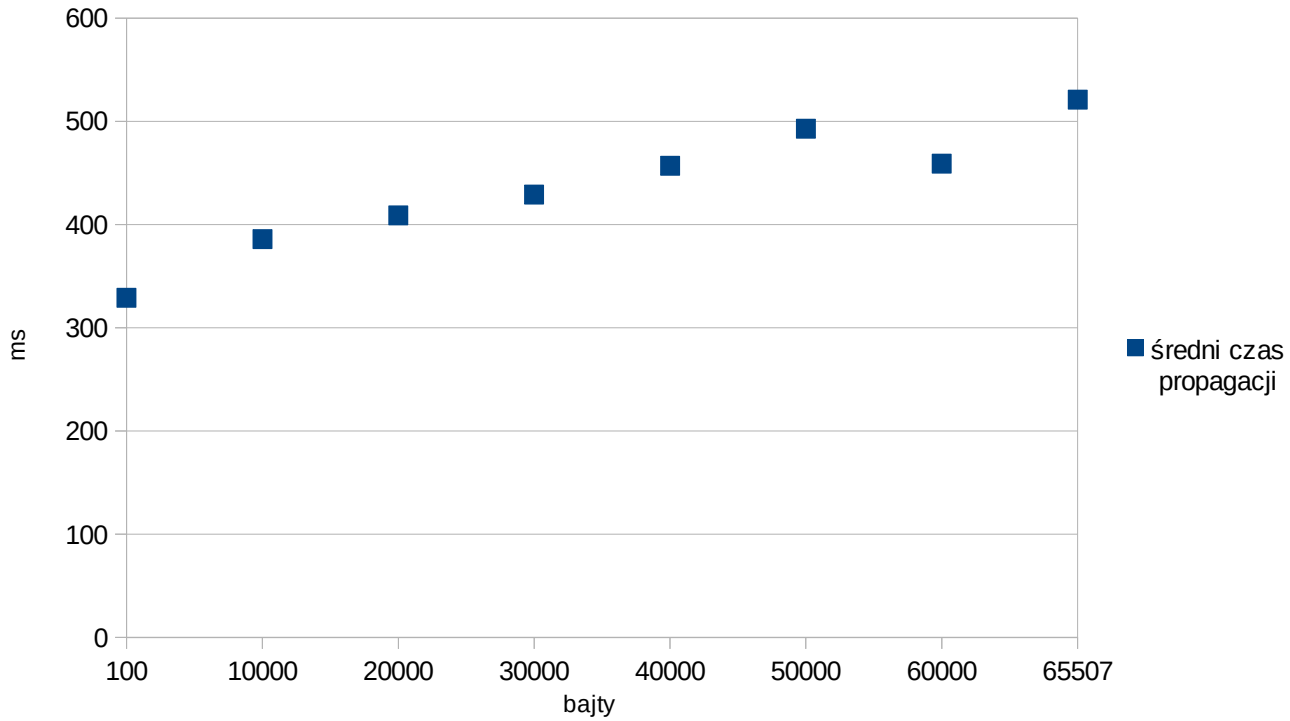
PING

Program ten wysyła pakiety ICMP ECHO_REQUEST do hostów sieciowych, służy do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami.

Testowanie zacząłem od wybrania serwera który znajduje się w znacznej odległości od mojego komputera, poszukiwania zacząłem od Nowej Zelandii (www.govt.nz) gdyż jest jednym z najdalej położonych krajów od Polski. Kombinując z ustaleniem optymalnej wartości wskaźnika TTL (ping -t) tak aby wiadomość dotarła do celu, uzyskałem wynik 15, w pakiecie powrotnym TTL wynosiło 55 wywnioskowałem z tego, że droga powrotna wynosi 65-55 czyli 10 węzłów. Jednak jak mogło by się wydawać nie była to najdłuższa trasa pod względem ilości węzłów, okazała się droga do serwera w Brazylii (www.brasil.gov.br) gdzie ilość węzłów w drodze do wniosła 20, natomiast z powrotem było ich zapewne 255-238 czyli 17. Dłuższej trasy nie udało mi się znaleźć, więc dalsze testy będą przeprowadzane na domenie z Brazylii.

Po ustaleniu trasy zabrałem się za sprawdzenie jak wielkość pakietu wpływa na długość trasy. Pozwoliłem programowi na fragmentację pakietu, zacząłem od 100 bajtów i dodawałem co krok 5000 bajtów aż do wielkości maksymalnej pakietu, czyli 65507 bajtów, nie zauważyłem żadnej zmiany w ilości węzłów, jedyne co się zmieniało to ilość utraconych pakietów, wyraźnie zwiększała się wraz z wielkością pakietu.

Dla zależności czasu propagacji od wielkości wysłanego pakietu sporządziłem wykres, średni czas propagacji był ustalany dla 50 pakietów.
(ping -s l.bajtów -c 50 -q www.brasil.gov.br)

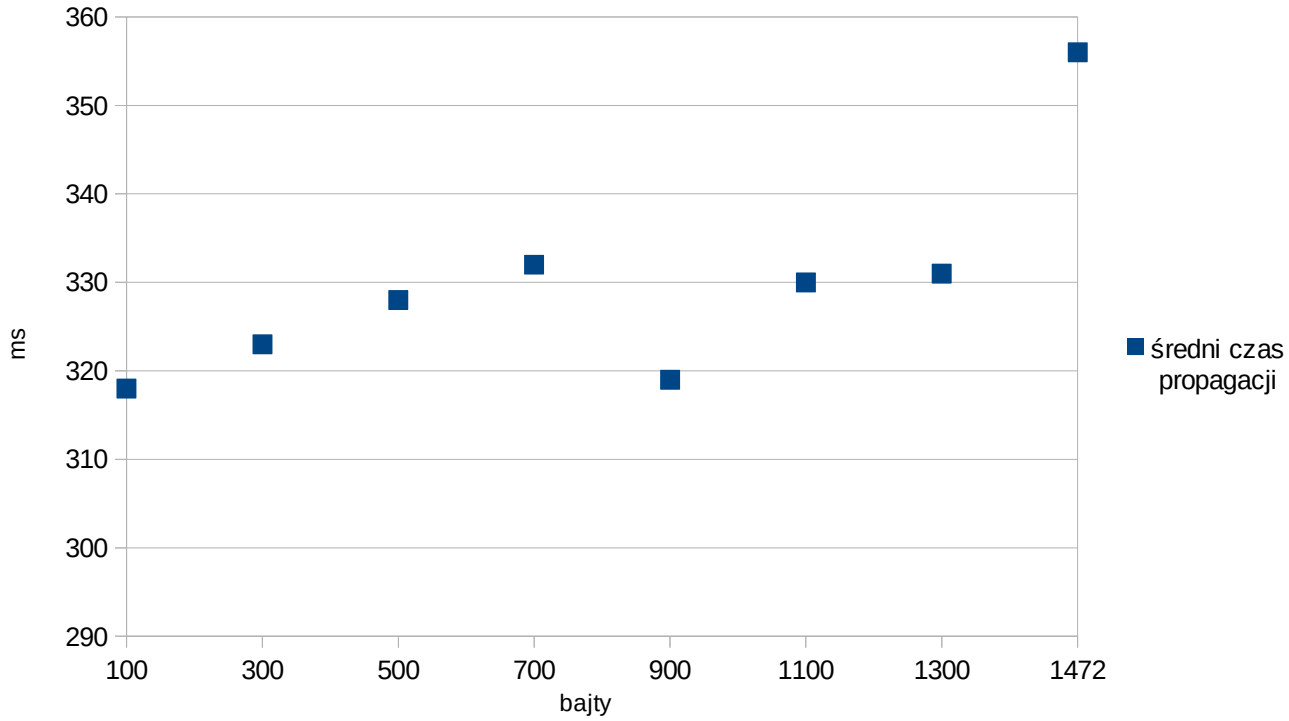


Widzimy, że na powyższym wykresie wystepuje tendencja wzrostowa.

Teraz powtórzymy dwa ostatnie doświadczenia bez fragmentacji pakietu. Tym razem również nie zauważyłem zmiany ilości TTL w zależności od wielkości pakietu, jedyna co się

zmieniło to maksymalna ilość bajtów jaka udało mi się wysłać, wyniosła ona 1472. Zdażały się utracone pakiety ale w znikomych ilościach.
(ping -s 1473 -M do www.brasil.gov.br)

Tutaj dla zależności czasu propagacji od wielkości wysłanego pakietu również sporządziłem wykres, lecz o nieco mniejszej skali średni czas propagacji był ustalany dla 50 pakietów. (ping -c 50 -s l.bajtów -M do www.brasil.gov.br)

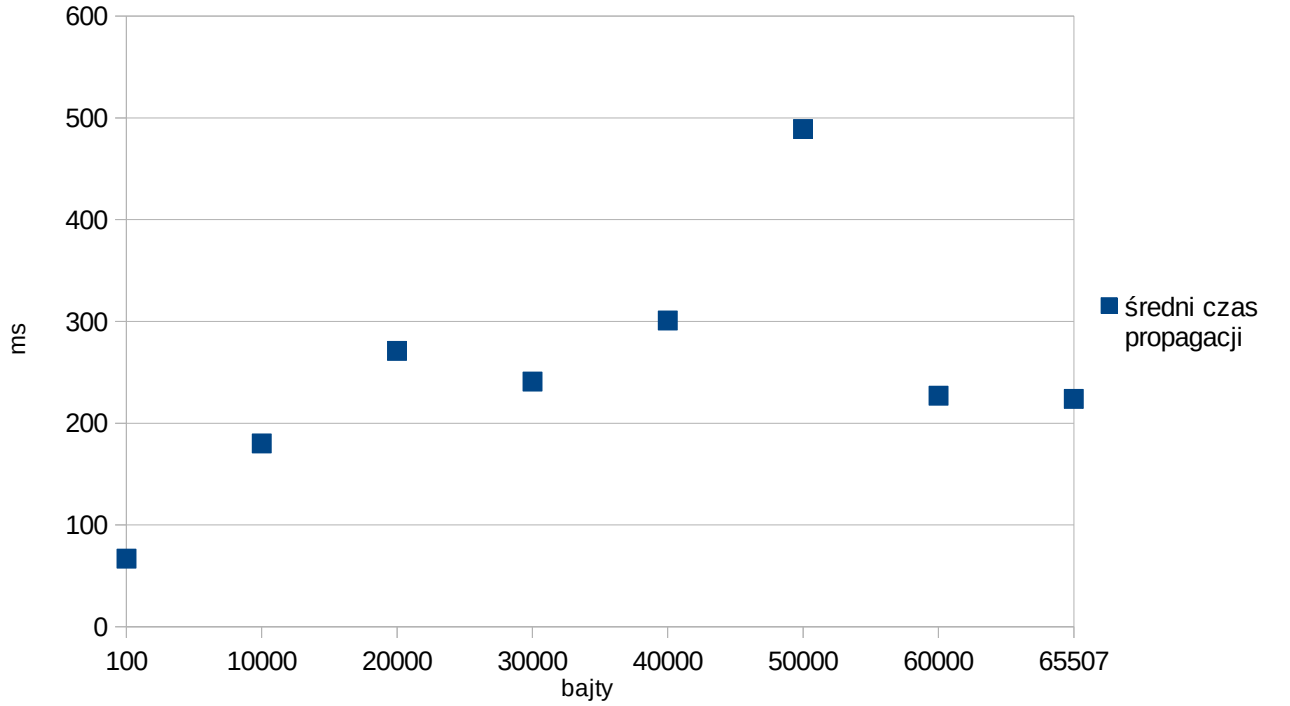


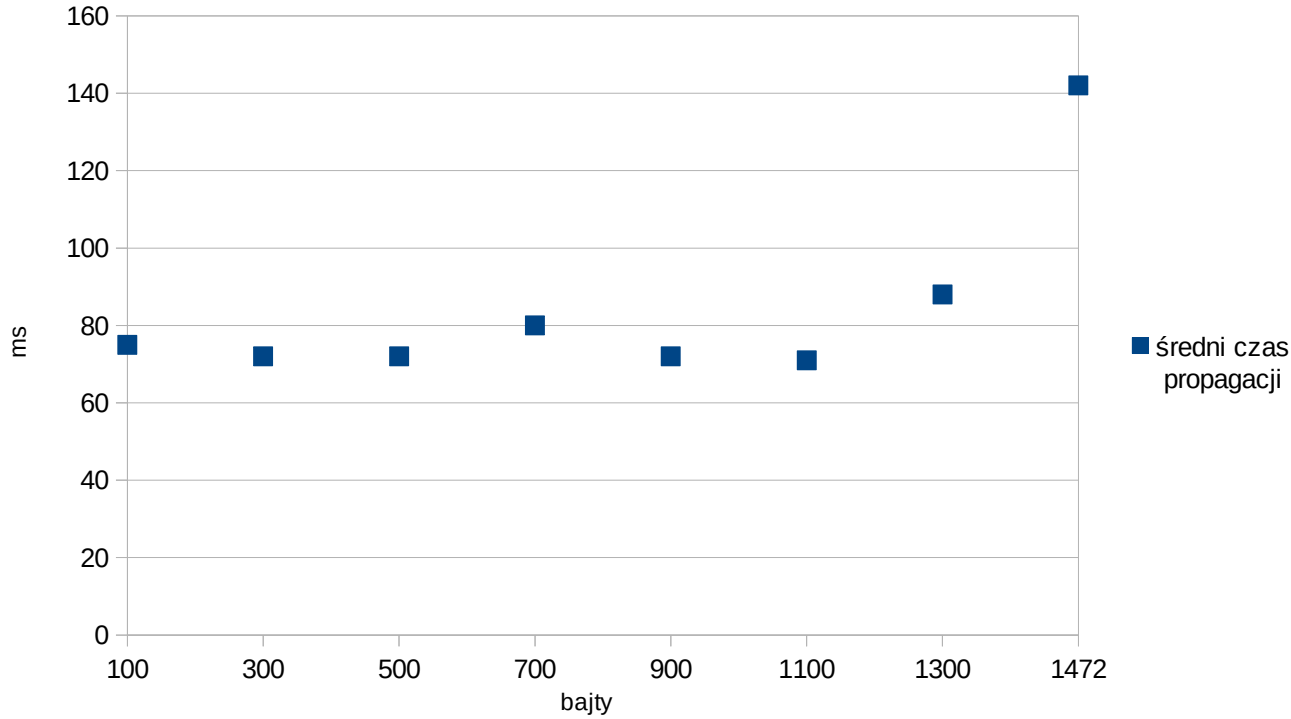
Tu również mamy do czynienia z tendencją wzrostową choć nie tak wyraźną jak wcześniej.

Jako domenę w bliższej odległości wybrałem www.wroclaw.pl , ilość węzłów które w drodze do wyniosła 9 natomiast z powrotem domyślam się, że było ich 65-53 czyli 13.

Ilość węzłów ze względu na wartość pakietu nie zmieniła się zarówno dla pakietów które były podzielone jak i dla tych gdzie zabroniłem fragmentacji. Również tym razem maksymalna wielkość wysłanego pakietu bez fragmentacji wyniosła 1472 a z fragmentacja 65507.

Tu również sporządziłem wykresy średnich czasów propagacji, pierwszy z fragmentacja drugi bez. Ilość utraconych pakietów wyraźnie się zmniejszyła, wartości te
były znikome. W obydwu przypadkach widzimy nadal tendencje wzrostową choć nie tak wyraźną jak dla domeny leżącej w znacznej odległości.





W moim przypadku najdłuższa trasa jaką udało mi się znaleźć to 20 węzłów, więc wydaje mi się, że „średnica internetu” jest bliska tej wartości.

Co do sieci wirtualnych, domena www.presidence.gov.mg
jest nie osiągalna przez program ping nawet przy parametrze -t ustawionym na maksymalna wartość czyli 255. Testowałem to połaczenie również za pomocą programu traceroute wpisując różne maksymalne wartości parametru -m czli maksymalna wartość węzłow na drodze, w okolicach 16 węzłu program zaczynał jakby krążyc routery szyfrowane czyli te oznaczone „***” przeplatały się z jednym zawsze tym samym adresem ip, trasy były różne ale nie udało się osiagnąć celu, myślę, że jest to dobry przykład sieci wirtualnej.

TRACEROUTE

Pokazuje on trasę jaką przechodzą pakiety między naszym komputerem, a sprawdzanym przez nas hostem. Wskazuje on czasy przesłania pakietów pomiędzy sąsiadującymi ze sobą routerami. Pozwala śledzić trasę pakietów oraz wykrywać różnego rodzaju problemy w sieciach np.: błądzenie pakietów w sieci. Brak odpowiedzi jest sygnalizowany znakiem „*” , może on wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń.

Zasada działania jest taka, że na początku wysyłany jest pakiet z polem TTL ustawionym na 1. Wartość ta jest zmniejszana przy przechodzeniu przez kolejne routery na trasie. Jeżeli pole TTL osiągnie wartość 0 to pakiet jest odrzucany przez router, który wysyła wtedy informację zwrotną w postaci komunikatu ICMP typu "Time to live exceeded". W ten sposób uzyskujemy adres ip pierwszego routera na trasie, jeśli chcemy uzyskać adres następnego routera ustawiamy wartość TTL na 2, analogicznie postępujemy w każdym następnym kroku, kiedy pakiet dotrze do hosta odpowiada on powiadomieniem ICMP "port unreachable".

Dla przykładu trasa do domeny www.wroclaw.pl biegła przez Krzynów woj.Wielkopolskie, znalazły się na nie również cztery zaszyfrowane routery a ostatnie 2 punkty na tej trasie były w Gdańsku. Po próbie zablokowania fragmentacji pakietu(opcja -F), czasy propagacji zwiększyły się, niektóre nawet dwukrotnie i zmieniła się również trasa. To samo zjawisko wystąpiło dla domeny znacznie oddalonej znajdującej się w Brazylii.

WIRESHARK

Wireshark jest graficznym analizatorem ruchu sieciowego. Umożliwia przechwytywanie danych transmitowanych przez określone interfejsy sieciowe. Ponadto szczegółowo wizualizuje strukturę przechwyconych danych dla wielu protokołów sieciowych. Wireshark działa w sposób pasywny, tzn. nie wysyła żadnych informacji, a tylko przechwytuje dane docierające do interfejsu sieciowego. Nie wpływa także w żaden sposób na działanie aplikacji przesyłających dane przez sieć. Program należy uruchomić z uprawnieniami roota. Program umożliwia przechwytywanie danych lecz nadawce i autora opisuje numerami IP, dla ułatwienia włączyłem w ustawieniach opcje która spowoduje to, że te adresy będą zamieniane na rzeczywiste nazwy domen.

W celu przechwycenia informacji wybieramy interfejs jakim chcemy się posługiwać w moim przypadku był to wlp2s0 i klikamy dwukrotnie, nasłuchiwanie rozpocznie się automatycznie. Byłem połączony z internetem więc wireshark zasypał mnie wieloma różnymi pakietami, żeby się w tym wszystkim odnaleźć program ten udostępnia nam opcje filtrowania np.: ze względu na protokół lub adres IP. Weźmy na warsztat protokół icmp zgodnie z którym działa program ping, po włączeniu przechwytywania nic się nie dzieje, uruchommy teraz program ping, i wyślijmy 10 pakietów. W programie wireshark pokazało mi się 20 pakietów jest to spowodowane tym, że na każdy pakiety wysłany z mojej strony serwer udzielił odpowiedzi.

Spróbujmy teraz odczytac dane logowania, wybrałem stronę chomikuj.pl, domyślnie jest ona zabezpieczona, lecz wystarczy po wejściu na nia, podmienić protokół https na nieszyfrowany http. Sprawdźmy działanie dla fałszywych danych, wpisałem losowy ciąg znaków w pole loginu oraz hasła. Następnie uruchomiłem wireshark na aktualnie używanym interfejsie sieciowym i ustawiłem filtrowanie pod kątem protokołu http. Teraz zalogowałem się na stronie chomikuj, w wiresharku widzimy, że z mojego komputera został wysłany jeden pakiet z którego w zakładce HTML Form URL Encoded z łatwością możemy znaleźć wysłany przez nas login i hasło. W pakiecie powrotnym jest m.in. zapisana informacja o tym ze próba logowania nie powiodła się.

Programy które wykorzystywałem pokazały mi jak wiele informacji mogę uzyskać za pomocą wydawać by się mogło tak prostych programów. Uświadomiły mi one również jak duze zagrożenie płynie z tego jeśli nie używamy połączeń szyfrowanych. Dowiedziałem się między innymi jak sprawdzić czy odległy serwer jest dostępny, poznałem znaczenie sieci wirtualnych w bezpieczeństwie serwerów wiem również jak sprawdzić czy ktoś mnie podsłuchuje przez sieć. Programy te w wprawnych rękach mogą wyrządzić wiele dobrego jak i złego(hakerzy).