Ćwiczenie 1.1.7 Korzystanie z poleceń ping i tracert na stacji roboczej

Cele

- Poznanie sposobów korzystania z polecenia TCP/IP Packet Internet Groper (**`ping`**) z poziomu stacji roboczej.
- Poznanie sposobów korzystania z polecenia traceroute (**`tracert`**) z poziomu stacji roboczej.
- Obserwacja procesu odwzorowywania nazw na adresy przeprowadzanego przez serwery WINS i/lub DNS.

Wprowadzenie

W tym ćwiczeniu zakłada się, że używana jest dowolna wersja systemu operacyjnego Windows. Jest to ćwiczenie nie mające negatywnego wpływu na system i może być przeprowadzane na dowolnym komputerze bez obawy o zmianę konfiguracji systemu.

Ćwiczenie to powinno być wykonywane w środowisku wyposażonym w sieć LAN mającą połączenie z Internetem. Można je przeprowadzić, korzystając z pojedynczego połączenia modemowego lub połączenia DSL. Uczestnik będzie potrzebował adresów IP, które zostały zapisane w poprzednim ćwiczeniu. Instruktor może podać dodatkowe adresy IP.

> **Uwaga:** Ping jest używany w wielu atakach polegających na zablokowaniu usług (DoS, *Denial-of-Service*) i wielu administratorów sieci szkolnych konfiguruje routery graniczne tak, aby uniemożliwić odpowiadanie na komunikaty „echo” wysyłane przez program ping. W takim przypadku odległy host może wydawać się odłączony lub nieaktywny także wówczas, gdy sieć działa.

Krok 1 Nawiąż i sprawdź połączenie z Internetem

Dzięki temu można się upewnić, że komputer ma adres IP.

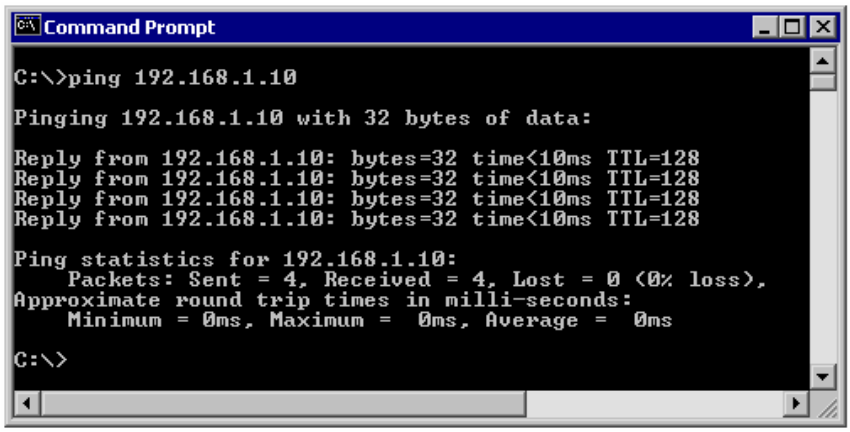
Krok 2 Otwórz okno wiersza poleceń

Użytkownicy systemów Windows 95 / 98 / Me — skorzystajcie z menu Start, aby otworzyć okno wiersza poleceń. Wybierz kolejno polecenia **Start** > **Programy** > **Akcesoria** > **Tryb MS-DOS** lub **Start** > **Programy** > **MS-DOS**.

Użytkownicy systemów Windows NT / 2000 / XP — skorzystajcie z menu Start, aby otworzyć okno wiersza poleceń. Wybierz kolejno polecenia **Start** > **Programy** > **Akcesoria** > **Wiersz poleceń** lub **Start** > **Programy** > **Wiersz poleceń** lub **Start** > **Wszystkie programy** > **Wiersz poleceń**.

Krok 3 Wyślij pakiety ping na adres IP innego komputera

W oknie wpisz polecenie **`ping`**, spację i adres IP komputera zanotowany podczas poprzedniego ćwiczenia. Na następującym rysunku pokazano wyniki pomyślnego wykonania polecenia **`ping`** dla podanego adresu IP.



Polecenie **ping** używa komunikatów ICMP typu „prośba o echo” (*echo request*) i „odpowiedź z echem” (*echo reply*) w celu przetestowania połączenia fizycznego. Polecenie **ping** przedstawia wyniki dla czterech przeprowadzonych prób, dlatego może stanowić wskaźnik niezawodności połączenia. Przejrzyj wyniki i sprawdź, czy polecenie **ping** zakończyło się pomyślnie. Jeśli nie, spróbuj rozwiązać ten problem. _____

Jeśli w sieci dostępny jest inny komputer, spróbuj wysłać pakiety **ping** na adres IP tego komputera. Zapisz wyniki. _____

Krok 4 Wyślij pakiety ping na adres IP domyślnej bramy

Spróbuj wysłać pakiety **ping** na adres IP domyślnej bramy, jeśli takowa została znaleziona w poprzednim ćwiczeniu. Jeśli polecenie **ping** zostało wykonane pomyślnie, oznacza to, że istnieje fizyczne połączenie z routerem znajdującym się w sieci lokalnej oraz prawdopodobnie z resztą świata.

Krok 5 Wyślij pakiety `ping` na adresy IP serwerów DHCP lub DNS

Spróbuj wysłać pakiety **ping** na adres IP dowolnego serwera DHCP i/lub DNS znalezionego w poprzednim ćwiczeniu. Jeśli polecenie zakończyło się pomyślnie dla któregokolwiek z serwerów, który jednak nie jest obecny w sieci, o czym to świadczy?

_____

Czy polecenie **ping** zostało wykonane pomyślnie? _____

Jeśli nie, spróbuj rozwiązać ten problem.

Krok 6 Wyślij pakiety ping na adres IP pętli zwrotnej

Wpisz następujące polecenie: **ping 127.0.0.1**

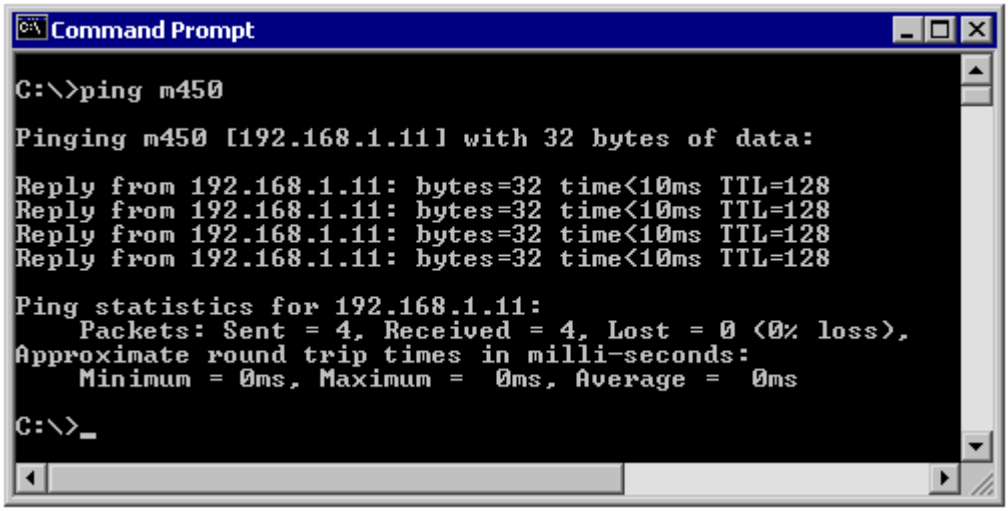
Sieć 127.0.0.0 jest zarezerwowana na potrzeby testowania wewnętrznego sprzężenia zwrotnego. Jeśli polecenie **ping** zakończyło się pomyślnie, oznacza to, że protokół TCP/IP jest prawidłowo zainstalowany i działa poprawnie na badanym komputerze.

Czy polecenie **ping** zostało wykonane pomyślnie? _____

Jeśli nie, spróbuj rozwiązać ten problem.

Krok 7 Wyślij pakiety `ping`, używając nazwy hosta innego komputera

Spróbuj użyć polecenia **ping**, używając nazwy hosta zanotowanej w poprzednim ćwiczeniu. Na rysunku pokazano wyniki pomyślnego wykonania polecenia **ping** z podaniem nazwy hosta.



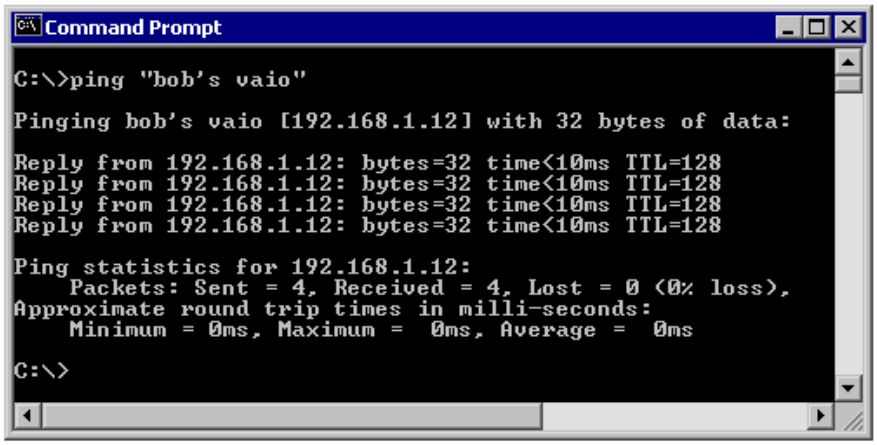
Zapoznaj się z wynikami. Zauważ, że w pierwszym wierszu wyniku działania polecenia znajduje się nazwa hosta, w tym przypadku m450, po której występuje adres IP. Oznacza to, że komputer potrafił odwzorować nazwę hosta na adres IP. Bez funkcji odwzorowywania nazw polecenie **ping** zakończyłoby się niepomyślnie, ponieważ protokół TCP/IP używa wyłącznie poprawnych adresów IP, a nie nazw.

Jeśli polecenie **ping** zakończyło się pomyślnie, oznacza to, że przy nawiązywaniu połączeń i rozpoznawaniu adresów IP można posługiwać się wyłącznie nazwami hostów. W ten sposób utrzymywano komunikację w wielu wczesnych sieciach. Jeśli polecenie **ping** używające nazwy hosta zakończyło się pomyślnie, oznacza to również, że w sieci prawdopodobnie pracuje serwer WINS. Serwery WINS lub lokalny plik “lmhosts” służą do zamiany nazw hosta komputerów na ich adresy IP. Jeśli polecenie **ping** zakończy się niepomyślnie, może to świadczyć, że nie działa rozpoznawanie nazw NetBIOS i ich zamiana na adresy IP.

> **Uwaga:** W sieciach Windows 2000 lub XP często się zdarza, że funkcje te nie są obsługiwane. Jest to stara technologia, która często jest zbędna.

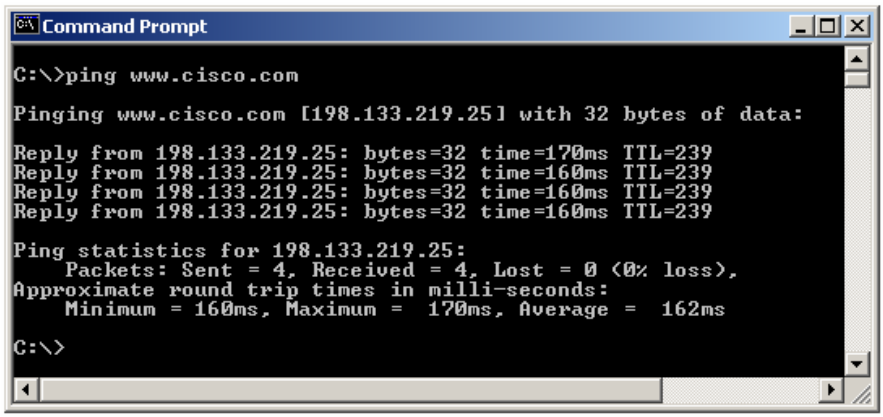
Jeśli ostatnie polecenie **ping** zakończyło się pomyślnie, spróbuj wykonać je, używając nazwy dowolnego innego komputera znajdującego się w sieci lokalnej. Na poniższym rysunku przedstawiono możliwe wyniki.

> **Uwaga:** Nazwa musiała być ujęta w cudzysłów, ponieważ język poleceń nie dopuszcza występowania spacji w nazwie.



Krok 8 Wyślij pakiety ping na adres witryny firmy Cisco

Wpisz następujące polecenie: **`ping www.cisco.com`**



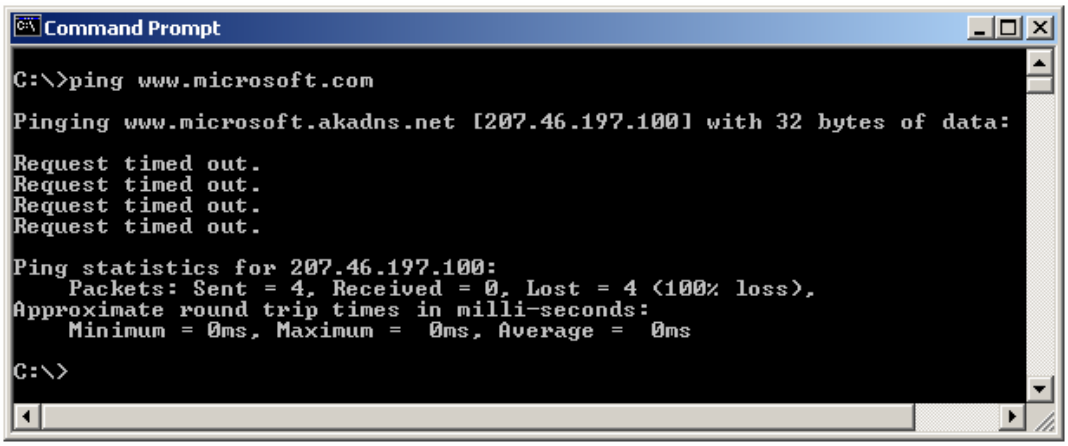
Pierwszy wiersz wyniku działania polecenia zawiera pełną nazwę domenową (*Fully Qualified Domain Name*, FQDN), po której występuje adres IP. Znajdujący się gdzieś w sieci serwer DNS (*Domain Name Service*) był w stanie zamienić podaną nazwę na adres IP. Serwery DNS zamieniają nazwy domen (nie nazwy hostów) na adresy IP.

Bez funkcji odwzorowywania nazw polecenie **`ping`** zakończyłoby się niepomyślnie, ponieważ protokół TCP/IP używa wyłącznie poprawnych adresów IP. Bez funkcji odwzorowywania nazw na adresy praca przeglądarek byłaby niemożliwa.

Korzystając z serwerów DNS, można sprawdzić połączenie z komputerami w Internecie, używając do tego celu dobrze znanych adresów WWW lub adresów domen, bez konieczności odwoływania się do ich adresów IP. Jeśli najbliższy serwer DNS nie zna danego adresu IP, wysyła zapytanie do innego serwera DNS znajdującego się wyżej w strukturze Internetu.

Krok 9 Wyślij pakiety ping na adres witryny firmy Microsoft

a. Wpisz następujące polecenie: **`ping www.microsoft.com`**



Zauważ, że serwer DNS rozpoznał nazwę i zamienił ją na adres IP, ale brak jest odpowiedzi. Niektóre serwery są tak skonfigurowane, aby ignorować pakiety **`ping`**. Jest to często stosowane zabezpieczenie.

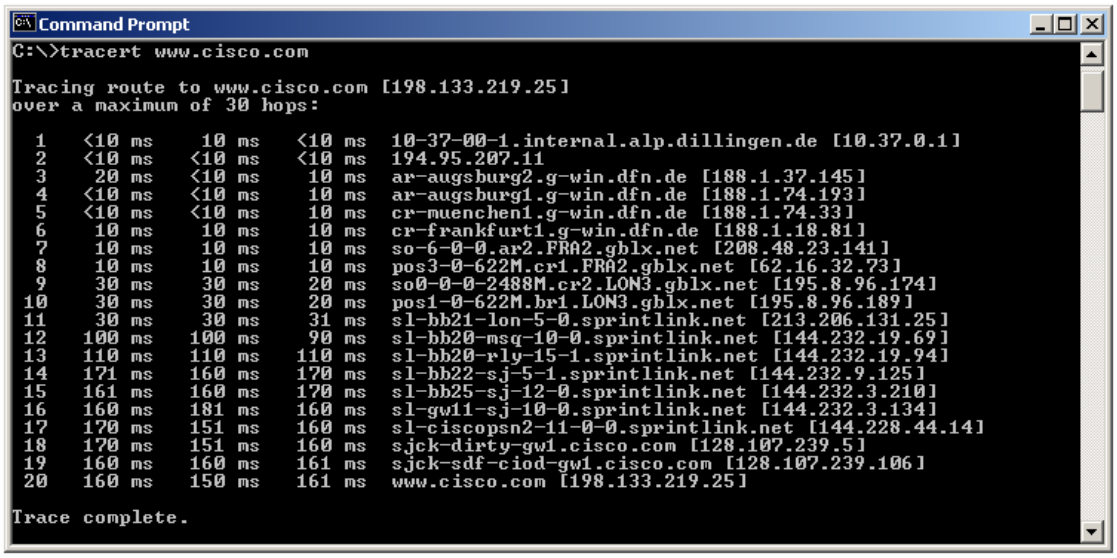
Wyślij pakiety **`ping`** na adresy innych domen i zapisz wyniki. Na przykład **`ping www.msn.de`**

_____

_____

Krok 10 Prześledź drogę do witryny firmy Cisco

Wpisz polecenie **tracert www.cisco.com** i naciśnij klawisz **Enter**.



Nazwa **tracert** stanowi skrót pojęcia trace route (śledź trasę). Na poprzednim rysunku pokazano wyniki pomyślnego uruchomienia polecenia **tracert** z Bawarii w Niemczech. Pierwszy wiersz wyniku działania polecenia zawiera nazwę FQDN, po której występuje adres IP. Oznacza to, że serwer DNS odwzorował nazwę na adres IP. Następnie wyświetlana jest lista wszystkich routerów, przez które musiały przejść żądania wysłane przez polecenie **tracert**, aby dotrzeć do miejsca przeznaczenia.

Polecenie **tracert** korzysta z takiego samego żądania i odpowiedzi protokołu echo, jak polecenie **ping**, lecz stosuje je w nieco inny sposób. Należy zauważyć, że polecenie **tracert** w rzeczywistości z każdym routerem kontaktowało się trzykrotnie. Porównaj te wyniki, aby ocenić spójność trasy. Zauważ, że w powyższym przykładzie występowały znaczące opóźnienia po routerach 11 i 13, zapewne spowodowane przeciążeniami. Głównym wnioskiem jest jednak to, że połączenie wydaje się być spójne.

Każdy router jest punktem przekazywania pakietów, w którym sieć łączy się z inną siecią.

Krok 11 Prześledź trasy do innych adresów IP lub nazw domen

Użyj polecenia **tracert**, stosując inne nazwy domen lub adresy IP, i zanotuj wyniki. Na przykład użyj polecenia **tracert www.msn.de**.

_____

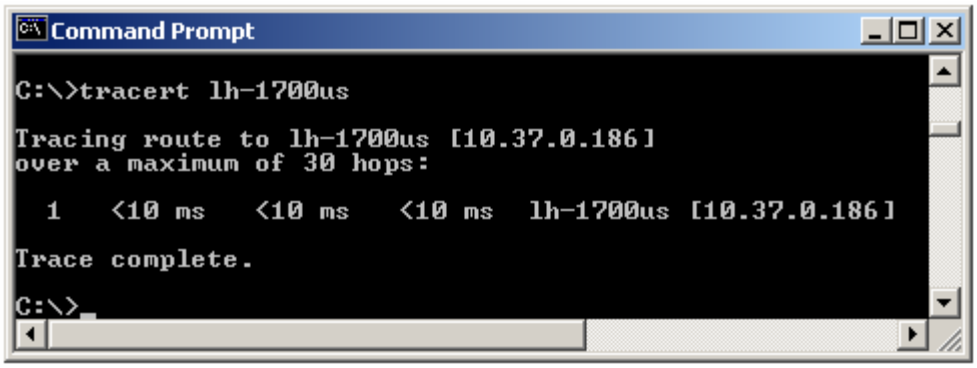
_____

_____

_____

Krok 12 Prześledź trasę do nazwy lokalnego hosta lub lokalnego adresu IP

Spróbuj użyć polecenia **tracert** w odniesieniu do nazwy lokalnego hosta lub adresu IP. Wykonanie polecenia nie powinno zabrać wiele czasu, ponieważ pakiety nie muszą przechodzić przez żadne routery.



To kończy zajęcia.

Do przemyślenia

Jeśli powyższe czynności zakończyły się powodzeniem i polecenia **ping** lub **tracert** potwierdziły łączność z witryną internetową, jakie wnioski można wyciągnąć na temat konfiguracji komputera oraz routerów znajdujących się między komputerem a witryną? Czy domyślna brama pełni tu jakąś rolę, a jeśli tak, to jaką?

_____

_____

_____

_____

