Wydział Fizyki i Informatyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Bezpieczeństwo w sieci

„Analiza sieci: ping, netstat, traceroute ”

laboratorium: 01

Kraków, 2012

Spis treści

Spis treści 2
1. Wiadomości wstępne 3
1.1. Tematyka laboratorium 3
1.2. Zagadnienia do przygotowania 3
1.3. Opis laboratorium 4
1.3.1. Ping 4
1.3.2. Netstat 7
1.3.3. Traceroute 9
1.4. Cel laboratorium 11
2. Przebieg laboratorium 13
2.1. Przygotowanie laboratorium 13
2.2. Zadanie 1. Obsługa programu ping 13
2.3. Zadanie 2. Obsługa programu netstat 14
2.4. Zadanie 3. Obsługa programu traceroute 14
2.5. Opracowanie i sprawozdanie 14

1. Wiadomości wstępne

Pierwsza część niniejszej instrukcji zawiera podstawowe wiadomości teoretyczne dotyczące podstawowych narzędzi umożliwiających badanie ruchu w sieci: **ping, netstat i traceroute**. Poznanie tych wiadomości umożliwi prawidłowe zrealizowanie praktycznej części laboratorium.

1.1. Tematyka laboratorium

Tematyką laboratorium jest zapoznanie się ze sposobem działania, a także możliwościami wykorzystania programów ping, netstat oraz traceroute w celu diagnozowania i testowania sieci.

Z uwagi na fakt, iż diagnostyka sieci jest zagadnieniem dość złożonym toteż trudno o właściwe oprogramowanie, które w ogólnym przypadku, bez ingerencji użytkownika dawałoby możliwość zdiagnozowania oraz wskazania w sposób jednoznaczny konkretnego problemu jak również jego przyczyny. Odpowiedzią mogą być wymienione powyżej polecenia umożliwiające monitorowanie, analizę pracy sieci, lokalizowanie potencjalnych błędów lub uszkodzeń sieci komputerowej.

Właściwa interpretacja danych otrzymywanych dzięki użyciu zaawansowanych opcji wywołania tych poleceń pozwala na uzyskanie wielu informacji o sieci IP.

Niewątpliwą zaletą programów omawianych w niniejszym dokumencie jest ich dostępność na wielu platformach systemowych jak również prostota ich wywołania. Celem ćwiczenia jest zapoznanie się z zasadą działania wspomnianych narzędzi a także ich praktyczne wykorzystanie

1.2. Zagadnienia do przygotowania

Przed przystąpieniem do realizacji laboratorium, poza jego opisem warto także zapoznać się z zagadnieniami dotyczącymi:

- protokołu IP; [RFC 791]
- protokołu ICMP; [RFC 792]
- protokołu UDP; [RFC 768]

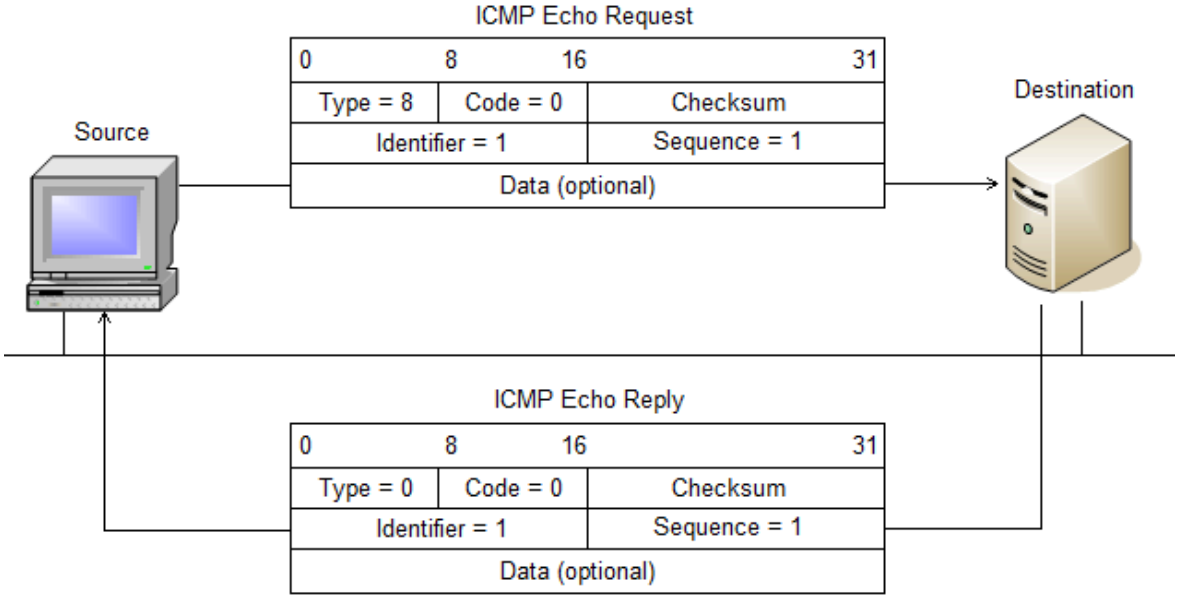
1.3. Opis laboratorium

W tym podrozdziale zostaną szczegółowo opisane trzy tytułowe programy wraz z przykładami ich użycia. Przedstawione tutaj informacje są niezbędne celem wykonania części praktycznej niniejszego laboratorium.

1.3.1. Ping

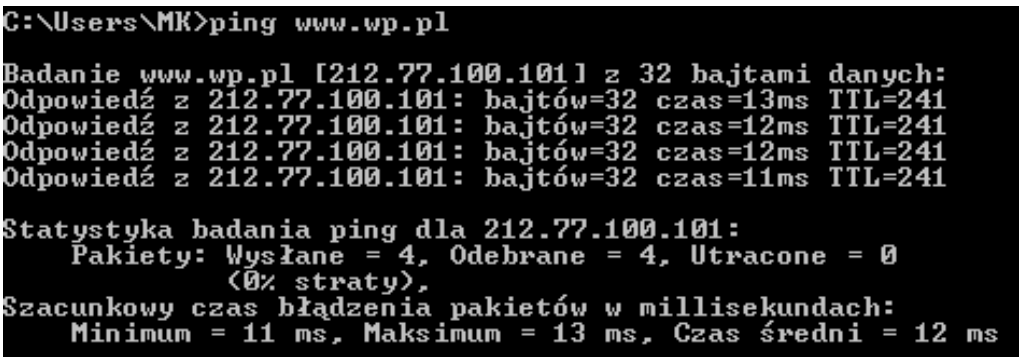
Ping jest narzędziem wykorzystywanym w sieciach komputerowych TCP/IP. Dzięki niemu możliwe jest diagnozowanie połączeń sieciowych - sprawdzamy czy istnieje połączenie pomiędzy hostami testującym i testowanym. *Ping* dostarcza również informacji dotyczących jakości połączenia wyrażona w % utraconych pakietów oraz opóźnień w ich transmisji.

Jego działanie można porównać do echosondy: *ping* wysyła sygnał do maszyny docelowej i czeka na odpowiedź. Tym sygnałem są komunikaty protokołu ICMP (ang. *Internet Control Message Protocol*) Echo Request (typ=0). Serwer dzięki wbudowanym funkcjom automatycznego odpowiadania na pakiety *ping* zaraz po ich otrzymaniu wysyła potwierdzenie w postaci komunikatów ICMP Echo Reply (typ=8).
Mierzony jest czas od wysłania sygnału do odebrania odpowiedzi - czas potrzebny na przejście pakietu informacji.



Rys. 1. Schemat opisanej powyżej komunikacji

Aby zbadać łączność z wybranym hostem należy podać jego nazwę w postaci numeru IP lub nazwy DNS-owej jako argument polecenia 'ping'.



Rys. 2. Przykład użycia programu ping

Wynikiem działania jest lista kolejnych odpowiedzi odległego hosta zawierająca następujące informacje:

- długość pakietu kontrolującego
- czas podróży pakietu w milisekundach
- wartość pola TTL (ang. *Time To Live*) czyli tzw. czas życia pakietu danych

Poniżej znajduje się podsumowanie informujące o liczbie utraconych pakietów, a także szacunkowe czasy - minimalny, średni i maksymalny - transmisji zapytań.
Analiza uzyskanych czasów pozwala określić jakość połączenia z daną maszyną.

Interpretacja wyników może stwarzać niekiedy problemy. Dzieje się tak wówczas gdy w ruch komunikatów ICMP ingerują firewalle. Warto pamiętać, że jeśli zdalny host nie odpowiada na wysłane pakiety ping, to nie musi to być jednoznaczne z tym, że nie jest on włączony bądź występuje problem z siecią między maszyną testującą, a testowaną. Przyczyną może być blokowanie wysyłania komunikatów ICMP Echo Reply celem ochrony przed potencjalnymi atakami z sieci. Blokowanie umożliwiają wspomniane już firewalle lub filtry w routerach.

Składnia polecenia (system Linux):

ping [-Rnf] [-c count] [-i wait] [-l preload] [-s packetsize] [-i TTL] host

gdzie:

-c count
Określa liczbę pakietów jaka ma być wysłana

-i wait
Pozwala określić czas oczekiwania w sekundach pomiędzy wysłaniem kolejnych pakietów. Linux domyślnie wysyła pakiet co sekundę.

-s packetsize
Pozwala określić rozmiar wysyłanego pakietu

-l preload
Umożliwia wysłanie określonej liczby pakietów najszybciej jak to tylko możliwe

-i TTL
Określa wartość pola czasu wygaśnięcia (TTL, Time To Live) w nagłówku protokołu IP dla wysyłanych komunikatów żądania echa. Domyślnie jest przyjmowana wartość domyślna TTL hosta. Dzięki tej opcji możemy określić maksymalna ilość routerów jakie chcemy przejść nim pakiet zostanie porzucony lub zwrócony przez router z kodem przekroczenia max TTL (255).

-R
Pozwala zobaczyć drogę pokonywaną przez pakiety w sieci lokalnej

-n
Wyłącza tłumaczenie adresów IP na nazwy DNS

-f
Stosowana bez liczby. Skutkuje zalewaniem danego komputera pakietami tak szybko jak otrzymywane są odpowiedzi, bądź 100 razy w ciągu sekundy - wybierana jest większa wartość

Ostatnia z opcji zasługuje na kilka słów komentarza. Umożliwia ona testowanie wydajności łącza. Korzystając z niej można wygenerować bardzo duży ruch na łączach, toteż nie powinno się z jej wykorzystaniem testować maszyn poza siecią lokalną.
Opcję tę można połączyć z opcją **-s rozmiar**. Wówczas jako zmienną rozmiar można podać dużą ilość danych w bajtach przesyłanych w komunikacie ICMP (doliczamy 8 bajtów nagłówka ICMP). Pozwala to również na określenie sposobu w jaki routery znajdujące się pomiędzy nami, a hostem docelowym fragmentują duże datagramy.

Dzięki tym opcjom możliwe jest dokonywanie ataków Dos i DDoS. Przykłady:

- ping -s duzypakiet nazwahosta
  Skutkuje wysyłaniem co sekundę dużego pakietu danych. Można w ten sposób zapchać łącze 'testowanej' maszyny
- ping -f nazwahosta
  Komenda wysyła bardzo dużo małych pakietów powodując zapchanie łącza.

Jest tak, gdyż analiza pakietów ICMP Echo Reply nie tylko potwierdza istnienie hosta pod danym adresem IP, ale często również pozwala na dokładne określenie systemu operacyjnego, co ułatwia zaatakowanie komputera.

1.3.2. Netstat

Kolejnym powszechnie używanym narzędziem jest *netstat*. Jest to jeden z najbardziej rozbudowanych programów służących do analizy sieci. Pokazuje otwarte gniazda komunikacyjne i nasłuchujące wg wybranych kryteriów, a także procesy, które z tych gniazd korzystają. Wyświetla aktywne połączenia sieciowe TCP, tabelę routingu protokołu IP, statystykę transmisji ramek ethernetowych, statystykę protokołu IPv4 (dla protokołów IP, ICMP, TCP oraz UDP), statystykę protokołu IPv6 (dla protokołów IPv6, ICMPv6, TCP przez IPv6 i UDP przez IPv6), połączenia masquerade oraz komunikaty netlinkowe.

Składnia polecenia (system Linux):

netstat [-a] [-s] [-t] [-u] [-e] [-n] [-r] [-o] [-p protocol] [interval]

gdzie:

-a
Wyświetla wszystkie aktywne połączenia protokołu TCP oraz porty protokołów TCP i UDP, na których komputer nasłuchuje.

-s
Pozwala na wyświetlanie oddzielnych statystyk dla poszczególnych protokołów. Domyślnie jest to statystyka protokołów IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP oraz UDPv6. Używając opcji **-p** możemy określić jej podzbiór.

-t
Wyświetla informacje o gniazdach TCP.

-u
Wyświetla informacje o gniazdach UDP.

-e

Służy do wyświetlania statystyki sieci Ethernet - drukuje liczbę wysłanych oraz odebranych bajtów i pakietów. Ta opcja może być używana z opcją **-s**.

-n

Powoduje wyświetlanie jedynie wartości numerycznych (nie determinuje nazwy użytkownika, symbolicznego hosta, czy nazwy usługi).

-r

Wyświetla zawartość tabeli routingu protokołu IP.

-o

Dla każdego aktywnego połączenia protokołu TCP wyświetla skojarzony z nim identyfikator procesu (PID), co umożliwia uzyskanie informacji o właścicielach portów dla każdego z połączeń.

-p protocol

Wyświetla połączenia dla określonego protokołu. Parametr **protocol** może przyjmować wartości TCP, UDP, TCPv6 oraz UDPv6, natomiast w przypadku użycia z opcją **-s** wartości IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP lub UDPv6.

-interval

Ponownie wyświetla wybraną statystykę, odczekując zadaną liczbę sekund po między każdym jej wyświetleniem.

```
C:\Users\MK>netstat

Aktywne połączenia

  Protokół  Adres lokalny          Obcy adres              Stan
  TCP       127.0.0.1:5939         PC:49159                USTANOWIONO
  TCP       127.0.0.1:49157        PC:49158                USTANOWIONO
  TCP       127.0.0.1:49158        PC:49157                USTANOWIONO
  TCP       127.0.0.1:49159        PC:5939                 USTANOWIONO
  TCP       192.168.1.102:52047    channel-hs-12-01-snc7:https  USTANOWIONO
  TCP       192.168.1.102:52163    www-12-03-frc1:https    USTANOWIONO
  TCP       192.168.1.102:52462    channel-hs-12-01-snc7:https  USTANOWIONO
  TCP       192.168.1.102:52579    fra07s07-in-f157:http   USTANOWIONO
  TCP       192.168.1.102:52619    2.22.52.27:http         USTANOWIONO
  TCP       192.168.1.102:52647    2.22.52.8:http          CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52812    muc03s01-in-f31:https   USTANOWIONO
  TCP       192.168.1.102:52823    www-slb-10-02-ash3:https  OCZEKIWANIE_ZAMKN
  TCP       192.168.1.102:52832    199.38.164.155:http     USTANOWIONO
  TCP       192.168.1.102:52838    api-read-12-05-prn1:https  CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52839    mia05s07-in-f24:https   USTANOWIONO
  TCP       192.168.1.102:52852    ad:http                 CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52854    ad:http                 CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52862    ad:http                 CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52864    ad:http                 CZAS_OCZEKIWANIA
  TCP       192.168.1.102:52869    ee-in-f132:https        USTANOWIONO
  TCP       192.168.1.102:52870    ee-in-f132:https        USTANOWIONO
  TCP       192.168.1.102:52871    muc03s01-in-f23:https   USTANOWIONO
  TCP       192.168.1.102:52872    muc03s01-in-f23:https   USTANOWIONO
  TCP       192.168.1.102:52873    muc03s01-in-f23:https   USTANOWIONO
  TCP       192.168.1.102:52874    muc03s01-in-f23:https   USTANOWIONO
  TCP       192.168.1.102:52875    fra07s07-in-f120:https  USTANOWIONO
  TCP       192.168.1.102:52876    fra07s07-in-f120:https  USTANOWIONO
  TCP       192.168.1.102:64794    www-14-03-frc1:https    USTANOWIONO
  TCP       192.168.1.102:64795    orcart-03-01-snc7:https  USTANOWIONO
  TCP       192.168.1.102:64796    193.120.199.14:12350    USTANOWIONO
  TCP       192.168.1.102:64815    fa-in-f125:5222         USTANOWIONO
  TCP       192.168.1.102:64822    213.199.179.148:40015   USTANOWIONO
  TCP       192.168.1.102:64961    189-11-90-9:5938        USTANOWIONO
```

Rys. 3. Przykład użycia programu netstat

1.3.3. Traceroute

Traceroute jest programem diagnostycznym rozszerzającym możliwości narzędzia ping. Poza informowaniem o braku łączności z hostem docelowym *traceroute* jest w stanie określić dokładne miejsce, w którym wysyłane datagramy są gubione.
Służy on do badania trasy pakietów w sieci IP. Dostarcza informacji o czasie przepływu danych zarówno do maszyny testowanej jak i pośredniczących routerów znajdujących się na trasie przepływu. Jego działanie oparte jest na dwóch protokołach komunikacyjnych ICMP oraz UDP.

Zasada działania narzędzia *traceroute* jest dość prosta. Na adres testowanej maszyny wysyłana jest seria specjalnych datagramów. Każdy z nich zawiera pakiet protokołu UDP skierowany na jeden z nieużywanych portów z zakresu 33434 - 33534.
Dodatkowo dla każdego przesyłanego datagramu host źródłowy uaktywnia zegar.
Za kluczowy element całego mechanizmu należy uznać manipulowanie wartością pola TTL datagramów IP. W pierwszym datagramie pole to przyjmuje wartość 1, w drugim wartość 2 itd. Wartość ta jest zmniejszana wraz z przechodzeniem przez kolejne routery na trasie. W sytuacji gdy pole TTL osiąga wartość 0, zgodnie z zasadami protokołu IP, pakiet jest automatycznie odrzucany przez router.
Wysyła on wówczas do hosta źródłowego informację zwrotną - ostrzegawczy komunikat ICMP Time Exceeded zawierający dane o adresie IP i nazwie takiego routera. W chwili dotarcia komunikatu ICMP do hosta źródłowego, ten uzyskuje od zegara wartość RTT (ang. *Round Trip Time*) pozwalającą określić łączny czas jaki upłynął od momentu wysłania pakietu do chwili otrzymania skojarzonego z nim komunikatu zwrotnego.
W momencie gdy datagram ostatecznie dociera do hosta docelowego z reguły zostaje odesłany komunikat ICMP Port Unreachable kończący badanie trasy. Dzieje się tak ponieważ, jak wspomniano powyżej, datagram zawiera segment UDP o bardzo wysokim numerze portu, na którym z reguły nie działają żadne usługi - żaden proces maszyny docelowej nie będzie chciał obsłużyć takiego pakietu.

Traceroute trzykrotnie wykonuje opisany powyżej proces, co oznacza że źródłowy host wysyła do docelowego 3*n pakietów. Standardowo wysyłane są zestawy złożone z trzech pakietów o jednakowej wartość TTL, w związku z czym dla każdej wartości TTL narzędzie zwraca po trzy wyniki. Gromadzone dane umożliwiają szczegółowe odtworzenie trasy pokonywanej przez transmitowane pakiety, co więcej pozwalają określić opóźnienia generowane przez pośredniczące routery.


```
C:\Users\MK>tracert www.onet.pl

Śledzenie trasy do www.onet.pl [213.180.141.140]
z maksymalną liczbą 30 przeskoków:

  1     3 ms     1 ms     1 ms  10.88.24.1
  2     1 ms     1 ms     1 ms  10.88.24.1
  3     1 ms     1 ms     1 ms  192.168.102.5
  4     3 ms     1 ms     1 ms  192.168.102.66
  5     1 ms     1 ms     1 ms  nat4-2.ghnet.pl [91.150.221.2]
  6     3 ms     1 ms     1 ms  rtr2.ghnet.pl [91.150.221.1]
  7     3 ms    22 ms     2 ms  GHNET-do-KroCORE1.krakow.aster.pl [213.134.162.46]
  8    68 ms     2 ms     2 ms  KroCORE1-do-ONET.net.aster.pl [213.134.162.22]
  9     3 ms     2 ms     3 ms  ruc-BR2.z.dab-BR2.net.onet.pl [213.180.151.2]
 10     2 ms     2 ms     2 ms  ruc-CR2.z.ruc-BR2.net.onet.pl [213.180.151.36]
 11     *        *        *     Upłynął limit czasu żądania.
 12     2 ms     2 ms     2 ms  ruc-agg1.z.ruc-agg2.m1r2.net.onet.pl [213.180.146.22]
 13     3 ms     3 ms     3 ms  sg1.any.onet.pl [213.180.141.140]

Śledzenie zakończone.
```

Rys. 3. Przykład działania narzędzia *traceroute* (brak odpowiedzi na pakiet)

W sytuacji gdy host źródłowy na wysłany datagram otrzyma od dowolnego routera mniej niż trzy komunikaty, wówczas w miejsce czasu wyświetlana jest gwiazdka.
Mimo to polecenie *traceroute* nadal wysyła datagramy, inkrementując wartość w polu TTL ponieważ jeden z kolejnych routerów może znowu odpowiednio zareagować co znajduje potwierdzenie na powyższym rysunku.

Brak odpowiedzi na zadany pakiet może wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń. Przykładowo router może zostać skonfigurowany w taki sposób, że nie zmniejsza wartości pola TTL przetwarzanych pakietów, wówczas nie będzie uwidoczniony przez *traceroute*. Przyczyną może być również filtrowanie zaporowe - firewalle filtrują pakiety skierowane na porty, które nie powinny być otwarte, a z tego właśnie korzysta *traceroute*.

Jak widać, każdy z routerów posiada adres, a część z nich również nazwę.
Należy pamiętać, że wyświetlane opóźnienia stanowią czas transmisji datagramu IP oraz czas powrotu komunikatu zwrotnego ICMP od każdego z routerów.

Każde z trzech opóźnień całkowitej trasy związanych z przesłaniem pakietu pomiędzy źródłowym hostem i routerem uwzględnia wszystkie opóźnienia składowe takie jak opóźnienie transmisji, przetwarzania przez router, propagacji i kolejkowania.
Z uwagi na fakt, iż opóźnienie kolejkowania zmienia się w czasie, opóźnienie całkowitej trasy pakietu transmitowanego do routera n w rzeczywistości może być większe od opóźnienia całkowitej trasy tego samego pakietu przesłanego do routera n+1.
Widać to na przykładzie routerów 8 i 9 dla pierwszego pakietu. Taka sytuacja możliwa jest w wyniku samej zasady działania sieci. Niekiedy datagram osiągnie cel w bardzo krótkim czasie, korzystając z wolnych w tym momencie łączy, a czasem będzie musiał zaczekać w kolejce, do momentu kiedy zostaną wytransmitowane wcześniej dostarczone dane.

Składnia polecenia (system Linux):

traceroute [-I] [-n] [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-w waittime] [-v] [-z msecs] host [packetsize]

gdzie:

-I

Wykorzystuje komendy ICMP Echo zamiast datagramów UDP

-n

Opcją umożliwiającą wyłączenie rozwiązywania nazw DNS-owych kolejnych routerów co skutkuje znacznym przyspieszeniem działania programu (oszczędza szukania w DNS skojarzenia adres-nazwa dla każdej bramki)

-m max_ttl

Ustawia maksymalny Time-To-Live (domyślnie 30 skoków - *ang. hops*)

-p port

Umożliwia zmianę podstawowego numer portu UDP (domyślnie datagram UDP wysyłany jest na port base 33434). Traceroute zakłada, iż nic nie nasłuchuje na portach UDP od base do base+nhops-1 na hoście docelowym. W przeciwnym wypadku opcja ta może być użyta do wybrania nieużywanego zakresu.

-q nqueries

Ustawia liczbę prób na każde TTL na **nqueries** (domyślnie trzy próby).

-s src_addr

Pozwala na zadanie adresu IP jako adresu źródłowego w wychodzących pakietach próbnych.

-w waittime

Pozwala ustawić czas (w sekundach) oczekiwania na odpowiedź na próbkę (domyślnie 3 sekundy).

-v

Interaktywne wyjście. Listowane są odebrane pakiety ICMP inne niż te zwracające komunikaty ICMP Time Exceeded i ICMP Port Unreachable.

***-z* msecs**

Daje możliwość ustawienia opóźnienia pomiędzy poszczególnymi próbkami (domyślna wartość wynosi zero)

1.4. Cel laboratorium

Celem laboratorium jest zapoznanie się z podstawowymi narzędziami umożliwiającymi analizę sieci IP. Opanowanie ich funkcji oraz sposobu działania pozwoli na gromadzenie oraz odpowiednie interpretowanie informacji mogących stanowić pomoc przy rozwiązywaniu problemów z bezpieczeństwem i wydajnością sieci.

2. Przebieg laboratorium

Druga część instrukcji zawiera zadania do praktycznej realizacji, które demonstrują zastosowanie technik z omawianego zagadnienia.

2.1. Przygotowanie laboratorium

Wszystkie trzy opisane narzędzia diagnostyczne (ping, netstat, traceroute) dostępne są z poziomu linii komend systemu Linux.

2.2. Zadanie 1. Obsługa programu ping

- Zbadaj adres pętli zwrotnej, aby sprawdzić, czy na lokalnej maszynie zainstalowano i skonfigurowano protokół TCP/IP.
- Uruchamiając program *ping* użyj opcji, która spowoduje jego bezwzględne zakończenie po 3 sekundach działania.
- Korzystając z odpowiedniej opcji polecenia *ping* prześledź całą trasę pakietu wysłanego na adres 91.198.174.225.
- Wyślij pojedyncze zapytanie na dowolnie wybrany host i odczekaj 10 sekund na odpowiedź.
- Zbadaj jak rozmiar wysyłanego pakietu wpływa na czas podróży w obie strony dla dwóch bardzo odległych węzłów sieci.
- Przeanalizuj i zinterpretuj działanie narzędzia ping dla hosta: www.microsoft.com
- Wymuś ciągłą pracę polecenie z dowolnie wybranym interwałem czasowym.

2.3. Zadanie 2. Obsługa programu netstat

- Zbadaj nasłuchujące porty UDP i TCP oraz nawiązane połączenia TCP.
- Utwórz dowolne połączenie TCP, a następnie wykaż jego obecność.
- Wyświetl wszystkie aktywne połączenia protokołu TCP raz z numerami IP hostów i portów, a drugi raz z nazwami hostów i portów.
- Użyj odpowiedniego polecenia celem wyświetlenia tablicy routingu. Określ numer bramy domyślnej zajmowanej maszyny.

2.4. Zadanie 3. Obsługa programu traceroute

- Przeanalizuj i zinterpretuj wyniki poniższego wywołania: traceroute allspice.lcs.mit.edu. Jakie uzyskujemy informacje ?
- Prześledź trasę danych wysłanych na adres 91.198.174.225. Uzyskane wyniki porównaj z otrzymanymi przy użyciu polecenia *ping*

2.5. Opracowanie i sprawozdanie

Realizacja laboratorium pt. *„Analiza sieci: ping, netstat, traceroute”* polega na wykonaniu wszystkich zadań podanych w drugiej części tej instrukcji. Wynikiem wykonania powinno być sprawozdanie w formie wydruku papierowego dostarczonego na kolejne zajęcia licząc od daty laboratorium, kiedy zadania zostały zadane.
Sprawozdanie powinno zawierać:

- analizę wyników wykonanych poleceń
- wskazówki dotyczące ewentualnej poprawy instrukcji celem lepszego zrozumienia sensu oraz treści zadań,

