

<i>Grupa ćwic.</i>	<i>Grupa lab.</i>	<i>Zespół</i>	<i>Data wykonania</i>	<i>Data odbioru</i>
<i>Nr ćwic.</i>	<i>Temat ćwiczenia</i> TCP			
<i>Imiona i nazwiska</i>				<i>Ocena i uwagi</i>

Wstęp:

Celem badania jest zapoznanie się z TCP oraz UDP. Przebieg wygląda następująco, skanowane będą dwa protokoły TCP oraz UDP na różnych zakresach adresów IP: 149.156.111.0/24 i 149.156.0.0/16. Na podstawie pliku wyjściowego programu Nmap dokonano analizy ilości znalezionych hostów, portów oraz ich stanu(otwarty, zamknięty, filtrowany, filtrowany|otwarty).

Skanowania:

-**sT** – skan TCP, wysyłający do drugiej strony prośbę o ustanowienie połączenia za pomocą wywołania usługi systemowej(system call) `connect`. Zamiast czytania pakietów-odpowiedzi, Nmap używa API(Berkely Socket API) to uzyskania informacji na temat każdej próby połączenia.

-**sU** – skan UDP wysyłający pakiet do każdego żadanego portu, najczęściej jest wysyłany pusty pakiet, chyba że sprecyzowano opcje Nmap. Jeśli port ICMP jest nieosiągalny, zwracany jest błąd (typ 3 kod 3) co oznacza że port jest zamknięty, typ 3, kod 0,1,9,10,13 – port jest filtrowany, jeśli nie uzyskano odpowiedzi zwrotnej port klasyfikowany jest jako otwarty|filtrowany natomiast w przeciwnym razie jest on otwarty.

Spotykane stany portów:

- **open** – port otwarty, host na bieżąco akceptuje połączenia TCP bądź datagramy UDP na tym porcie.

- **closed** – port zamknięty, jest dostępny a więc otrzymuje i wysyła z powrotem pakiety probe ale nikt nie nasłuchuje tego portu.

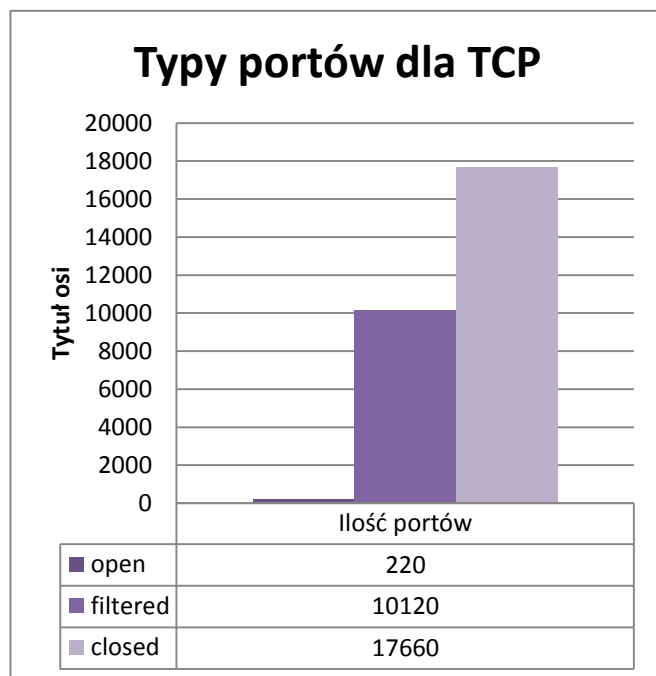
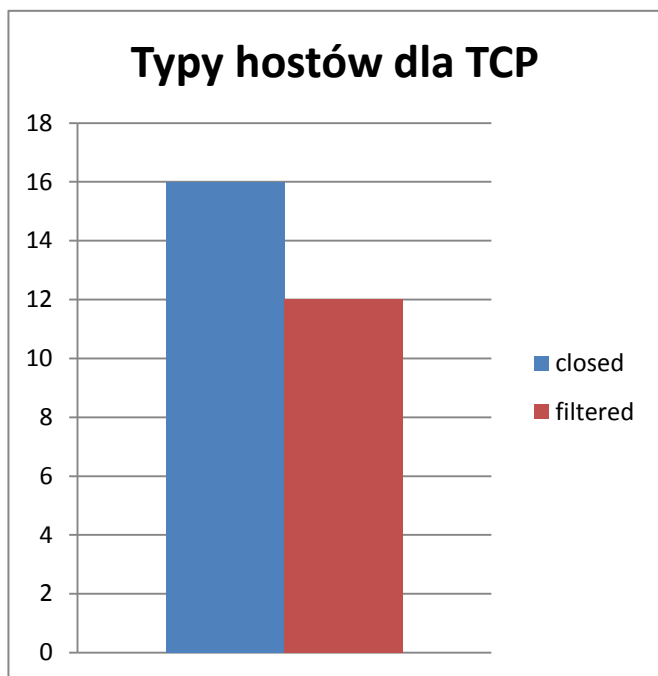
- **filtered** – port filtrowany, Nmap nie może określić czy port jest otwarty ponieważ filtrowanie zapobiega docieraniu przez pakiety próbne do portu.

- **open|filtered** – Nmap klasyfikuje w ten sposób porty, które są trudne do określenia czy są otwarte czy filtrowane. Dzieje się to w skanach w których otwarte porty nie wysyłają odpowiedzi.

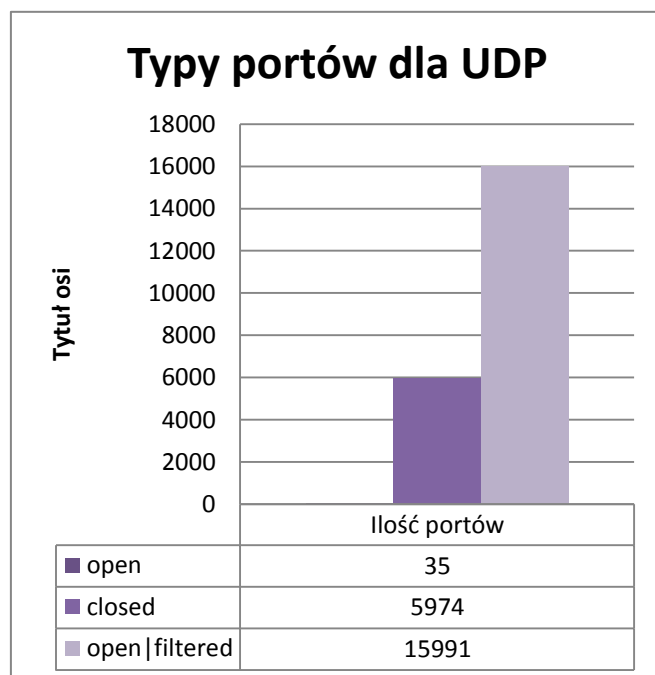
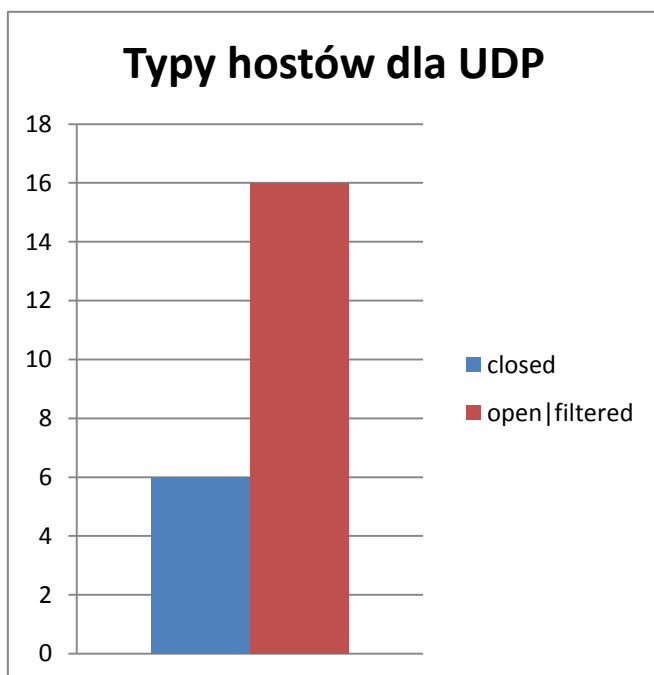
Dane i pomiary:

1. 149.156.111.0/24

TCP – łącznie 28 hostów, 1000 portów na hosta.

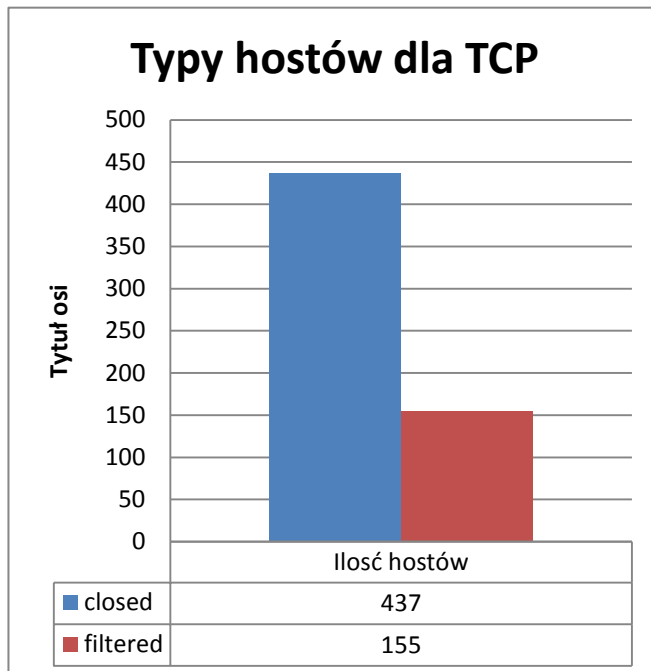


UDP – łącznie 22 hostów, 1000 portów na hosta.



2. 149.156.0.0/16

TCP – łącznie 592.



Niestety druga seria pomiarów nie jest miarodajna z dwóch powodów. Po pierwsze testy trwały tak długo, że nie byliśmy w stanie ich sfinalizować, po drugie z logu dla testu UDP nie uzyskano praktycznie żadnych statystyk poza informacją o tym, że niektóre hosty dają odpowiedź ale poza tym nie otrzymano żadnych statystyk na temat ilości i typu portów.

Podczas testów można było zauważyć pewną zależność, w dużej ilości przypadków wszystkie porty dla hosta były albo otwarte, otwarte|filtrowane lub zamknięte. Bardzo częstą sytuacją od takiego stanu było istnienie kilku pojedynczych portów na hoście które były otwarte/filtrowane bądź zamknięte w porównaniu do przeważającej reszty portów na hoście.

Analiz wyników:

Wnioski:

05-03-2016

Sprawozdanie z sieci komputerowych

Wifi

Wstęp

Celem naszego laboratorium było sprawdzenie zależności siły sygnału Wi-Fi od odległości a także wyszukanie na podstawie sygnału punktów dostępowych oraz ustalenia podstawowych parametrów znajdujących sieci

Nasze sprawozdanie dzieli się na dwie główne części, pierwsza poświęcona ogólnym informacją o sieciach na obu piętrach, druga analizująca Access Pointy, połączenie z daną siecią czy wyszukująca potencjalnie ciekawe sieci.

Do naszych testów wykorzystaliśmy aplikację Wifi Analyzer dostępną na platformę Android. Dla testu z połączeniem oraz bez wykorzystano dwa różne smartfony Huawei Ascend Y300 oraz Sony Xperia. Testowana były sieci Wi-Fi na piętrze 5 oraz 7 budynku B5 AGH.

Punkty pomiarowe piętro 5 i 7

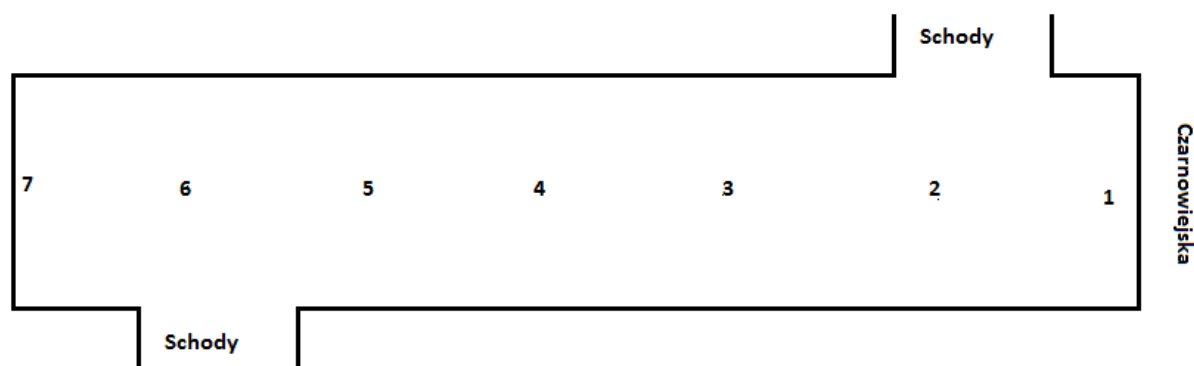
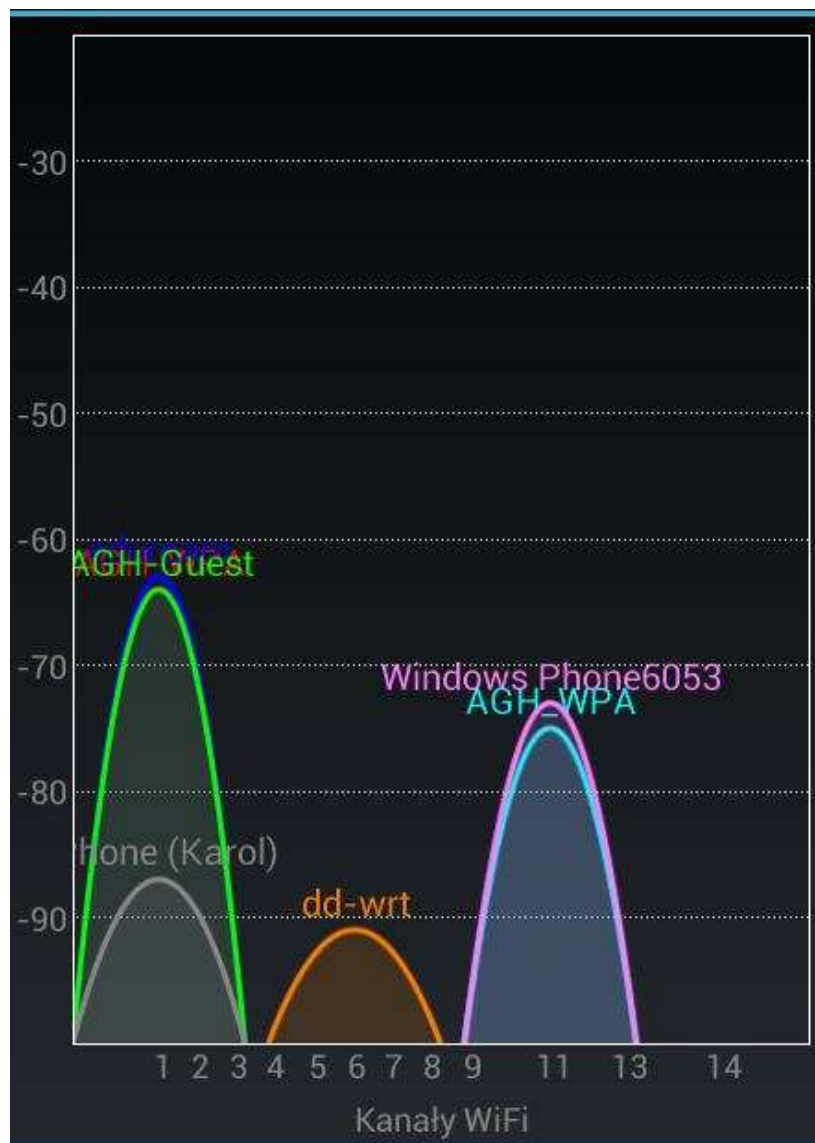


Diagram 1 - układ punktów pomiarowych na piętrze w budynku B5



Migawka 1-Rozkład sieci na 5 piętrze budynku B5 od strony parkingu AGH

Zebrane w ten sposób wyniki posłużyły do skonstruowania „mapy” dwóch pięter przedstawiających dwie sieci o najsilniejszym sygnale

Lista wszystkich wyszukanych sieci oraz ich parametry

SSID	Kanał	Adres MAC	Zabezpieczenia
NetGear 5GHz	44	c4:04:15:18:3a:b2	WPA2-PSK-CCMP WPS ESS
NetGear 2.4GHz	11	c4:04:15:18:3a:b3	WPA2-PSK-CCMP WPS ESS
SGS3 LTE	1	34:23:ba:9a:f2:1e	WPA-PSK-CCMP + TKIP ESS
ZIP-1	6	00:0f:55:6b:24:5c	ESS
	6	00:0f:66:90:7a:e8	ESS
dd-wrt	6	00:13:10:92:a6:c8	WPA2-PSK-CCMP + TKIP ESS
TP-LINIK_408	6	f8:1a:67:ed:f4:65	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP WPS ESS
AGH-Guest	1	00:23:33:2c:11:f0	ESS
AGH-Guest	1	00:23:33:2b:da:00	ESS
AGH-WPA	1	00:23::33:2c:11:f1	WPA-EAP-CCMP WPA2-EAP-CCMP ESS
	1	00:23:33:2b:da:01	WPA-EAP-CCMP WPA2-EAP-CCMP ESS
RezydencjaCzarnowiejska77	13	28:be:9b:d2:ed:f0	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
UPC Wi-Free	11	06:7c:34:b0:c7:e5	WPA-EAP-CCMP + TKIP WPA2-EAP-CCMP + TKIP ESS
	11	82:c6:ab:48:7d:df	WPA-EAP-CCMP + TKIP WPA2-EAP-CCMP + TKIP ESS
	13	2a:be:9b:d2:ed:f2	WPA-EAP-CMP + TKIP WPA2-EAP-CCMP + TKIP ESS
	11	8e:04:ff:7c:18:fd	WPA-EAP-CCMP + TKIP WPA2-EAP-CCMP + TKIP ESS
OpenWrt	1	56:e6:fc:b7:38:2f	ESS
eduroam	1	00:23:33:2c:11:f2	WPA-EAP-CCMP WPA2-EAP-CCMP ESS
	1	00:23:33:2b:da:02	WPA-EAP-CCMP WPA2-EAP-CCMP ESS
UPC0045475	11	80:c6:ab:48:7d:dd	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
ZIP407	1	54:e6:fc:b7:38:2e	WPA2-PSK-CCMP ESS
www.KlimatyzowanyDom.PL	3	f8:d1:11:21:ee:d0	WPA2-PSK-CCMP-preauth ESS
UPC123456	11	28:be:9b:06:09:38	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
UPC1383901	1	8c:04:ff:7c:18:fb	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
UPC243339347	1	34:7a:60:72:7a:9a	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
UPC0040683	6	00:26:24:3e:93:97	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
k121opl	11	00:1d:0f:fb:20:44	WPA2-PSK-CCMP-preauth ESS
TP-LINK_E9B0D0	1	54:e6:fc:e9:b0:d0	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP-preauth ESS

PhaseField@607	11	00:1d:7e:bc:9e:59	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP ESS
HaCiO	11	ec:1f:72:78:ef:6f	WPA2-PSK-CCMP ESS
Doktoranci KISiM	6	54:e6:fc:cb:b9:94	WPA2-PSK-CCMP + TKIP ESS
Doktoranci 605	1	54:e6:fc:fd:03:1e	WPA-PSK-CCMP + TKIP WPA2-PSK-CCMP + TKIP-preauth ESS
Prac. Mechaniki Obliczeniowej	12	b0:48:7a:be:fc:9a	WPA2-PSK-CCMP + TKIP WPS ESS
!@#\$%^&*()_+	11	14:cc:20:08:1b:bc	WPA2-PSK-CCMP + TKIP ESS
MSM_704	6	e8:de:27:fd:1e:d8	WPA2-PSK-CCMP + TKIP ESS
MSM_716	8	c4:6e:1f:63:fc:66	WPA2-PSK-CCMP WPS ESS
PORiR_771	2	f8:1a:67:c1:19:e3	WPA-PSK-CCMP WPA2-PSK-CCMP WPS ESS
PORiR_771	2	f8:1a:67:c1:19:e2	WPA-PSK-CCMP WPA2-PSK-CCMP WPS ESS
PORiR	11	f4:f2:6d:2c:de:bf	WPA-PSK-CCMP WPA2-PSK-CCMP WPS ESS
UPC_Spoko_6	64	dc:9f:db:8a:fb:b3	ESS
iPhone(Karol)	1	22:6d:52:7b:b2:bc	WPA2

Komentarz: Niektóre sieci występują kilka razy – zmieniają się tylko adresy MAC ewentualnie kanały – oznacza to różne punkty dostępu do sieci.

Obciążenie kanałów

Na podstawie migawek wyznaczono na każdym piętrze po 3 najbardziej rekomendowane kanały przez program, następnie na podstawie tych danych wybrano 3 najczęściej rekomendowane kanały przez program, wyniki są następujące:

Piętro 5:

1. Kanał 14
2. Kanał 9
3. Kanał 8

Piętro 7:

1. Kanał 14
2. Kanał 9
3. Kanał 8

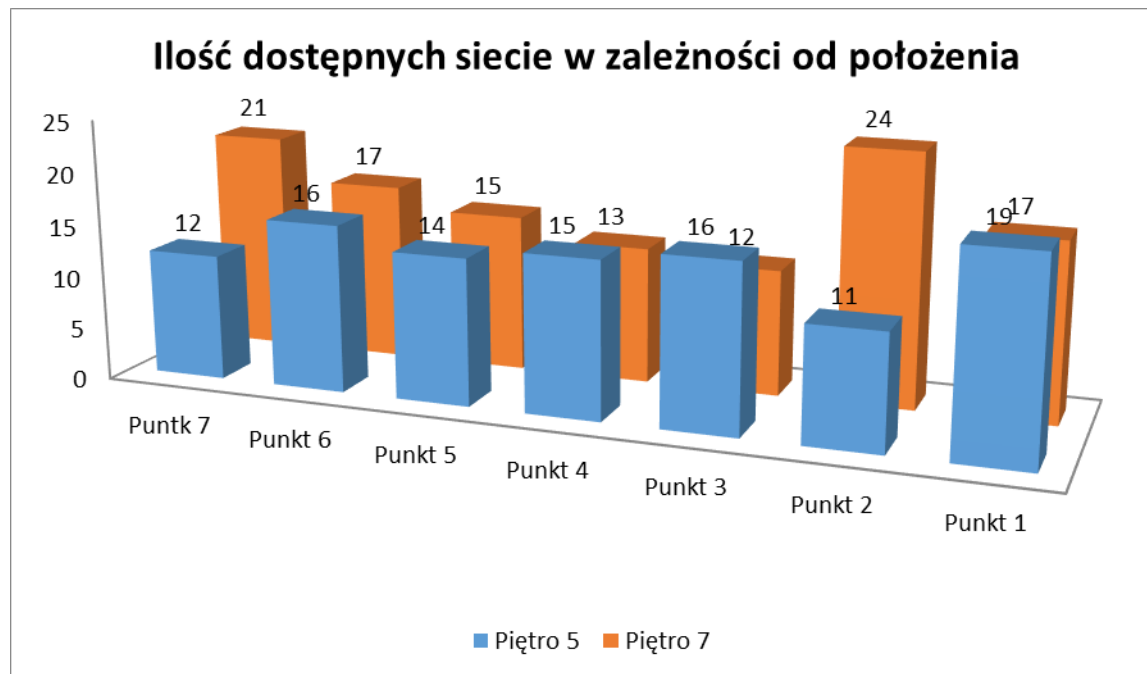


Komentarz: Wyraźnie widać że najlepszymi kanałami są

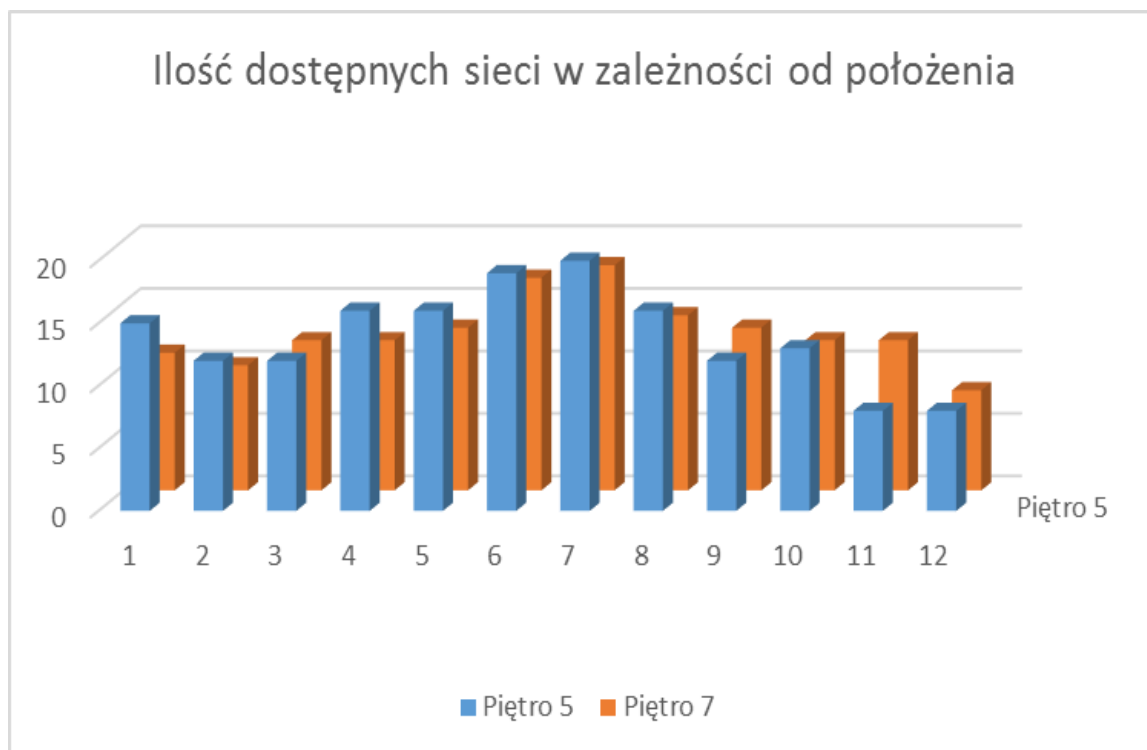
Migawka 2-rozkład ilości sieci na poszczególne kanały

zdecydowani 14, 9 i 8. Powyższa metodyka jest niezbyt profesjonalna ale ze względu na fakt że na mojej platformie [Xperia M2, Android 5.1] nie było wartości liczbowych które pozwalałyby na bezwzględnie obiektywną statystykę, występowały natomiast paski długości które były ciężkie do zmierzenia co widać na wyżej zamieszczonej migawce.

Pomiar dostępnych sieci będąc połączonym z określoną siecią [AGH-WPA]



Wykres 1 - Wykres zależności sieci do położenia (przy połączeniu)



Wykres 2 -Wykres zależności sieci do położenia (bez połączenia)

Powyższy wykresy przedstawiają ilość dostępnych sieci w zależności od miejsca pomiarowego. Pomiary zostały wykonane na piętrze 5 i 7 w 7 równoodległych od siebie punktach. Co do ułożenia punktów w przestrzeni – punkt 1 to miejsce najbliższe ul. Czarnowiejskiej czyli przy jednym końcu budynku, natomiast punkt 7 to miejsca najdalej ul. Czarnowiejskiej .

Komentarz: Jak widać ilość dostępnych sieci jest bardzo zrównoważona, w większości miejsc jest dostęp do średnio 13-15 sieci, natomiast na piętrze 7 w punktach 2 i 7 jest dostęp do odpowiednio aż 24 i 21 sieci.

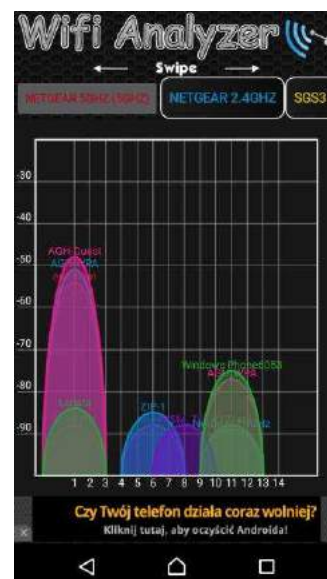
Wybrane sieci

Na początku skupiliśmy się na wybraniu sieci o dużym zasięgu. W naszym przypadku były to uczelniane Wi-Fi AGH-WPA oraz AGH-Guest.

Kryterium wybranych sieci był duży zasięg, mocny sygnał i zmieniające się adresy MAC, poniższe sieci spełniają wszystkie warunki oprócz mocnego sygnału który jest raczej przyzwoicie umiarkowany ale są to sieci najbardziej reprezentatywne.

1. AGH-WPA

- AP #1 Kanał: 1 MAC: 00:23::33:2c:11:f1
- AP #2 Kanał: 1 MAC: 00:23:33:2b:da:01



Migawka 3-rozkład jakości sygnału dla poszczególnych sieci

2. AGH-Guest

- AP #1 Kanał: 1 MAC: 00:23:33:2c:11:f0
- AP #2 Kanał: 1 MAC: 00:23:33:2b:da:00

Rozkład częstotliwości sieci w stosunku do położenia (Od lewej ul. Czarnowiejska):

AGH-WPA

5p	-82db	-78dB	-76db	-70dB	-69dB	-65dB	-52dB
7p	-90dB	-92dB	-93dB	-85dB	-79dB	-79dB	-65dB

AGH-GUEST

5p	-84dB	-75dB	-73dB	-73dB	-67dB	-66dB	-48dB
7p	-85dB	-85dB	-88dB	-86dB	-79dB	-79dB	-69dB

Na 5 piętrze sytuacja jest jednoznaczna. Dla obydwu sieci jakość stopniowo poprawia się praktycznie do samego końca (ostatni punkt pomiarowy znajduje się ok 3 metry od okna wychodzącego na parking). Można więc przypuszczać że w obu przypadkach zbliżamy się do Access Pointa. Na piętrze 7 sytuacja prezentuje się nieco inaczej. Zasięg obu sieci pogarsza się aż do 3 punktu i od tego momentu jakość zaczyna się polepszać. Zgodnie z tymi informacjami oraz adresami MAC przypuszczamy że od punktu 4 łączymy się z innym Access Pointem sieci AGH.

Jako sieci o nietypowych parametrach wybraliśmy: [iPhone\(Karol\)](#), [KlimatyzowanyDom.PL](#), [RezydencjaCzarnowiejska77](#). Sieci te zostały wybrane ze względu na ich nietypową lokalizację. Na mapce poniżej zaznaczono kolorami miejsca w których udało się odebrać sygnał tych sieci

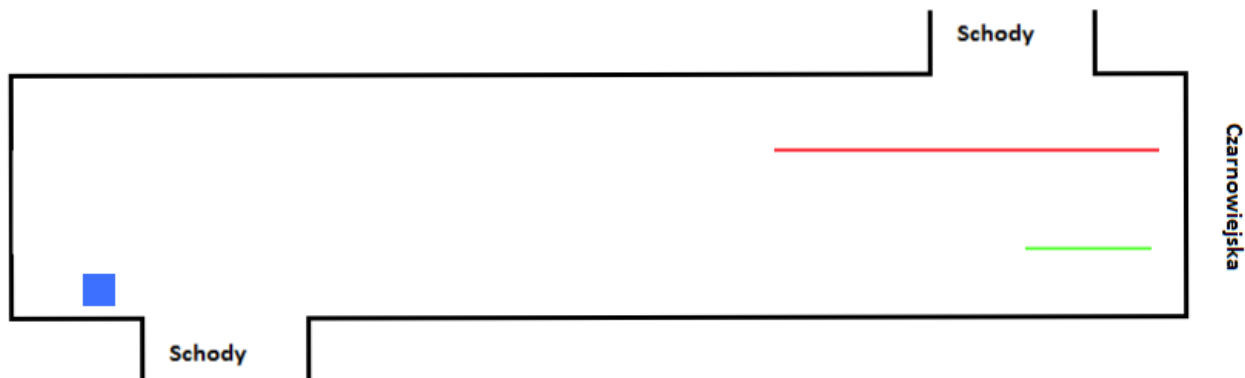


Diagram 2 - rozkład dostępności sygnałów dla odpowiednich sieci

Sieć **iPhone(Karol)** została prawdopodobnie założona aby udostępnić laptopowi możliwość korzystania z internetu, dostępnego na smartphonie (Opcja punkty dostępu w smartphonach z systemem iOS a także Android daje taką możliwość) Nasze przypuszczenie potwierdza obecność w tym miejscu osoby korzystającej z laptopa. Sieć ta cechuje się bardzo słabą jakością sygnału(sygnał jest dostępny tylko w jednym bądź dwóch punktach pomiarowych)

Sieć **KlimatyzowanyDom.PL** udało nam się zauważyć w kilku punktach pomiarowych od strony ulicy Czarnowiejskiej. Po sprawdzeniu nazwy sieci znaleźliśmy przybliżony adres Access Point(Adres siedziby firmy KlimatyzowanyDom) który znajduje się na ulicy Lea czyli aż 200m od budynku B5! Można łatwo zauważyć że sieć ta cechuje się bardzo dobrą siłą i jakością sygnału.

Ostatnią z nietypowych sieci jest **RezydencjaCzarnowiejska77**, dostępna jedynie bardzo blisko okna skierowanego w stronę ulicy Czarnowiejskiej. Po sprawdzeniu odległości między Czarnowiejską77 a budynkiem B5 AGH dowiadujemy się że w trakcie testu AP znajdował się około 50 metrów od analizującego sieci smartphona. Mimo że wynik ten jest znacznie gorszy niż sieci KlimatyzowanyDom w dalszym ciągu można zakwalifikować go jako sygnał o dużej sile.

Podsumowując, możemy zauważyć że dla jakości sieci bardzo duże znaczenia ma AP, od którego głównie zależeć będzie siła sygnału. W przypadku bardzo słabego routera w telefonie jakość sygnału była bardzo mała. Jednak sieć Wi-Fi w firmie bez problemu radziło sobie z odległością 200m. Oczywiście warto wspomnieć że tak dobre wyniki były zasługą umieszczenia smartphona na wysokości 5 piętra gdzie sygnał nie był blokowany przez budynki.

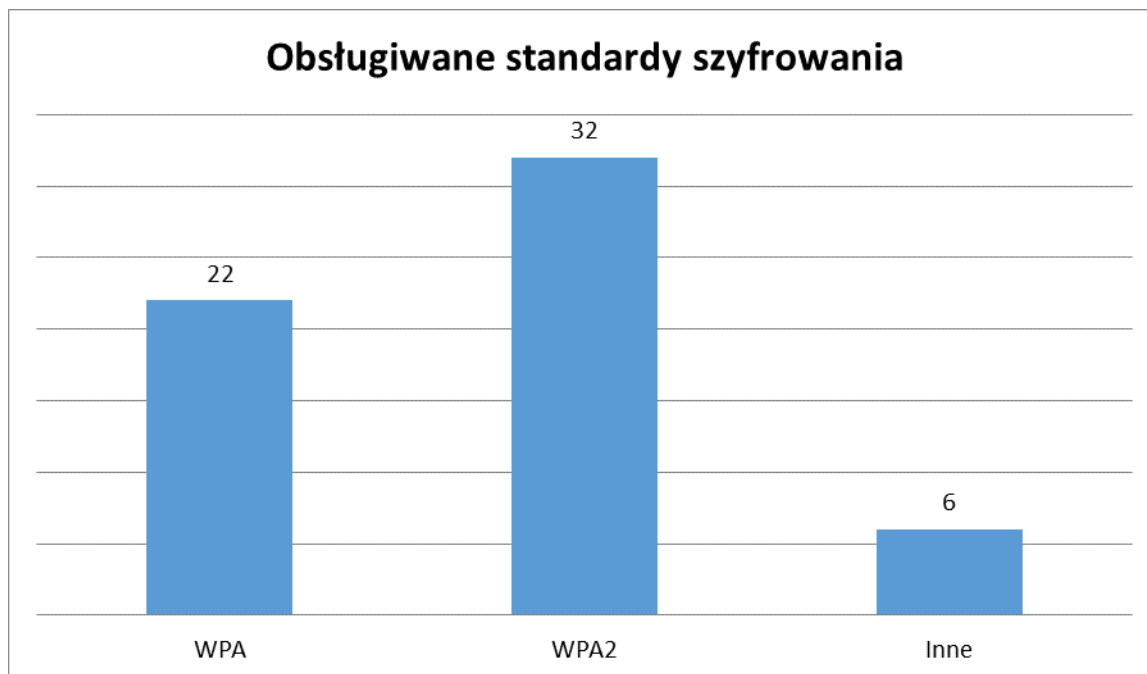
Dodatkowo doszliśmy do wniosku że nazewnictwo sieci nie pozostaje bez znaczenia i może służyć jako reklama firmy. Jednak często udostępnia publicznie, prywatne informacje (Czarnowiejska77)

Opracowanie statystyczne

Ilość unikalnych AP które zostały zanotowane: 40

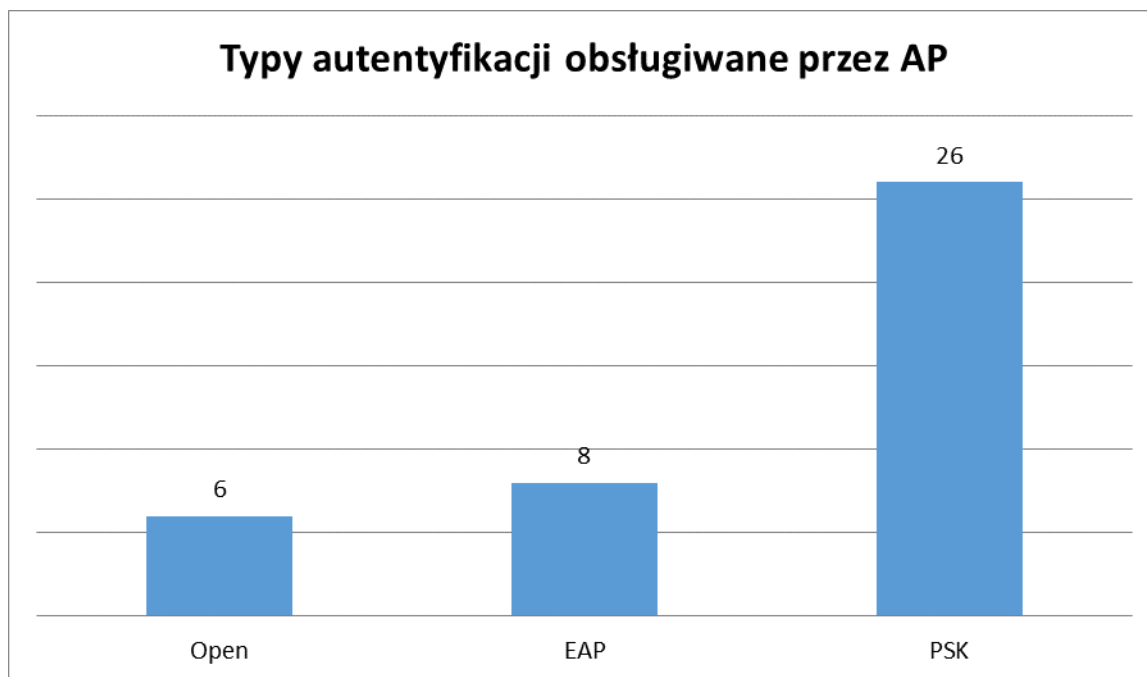
Komentarz: ilość oczywiście była większa, wynika to stąd, że niektóre z sieci były chwilowo na grafie a na liście ich nie odnaleziono co świadczy o tym że prawdopodobnie balansowały na krawędzi bycia uchwyconym, były też urządzenia studenckie w trybie Punktu Dostępu, które w pewnym momencie prawdopodobnie zostały wyłączone.

Standardy szyfrowania:



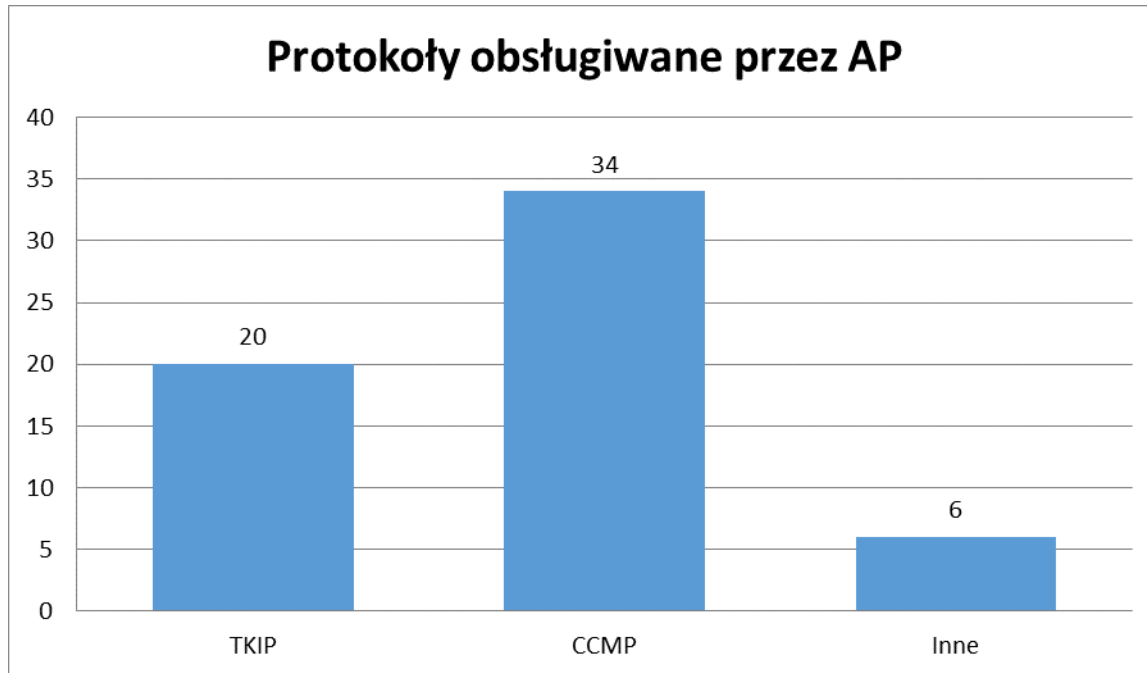
Wykres 3 - ilości sieci z danymi standardami szyfrowania

Autentyfikacja:



Wykres 4-rodzaje autentyfikacji dla poszczególnych sieci

Protokoły:



Wykres 5-rodzaje protokołów obsługiwanych przez AP

Komentarz: TKIP jest protokołem używanym w standardzie WPA, oparty jest on na dynamicznych kluczach i RC4 do szyfrowania. Natomiast CCMP jest protokołem który został stworzony po odkryciu pewnych luk w TKIP, jest on używany w standardzie WPA2 i oparty jest na szyfrowaniu AES.

Ponadto udało nam się poznać dokładną lokalizację wielu Access Pointów. Podstawową metodą było badanie sygnału, jednak często korzystaliśmy także z samej nazwy sieci. Oto lista najciekawszych Access Pointów, które udało nam się odnaleźć oraz ich lokalizacji:

IPhone(Karol)-piętro 5 zagłębienie za schodami od strony parkingu AGH

AGH-Guest- piętro 5 zagłębienie za schodami od strony parkingu AGH

Doktoranci605-sygnał nasilał się na środku piętra 5 i 7 więc wnioskujemy że AP rzeczywiście znajduje się w sali 605(piętro 6)

PhaseField@607-podobnie jak sieci poprzedniej sygnał nasilał się przy tym samym punkcie na obydwu piętrach a więc zakładamy że AP znajduje się na piętrze 6 konkretnie w pokoju 607(nazwa)

www.KlimatyzowanyDom.PL- zgodnie z danymi ze strony internetowej Access Point powinien znajdować się przy ulicy Juliusza Lea 22c/1, co potwierdza kierunek wzrostu/spadku sygnału.

Rezydencja Czarnowiejska 77 – korzystając z przybliżonego kierunku utraty/wzrostu sygnału oraz adresu w nazwie, przypuszczamy że AP znajduje się przy ulicy Czarnowiejskiej 77 (50m na północ od budynku b5 AGH)

Wnioski:

- Dostępność sieci

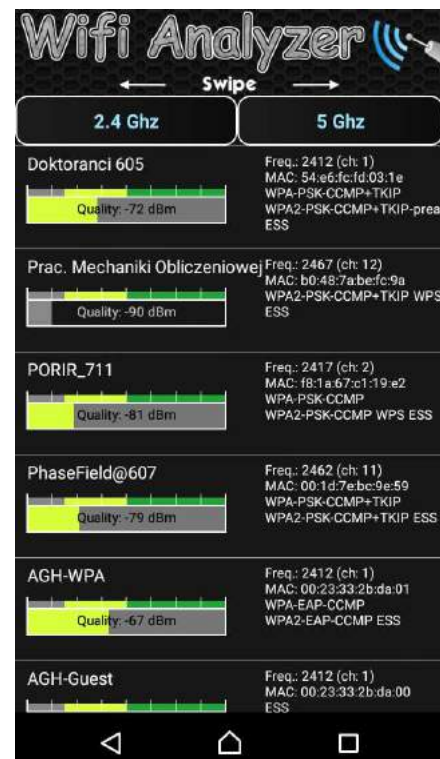
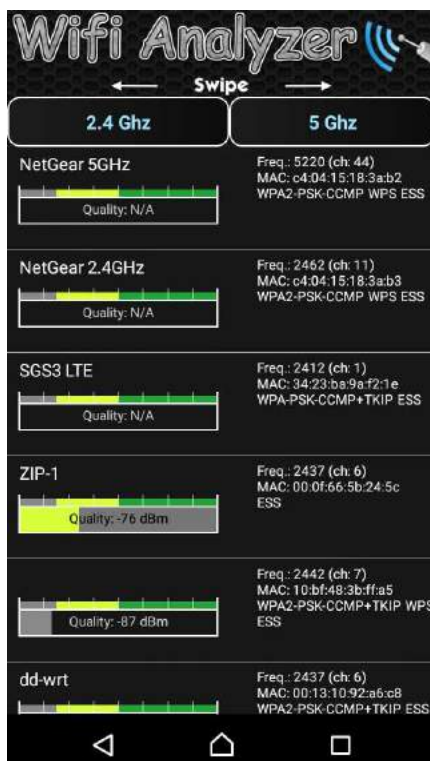
Ilość dostępnych sieci jest względnie spora (ok 32), jednak większość z nich prezentuje mierną siłę sygnału spowodowaną albo zabudowaniami albo znaczną odległością.

- AGH-WPA – testowanie

Siła sygnału w większości wypadków była zadowalająca na tyle żeby utrzymać połączenie z w/w siecią. Jak widać na dołączonych wykresach siła sygnału wzrasta wraz z odległością od ul. Czarnowiejskiej aż do samego końca korytarza, na czym bazuje twierdzenie że to właśnie tam znajdują się AP. Natomiast na 7 piętrze zauważono zmianę adresu MAC AP co oznacza że występuje tam (bądź w okolicach) inny AP.

- Bezpieczeństwo

Większość punktów dostępu obsługiwała standard WPA2, natomiast nie da się przeoczyć że ok 2/3 urządzeń obsługuje WPA (kompatybilność wsteczna) a tylko garstka nie wspiera żadnego z tych standardów, co ostatecznie świadczy o pewnej dbałości administratorów sieci o bezpieczeństwo.



- Oprogramowanie

Aplikacja spełnia swoje założenia aczkolwiek często występują problemy z wyznaczeniem siły sygnału danej sieci co w toku opracowywania sprawozdania nie pozwoliło mi na indeksowanie zasięgu wszystkich sieci. Dodatkowo graficzna interpretacja na pierwszym ekranie pozostawia dużo do życzenia jeśli chodzi o czytelność – przy większej ilości sieci nie można rozróżnić ich od siebie.

Zdobyte wyniki pozwalają na niemal bezproblemowe uzyskanie lokalizacji danego Access Pointa. Można poznać także adresy MAC oraz zajmowane kanały. Ilość sieci na obydwu piętrach budynku B5 jest zaskakująco dużo. Najmniejsza ilość znalezionych sieci to 8 zaś największa dochodzi nawet do 20. Widzimy więc że obecnie zakładanie sieci bezprzewodowej nie stanowi żadnego problemu. Wystarczy nawet zwykły telefon z internetem aby w ciągu kilku sekund zacząć udostępniać własną sieć. Zaskakująco duża jest też liczba sieci z brakiem lub bardzo słabymi zabezpieczeniami (sieci zabezpieczone protokołem WPA są o wiele bardziej podatne na ataki niż WPA2). Zasięg sieci także stanowi coraz mniejszy problem gdyż nawet najprostszy router potrafi nadawać sygnał do kilkudziesięciu metrów (wyjątkiem są wspomniane wcześniej telefony z racji na inne podstawowe funkcje). Duża ilość sieci jak i poprawiający się ich zasięg i jakość doprowadzają do sytuacji w którym w mieście (np Krakowie) niemalże zawsze można zlokalizować kilka do kilkunastu sieci. Jest to znaczna poprawa w stosunku do poprzedniego dziesięciolecia.

Migawki: https://drive.google.com/open?id=0B_j7u4SQMa4UGhPSVpvOHU1UUE

			<i>Data wykonania</i>	<i>Data odbioru</i>
	Routing			
	<i>Ocena i uwagi</i>			

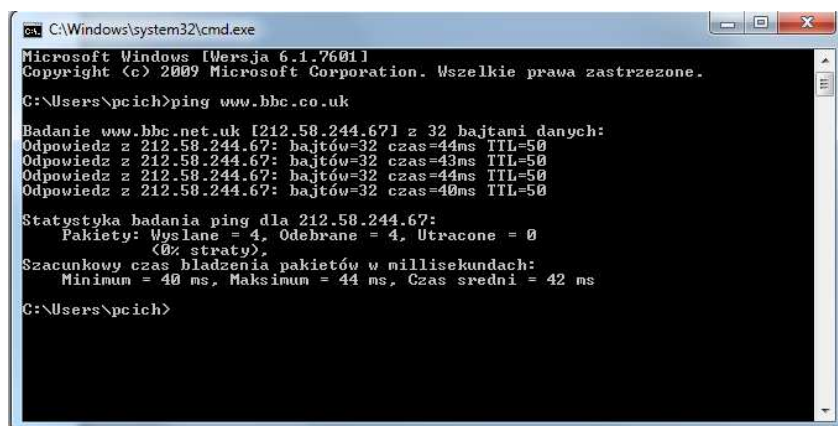
Wstęp

Celem laboratorium nr 2 – Routing, było sprawdzenie i zademonstrowanie tras pakietów wysyłanych od komputerów z pracowni komputerowej w B5 AGH do czterech wybranych domen internetowych. Strony wybrane przez nas to kolejno:

- www.bbc.co.uk
- www.aliexpress.com
- www.usa.gov
- www.govt.nz

Pierwszy adres to portal znanej brytyjskiej stacji telewizyjnej BBC. Drugi to zyskujący coraz większą popularność chiński sklep internetowy. Dwa ostatnie adresy to strony rządowe odpowiednio USA i Nowej Zelandii.

Adresy IP, średnie czasy, lokalizacja serwera



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\pcich>ping www.bbc.co.uk

Badanie www.bbc.net.uk [212.58.244.67] z 32 bajtami danych:
Odpowiedz z 212.58.244.67: bajtów=32 czas=44ms TTL=50
Odpowiedz z 212.58.244.67: bajtów=32 czas=43ms TTL=50
Odpowiedz z 212.58.244.67: bajtów=32 czas=44ms TTL=50
Odpowiedz z 212.58.244.67: bajtów=32 czas=40ms TTL=50

Statystyka badania ping dla 212.58.244.67:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
            (0% straty)
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 40 ms, Maksimum = 44 ms, Czas średni = 42 ms

C:\Users\pcich>
  
```

Snapshot 1 - komenda ping dla portalu stacji BBC

Nazwa portalu	Adres IP	Średni czas połączenia
www.bbc.co.uk	212.58.244.67	42 ms
www.aliexpress.com	198.11.132.241	177ms
www.usa.gov	104.94.137.151	6ms
www.govt.nz	103.28.251.187	283ms

Użyliśmy programu ping w konsoli Windows do określenia podstawowych informacji na temat adresu i czasu przesyłania pakietów.

Możemy łatwo zauważyć że czas połączenia z BBC oraz stroną rządową USA był wyjątkowo niski. Serwery te znajdowały się blisko Polski bądź miały wyjątkowo dobre połączenie/mało routerów przechodnych. Widać też że połączenie z Nową Zelandią

trwało najdłużej. Testy trasy pakietów pozwolą sprawdzić czy rzeczywiście była to najdłuższa trasa.

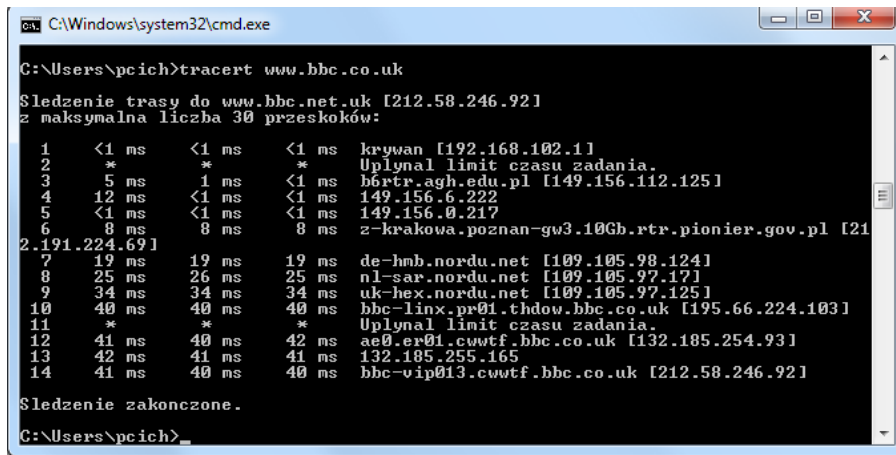
Lokalizacje serwerów:

- **bbc.co.uk** Tadworth, Surrey, Wielka Brytania 0.23W 51.28N (Domena Wielka Brytania)
- **aliexpress.com** Santa Clara, Kalifornia, Stany Zjednoczone 121.961W 37.396100N(Domena komercyjna)
- **usa.gov** Cambridge, Massachusetts, Stany Zjednoczone 71.08W 42.36N (Domena rządowa)
- **govt.nz** Auckland, Nowa Zelandia 174.76E 36.86S (Domena Nowa Zelandia)

Trasy pakietów

Dla poszczególnych adresów prześledziliśmy ich trasę korzystając z komendy **tracert** w konsoli Windows

- www.bbc.co.uk



```
C:\Windows\system32\cmd.exe
C:\Users\pcich>tracert www.bbc.co.uk

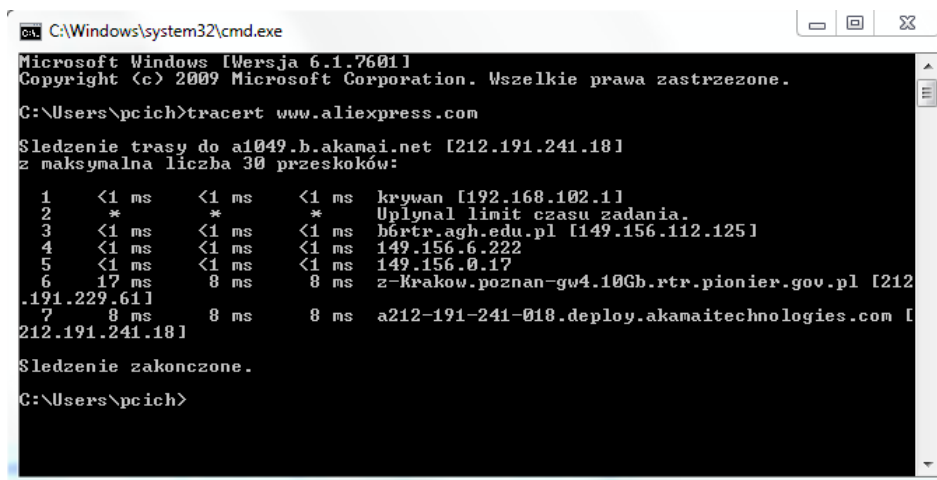
Śledzenie trasy do www.bbc.net.uk [212.58.246.92]
z maksymalną liczbą 30 przeskoków:

 1  <1 ms    <1 ms    <1 ms    krywan [192.168.102.1]
 2  *        *        *        Upłynął limit czasu zadania.
 3  5 ms     1 ms     <1 ms    b6rtr.agh.edu.pl [149.156.112.125]
 4  12 ms    <1 ms    <1 ms    149.156.6.222
 5  <1 ms    <1 ms    <1 ms    149.156.0.217
 6  8 ms     8 ms     8 ms     z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.69]
 7  19 ms    19 ms    19 ms    de-hmb.nordu.net [109.105.98.124]
 8  25 ms    26 ms    25 ms    nl-sar.nordu.net [109.105.97.17]
 9  34 ms    34 ms    34 ms    uk-hex.nordu.net [109.105.97.125]
10  40 ms    40 ms    40 ms    bbc-linx.pr01.thdow.bbc.co.uk [195.66.224.103]
11  *        *        *        Upłynął limit czasu zadania.
12  41 ms    40 ms    42 ms    ae0.er01.cwutf.bbc.co.uk [132.185.254.93]
13  42 ms    41 ms    41 ms    132.185.255.165
14  41 ms    40 ms    40 ms    bbc-vip013.cwutf.bbc.co.uk [212.58.246.92]

Śledzenie zakończone.
C:\Users\pcich>
```

Snapshot 2 - Trasa dla BBC

- www.aliexpress.com



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\pcich>tracert www.aliexpress.com

Śledzenie trasy do a1049.b.akamai.net [212.191.241.18]
z maksymalną liczbą 30 przeskoków:

 1  <1 ms    <1 ms    <1 ms    krywan [192.168.102.1]
 2  *        *        *        Upłynął limit czasu zadania.
 3  <1 ms    <1 ms    <1 ms    b6rtr.agh.edu.pl [149.156.112.125]
 4  <1 ms    <1 ms    <1 ms    149.156.6.222
 5  <1 ms    <1 ms    <1 ms    149.156.0.17
 6  17 ms    8 ms     8 ms     z-Krakow.poznan-gw4.10Gb.rtr.pionier.gov.pl [212.191.229.61]
 7  8 ms     8 ms     8 ms     a212-191-241-018.deploy.akamaitechnologies.com [212.191.241.18]

Śledzenie zakończone.
C:\Users\pcich>
```

Snapshot 3 - Trasa dla aliexpress

- www.usa.gov

```

C:\Windows\system32\cmd.exe
Sledzenie zakonczzone.
C:\Users\pcich>tracert www.usa.gov

Sledzenie trasy do e7990.dsch.akamaiedge.net [104.94.137.151]
z maksymalna liczba 30 przeskokow:

 1  <1 ms  <1 ms  <1 ms  krywan [192.168.102.1]
 2  *      *      *      Uplynal limit czasu zadania.
 3  1 ms   <1 ms  1 ms   b6rtr.agh.edu.pl [149.156.112.125]
 4  <1 ms  <1 ms  <1 ms  149.156.6.222
 5  <1 ms  <1 ms  <1 ms  149.156.0.217
 6  <1 ms  <1 ms  <1 ms  149.156.0.50
 7  6 ms   6 ms   6 ms   akamai.thinx.pl [212.91.0.251]
 8  6 ms   6 ms   6 ms   ai04-94-137-151.deploy.static.akamaitechnologies
.com [104.94.137.151]

Sledzenie zakonczzone.
C:\Users\pcich>_

```

Snapshot 4 -Trasa dla usa.gov

- www.govt.nz

```

C:\Windows\system32\cmd.exe
Sledzenie zakonczzone.
C:\Users\pcich>tracert www.govt.nz

Sledzenie trasy do www.govt.nz [103.28.251.187]
z maksymalna liczba 30 przeskokow:

 1  <1 ms  <1 ms  <1 ms  krywan [192.168.102.1]
 2  *      *      *      Uplynal limit czasu zadania.
 3  1 ms   <1 ms  <1 ms  b6rtr.agh.edu.pl [149.156.112.125]
 4  <1 ms  <1 ms  <1 ms  149.156.6.222
 5  <1 ms  <1 ms  <1 ms  149.156.0.217
 6  32 ms  12 ms   8 ms   z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl [21
2.191.224.69]
 7  14 ms  13 ms  13 ms  212.162.10.81
 8  29 ms  27 ms  27 ms  Tata-level3-40G.Amsterdam.Level3.net [4.68.63.42]
 9  299 ms 297 ms 290 ms  if-11-2.tcore2.AU2-Amsterdam.as6453.net [80.231.
152.251]
10  282 ms 282 ms 282 ms  if-8-2.tcore2.L78-London.as6453.net [80.231.131.
51]
11  292 ms 290 ms 291 ms  if-9-2.tcore2.WYN-Marseille.as6453.net [80.231.2
00.131]
12  295 ms 295 ms 295 ms  if-2-2.tcore1.WYN-Marseille.as6453.net [80.231.2
17.11]
13  285 ms 282 ms 282 ms  if-5-2.tcore1.MLU-Mumbai.as6453.net [80.231.217.
301]
14  281 ms 281 ms 281 ms  if-2-2.tcore2.MLU-Mumbai.as6453.net [180.87.38.2
1]
15  284 ms 284 ms 283 ms  if-16-2.tcore1.SUW-Singapore.as6453.net [180.87.
12.226]
16  293 ms 292 ms 292 ms  if-2-2.tcore2.SUW-Singapore.as6453.net [180.87.1
2.21]
17  284 ms 283 ms 283 ms  if-20-2.tcore1.SUQ-Singapore.as6453.net [180.87.
96.211]
18  291 ms 291 ms 291 ms  116.51.31.106
19  283 ms 283 ms 283 ms  103.28.251.187.ip.incapdns.net [103.28.251.187]

Sledzenie zakonczzone.
C:\Users\pcich>

```

Snapshot 5-Trasa dla govt.nz

Po zanalizowaniu tras dla każdej sieci możemy stwierdzić że nasze przypuszczenia potwierdziły się. Najdłuższą trasę zanotowano dla sieci znajdującej się w Nowej Zelandii. Ponadto ostatnim wspólnym serwerem dla wszystkich sieci był router o adresie **149.256.6.222**. Poniżej znajdują się informacje o tym adresie:

Średni czas połączenia: 1ms

Trasa: 192.168.102.1 -> 149.156.112.125 -> 149.156.6.222

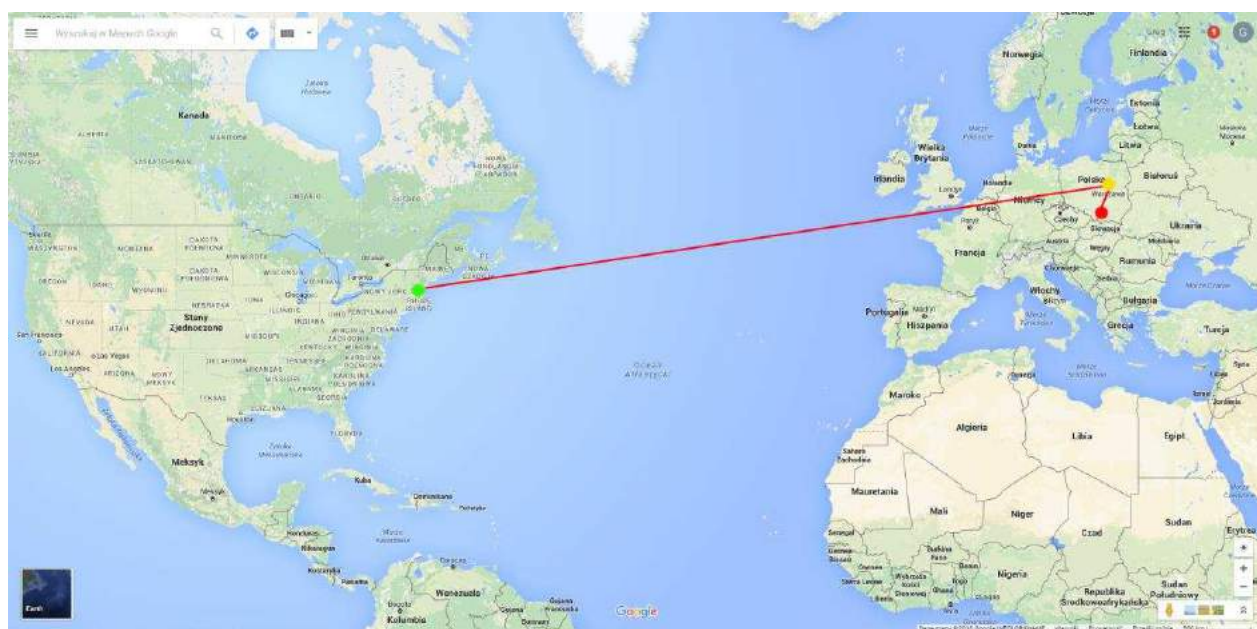
Przypuszczamy, że ostatnim wspólnym routerem jest komputer znajdujący się w wewnętrznej sieci AGH. Warto zwrócić uwagę iż nie zawsze powtarzający się komputer zawsze musi znajdować się w sieci wewnętrznej. Na 4 adresy 3 z nich miały wspólny router o adresie **212.191.224.69** i nazwie

z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl. Jest to więc serwer który często wykorzystuję się do wysyłania pakietów za granicę.

Mapy routingu

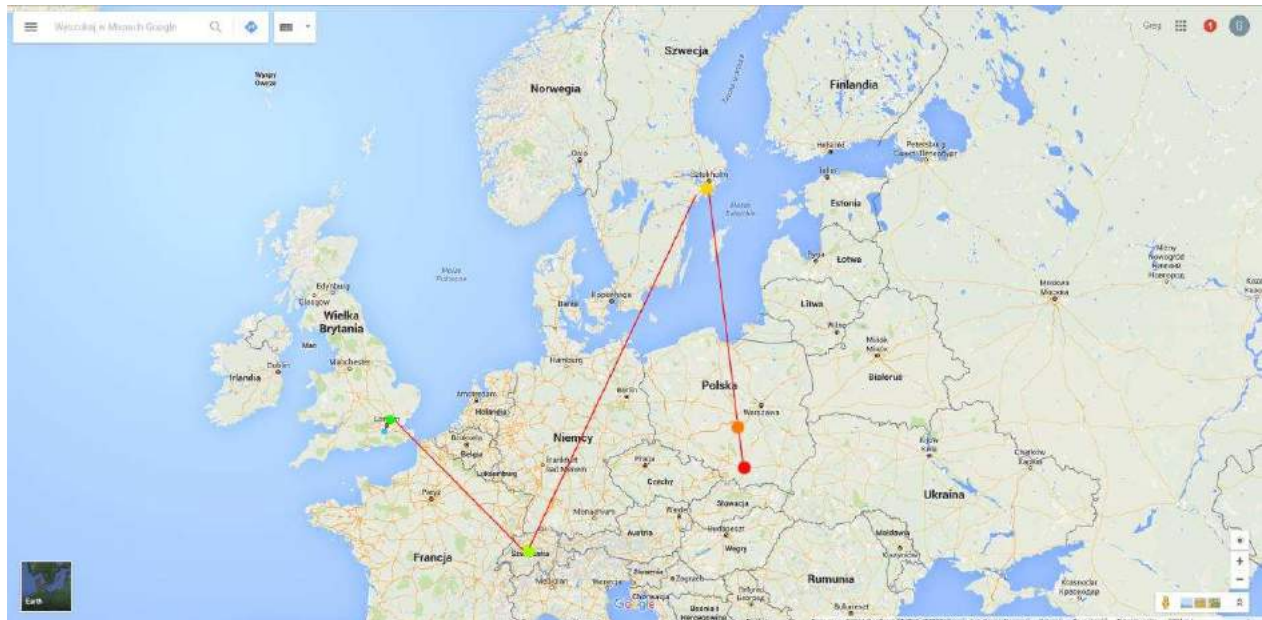
Dla adresu **www.usa.gov** oraz **www.bbc.co.uk** tworzymy mapę komputerów przez które przechodzą pakiety. W obydwu trasach pominięto serwery wewnętrzne AGH(zbyt duża skala mapy).

Mapa dla **www.usa.gov**



Map 1 - USA.GOV

Mapa dla www.bbc.co.uk



Map 2 - BBC.CO.UK

O ile trasa dla adresu w USA trasa jest prosta i korzysta tylko z niezbędnych komputerów pośrednich, pakiety wysyłane z i do portalu BBC wędrowały przez całą Europę Środkową a serwer docelowy był aż 5 (głównym) komputerem na ich drodze.

Informacje o sieciach

Korzystając z portalu **alexa.com** badamy informacje na temat poszczególnych sieci :

- **bbc.co.uk**
 - Global Rank: 97
 - National Rank: 7
 - Page views per Visitor: 4.51
 - Time on site: 5:28
 - Audience Geography: Wielka Brytania, Stany Zjednoczone, Indie
 - Sites before: google.co.uk, google.com, facebook.com
- **aliexpress.com**
 - Global Rank: 50
 - National Rank: 11
 - Page views per Visitor: 17
 - Time on site: 12:18
 - Audience Geography: Rosja, Chiny, Stany Zjednoczone
 - Sites before: google.com, facebook.com, youtube.com

- **usa.gov**
 - Global Rank: 7503
 - National Rank: 1755
 - Page views per Visitor: 1.81
 - Time on site: 1:24
 - Audience Geography: Stany Zjednoczone, Indie, Chiny
 - Sites before: google.com, facebook.com, noaa.gov

Portal **bbc.co.uk** oraz **aliexpress.com** cieszą się bardzo dużą popularnością. Interesujące treści oraz ciekawy design zapewniają im wiele unikatowych odwiedzin. Strona rządowa Stanów Zjednoczonych cieszy się znacznie mniejszą popularnością ponad 70 razy mniejszą (Ranking) niż BBC. Można tylko przypuszczać że mało osób chce odwiedzać strony rządowe. To samo tyczy się strony govt.nz która jest tak mało znana i popularna że nie znalazła się dla niej żadna adnotacja.

Powtórzenie prób

W celu sprawdzenia ewentualnych różnic powtórzyliśmy trasowanie dla wszystkich sieci. Dla trzech pierwszych nie odnotowano znaczących różnic. Zdarzało się że ostatnie cyfry adresu serwera różniły się, jednak przy sporządzaniu mapy trasy nie miało to znaczenia. Spowodowana jest to krótką (w porównaniu do Nowej Zelandii) trasą pakietów i mało możliwości alternatywnych tras. Jedyną trasą ze znaczącymi różnicami jest adres govt.nz

```

C:\Windows\system32\cmd.exe
C:\Users\pcich>tracert www.govt.nz

Śledzenie trasy do www.govt.nz [103.28.250.187]
z maksymalną liczbą 30 przeskoków:

 1  <1 ms    <1 ms    <1 ms    krywan [192.168.102.1]
 2  *        *        *        Upłynął limit czasu zadania.
 3  16 ms    <1 ms    <1 ms    b6rtr.agh.edu.pl [149.156.112.125]
 4  <1 ms    <1 ms    <1 ms    149.156.6.222
 5  <1 ms    <1 ms    <1 ms    149.156.0.217
 6  8 ms     8 ms     8 ms     z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.162.10.81]
 7  14 ms    14 ms    14 ms    212.162.10.81
 8  28 ms    28 ms    28 ms    NTT-level3-4x10G.Amsterdam.Level3.net [4.68.63.218]
 9  28 ms    28 ms    28 ms    ae-7.r25.amstn102.nl.bb.gin.ntt.net [129.250.2.158]
10  110 ms   112 ms   110 ms   ae-5.r23.asbnva02.us.bb.gin.ntt.net [129.250.6.162]
11  110 ms   110 ms   110 ms   ae-0.r22.asbnva02.us.bb.gin.ntt.net [129.250.3.84]
12  174 ms   174 ms   174 ms   ae-5.r23.lsanca07.us.bb.gin.ntt.net [129.250.3.189]
13  174 ms   174 ms   174 ms   ae-2.r01.lsanca07.us.bb.gin.ntt.net [129.250.4.107]
14  175 ms   185 ms   174 ms   ae-0.incapsula.lsanca07.us.bb.gin.ntt.net [165.254.106.46]
15  174 ms   174 ms   174 ms   103.28.250.187.ip.incapedns.net [103.28.250.187]

Śledzenie zakończone.
C:\Users\pcich>

```

Snapshot 6- druga próba dla govt.nz

Jak widać na załączonym snapshocie trasa uległa znacznemu skróceniu. Inne są też poszczególne komputery pośrednie (różnice zaczynają się po „opuszczeniu” Polski czyli przejście przez komputer z-*krakow.poznan...*). Widać wyraźnie że to połączenie jest przykładem routingu DYNAMICZNEGO który w każdym momencie szuka aktualnie najlepszego połączenia między dwoma komputerami .

Poczta E-Mail

Ćwiczenie z wykorzystaniem e-maili polegało na przesłaniu dwóch listów elektronicznych z jednej na drugą skrzynkę elektroniczną, raz z laboratorium B5-410 a drugi z sieci domowej. Następnie przeanalizować nagłówki wysłanych i odebranych maili. Do ćwiczenia wykorzystano 2 skrzynki pocztowe na domenie **gmail.com**.

Sieć AGH

Informacje jakie możemy wyczytać z nagłówków to przede wszystkim nadawca, odbiorca, tytuł i treść maila, czas nadania, unikalne ID maila nadawane w tym wypadku przez pocztę **gmail.com** oraz ewentualne serwery przez które korespondencja została przekazana do punktu docelowego tj. adresata.

Określenie nadawcy po przeanalizowaniu nagłówka jest trywialne:

```
"Received: by 10.129.106.132 with HTTP; Mon, 7 Mar 2016 23:59:34 -0800 (PST)
Date: Tue, 8 Mar 2016 08:59:34 +0100
Message-ID: <CAGGjC9kRoKrpns-Ae8GEAv-0LPo0=V3zQh3uw4FdpK3XrVJJJg@mail.gmail.com>
Subject: Probe 1
From: Greg Sakaszwili <feonrr@gmail.com>
To: Piotr Kowalski fadityyt@gmail.com"
Nadawcą jest oczywiście feonrr@gmail.com.
```

Serwery pośredniczące:

- 10.129.106.132 – protokół Web
- 10.13.233.68 – protokół SMTP
- mail-yw0-f172.google.com – protokół SMTP
- mx.google.com – protokół ESMTPS
- 10.13.227.1 – protokół SMTP
- 10.107.191.198 – protokół SMTP

Pierwsze połączenie służyło do przesłania maila z protokołu webowego (mail pisano z przeglądarki sieci www) na serwery SMTP które przekazywały sobie mail aż do głównego serwera **mail-yw0-f172.google.com**, który następnie przesłał mail ponownie przez serwery SMTP aż do adresata.

Jedyny serwer, który udało się zlokalizować jest właśnie **mail-yw0-f172.google.com** należący do korporacji **Google** znajdującej się w Mountain View, California, Stany Zjednoczone.

Sieć Domowa

Określenie nadawcy jak poprzednio:

```
Received: by 10.129.106.132 with HTTP; Sun, 13 Mar 2016 08:06:26 -0700 (PDT)
Date: Sun, 13 Mar 2016 16:06:26 +0100
Message-ID: <CAGGjC9nbFvrLvypk-0ulmN8RCzE5hw1axcimnCDU2h5pDCxcnQ@mail.gmail.com>
Subject: Probe 4
From: Greg Sakaszwilli <feonrr@gmail.com>
To: Piotr Kowalski fadityyt@gmail.com
```

Jak w poprzednik wypadku nadawcą jest feonrr@gmail.com na co wskazuje powyższy wpis w nagłówku.

Serwery pośredniczące:

- 10.129.106.132 – protokół Web
- 10.13.219.14 – protokół SMTP
- mail-yw0-x234.google.com – protokół SMTP
- mx.google.com – protokół ESMTPS
- 10.129.131.139 – protokół SMTP
- 10.107.191.198 – protokół SMTP

Jak w poprzednim wypadku następuje przekazanie maila z serwera sieci web do serwerów SMTP które przekazują sobie dalej korespondencję aż do serwera głównego, który następnie skierowuje mail do adresata także przez serwery SMTP. W tym przypadku nie udało się zlokalizować żadnego z serwerów.

Uwagi

Porównując nagłówki łatwo zauważyć było że nagłówek adresata zawiera o wiele więcej informacji w porównaniu do nadawcy gdzie widnieje informacja gdzie została przekazana pocztą.

Nagłówek odbiorcy zawiera pełną trasę serwerów przez które przeszła wiadomość.

Wnioski

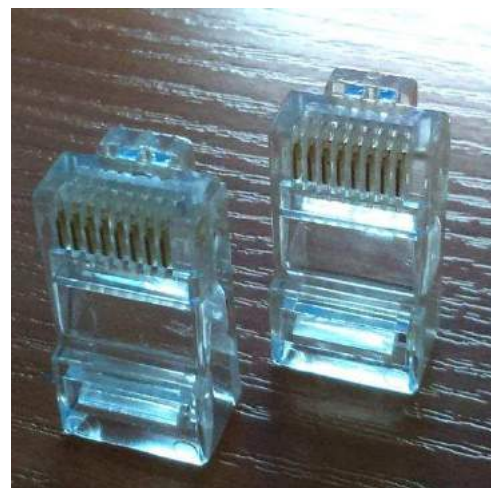
Powyższe zadanie pozwoliło nam się zapoznać z sposobami routingu stosowanych w przypadku przesyłania informacji między serwerami. W większości przypadków da się zauważyć dynamiczny routing co widać po zmieniających się trasach przesyłania danych. Miało to oczywiście swój wpływ na czas podróży próbek testowych wysyłanych przez program **ping** z konsoli Windows, jednakże typ routingu nie jest jedynym czynnikiem wpływającym na opóźnienia. Przede wszystkim największy wpływ ma ilość serwerów przez które przechodzi próbka, ponieważ każde informacje muszą zostać wysłane dalej co zmusza serwer do obliczenia następnego serwera docelowego bądź klienta. Największy wpływ natomiast ma oczywiście odległość co najbardziej widać w przypadku azjatyckich i nowozelandzkich serwerów gdzie opóźnienia sięgają poziom 170-250 ms co np. przy rozmowie jest już znaczącym utrudnieniem ale w przypadku surfowania po sieci bądź wysyłania korespondencji nie robi to wielkiej różnicy. Niestety nie byliśmy w stanie przeprowadzić testów za pomocą programu VisualWare – w laboratorium AGH nie posiadaliśmy uprawnień do przygotowania środowiska dla programu natomiast na komputerach osobistych pomimo usilnych prób instalacji i konfiguracji Java Runtime Environment nie udało się programu uruchomić.

<i>Grupa ćwicz.</i>	<i>Grupa lab.</i>	<i>Zespół</i>	<i>Data wykonania</i>	<i>Data odbioru</i>
<i>Nr ćwicz.</i>				
<i>Imiona i nazwiska</i>				<i>Ocena i uwagi</i>

Przebieg ćwiczenia

Przygotowane narzędzia:

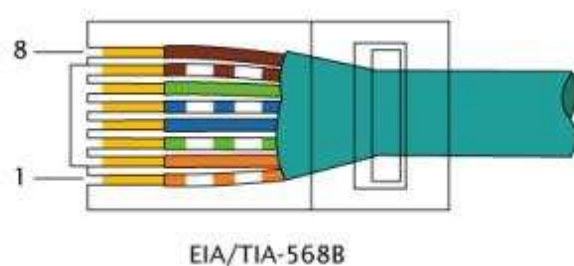
- Wtyki RJ45
- Zaciskarka/stripper do kabli
- Odcinek kabla sieciowego
- Tester kabli



Wykonanie:

Najpierw przygotowano 43 centymetrowy odcinek kabla, następnie na każdym z końców odsłonięto ok. 15 mm w celu ułożenia przewodów w odpowiedniej kolejności. W kablu zidentyfikowaliśmy 8 różnych przewodów o różnych kolorach, uziemienie oraz sznurek służący do rozrywania osłony kabla.

Następnym etapem było ustawienie w odpowiedniej kolejności kabli oraz przycięcie ich przy końcach w celu zmniejszenia ryzyka nieprzecięcia kabli przez zaciskające się zęby wtyczek. Standard w którym układamy przewody to TIA/EIA-568-B, ustawienie na końcówkach jest symetryczne tzn. pin 1-1, 2-2,... Następnym krokiem było zaciśnięcie wtyczek zaciskarką.



Testowanie

Kabel przetestowane urządzeniem **MASTER HSHL468 CABEL TESTER**, które oferuje testowanie kabli RJ45 zarówno jak RJ11. Przeprowadzenie testu przebiegało następująco: podłączono każdy koniec kabla do jednej z części urządzenia do odpowiedniego portu, ustabilizowano je a następnie przestawiono przełącznik z OFF na ON. Następuje testowanie w postaci wysyłania sygnału z jednego końca kabla do drugiego co jest sygnalizowaniem zapaleniem się odpowiednich diod po obu stronach (w przypadku sprawnego połączenia pinu). W naszym przypadku każdemu zapaleniu się diody numer 1,2,3,...,8 towarzyszyło mu zapalenie się tej samej kontrolki po drugiej stronie kabla, co udowodniło poprawne zmontowanie kabla symetrycznego.

Z powodu niesprawności bardziej zaawansowanego sprzętu, nie byliśmy w stanie sprawdzić klasy kabla czyli szybkości połączenia przez kabel ani dalszych parametrów zmontowanego kabla.



Wniosk

Zbudowanie kabla okazała się prostym zadaniem. Mimo to już podczas tego prostego testu zauważyliśmy kilka właściwości kabla. Przedewszystkim delikatną trudność sprawiło ustawienie (odgięcie) kabli w odpowiednie miejsce. Sądzymy więc że każda z par kabli miała różną długość skręcania, co zgadza się z ogólną specyfikacją. Taką technikę stosuje się w celu wyeliminowania wzajemnych zakłóceń (przesłuchów). Dodatkowo podczas zdejmowania izolacji z początków kabla zauważyliśmy folię owiniętą wokół wszystkich par kabli. Był to dowód że kabel ten jest w rzeczywistości skrętką ekranową typu F/UTP. Folia ta stosowana jest w celu tłumienia zakłóceń zewnętrznych oraz minimalizacji zakłóceń fal radiowych.

Jak łatwo można zauważyć, budowa kabla skrętkowego nie jest zbyt skomplikowana i pokazuje że do przesyłania sygnały internetowego (nawet dużych prędkości) nie trzeba skomplikowanego okablowania. Jego prostota wpływa też na łatwość diagnozowania ewentualnych uszkodzeń sieci. Wadą takiego rozwiązania jest krótka długość pojedynczego segmentu, w przypadku skrętek nieekranowych duża podatność na zakłócenia oraz łatwość uszkodzeń.

Mimo to kabel tego typu w dalszym ciągu cieszy się dużą popularnością, zwłaszcza w sieciach lokalnych.



Grupa ćwiczw.	Grupa lab.	Zespół	Data wykonania	Data odbioru
Nr ćwiczw.				
Imiona i nazwiska				Ocena i uwagi

Przygotowanie

Do ćwiczenia wykorzystano dwa stanowiska o tej samej specyfikacji. Użyty został system CentOS a do strumieniowania i odbioru strumienia darmowy odtwarzacz VLC. Zadanie składało się z testowania protokołu http(:8080) i rtp(:5004), za pomocą kilku profili, które zostały przedstawione poniżej. Strumieniowane były 3 pliki o rozdzielczości kolejno: 1080p, 720p, 480p kodowane różnymi kodekami. Z powodów technicznych niestety nie byliśmy w stanie przeprowadzić testu sieci rtp więc testu ogranicza się do porównywania wartości z protokołu http.

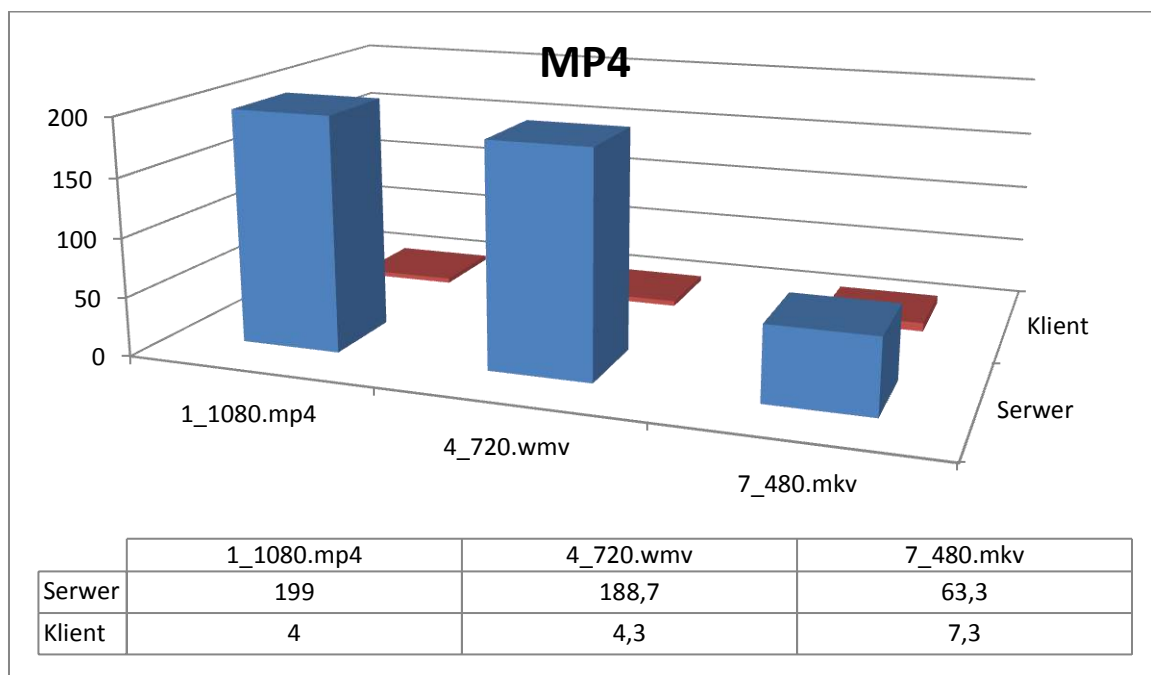
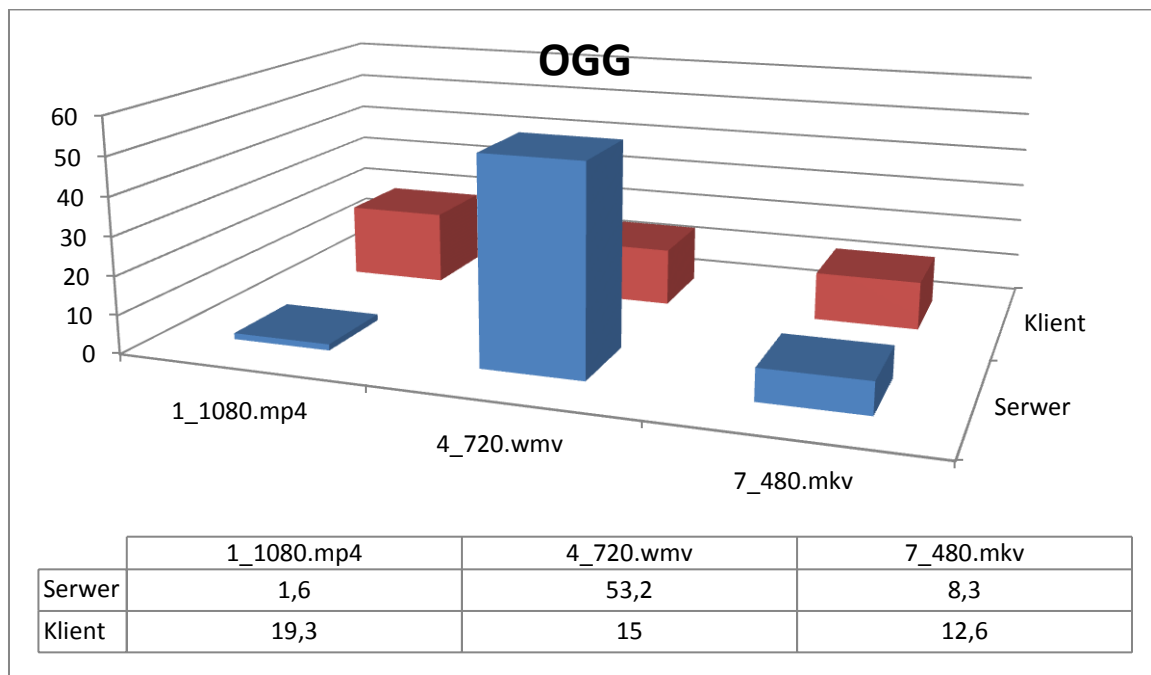
The first two screenshots show the 'Kodek' (Codec) tab for Stream 0 and Stream 1. Stream 0 is an H264 - MPEG-4 AVC (part 10) (avc1) video stream with resolution 1920x1080 and 25 frames/s. Stream 1 is an MPEG AAC Audio (mp4a) audio stream with a sampling rate of 44100 Hz and a bitrate of 1411 kb/s.

The third screenshot shows the 'Kodek' tab for Stream 0 and Stream 1. Stream 0 is an MPEG AAC Audio (mp4a) audio stream with a sampling rate of 48000 Hz. Stream 1 is an H264 - MPEG-4 AVC (part 10) (avc1) video stream with resolution 864x480 and a language of English.

Położenie:

Zamknij (c)

Protokół	Parametry strumienia	Nazwa i parametry pliku	Serwer	Klient
http(:8080)	Enkapsulacja: Ogg/Ogm Video: Theora, 25 fps, 800 kb/s Audio: Vorbis, 2 kanały, 128 kb/s, 44,1 kHz	1_1080.mp4, 40,5 MB, 2:17 min video: H264-mpeg4-AVC, 1920x1080 audio: MPEG AAC, 44.1 kHz,	Ilość klientów: 1 Średnie zużycie procesora : 1,6%	Średnie zużycie procesora : 19,3% Ocena: przyzwoita jakość, występowanie dużej ilości małych artefaktów
	Enkapsulacja: MP4/MOV Video: H264, 25 fps Audio: MPEG Audio, 128 kb/s, 2 kanały, 44,1 kHz		Ilość klientów: 1 Średnie zużycie procesora : 199%	Średnie zużycie procesora : 4,0% Ocena: jakość perfekcyjna, brak artefaktów
	Enkapsulacja: Ogg/Ogm Video: Theora, 29,96 fps, 800 kb/s Audio: Vorbis, 2 kanały, 128 kb/s, 44,1 kHz	4_720.wmv, 150 MB, 3:09 min video: WMV3, 1280x736 audio: WMA2, 48 kHz,	Ilość klientów: 1 Średnie zużycie procesora : 53,2%	Średnie zużycie procesora : 15,0% Ocena: jakość przeciętna, obraz zawiera przeciętną ilość szczegółów, obecność artefaktów
	Enkapsulacja: MP4/MOV Video: H264, 29,96 fps Audio: MPEG Audio, 128 kb/s, 2 kanały, 44,1 kHz		Ilość klientów: 1 Średnie zużycie procesora : 188,7%	Średnie zużycie procesora : 4,3% Ocena: przyzwoita jakość, spadła ilość szczegółów, sporadyczne artefakty
	Enkapsulacja: Ogg/Ogm Video: Theora, 800 kb/s Audio: Vorbis, 2 kanały, 128 kb/s, 44,1 kHz	7_480.mkv, 16,9 MB, 4:54 min video: H264-mpeg4-AVC, 864x482 audio: MPEG AAC, 48 kHz	Ilość klientów: 1 Średnie zużycie procesora : 8,3%	Średnie zużycie procesora : 12,6% Ocena: Wyraźne artefakty, kiepska jakość obrazu, mało szczegółów obrazu
	Enkapsulacja: MP4/MOV Video: H264 Audio: MPEG Audio, 128 kb/s, 2 kanały, 44,1 kHz		Ilość klientów: 1 Średnie zużycie procesora : 63,3%	Średnie zużycie procesora : 7,3% Ocena: Mała ilość szczegółów, przeciętna jakość, sporadyczne artefakty



Analiza wyników

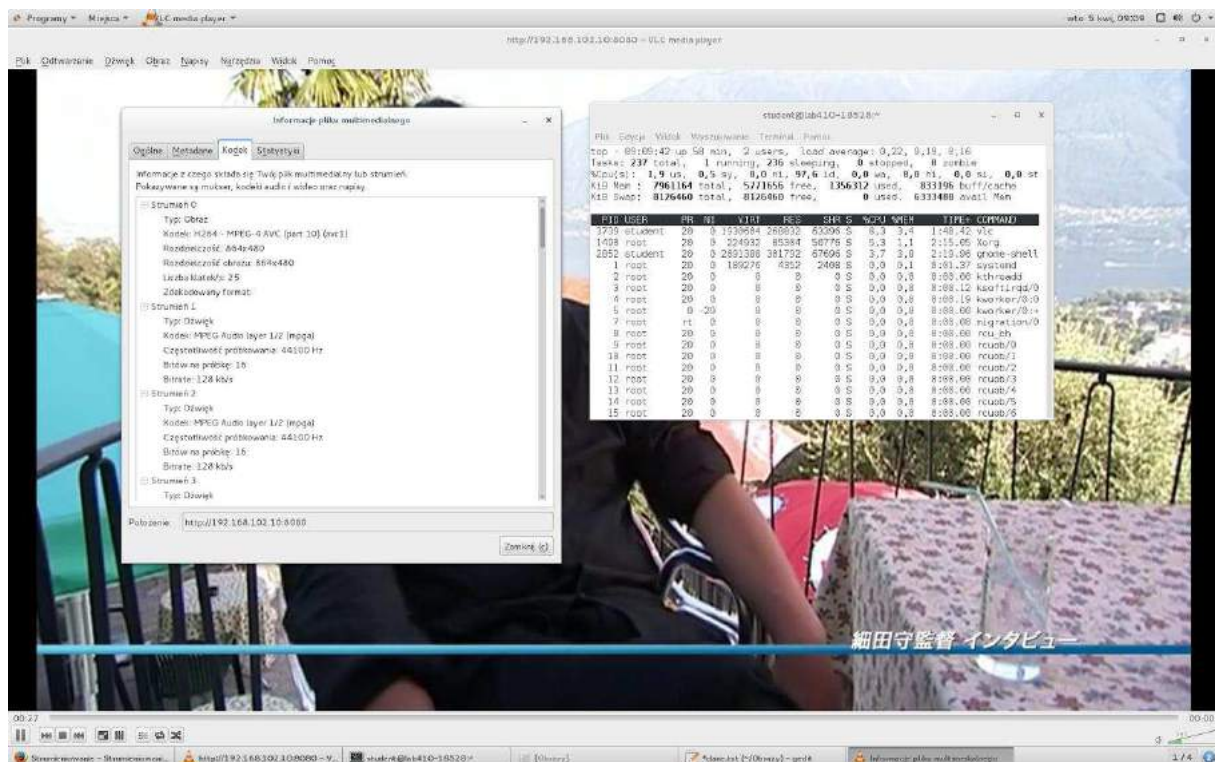
Łatwo zauważyć że największe zużycie procesora dla serwera występowało w przypadku użycia kodowania MP4. Dla wszystkich rozdzielczości było ono zauważalnie większe od zużycia procesora przy kodowania OGG. (Wartości większe od 100% oznaczają uruchomienie kolejnych rdzeni procesora) Jak należałoby się spodziewać jakość w kodowanie mp4 jest o wiele lepsza niż w przypadku konkurenta. W przypadku Ogg często mogliśmy zobaczyć dużą ilość artefaktów które w

znacznym stopniu utrudniały oglądanie. Zdecydowanym zaskoczeniem było stwierdzenie że najmniejsze zniekształcenia otrzymywaliśmy przy strumieniowaniu pliku w jakości 1080p (mogłoby się wydawać że przesyłania tak dużego pliku może być utrudnione). Niezależnie od wybranego kodowania im większa jakoś pliku wyjściowego tym lepszy odbierany obraz. W ostatecznym rozrachunku pliki w rozdzielczości 480p i kodowaniu Ogg praktycznie nie nadawały się do oglądania. Trzeba też zauważyć że komputery wykorzystywane do badania połączone były w sieci lokalnej a więc zakłócenia, normalnie spotykane w globalnej sieci praktycznie nie występowały.

The screenshot shows a VLC media player window with a video stream of a person in a plaid shirt. Two windows are overlaid on the video:

- Informacje pliku multimedialnego (Media Information):**
 - Typ: Obyraz
 - Kodek: H264 - MPEG-4 AVC (part 10) (h264)
 - Rozdzielczość: 1920x1080
 - Rozdzielczość obrazu: 1920x1080
 - Łączna klatki: 25
 - Zakodowany format:
 - Strumień 1:
 - Typ: Dźwięk
 - Kodek: MPEG Audio layer 1/2 (mpga)
 - Capośćkliwość próbkowania: 44100 Hz
 - Bitów na próbkę: 16
 - Wzrost: 128 kbit/s
 - Strumień 2:
 - Typ: Dźwięk
 - Kodek: MPEG Audio layer 1/2 (mpga)
 - Capośćkliwość próbkowania: 44100 Hz
 - Bitów na próbkę: 16
 - Wzrost: 128 kbit/s
 - Strumień 3:
 - Typ: Dźwięk
- Terminal window:**
 - Top: 00:48:30 up 37 s, 2 users, load average: 0,31, 0,21, 0,17
 - Tasks: 239 total, 1 running, 238 sleeping, 0 stopped, 0 zombie
 - Mem: 1,1 us, 0,5 sv, 0,0 ni, 98,3 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
 - Mem: 7961168 total, 8143764 free, 1239248 used, 570220 buffers
 - Mem: 8126468 total, 8126460 free, 8 used, 6457156 avail Mem
 - Table with 10 columns: PID, USER, PR, NI, VIRT, RES, SHR, S, CPU, MEM, COMMAND

Na zamieszczonym powyżej snapshot'cie możemy zauważyć plik wideo w jakości 1080p(kodek MP4 czyli najlepszą jakość którą odbierany przez klienta. Jakość tego stream'u jest więcej niż zadowalająca. Można bez najmniejszych problemów cieszyć się jakością Full HD niemalże bez zakłóceń. Dla porównania poniżej zamieszczamy snapshot dla pliku wideo w jakości 480p (także z użyciem kodeka). Można zauważyć znaczną utratę danych (w stosunku do oryginalnego pliku)



Wnioski

Podsumowując nasze spostrzeżenia, strumieniowanie jest użytecznym sposobem wysyłania plików wideo. Często wykorzystywany jest do tworzenia video blogów wyświetlanych „na żywo”. W związku z tym że nie udało nam się przetestować protokołu rtp (na danym sprzęcie strumieniowanie działało tylko na http). Mimo to zebraliśmy interesujący zestaw danych.

Według testów, najlepiej podczas strumieniowania spisywał się kodek MP4, zaś Ogg nakładał mniejszy stres na procesor w przypadku serwera. Jakości połączeń były bardzo dobre, co wiąże się z zamieszczeniem klienta i serwera w sieci lokalnej. Dodatkowo, przy dużej szerokości pasma w pracowni komputerowej najlepiej wypadły streamy w jakości wyjściowej jak najlepszej; Straty na wszystkich jakościach były porównywalne więc pliki z mniejszą początkową rozdzielczością bardziej cierpiały od utraty danych.



Grupa ćwicz.	Grupa lab.	Zespół	Data wykonania	Data odbioru
Nr ćwicz.				
Imiona i nazwiska				Ocena i uwagi

Wstęp:

Celem ćwiczenia jest przetestowanie różnych typów szyfrowania oraz ich wpływu na zużycie zasobów sprzętowych przy transferze plików za pomocą tunelu stworzonego między maszynami wirtualnymi pod kontrolą systemu Linux. Przesłane zostały 3-krotnie 2 różne pliki, plik binarny o wadze 400MB oraz plik wideo o wadze 200MB za pomocą 2 typów szyfrowania Blowfish oraz Arcfour na 3 poziomach kompresji – 0, 1 i 9.

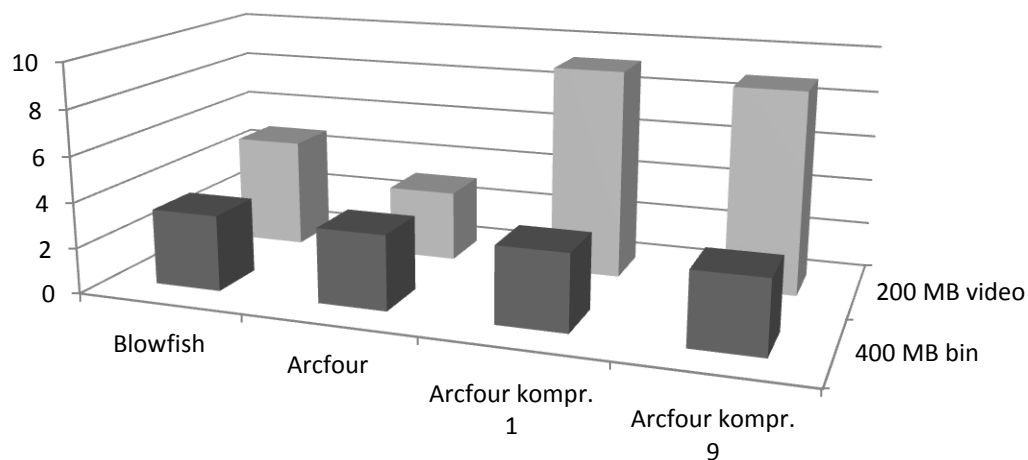
Dane oraz pomiary:

	plik binarny 400MB			
	zużycie procesora serwer [%]	zużycie procesora klient [%]	prędkość transmisji [MB/s]	czas transferu [s]
Blowfish bez kompresji	11	9,8	149	3,4
	10,3	7,9	147	3,4
	12,1	9,2	153	3,2
	11,13	8,97	149,67	3,33
Arcfour bez kompresji	13,4	10,7	155	3,2
	14	12,5	154	3,3
	12,6	10,1	149	3,3
	13,33	11,10	152,67	3,27
Arcfour kompresja 1	19,5	10,5	150	3,3
	16,9	12	147	3,4
	17,1	11,2	149	3,3
	17,83	11,23	148,67	3,33
Arcfour kompresja 9	30,1	9,9	149	3,3
	18	11,5	153	3,1
	23,2	12,4	155	3,1
	23,77	11,27	152,33	3,17

	plik wideo 200MB			
	zużycie procesora serwer [%]	zużycie procesora klient [%]	prędkość transmisji [MB/s]	czas transferu [s]
Blowfish bez kompresji	33,2	9,9	70,2	4,9
	35	9	69,4	5
	31,5	10,4	73	4,6
	33,23	9,77	70,87	4,83
Arcfour bez kompresji	39,7	10,6	91	3,1
	32,2	12,8	97,6	3,2
	41,9	10	98,5	3
	37,93	11,13	95,70	3,10
Arcfour kompresja 1	50,6	2,1	22,3	9,2
	49,5	2,4	24,6	8,8
	54	1,8	20,9	9,5
	51,37	2,10	22,60	9,17
Arcfour kompresja 9	56,1	2	25,6	9
	52,1	2,4	24,9	8,7
	53,3	2,4	25	8,8
	53,83	2,27	25,17	8,83

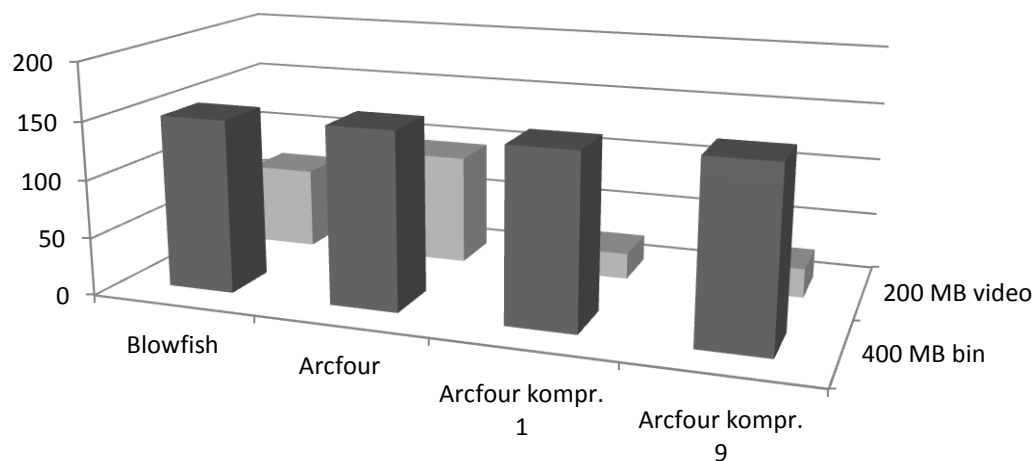
Statystyki i opracowanie danych:

Czas transferu [s]



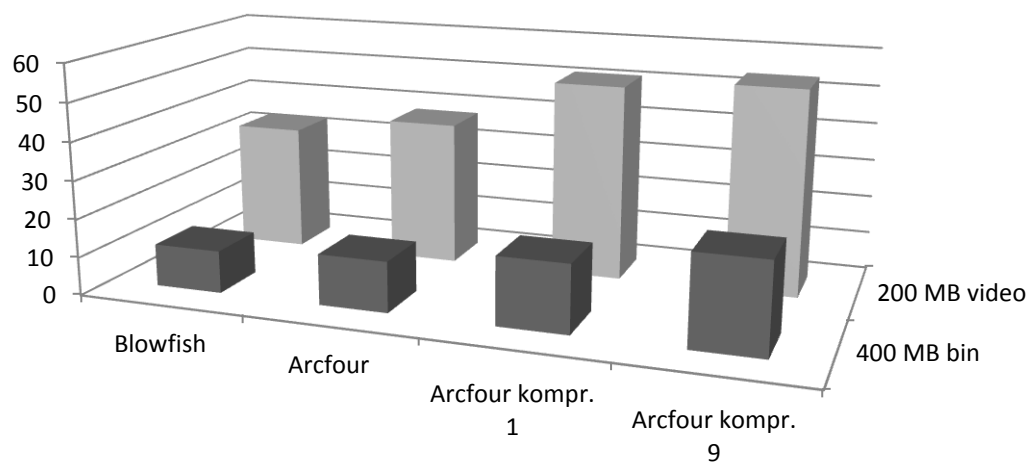
	Blowfish	Arcfour	Arcfour kompr. 1	Arcfour kompr. 9
400 MB bin	3,33	3,27	3,33	3,17
200 MB video	4,83	3,1	9,17	8,83

Prędkość transmisji [MB/s]



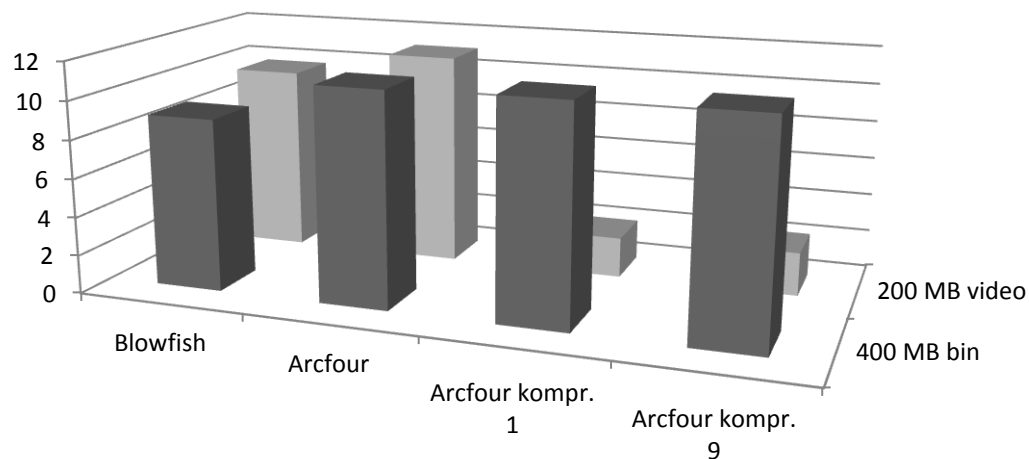
	Blowfish	Arcfour	Arcfour kompr. 1	Arcfour kompr. 9
400 MB bin	149,67	152,67	148,67	152,33
200 MB video	70,87	95,7	22,6	25,17

Zużycie procesora - serwer [%]



	Blowfish	Arcfour	Arcfour kompr. 1	Arcfour kompr. 9
400 MB bin	11,13	13,33	17,83	23,77
200 MB video	33,23	37,93	51,37	53,83

Zużycie procesora - klient [%]



	Blowfish	Arcfour	Arcfour kompr. 1	Arcfour kompr. 9
400 MB bin	8,97	11,1	11,23	11,27
200 MB video	9,77	11,13	2,1	2,27

Analiza:

Jak widać przesyłanie danych przez stworzony tunel kładzie obciążenie w szczególności na serwerze, gdzie obciążenie na serwerze sięga od 10 do 50% natomiast na kliencie waha się między 2 a 11%. Bezpośrednim skutkiem stosowania kompresji jest oczywiście zwiększenie zużycia procesora w szczególności na serwerze, co jest wytłumaczalne przez obliczenia które musi wykonać serwer nad plikiem aby przestać go już skompresowany. Porównując Arcfour i Blowfish bez kompresji, widać, że Blowfish jest nieznacznie mniej wymagający co do zużycia procesora. Jeśli chodzi o transfer osiągnięty przez szyfrowania i pliki to widać wyraźną różnicę. Jeśli chodzi o plik binarny to mimo zastosowania różnych stopni kompresji transfer wyniósł ~145 MB/s we wszystkich przypadkach. Natomiast jeśli chodzi o plik wideo to transfer jest o wiele mniejszy, w szczycie sięga 95 MB/s dla szyfrowania bez kompresji, kiedy kompresja jest stosowana to transfer spada o ponad połowę do niewielkiej szybkości ~25 MB/s. Co do czasu przesyłania to jest on poniekąd bezpośrednim skutkiem szybkości transferu, która jest skutkiem typu szyfrowania, zastosowanej kompresji oraz narzutu jaki ona wywołuje na procesorze. Niemniej jednak da się zaobserwować ciekawe zjawisko a mianowicie, dla pliku binarnego czas przesyłania oscyluje w okolicy 3 s, a w przypadku pliku video czas przesyłania wynosi 3-4s przy braku kompresji a przy jej stosowaniu ten czas się podwaja aż do 9s.

Wnioski:

Z eksperymentu jasno widać że o wiele lepsze prędkości osiągamy przy przesyłaniu pliku binarnego, którego prędkość przesyłania jest często kilkakrotnie większa niż w przypadku pliku wideo nawet mimo tego że wideo było 2 razy mniejszym plikiem. Jeśli porównujemy Arcfour i Blowfish bez kompresji to widać, że Arcfour wymaga większej pracy procesora w porównaniu do Blowfish, co widać w przypadku gdy plik jest wysyłany oraz odbierany, ma to swoje odbicie w prędkości przesyłania na korzyść Arcfour. Natomiast w przypadku Arcfour z użyciem kompresji widać pewną zależność. Im więcej obliczeń wykona serwer nad plikiem tym mniej jej wykonuje klient. Podsumowując, wyraźnie widać, że znacznie lepiej przysyłać pliki binarne w porównaniu do plików wideo, jeśli chodzi o przesyłanie bez kompresji to zauważalnie lepiej spisuje się Arcfour gdzie prędkości przewyższają nieznacznie Blowfish kosztem większego obciążenia serwera. Jeśli idzie o przysyłanie za pomocą kompresji to widać że przy kompresowaniu wideo dużo obliczeń musi wykonać serwer a znacznie mniej klient co widać po obciążeniu procesora, natomiast w przypadku pliku binarnego sytuacja jest dokładnie odwrotna.



Grupa ćwicz.	Grupa lab.	Zespół	Data wykonania	Data odbioru
Nr ćwicz.				
Imiona i nazwiska			Ocena i uwagi	

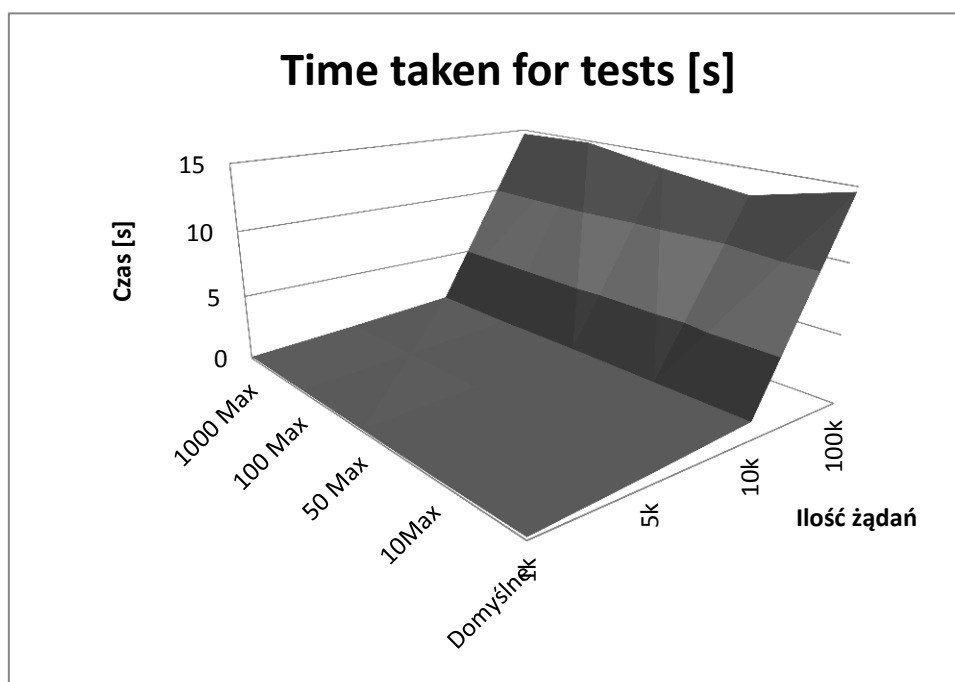
Wstęp:

Celem ćwiczenia jest poznanie technik optymalizacji serwera Apache na podstawie przeprowadzonych pomiarów ze zmianą różnych parametrów. Przebieg pomiarów wygląda następująco, testujemy 4 różne profile tj.1. domyślny, 2. KeepAlive ON-MaxClients 10, 3.KeepAlive ON-MaxClients 50, 4. KeepAlive ON-MaxClients 100 oraz 5. KeepAlive ON-MaxClients 1000 za każdym razem wywołując 1000, 5000, 10000, 100000 żądań. Badane są 4 parametry związane z czasem pomiaru, ilością żądań na sekundę oraz czas na jedno żądanie.

Dane i pomiary:

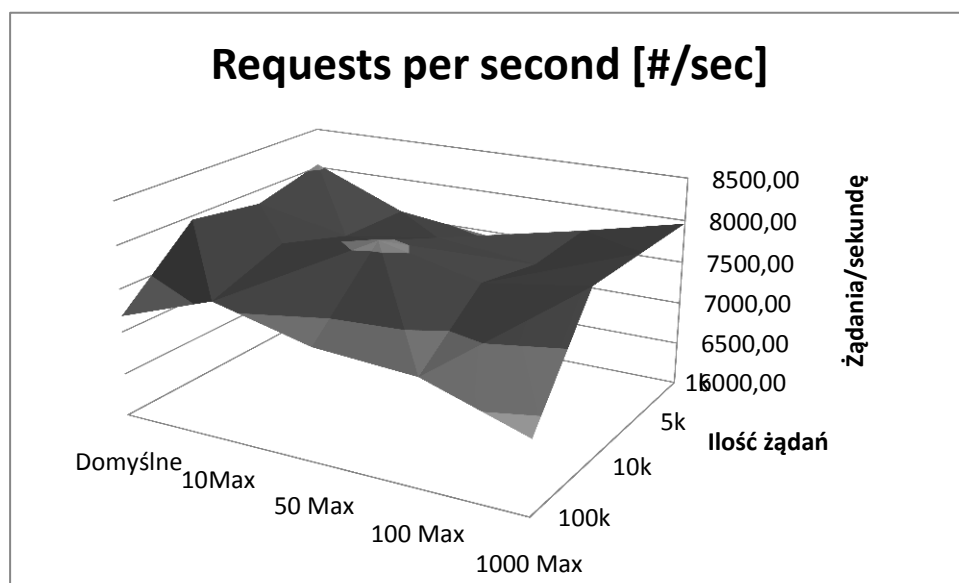
Pomiar parametru „Time taken for tests [s]”

		MaxClients									
Liczba żądań do wykonania		Domyślne		10		50		100		1000	
		Pomiar [s]	Odch. std	Pomiar [s]	Odch. std	Pomiar [s]	Odch. std	Pomiar [s]	Odch. std	Pomiar [s]	Odch. std
	1000	0,20	0,12	0,13	0,00	0,13	0,01	0,12	0,00	0,13	0,02
	5000	0,71	0,15	0,64	0,01	0,63	0,01	0,64	0,01	0,65	0,02
	10000	1,31	0,07	1,30	0,05	1,30	0,02	1,22	0,05	1,26	0,01
	100000	14,66	0,05	13,12	0,11	13,88	0,24	14,86	0,39	14,67	0,49



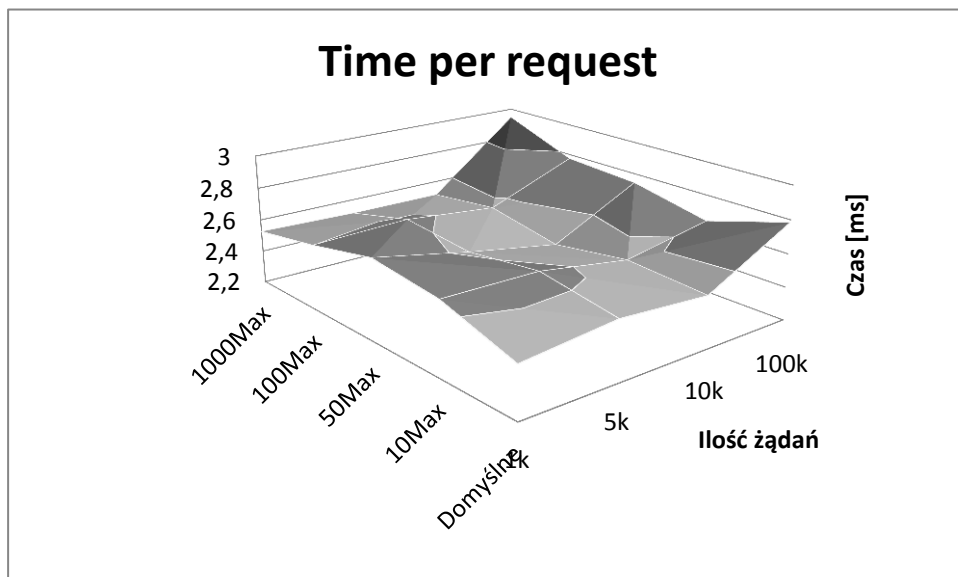
Pomiar parametru "Requests per second [#/sec]"

Liczba żądań do wykonania		MaxClients									
		Domyślne		10		50		100		1000	
		Pomiar	Odch. std	Pomiar	Odch. std	Pomiar	Odch. std	Pomiar	Odch. std	Pomiar	Odch. std
	1000	8037,09	691,91	7580,67	203,72	7439,00	284,04	7695,67	148,53	7963,67	736,19
	5000	7827,94	12,26	7600,00	173,43	7768,00	136,17	7644,33	281,22	7975,33	255,47
	10000	7957,81	174,27	7860,00	150,84	8083,67	193,79	7810,33	107,02	7985,67	346,70
	100000	7183,91	109,87	7572,67	54,15	7295,33	90,28	7218,00	191,50	6833,33	608,91



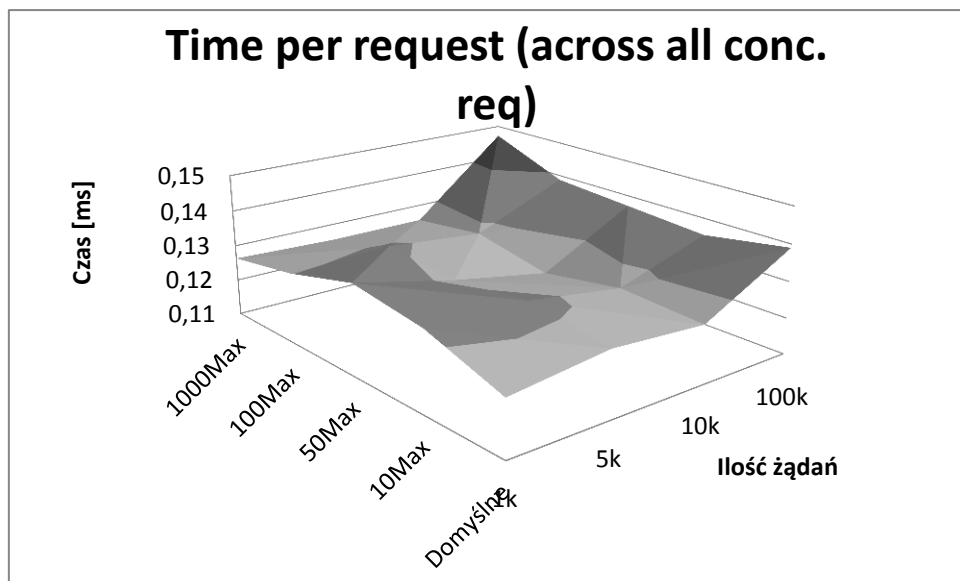
Pomiar parametru "Time per request [ms] (mean)"

Liczba żądań do wykonania		MaxClients									
		Domyślne		10		50		100		1000	
		Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std
	1000	2,50	0,22	2,64	0,07	2,69	0,10	2,60	0,05	2,53	0,24
	5000	2,56	0,00	2,63	0,06	2,58	0,05	2,62	0,09	2,51	0,08
	10000	2,51	0,05	2,55	0,05	2,48	0,06	2,56	0,03	2,51	0,11
	100000	2,78	0,04	2,64	0,02	2,74	0,03	2,77	0,07	2,94	0,27



Pomiar parametru "Time per request [ms] (mean, across all conc. req)"

Liczba żądań do wykonania		MaxClients									
		Domyślne		10		50		100		1000	
		Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std	Pomiar [ms]	Odch. std
	1000	0,13	0,01	0,13	0,00	0,14	0,01	0,13	0,00	0,13	0,01
	5000	0,13	0,00	0,13	0,00	0,13	0,00	0,13	0,00	0,13	0,00
	10000	0,13	0,00	0,13	0,00	0,12	0,00	0,13	0,00	0,13	0,01
	100000	0,14	0,00	0,14	0,01	0,14	0,00	0,14	0,00	0,15	0,01



Analiz wyników:

Podczas pomiaru parametru „Time Taken For Test” wszystkie profile przy małej i średniej ilości zadań do wykonania cechowała się niemal identycznymi oraz niezmiennymi wynikami. (Różnica w granicy 0.1). Dopiero od 100000 zadań następuje znaczne wydłużenie czasu.

Dla pomiaru „Request per Second” sytuacja nie jest aż tak klarowna. Najwięcej zadan w ciągu sekundy wykonać mogły profile Domyślny i 1000 MAX , przy czym dla profilu 50MAX też występowało ekstremum lokalne sugerujące, zwiększoną liczbę zadań.

Dla obydwóch parametrów Tiem per Request, najlepsze („Najniższe”) wyniki otrzymywaliśmy dla środkowych profili czyli 10,50 oraz 100 MAX. Oczywiście także i tutaj można było zauważyć znaczne wydłużenie czasu przy 100000 zadań

Wnioski:

Optymalizacja , jest ważna nie tylko przy tworzenia własnego serwera HTTP. Każdy program, czy to pisany jako projekt zaliczeniowy, czy zlecenie zawodowe, musi zmierzać do jak największej optymalizacji kosztów pracy. W przypadku programów, są to zasoby takie jak pamięć czy procesor. W przypadku serwera mogą być to zarówno łącze jak również zasoby obliczeniowe.

Analizując powyższe przykłady, wybraliśmy dwa profile, które naszym zdaniem najbardziej optymalizowały powierzone zadania. Są to odpowiednio profile 10MAX i 50 MAX. Obydwa te profile osiągnęły bardzo dobre wyniki w pomiarach czasu zadania. Dla ilości zadań do 100000 wynik był bardzo dobry. Przy pomiarze parametru „Time taken for tests [s]” profile te osiągnęły najlepszy wynik spośród wszystkich innych profili(Mimo niewielkiej różnicy jest ona zdecydowania wyraźniejsza tylko dla tych dwóch profili). Dla parametru „Ilości zadań na sekunde”, profile te osiągnęły zadowalający poziom. Nie były one najwyższe, ale znajdowały się na dwóch krańcach ekstremum lokalnego, więc ilość wykonywanych zadań nie była mała. Mimo jednego słabszego wyniku, reszta w zupełności rekompensuje tę stratę. Profile 10 i 50 są najbardziej z optymalizowanymi ze względu na „średnio” najlepsze wartości w każdym wybranym parametrze.

Optymalizacja nie zawsze wybiera same najlepsze rozwiązania. Wybiera te które w wynikach i efektach długo falowych dadzą najlepszy efekt