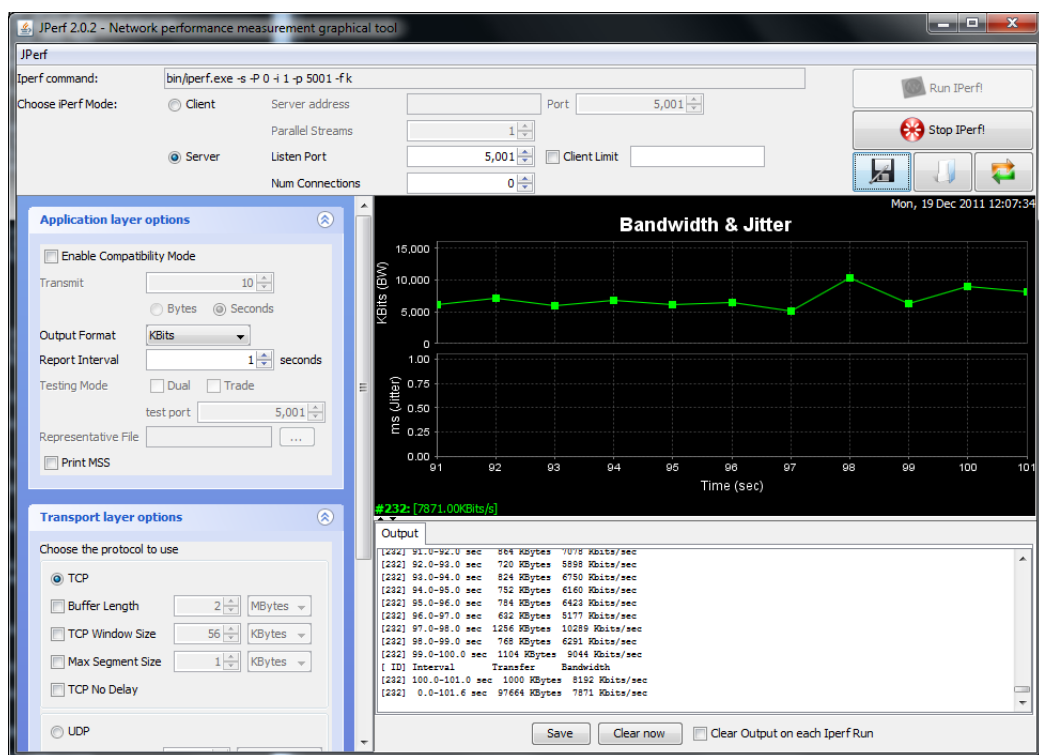
Rysunek 11: Połączenie nieszyfrowane - nadawca



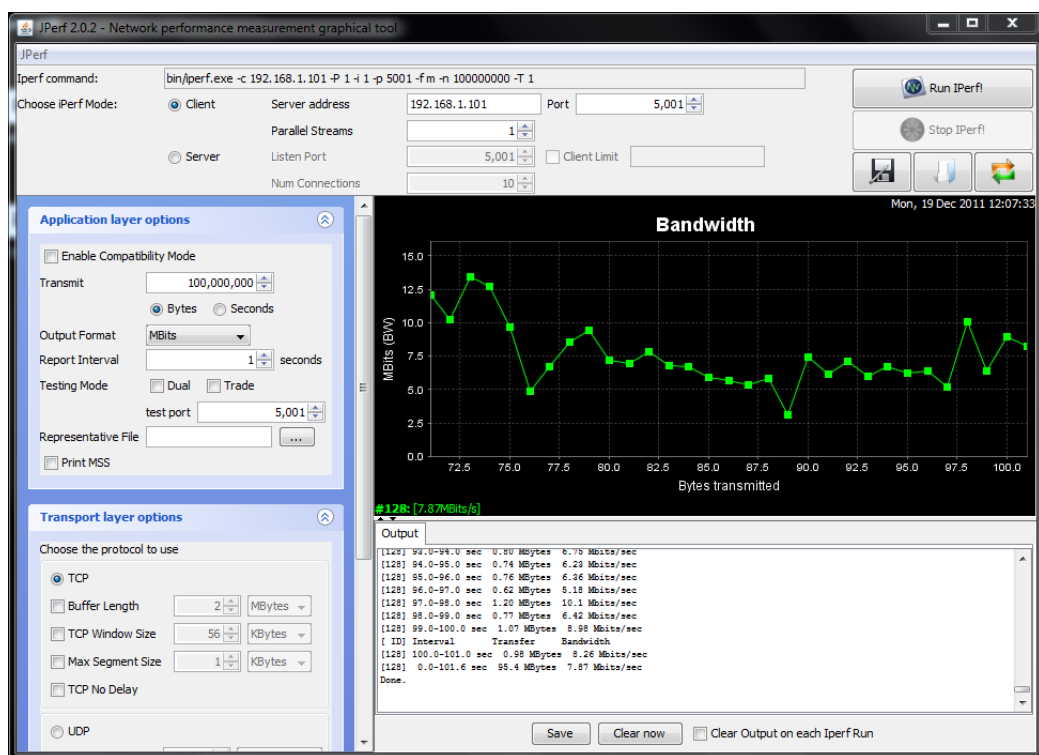
Rysunek 12: Połączenie nieszyfrowane, wielkość danych : 100mb - odbiorca



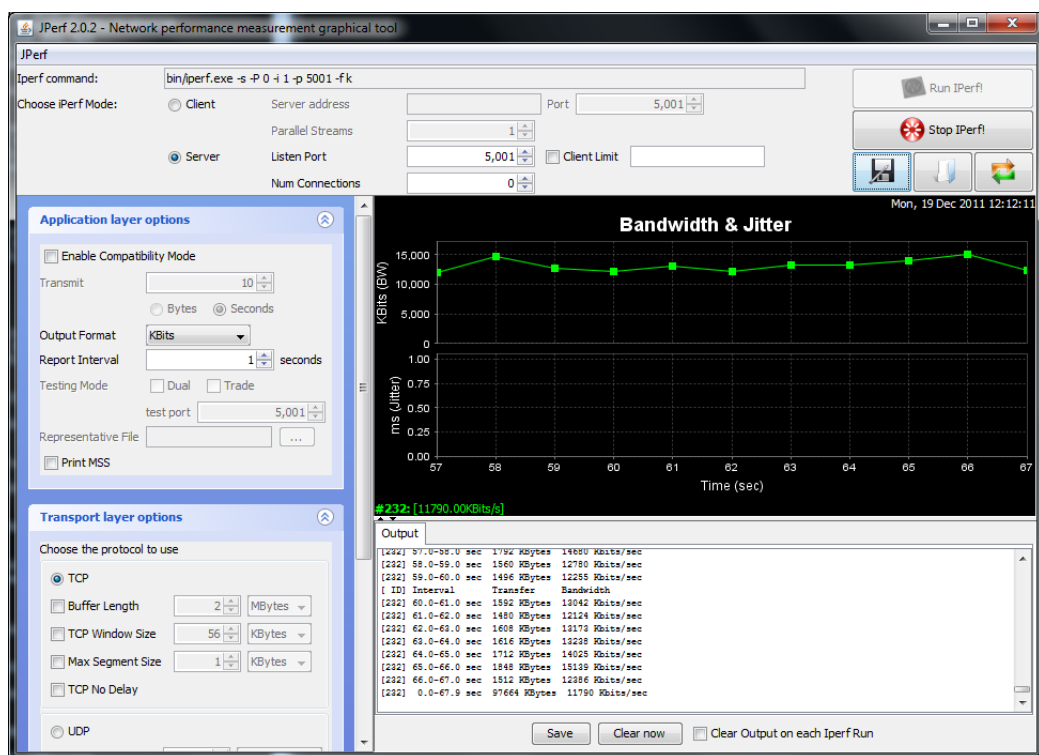
Rysunek 13: Połączenie nieszyfrowane, wielkość danych : 100mb - nadawca



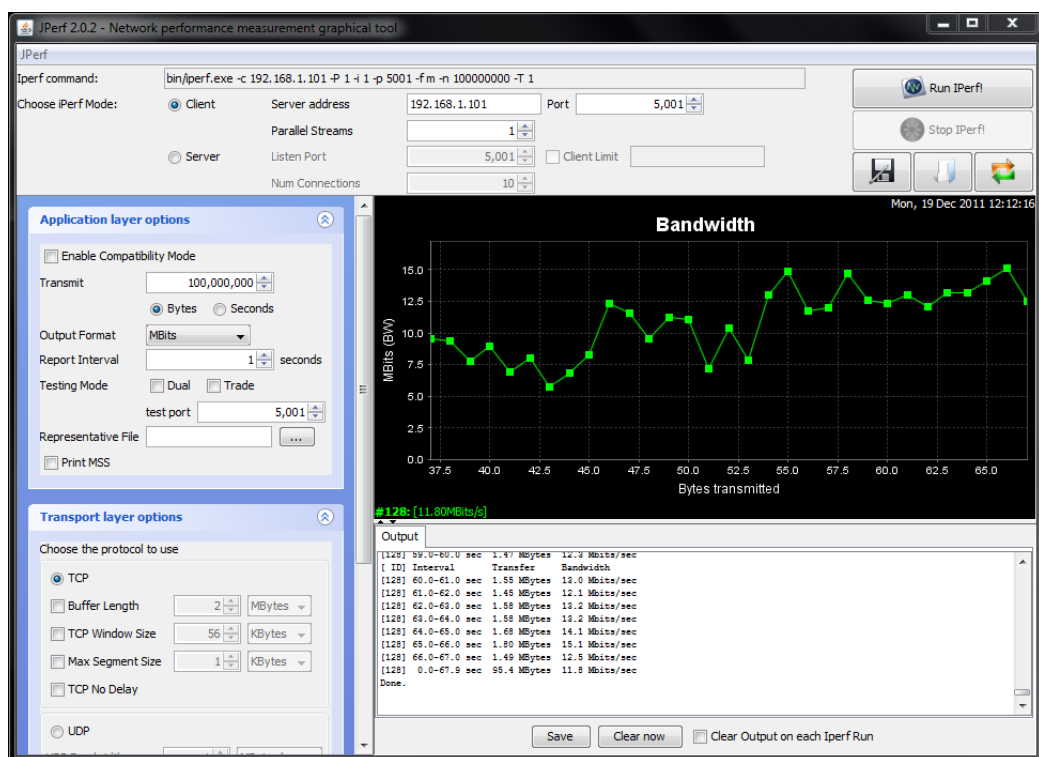
Rysunek 14: Połączenie nieszyfrowane, wielkość danych : 100mb, zakryta antena - odbiorca



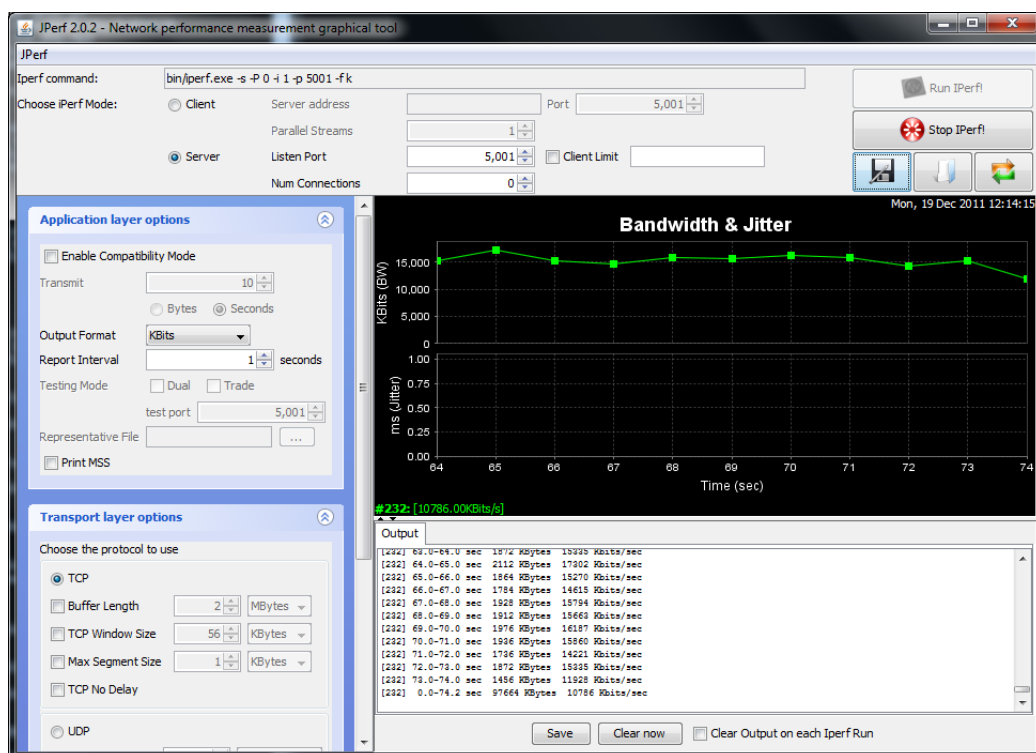
Rysunek 15: Połączenie nieszyfrowane, wielkość danych : 100mb, zakryta antena - nadawca



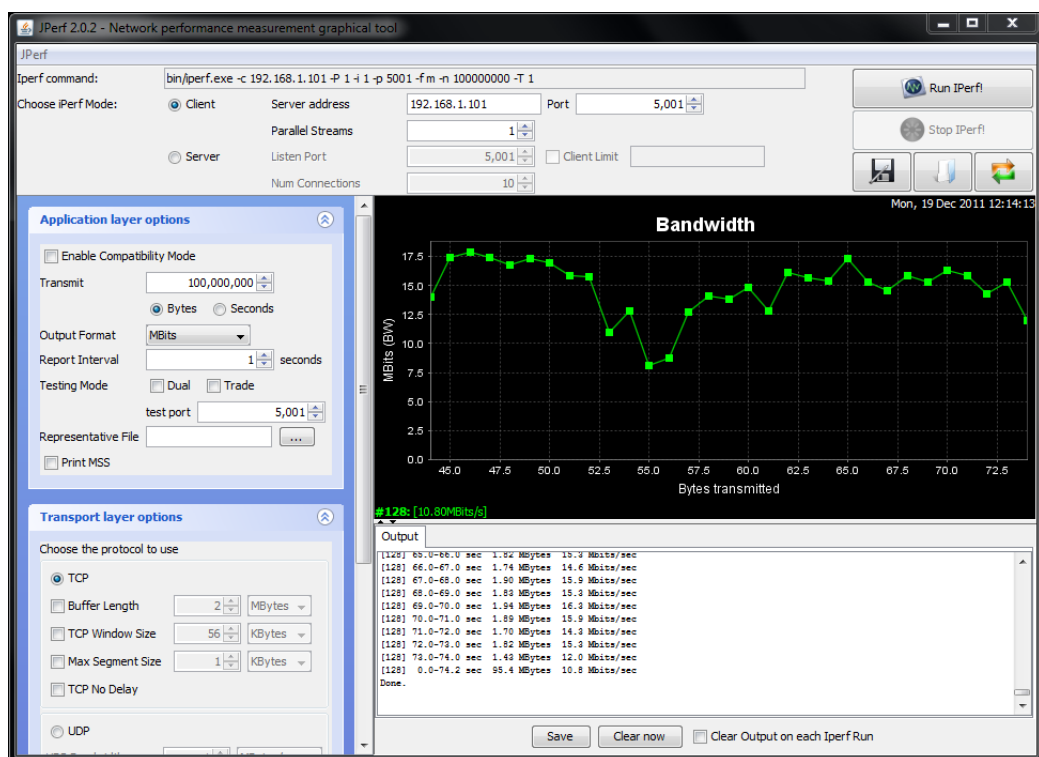
Rysunek 16: Połączenie szyfrowane, wielkość danych : 100mb, zakryta antena - odbiorca



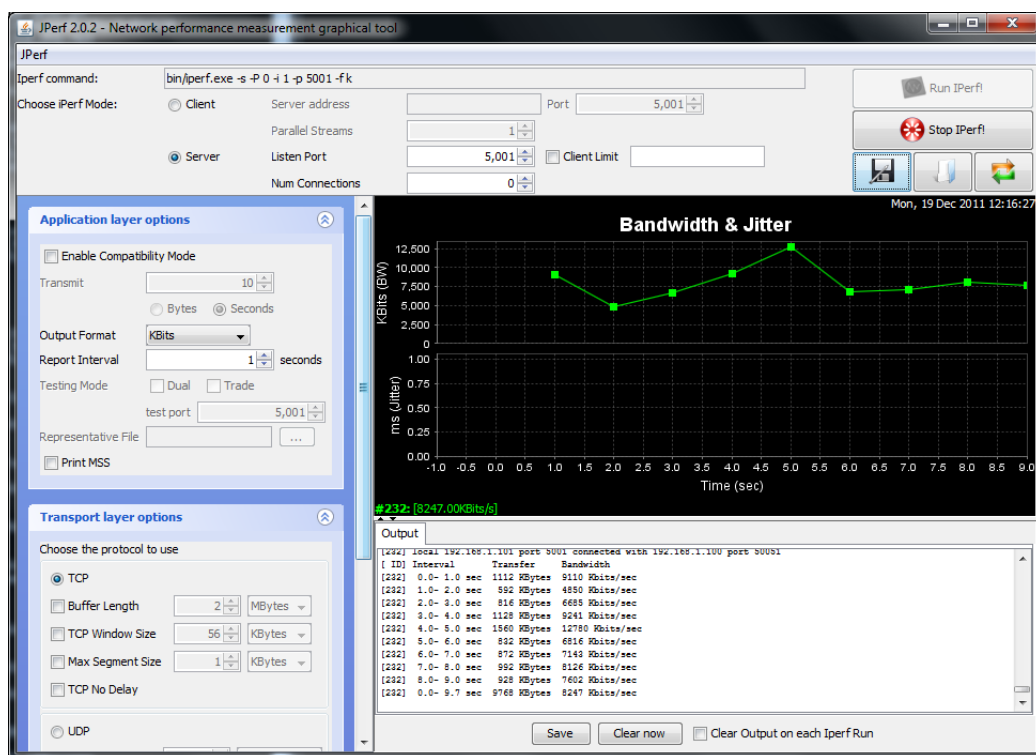
Rysunek 17: Połączenie szyfrowane, wielkość danych : 100mb, zakryta antena - nadawca



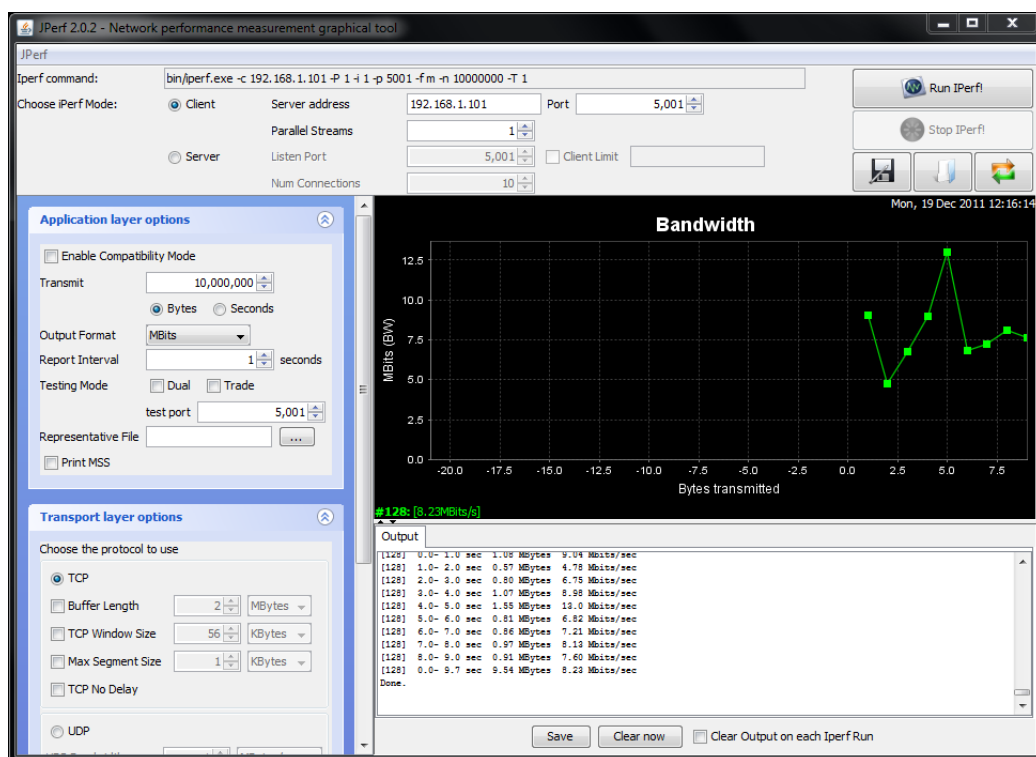
Rysunek 18: Połączenie szyfrowane, wielkość danych : 100mb, odkryta antena - odbiorca



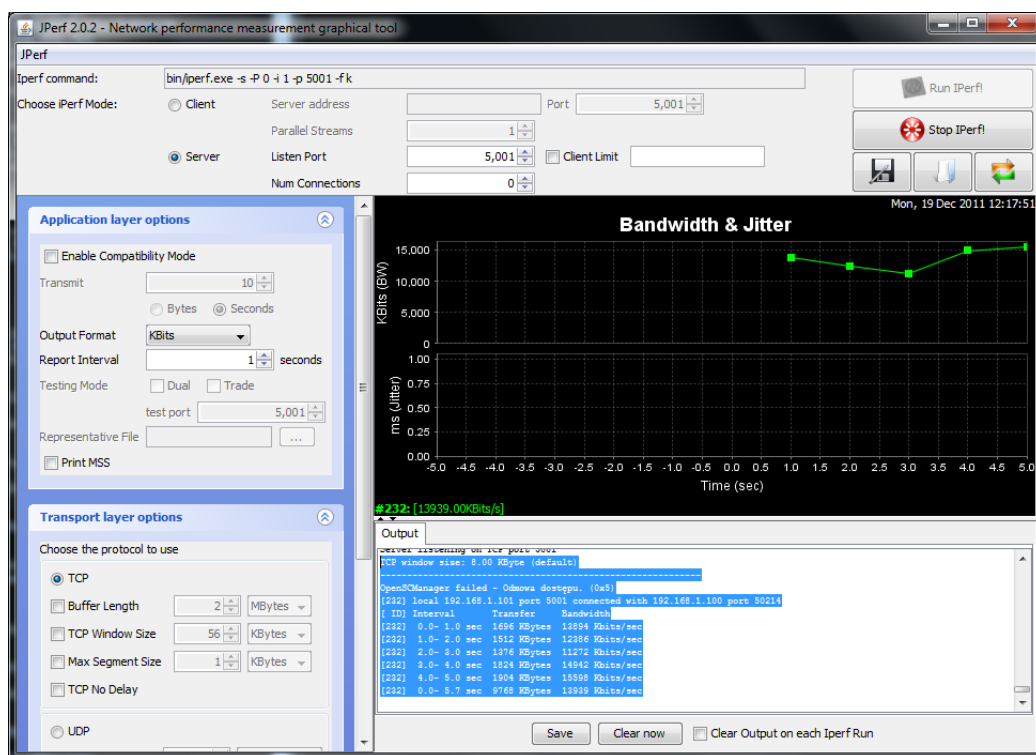
Rysunek 19: Połączenie szyfrowane, wielkość danych : 100mb, odkryta antena - nadawca



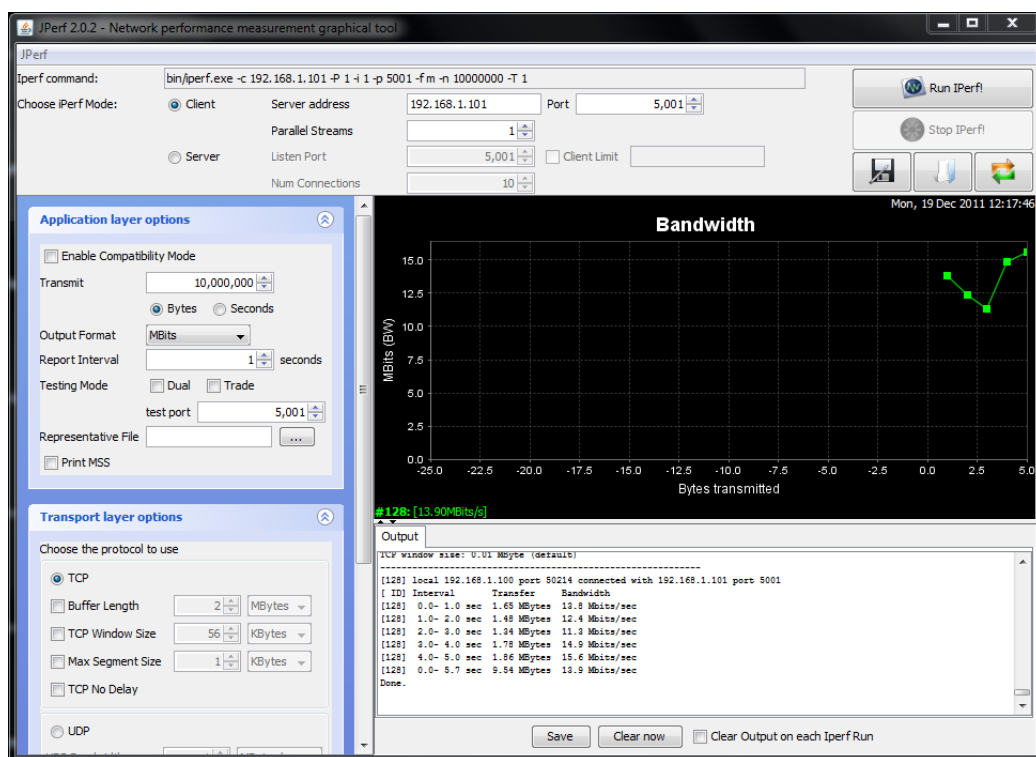
Rysunek 20: Połączenie szyfrowane, wielkość danych : 10mb, odkryta antena - odbiorca



Rysunek 21: Połączenie szyfrowane, wielkość danych : 10mb, odkryta antena - nadawca



Rysunek 22: Połączenie nieszyfrowane, wielkość danych : 10mb, odkryta antena - odbiorca



Rysunek 23: Połączenie nieszyfrowane, wielkość danych : 10mb, odkryta antena - nadawca

Rysunki od 10 do 23 przedstawiają wyniki pomiaru wydajności łącza dla różnych parametrów danych. Analizując przedstawione dane, zauważyliśmy iż wyniki symulacji w przedstawionych sytuacjach znacząco od siebie nie odbiegały. Bezpośredni wpływ na to miała odległość stacji roboczych od punktu dostępowego, która nie przekraczała 1m. By otrzymać wiarygodne dane, należałoby przeprowadzić testy dla stacji roboczych oddalonych o kilkanaście metrów od siebie i punktu dostępowego, najlepiej znajdujące się w osobnych pomieszczeniach. Niestety warunki panujące w laboratorium nie pozwoliły nam na przeprowadzenie takowych testów.

Badając zabezpieczenia sieci, trudno jest jednoznacznie określić najlepszy sposób ograniczenia dostępu. Na pewno nie jest nim wyłączenie broadcastu SSID, bo nawet wtedy istnieje możliwość w łatwy sposób przechwycenia identyfikatora sieci i uzyskania dostępu.

Listy ACL są dobrym rozwiązaniem w przypadku w miarę stałej grupy osób korzystających z sieci. Możemy wtedy indywidualnie nadawać uprawnienia i ograniczenia użytkownikom. Odbyna się to poprzez filtrowanie adresów MAC.

Szyfrowanie jest jedną z najlepszych metod zabezpieczenia sieci, gdy liczba użytkowników nie jest stała i pojawiają się nowi użytkownicy. Jednak poziom zabezpieczenia zależy od wybranego sposobu szyfrowania, co ma bezpośredni wpływ na łatwość złamania klucza i nieporządanego dostępu.

Połączenie typu ad hoc jest szybsze niż infrastrukturalne, ponieważ bazuje na bezpośrednim połączeniu dwóch stacji roboczych, eliminując pośrednika sieciowego jakim jest router.

Wykorzystanie szyfrowania nie ma znaczącego wpływu na szybkość transmisji, ponieważ narzuty informacji, w stosunku do rozmiaru pakietu, jest niewielki.

Rzeczywista prędkość transmisji jest niższa niż podana w standardzie, ponieważ zwiększenie ruchu sieciowego zwiększa również liczbę kolizji, a w rezultacie retransmisję pakietów. Gdy nie ma odpowiedzi od odbiorcy o otrzymaniu pakietu, następuje jego retransmisja. Czynnikiem pogorszającymi prędkość transmisji są również odległość od punktu dostępowego czy występowanie fizycznych przeszkód (ściany, drzwi), ilość stacji roboczych - im więcej, tym więcej kolizji w sieci.

Standard WiFi umożliwia transmisję na 14 różnych kanałach, lecz w Polsce wykorzystywanych jest jedynie 13. Częstotliwości kanałów nachodzą na siebie, co oznacza, że zupełnie niezależnych sieci jest tylko 5. Na danym obszarze może pracować do 14 sieci.

4 Wnioski

KOnfiguracja sieci bezprzewodowej przy użyciu współczesnych urządzeń nie jest skomplikowanym procesem. Dlatego na potrzeby stworzenia sieci domowej utworzenie sieci bezprzewodowej jest możliwe dla osób nieposiadających specjalistycznej wiedzy z tego zakresu.