1)ping

Ping- polecenie, którego używamy w diagnostyce sieci komputerowych. Działa on na zasadzie wysyłania pakietów ICMP (Internet Control Message Protocol) "Echo Request" do określonego hosta i oczekiwania na pakiet "Echo Reply" od tego hosta. Proces ten służy do oceny dostępności celu w sieci oraz do pomiaru czasu trwania podróży pakietu. Kiedy używamy ping do sprawdzenia dostępności urządzenia w sieci, pakiety danych przemierzają określoną trasę w sieci komputerowej. Ta trasa składa się z wielu segmentów i może przebiegać przez różne urządzenia sieciowe (takie jak routery i przełączniki), aby dotrzeć do docelowego hosta. Program ping umożliwia identyfikację czasu, który jest potrzebny pakietowi na pokonanie trasy do celu i z powrotem, co daje użytkownikowi informacje na temat stanu połączenia i potencjalnych opóźnień w sieci.

Trasa: Trasa w kontekście sieci komputerowej to sekwencja węzłów sieciowych (routery lub przełączniki), które pakiet danych musi przejść, aby dotrzeć od nadawcy do odbiorcy. Można ją również nazwać "ścieżką pakietu". Trasa może być różna w zależności od różnych czynników, takich jak obciążenie sieci, konfiguracja routingu itp.

Węzeł: Węzeł w kontekście sieci komputerowej to urządzenie sieciowe, które jest punktem pośredniczącym na trasie pakietów danych. Węzły mogą być różnymi urządzeniami, takimi jak routery, przełączniki, bramy itp. Węzły są odpowiedzialne za przekazywanie pakietów danych z jednego segmentu sieci do drugiego, aż dotrą one do swojego przeznaczenia.

Kiedy korzystamy z ping możemy zobaczyć parametr TTL. TTL (Time to Live) to pole znajdujące się w nagłówku pakietu IP, które określa maksymalną liczbę skoków, które pakiet może wykonać przed zostanie odrzucony przez sieć.

Każdy router na trasie pakietu IP zmniejsza wartość pola TTL o jeden. Gdy wartość TTL osiągnie zero, pakiet jest odrzucany, a do nadawcy jest wysyłane powiadomienie o czasie życia pakietu. Dzięki temu mechanizmowi zapobiega się utrzymywaniu się "martwych" pakietów w sieci, które mogłyby krążyć w nieskończoność.

Program ping oferuje wiele opcji, które pozwalają dostosować jego działanie. Do najważniejszych należą:

-c liczba: Określa liczbę pakietów, które mają być wysłane.

-i sekundy: Ustawia interwał między kolejnymi pakietami.

-s rozmiar: Pozwala na zmianę rozmiaru wysyłanego pakietu danych.

-t ttl: Ustawia wartość TTL (Time To Live) dla pakietów, co wpływa na maksymalną liczbę przeskoków sieciowych.

Testowałam port 8.8.8.8 i zauważyłam, że nie ma wielkiej różnicy, kiedy wysyłam 1 czy 1400 bajtów - średni czas to 10-20 sekund. Jednak gdy liczba przekracza 1480, wszystkie pakiety zostają utracone. Jest to możliwe, ponieważ w przypadku sieci o wysokiej przepustowości, jaką może mieć serwer Google (8.8.8.8), czas przesyłania danych może być stosunkowo krótki, niezależnie od rozmiaru pakietu.

Ale kiedy przetestowałam pralnie.org, zauważyłam, że kiedy wysyłam pakiet o rozmiarze 7 (czas 2-3 sekundy), a kiedy wysyłam pakiet o rozmiarze 1400 (10-16 sekund), czas propagacji znacznie rośnie.

Jeśli chodzi o fragmentację, większe pakiety mogą wymagać fragmentacji, co może wpłynąć na wybór trasy, ponieważ niektóre węzły mogą obsługiwać fragmentację w inny sposób. Większe pakiety mogą wymagać fragmentacji, gdyż niektóre sieciowe urządzenia mogą mieć ograniczenia dotyczące maksymalnej wielkości pakietu, którą mogą przekazać ("truncated" może pojawić się podczas korzystania z polecenia ping na Ubuntu, gdy pakiet przekracza dozwolony rozmiar.). Fragmentacja polega na podziale dużego pakietu na mniejsze części, aby zmieścić się w tych ograniczeniach. W moim przypadku największy rozmiar pakietu, który udało się przesłać, to 1472 bajty. Ten parametr zależy od MTU (Maximum Transmission Unit): maksymalna wielkość pakietu, która może być przesłana bez fragmentacji, standardowy rozmiar MTU dla większości sieci to 1500 bajtów, ale ta liczba zależy od urządzeń znajdujących się na trasie.

Analiza serwerow

ping uwr.edu.pl-strona internetowa Uniwersytetu Wroclawskiego

Pinging uwr.edu.pl [156.17.87.85] with 32 bytes of data:

Reply from 156.17.87.85: bytes=32 time=7ms TTL=53

Reply from 156.17.87.85: bytes=32 time=2ms TTL=53

Reply from 156.17.87.85: bytes=32 time=5ms TTL=53

Reply from 156.17.87.85: bytes=32 time=5ms TTL=53

Ping statistics for 156.17.87.85:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 7ms, Average = 4ms

Pinging uw.edu.pl [193.0.115.152] with 32 bytes of data: - strona internetowa Uniwersytetu Warszawskiego

Reply from 193.0.115.152: bytes=32 time=11ms TTL=242

Reply from 193.0.115.152: bytes=32 time=13ms TTL=242

Reply from 193.0.115.152: bytes=32 time=10ms TTL=242

Reply from 193.0.115.152: bytes=32 time=10ms TTL=242

Ping statistics for 193.0.115.152:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 10ms, Maximum = 13ms, Average = 11ms

Czas się trochę różni bo jest zależny od polożenia geograficznego

Średnica Internetu to pojęcie związane z topologią sieci, które odnosi się do najdłuższej ścieżki, jaką można znaleźć w sieci internetowej, mierzonej jako maksymalna liczba skoków między dwoma punktami końcowymi. Innymi słowy, jest to najdłuższa trasa, jaką pakiet danych musi przejść, aby dotrzeć z jednego punktu w sieci do drugiego.

Można założyć, że największą trasę będą miały hosty umieszczone na odległych kontynentach, takich jak Ameryka Północna, Ameryka Południowa, Australia czy Azja Wschodnia.

Przykładowe hosty, które mogą mieć najdłuższą trasę od urządzenia we Wrocławiu, to:

Host w Sydney, Australia. [www.sydneyoperahouse.com](http://www.sydneyoperahouse.com) 17 skoków

Host w Los Angeles, Stany Zjednoczone. [www.musiccenter.org](http://www.musiccenter.org) ponad 30

Host w Santiago, Chile. [www.mssa.cl](http://www.mssa.cl) ponad 30

Host w Tokio, Japonia. www.tnm.jp

Host w Auckland, Nowa Zelandia. [www.aucklandmuseum.com](http://www.aucklandmuseum.com)

Zdalne platformy "cloud computing" to platformy lub usługi oferujące dostęp do zasobów obliczeniowych, takich jak serwery, pamięć, bazy danych, sieci, oprogramowanie i inne, przez internet. Termin "chmura" (cloud) odnosi się do sieci zdalnych serwerów, do których użytkownicy mają dostęp za pośrednictwem internetu.

Sieci wirtualne w kontekście "cloud computing" (przetwarzania w chmurze) to abstrakcyjne warstwy sieciowe, które umożliwiają izolację i zarządzanie zasobami sieciowymi w środowisku chmury. Są to wirtualne wersje fizycznych sieci, które umożliwiają komunikację między zasobami wirtualnymi, takimi jak wirtualne maszyny (VM), kontenery, aplikacje, i inne usługi, działające w infrastrukturze chmury.

W dużym uproszczeniu, sieci wirtualne w chmurze pozwalają na:

* **Izolację**: Rozdzielenie zasobów sieciowych dla różnych klientów lub projektów w obrębie tej samej fizycznej infrastruktury, zapewniając bezpieczeństwo i prywatność.
* **Elastyczność**: Możliwość szybkiego dostosowywania konfiguracji sieci, takich jak zakresy adresów IP, tablice routingu, zasady zapory sieciowej, bez konieczności zmian w fizycznej infrastrukturze.
* **Automatyzacja**: Uproszczenie zarządzania siecią przez automatyzację zadań konfiguracyjnych i operacyjnych, co jest kluczowe dla szybkiego wdrażania i skalowania aplikacji w chmurze.
* **Dostępność**: Wysoka dostępność i odporność na awarie poprzez wykorzystanie redundantnych ścieżek sieciowych i automatycznych mechanizmów failover.

W kontekście chmury, dostawcy usług takich jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) oferują różnorodne usługi sieciowe, które umożliwiają tworzenie i zarządzanie sieciami wirtualnymi, w tym wirtualne sieci prywatne (VPC), sieci definowane programowo (SDN), równoważenie obciążenia, sieci prywatne i publiczne, VPN i wiele innych.

Wykorzystanie sieci wirtualnych w chmurze umożliwia organizacjom elastyczne i skalowalne zarządzanie zasobami IT, zapewniając jednocześnie bezpieczeństwo i izolację niezbędną dla wielu aplikacji i danych.

Udało się połączyć z Google Cloud Platform

2)Traceroute(tracert w Windows)

Traceroute jest narzędziem diagnostycznym służącym do śledzenia trasy pakietów w sieci komputerowej. Pozwala on na identyfikację wszystkich routerów lub węzłów sieciowych, przez które przechodzą pakiety w drodze do docelowego hosta, oraz określenie czasu odpowiedzi (ping) każdego z tych węzłów.

Oto ogólny opis działania programu traceroute:

Program traceroute otrzymuje jako argument docelowy adres IP lub nazwę domenową hosta, do którego ma zostać wysłany pakiet.

Program tracert wysyła serię pakietów ICMP Echo Request (żądanie echo) do docelowego hosta z niewielkimi wartościami TTL (Time to Live), zaczynając od 1.

Każdy pakiet przekierowany przez routery na trasie do docelowego hosta. Po przejściu przez każdy router, TTL pakietu jest zmniejszany o 1.

Jeśli TTL osiągnie wartość 0, router odsyła odpowiedź ICMP Time Exceeded, a program tracert rejestruje adres IP routera i czas odpowiedzi.

Proces powtarza się dla kolejnych pakietów zwiększając TTL o 1 przy każdej iteracji, aż docelowy host zostanie osiągnięty lub zostanie osiągnięty maksymalny limit przekierowań.

Wynikiem działania programu tracert jest lista kolejnych węzłów sieciowych (routery lub bramy) na trasie od twojego komputera do docelowego hosta, wraz z informacjami o czasie odpowiedzi dla każdego węzła. Ta lista umożliwia zidentyfikowanie tras i potencjalnych problemów z siecią.

Traceroute może pomóc w poszukiwaniu “średnicy” internetu

Jeżeli spróbowac puścić tracert to wyswietli się napis “Tracing route to dns.google [8.8.8.8]

over a maximum of 30 hops:” co znaczy że morzemy prześledzieć tylko 30 skoków.

Analizując potencjalne trasy pakietów ICMP Echo Request z urządzenia znajdującego się we Wrocławiu do różnych hostów na całym świecie. Należy jednak pamiętać, że nie wszystkie węzły na trasie zawsze odpowiedzą na zapytania traceroute, ponieważ niektóre sieci mogą blokować lub ograniczać ruch ICMP z powodów bezpieczeństwa.

3)Wireshark

Wireshark jest narzędziem do analizy sieci, które umożliwia przechwytywanie i interaktywną analizę ruchu sieciowego. Użytkownik może obserwować szczegółowe informacje o pakietach przesyłanych w sieci, włącznie z protokołami. Wireshark jest nieoceniony w diagnozowaniu problemów sieciowych i analizie bezpieczeństwa, bo jeżeli strona nie jest zabiwspieczona łatwo za pomocą Wireshark przychwycić hasło i username.

Wireshark daje możliwość analizy ruchu w realnej sieci i ocena jej prawidłowego funkcjonowania, przechwycony ruch możemy zapisać do plików, które potem można było obejrzeć w celu głębszej analizy ruchu sieciowego.

Po uruchomieniu Wiresharka i rozpoczęciu przechwytywania na wybranej interfejsie sieciowym, użytkownik otrzymuje wgląd w ruch sieciowy w czasie rzeczywistym. Przykładowo, analizując ruch HTTP, można zobaczyć żądania i odpowiedzi pomiędzy klientem a serwerem, w tym nagłówki, ciasteczka, kody odpowiedzi itd.

Widać że na dole ekranu liczba przechwyconych pakietów rośnie cały czas, pomimo tego, że na pierwszy rzut oka nic się nie dzieje. Tak się dzieje bo w systemie operacyjnym mamy wiele usług, które korzystają z dostępu do sieci i cały czas przesyłają jakieś dane.

Żeby było łatwiej przeglądać dane program dysponuje możliwością filtrowania tego, co chcemy przechwytywać, bądź też filtrowania tego, co już zostało przechwycone. Jeśli na początku przed rozpoczęciem pracy nie zdefiniowaliśmy jaki rodzaj ruchu, chcemy przechwytywać. Program domyślnie przechwytuje wszystko, co przechodzi przez kartę sieciową.