



darmowe ebooki
aktualne czasopisma



ebookgigs.com

PROGRAM AKADEMII SIECI KOMPUTEROWYCH CISCO



CCNA 1:

Podstawy działania sieci komputerowych, wersja 3.1

Podręcznik laboratoryjny studenta

Ten dokument jest wyłączną własnością Cisco Systems, Inc. Zezwala się na drukowanie i kopiowanie tego dokumentu dla celów niekomercyjnych i do wyłącznego użytku przez instruktorów w ramach kursu CCNA 1: Podstawy działania sieci komputerowych jako część oficjalnego programu Akademii Sieci Komputerowych Cisco.



Ćwiczenie 1.1.2 Podzespoły komputera PC

Cele

- Zapoznanie się z podstawowymi podzespołami komputera PC.
- Identyfikacja gniazd komputera PC, w tym gniazd służących do łączenia się z siecią.
- Zapoznanie się z budową wewnętrzną komputera PC oraz identyfikacja głównych podzespołów.
- Obserwacja procesu uruchamiania systemu operacyjnego Windows.
- Korzystanie z Panelu Sterowania w celu pozyskania informacji o komputerze.

Wprowadzenie

Znajomość podzespołów komputera PC jest niezbędna do rozwiązywania problemów. Wiedza ta jest również istotna dla wszystkich osób zajmujących się sieciami komputerowymi.

Przed rozpoczęciem zajęć instruktor powinien przygotować typowy komputer PC ze wszystkimi urządzeniami peryferyjnymi. Do urządzeń peryferyjnych zaliczamy klawiaturę, monitor, mysz, głośniki lub słuchawki, kartę sieciową i kabel sieciowy. Należy zdjąć pokrywę komputera. Jeśli pokrywa nie została zdjęta, należy przygotować służące do tego narzędzia. Praca odbywa się indywidualnie lub w grupach. Ponadto instruktor powinien wskazać miejsce, w którym znajdują się materiały szkoleniowe kursu A+ lub dotyczące podzespołów komputera PC.

Krok 1 Przyjrzyj się komputerowi i podzespołom peryferyjnym

Przyjrzyj się komputerowi i podzespołom peryferyjnym znajdującym się z przodu i z tyłu komputera.

Uwaga: Poszczególne egzemplarze komputera PC mogą różnić się między sobą podzespołami i konfiguracją.

Kto jest producentem komputera i jaki jest jego model?

Producent:	
Model:	

Jakie są główne zewnętrzne podzespoły komputera PC, w tym podzespoły peryferyjne?

Nazwa podzespołu	Producent / Opis / Charakterystyka
1.	
2.	
3.	
4.	
5.	

Krok 2 Zdejmij pokrywę komputera i obejrzyj podzespoły wewnętrzne

Wypisz co najmniej 8 głównych podzespołów wewnętrznych znajdujących się w komputerze. Skorzystaj z procedury opisanej w kroku 4, aby poznać typ procesora i wielkość pamięci RAM.

Nazwa podzespołu	Producent / Opis / Charakterystyka
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Krok 3 Złóż w całość podzespoły komputera i przyjrzyj się procesowi rozruchu

Złóż w całość podzespoły komputera, dołącz elementy peryferyjne i wykonaj rozruch komputera. Obserwuj proces rozruchu. Na komputerze powinien zostać uruchomiony system operacyjny Windows. Jeśli komputer nie uruchamia się, powiadom o tym instruktora.

Czy system operacyjny Windows uruchomił się prawidłowo? _____

Czy podczas rozruchu na ekranie została wyświetlona wielkość pamięci? _____

Krok 4 Zbierz podstawowe informacje o procesorze i pamięci RAM komputera

Zbierz podstawowe informacje o procesorze i pamięci komputera. Instrukcje wymagane do ukończenia tego kroku mogą się nieznacznie różnić w zależności od wersji systemu Windows. W razie potrzeby poproś o pomoc instruktora.

Kliknij przycisk Start. Wybierz kolejno opcje Ustawienia i Panel sterowania. Kliknij ikonę System, a następnie wybierz zakładkę Ogólne. Wyświetl informacje o komputerze, korzystając z funkcji systemu operacyjnego.

Jaki jest typ procesora? _____

Jaka jest prędkość procesora (w MHz)? _____

Ile pamięci RAM znajduje się w systemie? _____

Po zakończeniu zajęć należy doprowadzić sprzęt do stanu wyjściowego lub stanu określonego przez instruktora.

Ćwiczenie 1.1.6 Konfiguracja sieci TCP/IP na komputerze PC

Cele

- Identyfikacja narzędzi używanych do sprawdzania konfiguracji sieciowej komputera w różnych systemach operacyjnych.
- Zebranie informacji dotyczących połączenia, nazwy hosta, adresu warstwy 2 (MAC) oraz adresu sieciowego warstwy 3 (adresu IP).
- Porównanie informacji sieciowych zebranych z różnych komputerów.

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 sieci LAN mającej połączenie z Internetem. Można je przeprowadzić, korzystając z pojedynczego połączenia modemowego lub połączenia DSL. Adresy IP zostaną podane przez instruktora.

Ćwiczenie należy wykonać dwukrotnie, aby zaobserwować różnice między systemami operacyjnymi Windows 95/98/ME i NT/2000/XP. Jeśli jest to możliwe, uczestnicy kursu powinni je wykonać na obu typach systemów operacyjnych.

Uwaga: Wszyscy użytkownicy wykonują krok 1

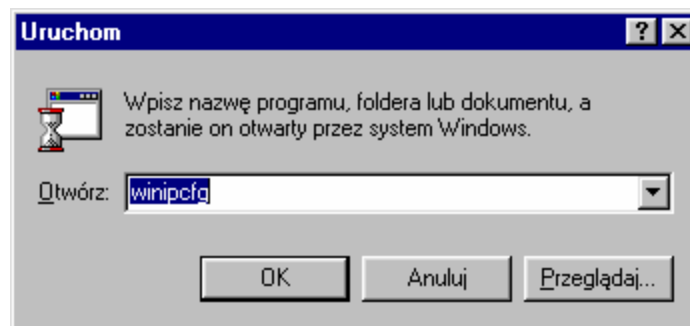
Krok 1 Nawiąż połączenie z Internetem

Nawiąż i sprawdź połączenie z Internetem. Dzięki temu można się upewnić, że komputer ma adres IP.

Uwaga: Użytkownicy systemów Windows 95/98/Me wykonują kroki od 2 do 6.

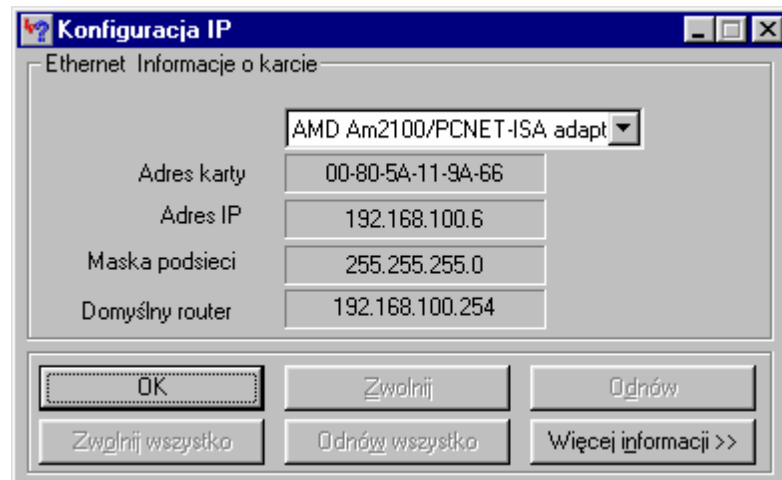
Krok 2 Zbierz podstawowe informacje o konfiguracji TCP/IP

Z paska zadań wybierz kolejno polecenia **Start** i **Uruchom**. Zostanie wyświetlone następujące okno.



Wpisz **winipcfg** i naciśnij klawisz **Enter** (wielkość liter nie ma znaczenia). Nazwa ta stanowi skrót polecenia Windows IP Configuration (Konfiguracja IP w systemie Windows). W pierwszym polu

wyświetlany jest adres karty sieciowej, czyli adres MAC komputera. Oprócz tego wyświetlany jest również adres IP, maska podsieci i domyślna brama. Poniższy rysunek przedstawia okno podstawowej konfiguracji sieci IP. Jeśli na liście znajduje się kilka kart sieciowych, wybierz właściwą.



Adres IP i domyślna brama powinny znajdować się w tej samej sieci lub podsieci. W przeciwnym przypadku host nie będzie mógł komunikować się z komputerami znajdującymi się poza lokalną siecią. Maska podsieci widoczna na poprzednim rysunku wskazuje, że jeśli trzy pierwsze oktety adresu są takie same, to urządzenia znajdują się w tej samej sieci. Adresy IP zostaną omówione w module 9.

Uwaga: W przypadku komputera znajdującego się w sieci LAN domyślna brama może być niewidoczna, jeśli znajduje się ona za serwerem proxy. Zapisz następujące informacje dla używanego komputera:

Adres IP: _____

Maska podsieci: _____

Domyślna brama: _____

Krok 3 Porównaj konfiguracje TCP/IP

Jeśli dany komputer znajduje się w sieci LAN, porównaj informacje zebrane z kilku komputerów.

Czy występują podobieństwa?

Jakie są podobieństwa między adresami IP?

Jakie są podobieństwa między adresami domyślnych bram?

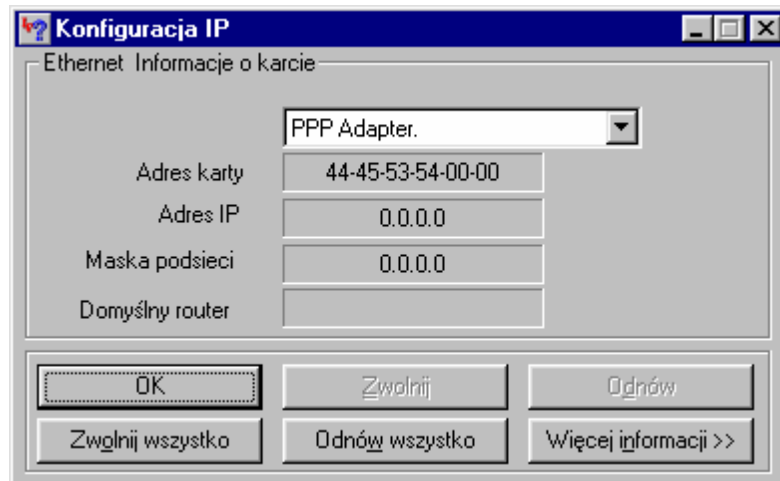
Jakie są podobieństwa między adresami MAC? _____

W adresach IP część dotycząca sieci powinna być taka sama. Wszystkie komputery znajdujące się w jednej sieci LAN powinny używać takiego samego adresu domyślnej bramy. Chociaż nie jest to konieczne, większość administratorów sieci LAN stara się używać ujednoczonych podzespołów, na przykład kart sieciowych. Z tego powodu adresy kart sieciowych we wszystkich komputerach mogą mieć takie same trzy pierwsze pary cyfr szesnastkowych. Te trzy pary identyfikują producenta karty.

Zapisz kilka adresów IP

Krok 4 Sprawdź konfigurację wybranej karty sieciowej

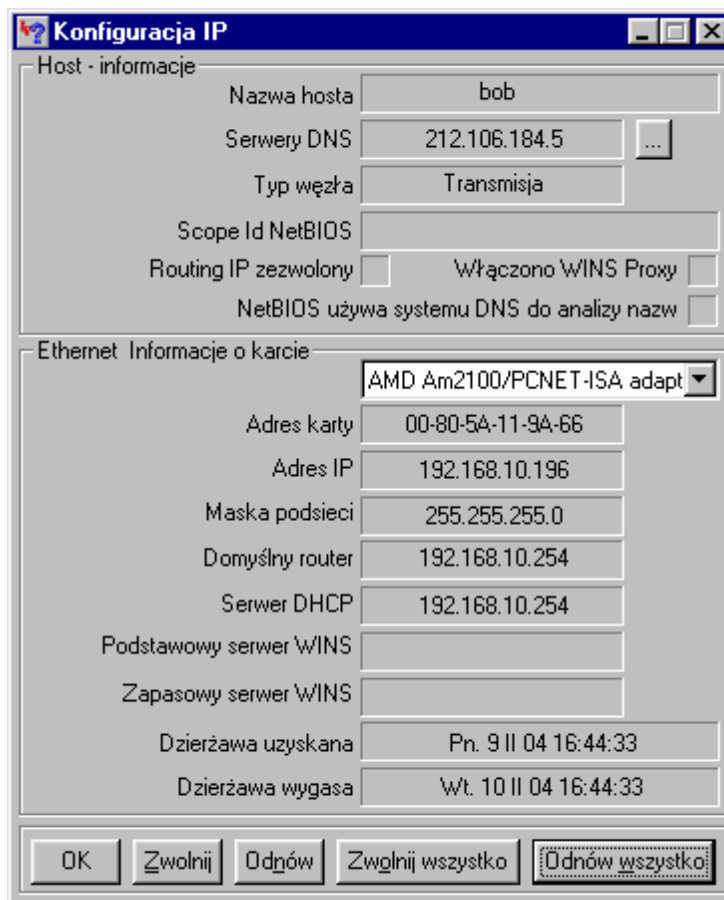
Model karty sieciowej dla danego komputera powinien być wyświetlany w polu u góry okna. Użyj strzałki znajdującej się w tym polu, aby rozwinąć jego zawartość i sprawdzić, czy istnieją inne konfiguracje dla tej karty, takie jak PPP. Może tak być w przypadku modemu, jeśli komputer łączy się z Internetem przy użyciu połączenia telefonicznego. W przypadku serwera możliwe jest znalezienie innej karty sieciowej lub też karty sieciowej i modemu. Na następnym rysunku pokazano ekran konfiguracyjny sieci IP dla połączenia modemowego AOL. Należy zauważyć, że na rysunku nie występuje adres IP. Może tak być w przypadku komputera domowego, jeśli użytkownik nie zalogował się jeszcze do Internetu.



Należy powrócić do karty sieciowej, dla której wyświetlane są dane dotyczące karty lub modemu zawierające adres IP

Krok 5 Sprawdź dodatkowe informacje dotyczące konfiguracji TCP/IP

Kliknij przycisk **Więcej informacji >>**. Na następnym rysunku pokazano szczegółowe informacje wyświetlane w oknie Konfiguracja IP.



Kliknięcie przycisku **Więcej informacji** powoduje wyświetlenie nazwy hosta, która zawiera nazwę komputera oraz nazwę NetBIOS. Wyświetlany jest również adres serwera DHCP, jeśli taki jest używany, oraz data rozpoczęcia i zakończenia dzierżawy adresu IP. Zapoznaj się z pozostałymi informacjami. Mogą być również wyświetlane pozycje dotyczące serwerów DNS i WINS. Pozycje te są używane przy odwzorowywaniu nazw na adresy.

Zapisz adresy IP wszystkich serwerów znajdujących się na liście:

Zapisz nazwę hosta dla danego komputera:

Zapisz nazwy hostów dla kilku innych komputerów: _____

Czy wszystkie serwery i stacje robocze mają taką samą część sieciową adresu IP jak używana stacja robocza? _____

Uwaga: Sytuacja, gdy niektóre lub wszystkie serwery i stacje robocze znajdują się w innej sieci, nie jest niczym niezwykłym. Za komunikację z hostami znajdującymi się w innej sieci odpowiada wtedy domyślna brama dla danego komputera.

Krok 6 Zamknij okno po zakończeniu sprawdzania ustawień sieciowych

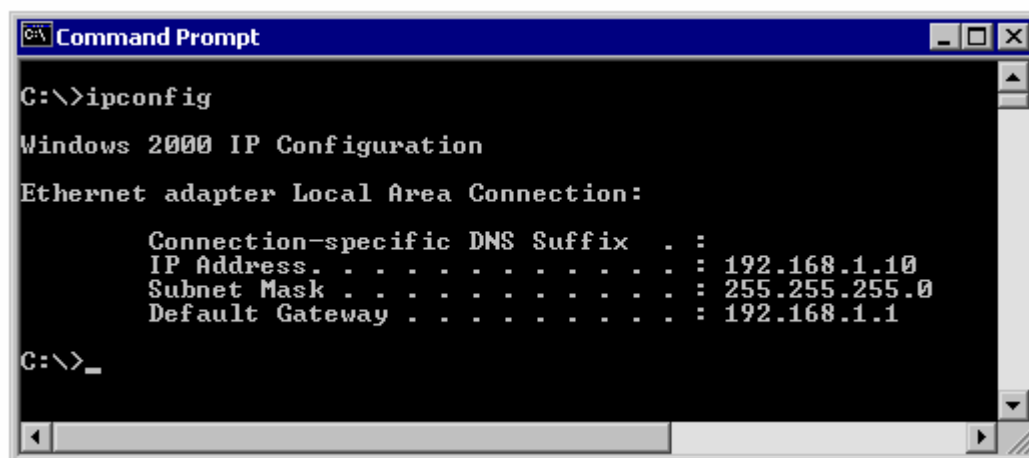
Jeśli uważasz to za konieczne, powtórz wykonane czynności, aby upewnić się, że nie występują żadne problemy przy wyświetlaniu okna dialogowego i interpretowaniu prezentowanych w nim informacji.

Uwaga: Użytkownicy systemów operacyjnych Windows NT/2000/XP wykonują kroki od 7 do 11.

Step 7 Zbierz informacje o konfiguracji TCP/IP

Skorzystaj z menu Start, aby otworzyć okno wiersza poleceń, przypominające okno systemu MS-DOS. Wybierz kolejno polecenia **Start > Programy > Akcesoria > Wiersz poleceń** lub **Start > Programy > Wiersz poleceń**.

Na poniższym rysunku jest pokazane okno wiersza poleceń. Wpisz `ipconfig` i naciśnij klawisz **Enter** (wielkość liter nie ma znaczenia). Nazwa ta stanowi skrót polecenia IP Configuration (Konfiguracja IP).



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\>_
```

W prezentowanym pierwszym oknie jest wyświetlany adres IP, maska podsieci i domyślna brama. Adres IP i domyślna brama powinny znajdować się w tej samej sieci lub podsieci, w przeciwnym przypadku host nie będzie mógł nawiązać połączenia z komputerami znajdującymi się poza własną siecią. Maska podsieci widoczna na rysunku wskazuje, że jeśli trzy pierwsze oktety adresu są takie same, to urządzenia znajdują się w tej samej sieci.

Uwaga: W przypadku komputera znajdującego się w sieci LAN domyślna brama może być niewidoczna, jeśli znajduje się ona za serwerem proxy.

Krok 8 Zapisz następujące informacje o sieci TCP/IP dla używanego komputera

Adres IP: _____

Maska podsieci: _____

Domyślna brama: _____

Krok 9 Porównaj konfigurację TCP/IP tego komputera z innymi komputerami znajdującymi się w sieci LAN

Jeśli dany komputer znajduje się w sieci LAN, porównaj informacje zebrane z kilku komputerów.

Czy występują podobieństwa?

Jakie są podobieństwa między adresami IP?

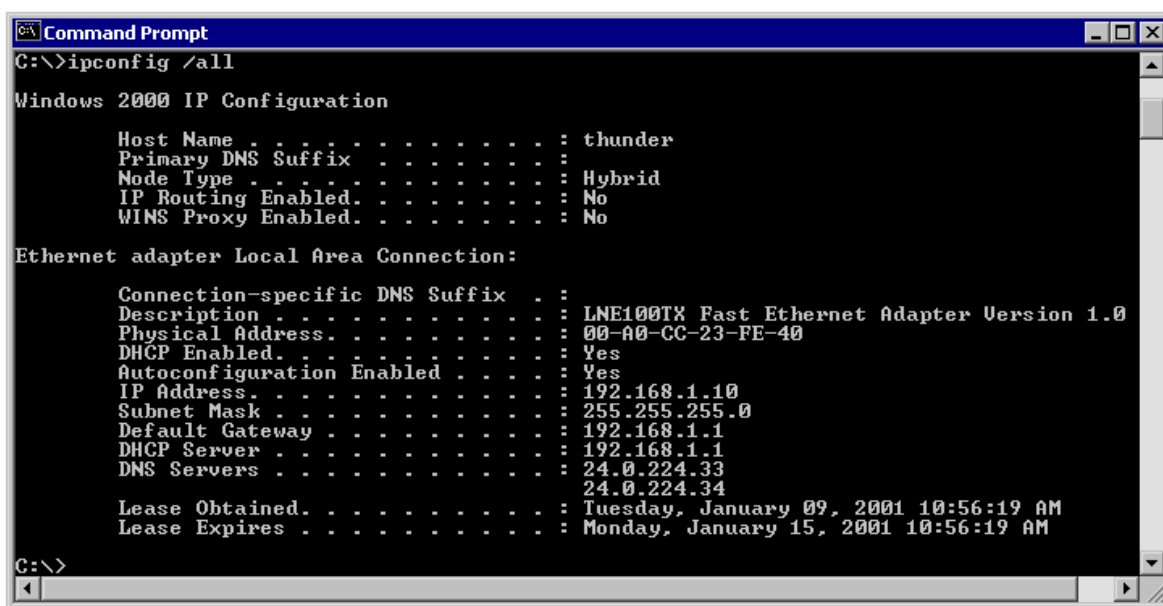
Jakie są podobieństwa między adresami domyślnych bram?

W adresach IP część dotycząca sieci powinna być taka sama. Wszystkie komputery znajdujące się w jednej sieci LAN powinny używać takiego samego adresu domyślnej bramy.

Zapisz kilka adresów IP:

Krok 10 Sprawdź dodatkowe informacje dotyczące konfiguracji TCP/IP

Aby zapoznać się z informacjami szczegółowymi, wpisz polecenie `ipconfig /all` i naciśnij klawisz **Enter**. Na rysunku pokazano wyświetlane na ekranie szczegółowe informacje dotyczące konfiguracji IP.



```
Command Prompt
C:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : thunder
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : LNE100TX Fast Ethernet Adapter Version 1.0
    Physical Address. . . . . : 00-A0-CC-23-FE-40
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 24.0.224.33
    . . . . . : 24.0.224.34
    Lease Obtained. . . . . : Tuesday, January 09, 2001 10:56:19 AM
    Lease Expires . . . . . : Monday, January 15, 2001 10:56:19 AM

C:\>
```

Powinno zostać wyświetlona nazwa hosta, która zawiera nazwę komputera i nazwę NetBIOS. Wyświetlany powinien być również adres serwera DHCP, jeśli taki jest używany, oraz data rozpoczęcia i zakończenia dzierżawy adresu IP. Zapoznaj się z tymi informacjami. Mogą również być wyświetlane adresy serwerów DNS używane do odwzorowywania nazw na adresy.

Dane wyświetlane na poprzednim rysunku wskazują, że router dostarcza w danej sieci usługi DHCP. Dzieje się tak często w przypadku małych firm lub biur domowych (SOHO, ang. small office or home office) albo w przypadku oddziałów większych przedsiębiorstw.

Należy zwrócić uwagę na adres fizyczny (MAC) oraz model karty sieciowej (Opis).

Jakie są podobieństwa adresów fizycznych (MAC) używanych w sieci LAN?

Chociaż nie jest to konieczne, większość administratorów sieci LAN stara się używać ujednoliconych podzespołów, na przykład kart sieciowych. Nie byłoby zatem dziwne, gdyby adresy kart sieciowych wszystkich komputerów miały takie same trzy pierwsze pary cyfr szesnastkowych. Te trzy pary identyfikują producenta karty.

Zapisz adresy IP wszystkich serwerów znajdujących się na liście:

Zapisz nazwę hosta dla danego komputera:

Zapisz nazwy hostów dla kilku innych komputerów:

Czy wszystkie serwery i stacje robocze mają taką samą część sieciową adresu IP jak używana stacja robocza? _____

Nie byłoby w tym nic dziwnego, gdyby niektóre lub wszystkie serwery i stacje robocze znajdowały się w innej sieci. Oznacza to, że domyślna brama dla tego komputera będzie przekazywała żądania do tej sieci.

Krok 11 Zamknij okno

Po zakończeniu sprawdzania ustawień sieciowych zamknij okno.

Jeśli jest to konieczne, powtórz poprzednie kroki. Sprawdź, czy potrafisz otworzyć ponownie to okno i zinterpretować wyświetlane wyniki.

To kończy zajęcia.

Do przemyślenia

Jakie na podstawie przeprowadzonych obserwacji możesz wyciągnąć wnioski, dysponując informacjami z trzech komputerów dołączonych do przełącznika?

Komputer 1

Adres IP: 192.168.12.113

Maska podsieci: 255.255.255.0

Domyślna brama: 192.168.12.1

Komputer 2

Adres IP: 192.168.12.205

Maska podsieci: 255.255.255.0

Domyślna brama: 192.168.12.1

Komputer 3

Adres IP: 192.168.112.97

Maska podsieci: 255.255.255.0

Domyślna brama: 192.168.12.1

Czy komputery mogą komunikować się ze sobą? Czy znajdują się w tej samej sieci? Dlaczego tak sądzisz? Jeśli nie wszystko jest w porządku, jaka jest najbardziej prawdopodobna przyczyna problemu?

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.

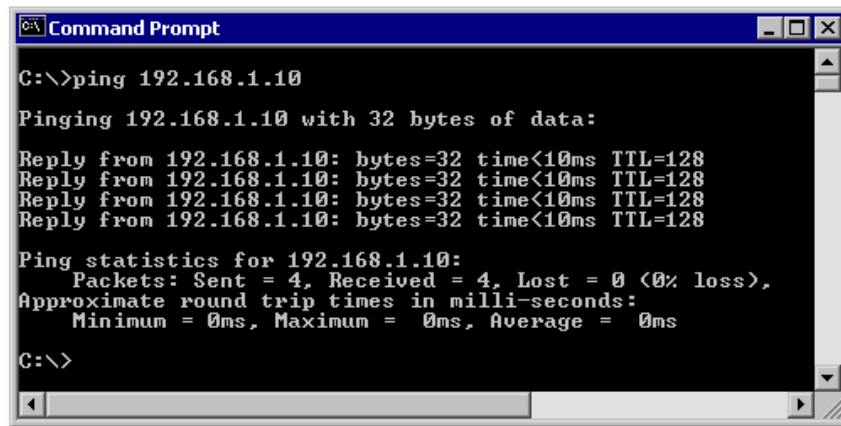
Krok 2 Otwórz okno wiersza poleceń

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.



```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

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 znalezionej 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`

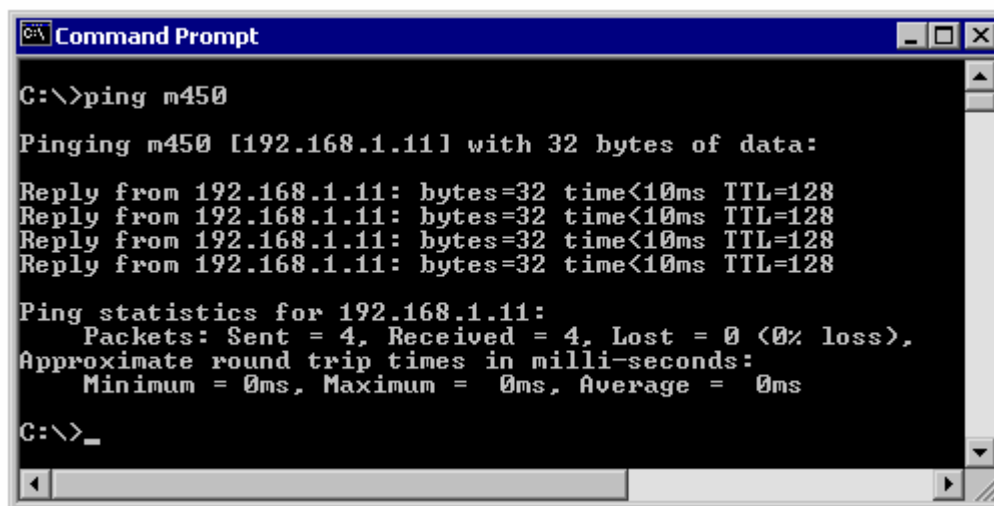
Sieć 127.0.0.0 jest zarezerwowana na potrzeby testowania wewnętrznego sprzężenia zwrotnego. Jeśli polecenie `ping` zakończyło się pomyślnie, oznacza to, że protokół TCP/IP jest prawidłowo zainstalowany i działa poprawnie na badanym komputerze.

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.



```
C:\>ping m450

Pinging m450 [192.168.1.11] with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

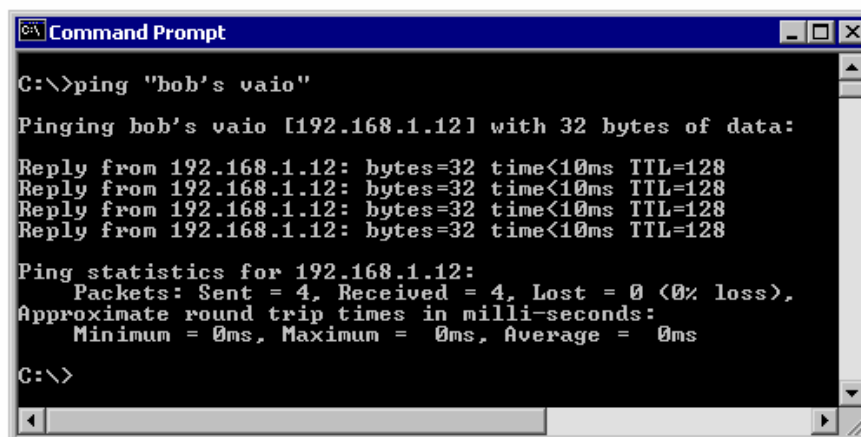
Zapoznaj się z wynikami. Zauważ, że w pierwszym wierszu wyniku działania polecenia znajduje się nazwa hosta, w tym przypadku m450, po której występuje adres IP. Oznacza to, że komputer potrafił odwzorować nazwę hosta na adres IP. Bez funkcji odwzorowywania nazw polecenie `ping` zakończyłoby się niepomyślnie, 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.



```
C:\>ping "bob's vaio"

Pinging bob's vaio [192.168.1.12] with 32 bytes of data:

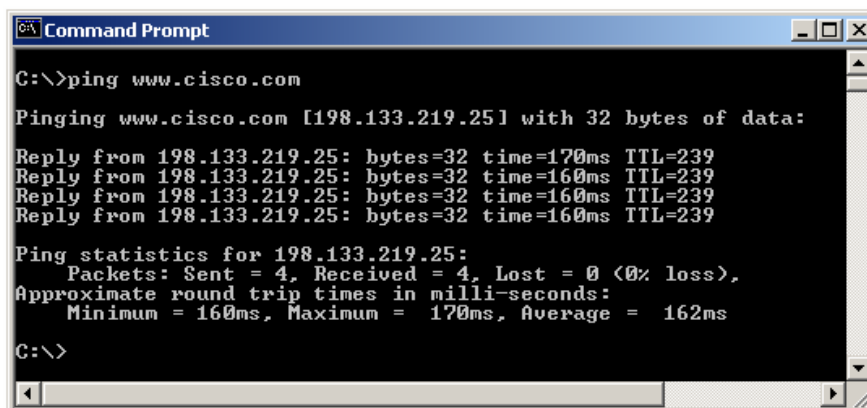
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Krok 8 Wyślij pakiety ping na adres witryny firmy Cisco

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



```
C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=170ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 160ms, Maximum = 170ms, Average = 162ms

C:\>
```

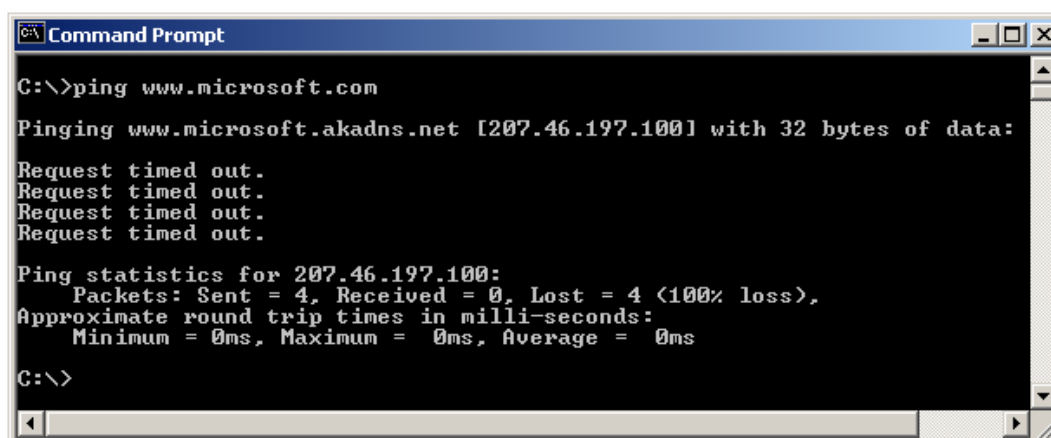
Pierwszy wiersz wyniku działania polecenia zawiera pełną nazwę domenową (*Fully Qualified Domain Name*, FQDN), po której występuje adres IP. Znajdujący się gdzieś w sieci serwer DNS (*Domain Name Service*) był w stanie zamienić podaną nazwę na adres IP. Serwery DNS zamieniają nazwy domen (nie nazwy hostów)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



```
C:\>ping www.microsoft.com

Pinging www.microsoft.akadns.net [207.46.197.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.197.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

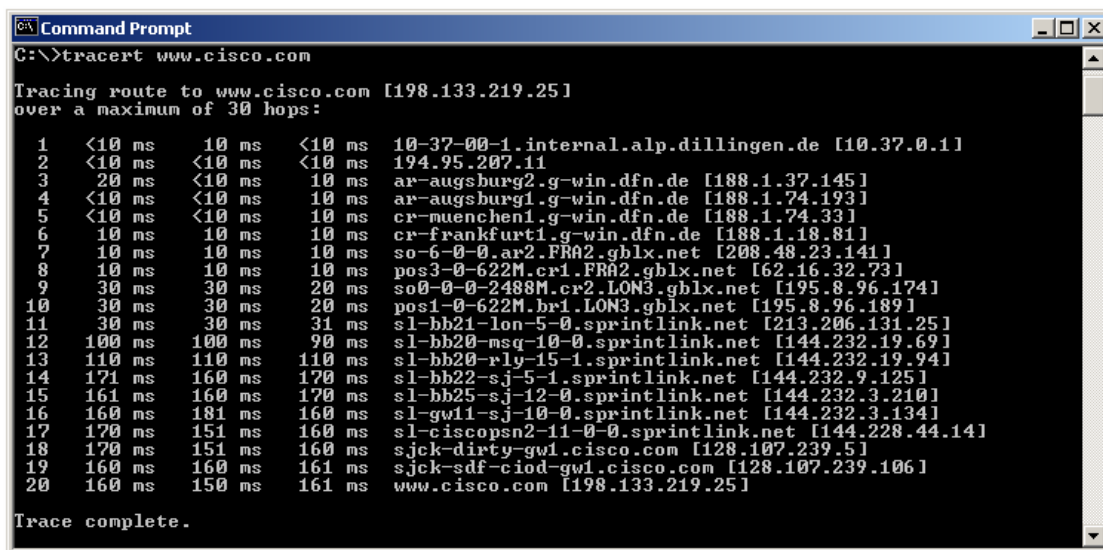
C:\>
```

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`.



```
Command Prompt
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.251]
over a maximum of 30 hops:
  0  <10 ms  <10 ms  <10 ms  10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ms  <10 ms  <10 ms  194.95.207.11
  2  20 ms  <10 ms  <10 ms  ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ms  <10 ms  <10 ms  ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ms  <10 ms  <10 ms  cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  <10 ms  <10 ms  <10 ms  cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  10 ms  10 ms  10 ms  so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  10 ms  10 ms  10 ms  pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  30 ms  30 ms  20 ms  so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  30 ms  30 ms  20 ms  pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  30 ms  30 ms  31 ms  sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11 100 ms 100 ms 90 ms  sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
 12 110 ms 110 ms 110 ms sl-bb20-rlv-15-1.sprintlink.net [144.232.19.94]
 13 171 ms 160 ms 170 ms sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
 14 161 ms 160 ms 170 ms sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15 160 ms 181 ms 160 ms sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16 170 ms 151 ms 160 ms sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17 170 ms 160 ms 161 ms sjck-dirty-gw1.cisco.com [128.107.239.5]
 18 160 ms 160 ms 161 ms sjck-sdf-ciod-gw1.cisco.com [128.107.239.106]
 19 160 ms 150 ms 161 ms www.cisco.com [198.133.219.251]
 20 160 ms 150 ms 161 ms

Trace complete.
```

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.

```
C:\>tracert lh-1700us

Tracing route to lh-1700us [10.37.0.186]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  lh-1700us [10.37.0.186]

Trace complete.

C:\>
```

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?

Ćwiczenie 1.1.8 Podstawy obsługi przeglądarki WWW

Cele

- Zapoznanie się ze sposobami korzystania z przeglądarki WWW.
- Zapoznanie się z pojęciem adresu URL.
- Używanie serwisów wyszukiwawczych do znajdowania informacji w Internecie.
- Uzyskanie dostępu do wybranych witryn WWW w celu zapoznania się z definicjami pojęć dotyczących sieci.
- Używanie hiperłączy do przechodzenia z bieżącej witryny WWW do innych witryn WWW.

Wprowadzenie

Przeglądarka WWW jest potężnym narzędziem używanym codziennie przez wielu ludzi do przeglądania różnych witryn sieci WWW. Przeglądarka WWW może pomóc w poszukiwaniu różnorodnych informacji, na przykład informacji o rozkładach lotów lub też wskazówek, jak dotrzeć w wybrane miejsce. Przeglądarka jest aplikacją kliencką znajdującą się na komputerze, za pomocą której można uzyskać dostęp do Internetu oraz do lokalnych stron WWW

Nazwa witryny WWW, taka jak **www.cisco.com**, jest przykładem adresu URL (*Universal Resource Locator*). Ten adres URL wskazuje na serwer WWW (*World Wide Web*) w domenie Cisco, która znajduje się w domenie COM (*Commercial*).

Po wpisaniu adresu URL przeglądarka wysyła do serwera DNS (*Domain Name Server*) żądanie zamiany adresu URL na adres IP. Ten adres IP jest używany do nawiązywania kontaktu z witryną.

Przy użyciu przeglądarki można uzyskać dostęp do serwisów wyszukiwawczych, wpisując ich nazwę w pasku adresu. Niektórymi znanymi wyszukiwarkami internetowymi są www.yahoo.com, www.excite.com, www.lycos.com i www.google.com.

Istnieje wiele witryn WWW, które zawierają definicje pojęć i akronimów związanych z komputerami i siecią. Można z nich skorzystać, aby dowiedzieć się więcej o zagadnieniach związanych z siecią oraz uzyskać informacje o Internecie. Przykładami takich witryn są www.whatis.com i www.webopedia.com.

Większość witryn zawiera hiperłączy. Hiperłączy najczęściej mają postać wyrazów, które są podkreślone i wyróżnione. Klikając hiperłączy, użytkownik „skacze” do innej strony w bieżącej witrynie lub do strony w innej witrynie WWW.

Do uczestnictwa w zajęciach wymagany jest skonfigurowany komputer oraz nowoczesna przeglądarka i dostęp do Internetu.

Krok 1 Uruchom przeglądarkę WWW

Jeśli wykorzystywane jest połączenie modemowe, przed uruchomieniem przeglądarki wybierz numer dostępowy. Jakiej wersji przeglądarki (Netscape lub Internet Explorer) używasz?

Krok 2 Znajdź pole adresu

Po uruchomieniu przeglądarki kliknij i zaznacz znajdujące się u góry strony pole **Location** (Lokalizacja) w przeglądarce Netscape lub **Adres** w przeglądarce Internet Explorer. Naciśnij klawisz **Delete**, aby usunąć bieżący adres.

Krok 3 Wpisz adres URL witryny WWW

Wpisz www.cisco.com i naciśnij klawisz **Enter**. W ten sposób można przechodzić od jednej witryny WWW do drugiej.

Krok 4 Wpisz inny adres URL

Aby załadować nową stronę, wpisz nowy adres URL, na przykład www.cnn.com. Zauważ, jaki stan jest wyświetlany na dolnym pasku przeglądarki. Co to oznacza? _____

Krok 5 Skorzystaj z przycisków zarządzania przeglądarki

Każdemu przyciskowi w górnej części przeglądarki jest przypisana określona funkcja. Po umieszczeniu nad przyciskiem wskaźnika myszy zostanie wyświetlone pole z opisem przycisku.

Kliknij przycisk **Back** (Wstecz). Co się stało? _____

Kliknij przycisk **Forward** (Dalej). Czy nastąpił powrót do witryny CNN?

Kliknij przycisk **Reload** (Załaduj ponownie) lub **Refresh** (Odśwież). Co się stało?

Wpisz www.microsoft.com i naciśnij klawisz **Enter**. Podczas ładowania zawartości okna kliknij przycisk **Stop** (Zatrzymaj). Co się stało?

Krok 6 Korzystanie z serwisów wyszukiwawczych

Wpisz adres URL serwisu wyszukiwawczego, na przykład www.google.com. W polu wyszukiwania wpisz wyraz **browser**. Jaki był wynik?

Krok 7 Dostęp do witryn WWW zawierających definicje pojęć związanych z siecią

Wpisz adres URL www.webopedia.com. Wprowadź słowo kluczowe **browser**. Jaki był wynik?

Jakie hiperłącza były dostępne?

Wprowadź adres URL www.whatis.com. Wyszukaj słowo kluczowe **DNS**. Kliknij przycisk Exact Match (Dokładne dopasowanie) dla słowa DNS w polu **whatis.com terms** (pojęcia whatis.com). Jakie informacje dotyczące DNS zostały wyświetlone?

To kończy zajęcia.

Do przemyślenia

Znajdź sposób przechodzenia między witrynami.

Jeśli przy następnych odwiedzinach witryny Euroleague.net wyświetlane są te same rysunki i tekst co poprzednio, co trzeba zrobić, aby upewnić się, że wyświetlane są zaktualizowane informacje?

Ćwiczenie 1.1.9 Podstawowa procedura rozwiązywania problemów z komputerem i siecią

Cele

- Poznanie prawidłowej kolejności czynności wykonywanych podczas rozwiązywania problemów związanych z komputerem i siecią.
- Zapoznanie się z najczęściej występującymi problemami sprzętowymi i programowymi.
- Nabycie umiejętności diagnozowania i rozwiązywania najczęściej występujących problemów.

Wprowadzenie

Umiejętność sprawnego rozwiązywania problemów związanych z komputerami jest bardzo istotna. Procedura identyfikowania problemu i rozwiązywania go wymaga systematycznego, etapowego podejścia. W tym ćwiczeniu zostaną przedstawione niektóre podstawowe problemy sprzętowe i programowe. Pomoże ono oswoić się z podzespołami komputera oraz z oprogramowaniem używanym w programie szkoleniowym Cisco. Procedura rozwiązywania problemów jest całkiem prosta. Niektóre przedstawione tu porady wykraczają poza wiedzę wymaganą do rozwiązywania podstawowych problemów sprzętowych i programowych. Stanowią one ogólne ramy postępowania i wskazówki w przypadku wystąpienia bardziej skomplikowanych problemów. Lista przykładowych problemów, które zostaną przedstawione, znajduje się w materiałach szkoleniowych przeznaczonych dla instruktora.

Osiem zasadniczych etapów procedury rozwiązywania problemów związanych z komputerem i siecią

Krok 1 Zdefiniuj problem

Opisz zdarzenie przy użyciu odpowiedniej terminologii. Na przykład: „komputer nie może nawiązać połączenia z Internetem” lub „nie można niczego wydrukować z komputera”.

Krok 2 Zbierz fakty

Zaobserwuj objawy i spróbuj scharakteryzować lub zidentyfikować źródło problemu:

- Czy jest związany ze sprzętem? (Sprawdź stan diod LED lub wydobywające się dźwięki.) Czy jest związany z oprogramowaniem, czy na ekranie są wyświetlane komunikaty o błędach?
- Czy problem dotyczy tylko danego komputera lub użytkownika, czy występuje także w innych miejscach lub u innych użytkowników?
- Czy dotyczy jednej, czy wielu aplikacji?
- Czy problem wystąpił po raz pierwszy, czy też pojawiał się wcześniej?
- Czy ostatnio dokonano jakichś zmian w komputerze?
- Zasięgnij opinii u innych, bardziej doświadczonych osób.
- Poszukaj informacji w witrynach WWW i w bazach wiedzy dotyczących rozwiązywania problemów.

Krok 3 Rozważ wszystkie rozwiązania

Wnioskujej na podstawie uzyskanych informacji. Znajdź jedną lub kilka możliwych przyczyn i potencjalnych rozwiązań. Uporządkuj rozwiązania w kolejności od najbardziej do najmniej prawdopodobnego.

Krok 4 Utwórz plan działania

Utwórz plan, biorąc pod uwagę jedno najbardziej prawdopodobne rozwiązanie. Inne opcje mogą być brane pod uwagę, jeśli wybrane rozwiązanie zawiedzie. Podczas tworzenia planu weź pod uwagę następujące czynniki:

- Sprawdź najpierw najprostszą możliwą przyczynę. Czy jest włączone zasilanie?
- Sprawdź najpierw sprzęt, a potem oprogramowanie.
- Jeśli problem jest związany z siecią, zacznij od warstwy 1 modelu OSI, po czym badaj kolejne warstwy. Badania wykazują, że najczęściej problemów występuje w warstwie 1.
- Czy zastąpienie podzespołu pomoże w wyizolowaniu problemu? Jeśli monitor nie działa, może to być wywołane uszkodzeniem monitora, karty graficznej lub kabli. Wypróbuj inny monitor, aby sprawdzić, czy rozwiązuje to problem.

Step 5 Wykonaj plan

Wykonaj zaplanowane zmiany, aby przetestować pierwsze możliwe rozwiązanie.

Krok 6 Obserwuj wyniki

Jeśli problem został rozwiązany, przejdź do udokumentowania rozwiązania. Sprawdź jeszcze raz, czy wszystko działa poprawnie.

Jeśli problem nie został rozwiązany, przywróć sytuację sprzed zmian i powróć do planu, wypróbując kolejne rozwiązanie. Jeśli stan sprzed zmiany nie zostanie przywrócony, nie będzie wiadomo, czy rozwiązanie problemu nastąpiło dzięki wprowadzonej później zmianie, czy też kombinacji obu zmian.

Krok 7 Udokumentuj wyniki

Zawsze dokumentuj wyniki, aby ułatwić postępowanie w przypadku wystąpienia podobnych problemów. Takie postępowanie pomaga również w tworzeniu historii dokumentacji dla danego urządzenia. Jeśli część urządzeń ma zostać zastąpiona, informacja o tym, czy któreś z nich jest przyczyną częstych kłopotów lub też czy było ostatnio naprawiane, może okazać się przydatna.

Krok 8 Wywołuj problemy i rozwiązuje je

Praca przebiega w grupach dwuosobowych. Celem jest przejrzanie jednego z nagrań wideo znajdujących się w materiałach szkoleniowych online lub na dysku CD. Każdy z członków grupy powinien wypełnić tabelę na podstawie zaobserwowanych objawów, zidentyfikowanych problemów i rozwiązań problemu.

Czynności wykonywane przez jednego z członków zespołu (A) lub instruktora:

1. Z listy często spotykanych problemów sprzętowych i programowych wybierz dwie pozycje.
2. Podczas nieobecności drugiego członka zespołu wywołaj w komputerze problemy sprzętowe lub programowe.
3. Wyłącz komputer i monitor.

Czynności wykonywane przez drugiego z członków zespołu (B):

1. Zidentyfikuj problemy.
2. Rozwiąż problemy.

Zamieńcie się miejscami i wykonajcie ponownie powyższe czynności.

Członek A zespołu

	Zaobserwowany objaw	Zidentyfikowany problem	Rozwiązanie
1. problem			
2. problem			

Członek B zespołu

	Zaobserwowany objaw	Zidentyfikowany problem	Rozwiązanie
1. problem			
2. problem			

To kończy zajęcia.

Ćwiczenie 1.2.5 Zamiana liczb dziesiętnych na dwójkowe

Cele

- Nauka zamiany wartości dziesiętnych na dwójkowe.
- Nabycie praktyki w zamianie liczb dziesiętnych na dwójkowe.

Wprowadzenie

Znajomość sposobów zamiany wartości dziesiętnych na dwójkowe jest wymagana podczas zamiany adresów IP zapisanych w zrozumiałej dla człowieka notacji kropkowo-dziesiętnej na zrozumiałą dla komputera format dwójkowy. Jest ona przydatna przy obliczaniu masek podsieci i przy innych zadaniach. W przykładzie przedstawiono adres IP w 32-bitowym formacie dwójkowym i w notacji kropkowo-dziesiętnej.

Adres IP w zapisie dwójkowym: 11000000.10101000.00101101.01111001
Adres IP w zapisie dziesiętnym: 192.168.45.121

Narzędziem ułatwiającym zadanie zamiany wartości dziesiętnych na dwójkowe jest następująca tabela. Pierwszy wiersz, oznaczający pozycję, jest utworzony z cyfr od 1 do 8 wypisanych od prawej do lewej. Tabeli tej można używać dla danych dwójkowych o dowolnej wielkości. Wiersz wartości rozpoczyna się od jedynki, a każda następna wartość jest dwukrotnie większa od poprzedniej (system o podstawie 2).

	8	7	6	5	4	3	2	1	
	128	64	32	16	8	4	2	1	
Wartość pozycji									

$$\begin{array}{r}
 128 \overline{) 207} \\
 \underline{128} \\
 64 \overline{) 79} \\
 \underline{64} \\
 8 \overline{) 15} \\
 \underline{8} \\
 4 \overline{) 7} \\
 \underline{4} \\
 2 \overline{) 3} \\
 \underline{2} \\
 1
 \end{array}$$

Taka sama tabela wraz z prostymi operacjami dzielenia może służyć do zamiany wartości dwójkowych na dziesiętne.

Kroki

Aby zamienić liczbę 207 na postać dwójkową:

1. Rozpocznij od liczby znajdującej się na skrajnie lewej pozycji w tabeli. Sprawdź, czy w wyniku dzielenia wartości dziesiętnej przez nią otrzymujemy liczbę większą niż jeden. Ponieważ wartość ta mieści się w liczbie jeden raz, wpisujemy 1 w trzecim rzędzie tabeli konwersji pod wartością 128 i obliczamy resztę z dzielenia, 79.
2. Ponieważ reszta może zostać podzielona przez następną wartość, 64, wpisz 1 w trzecim rzędzie tabeli pod wartością 64.

3. Ponieważ kolejna reszta nie może zostać podzielona przez 32 ani przez 16, wpisz 0 w trzecim wierszu tabeli pod wartościami 32 i 16.
4. Kontynuuj obliczenia aż do momentu, gdy nie zostanie żadna reszta.
5. Jeśli jest to konieczne, skorzystaj z czwartego wiersza w celu sprawdzenia obliczeń.

Wartość pozycji

8	7	6	5	4	3	2	1	
128	64	32	16	8	4	2	1	
1	1	0	0	1	1	1	1	
128	64			8	4	2	1	= 207

6. Zamień następujące wartości dziesiętne na dwójkowe:

a. 123 _____

b. 202 _____

c. 67 _____

d. 7 _____

e. 252 _____

f. 91 _____

g. 116.127.71.3 _____

h. 255.255.255.0 _____

i. 192.143.255.255 _____

j. 12.101.9.16 _____

To kończy zajęcia.

Ćwiczenie 1.2.6 Zamiana liczb dwójkowych na dziesiętne

Cele

- Nauka zamiany wartości dwójkowych na dziesiętne.
- Nabycie praktyki w zamianie wartości dwójkowych na dziesiętne.

Wprowadzenie

W następującym przykładzie przedstawiono adres IP w 32-bitowym formacie dwójkowym i w notacji kropkowo-dziesiętnej.

Adres IP w zapisie dwójkowym: **11000000.10101000.00101101.01111001**
Adres IP w zapisie dziesiętnym: **192.168.45.121**

Dane binarne składają się z zer i jedynek. Jedyнки reprezentują stan włączenia, a zera — stan wyłączenia. Dane binarne można łączyć w grupy o różnej długości, na przykład 110 lub 1011. W sieciach TCP/IP dane binarne są najczęściej gromadzone w grupach składających się z ośmiu bitów, czyli w tak zwanych bajtach.

Bajt, czyli 8 bitów, może przybierać wartości od 00000000 do 11111111, co daje $2^8 = 256$ kombinacji o wartościach dziesiętnych od 0 do 255. Adres IP składa się z 4 bajtów (32 bitów) i może służyć do identyfikacji zarówno sieci, jak i konkretnego urządzenia. Takim urządzeniem może być węzeł lub host. W przykładzie przedstawionym na początku tego ćwiczenia podano adres IP w formacie dwójkowym i dziesiętnym.

Narzędziem ułatwiającym zadanie zamiany wartości dwójkowych na dziesiętne jest następująca tabela. Pierwszy wiersz, oznaczający pozycję, jest utworzony z cyfr od 1 do 8 wypisanych od prawej do lewej. Tabeli tej można używać dla danych dwójkowych o dowolnej wielkości. Wiersz wartości rozpoczyna się od jedynki, a każda następna wartość jest dwukrotnie większa od poprzedniej (system o podstawie 2).

Wartość pozycji	8	7	6	5	4	3	2	1
	128	64	32	16	8	4	2	1

Kroki

1. Wpisz bity wartości dwójkowej w trzecim wierszu. Na przykład 10111001
2. Wpisz liczby dziesiętne w czwartym wierszu tylko wtedy, gdy wartością w trzecim wierszu jest 1. Technicznie odpowiada to pomnożeniu wartości z wiersza drugiego przez odpowiadające im wartości z wiersza trzeciego.
3. Teraz wystarczy dodać do siebie wszystkie wartości z wiersza czwartego.

Wartość pozycji	8	7	6	5	4	3	2	1	
	128	64	32	16	8	4	2	1	
	1	0	1	1	1	0	0	1	
	128		32	16	8			1	= 185

4. Zamień następujące wartości dwójkowe na dziesiętne:

a. 1110 _____

b. 100110 _____

c. 11111111 _____

d. 11010011 _____

e. 01000001 _____

f. 11001110 _____

g. 01110101 _____

h. 10001111 _____

i. 11101001.00011011.10000000.10100100

j. 10101010.00110100.11100110.00010111

Ćwiczenie 1.2.8 Zamiana liczb szesnastkowych

Cele

- Nauka zamiany wartości szesnastkowych na dziesiętne i dwójkowe.
- Nauka zamiany wartości dziesiętnych i dwójkowych na szesnastkowe.
- Nabycie praktyki w zamianie wartości dziesiętnych, dwójkowych i szesnastkowych.

Wprowadzenie i przygotowanie

Szesnastkowy (heksadecymalny) system liczbowy jest używany w przypadku adresów kart sieciowych oraz adresów protokołu IPv6. Słowo „heksadecymalny” pochodzi z języka greckiego i oznacza „szesnastkowy”. Do oznaczania liczb szesnastkowych często używany jest skrót „0x”, zero i mała litera x. Liczby szesnastkowe są zapisywane za pomocą szesnastu różnych cyfr, zaś każdą ośmiocyfrową liczbę dwójkową można zapisać w postaci jedynie dwóch cyfr szesnastkowych.

Bajt, czyli 8 bitów, może przybierać wartości od 00000000 do 11111111, co daje $2^8 = 256$ kombinacji o wartościach dziesiętnych od 0 do 255, lub szesnastkowo od 0 do FF. Każda cyfra szesnastkowa reprezentuje cztery bity. Wielkość używanych w zapisie szesnastkowym znaków alfanumerycznych nie ma znaczenia (np. 0xAF = 0xaf).

Narzędziem ułatwiającym zadanie zamiany wartości szesnastkowych na dziesiętne jest poniższa tabela. Wykorzystywana jest ta sama metoda co w przypadku zamiany wartości dwójkowych na dziesiętne. Pierwszy wiersz wskazuje dwie pozycje szesnastkowe. Wiersz wartości rozpoczyna się od wartości 1 i 16, co odpowiada podstawie systemu równej 16.

Wartość pozycji

2	1
16	1

Dzi	Szes	Dwójk
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Uwaga: Na końcu tego ćwiczenia opisano, w jaki sposób można sprawdzić wyniki za pomocą kalkulatora znajdującego się w systemie Windows.

Kroki wymagane do konwersji wartości dziesiętnych na szesnastkowe

1. Na potrzeby tych ćwiczeń będą używane tylko wartości dziesiętne należące do przedziału od 0 do 255. Pierwsza cyfra szesnastkowa jest otrzymywana przez podzielenie wartości dziesiętnej przez 16. Jeśli wynik dzielenia jest większy niż 9, należy zapisać cyfrę jako odpowiednią literę z przedziału od A do F.
2. Druga cyfra jest resztą z dzielenia w kroku 1. Jeśli jej wartość jest większa niż 9, należy ją zapisać jako odpowiednią literę z przedziału od A do F.

- Na przykład liczba 209 dzielona na 16 daje 13 z resztą 1. 13 w zapisie szesnastkowym to litera D. Stąd liczbie 209 odpowiada D1.

Kroki wymagane do konwersji wartości szesnastkowych na dwójkowe

- Jest to najprostsza z konwersji. Należy pamiętać, że każda cyfra szesnastkowa jest zamieniana na cztery bity, a operację należy przeprowadzać od strony prawej do lewej.
- Oto przykład zamiany liczby **77AE** na postać dwójkową. Rozpocznij od litery E. Użyj tabeli znajdującej się początku tego ćwiczenia, aby przejść bezpośrednio do postaci dwójkowej. Innym sposobem jest zamiana na postać dziesiętną, $E = 14$, i następnie użycie czterech ostatnich pozycji w tabeli stosowanej do konwersji wartości dziesiętnych na dwójkowe.

14 dzielone przez 8 daje 1 z resztą 6.

6 dzielone przez 4 daje 1 z resztą 2.

2 dzielone przez 2 daje 1 bez reszty.

Jeśli jest to konieczne, dodaj zera, aby uzupełnić wynik do czterech bitów.

Wartość pozycji	4	3	2	1	= 14
	8	4	2	1	
	1	1	1	0	
	8	4	2		

- Stosując tę samą metodę, A staje się 1010 i cała bieżąca wartość wynosi 10101110.

Wartość pozycji	4	3	2	1	= 10
	8	4	2	1	
	1	0	1	0	
	8		2		

- Stosując tę samą metodę, każda z dwóch siódemek staje się liczbą 0111, co łącznie daje 01110111.10101110.

Wartość pozycji	4	3	2	1	= 7
	8	4	2	1	
	0	1	1	1	
		4	2	1	

Kroki wymagane do konwersji wartości dwójkowych na szesnastkowe

- Każda cyfra szesnastkowa odpowiada czterem bitom. Zaczynaj od podziału liczby dwójkowej na grupy 4-bitowe, zaczynając od prawej strony. Jeśli jest to konieczne, uzupełnij ostatnią grupę zerami, tak aby każda grupa składała się z 4 bitów. 01101110. 11101100 stanie się 0110 1110 1110 1100.
- Skorzystaj z tabeli znajdującej się na początku ćwiczenia, aby przejść bezpośrednio do postaci szesnastkowej. Alternatywnym rozwiązaniem jest zamiana każdej czterobitowej wartości na wartość dziesiętną z przedziału od 0 do 15. Następnie otrzymane wartości należy zamienić na postać szesnastkową, od 0 do F.

Wartość pozycji	4	3	2	1	= 12 lub C
	8	4	2	1	
	1	1	0	0	
	8	4			

Wartość pozycji	4	3	2	1	= 14 lub E
	8	4	2	1	
	1	1	1	0	
	8	4	2		

3. W rezultacie otrzymujemy liczbę 6E-EC.

Ćwiczenia

Zamień następujące wartości na pozostałe dwie postaci:

	Dziesiętnie	Szesnastkowo	Dwójkowo
1		a9	
2		FF	
3		Bad1	
4		E7-63-1C	
5	53		
6	115		
7	19		
8	212.65.119.45		
9			10101010
10			110
11			11111100.00111100
12			00001100.10000000.11110000.11111111

Używanie kalkulatora systemu Windows do sprawdzania wyników konwersji

Ważne jest, aby umieć ręcznie wykonać przedstawione powyżej obliczenia. Można jednak sprawdzić obliczenia za pomocą aplikacji Kalkulator systemu Windows. Wybierz kolejno polecenia **Start > Programy > Akcesoria**, a następnie **Kalkulator**. Kliknij menu **Widok** i sprawdź, czy kalkulator pracuje w trybie **Naukowy**. Klikając odpowiedni przycisk, wybierz rodzaj wprowadzanej liczby: Hex (szesnastkowa), Dec (dziesiętna) lub Bin (dwójkowa). Wprowadź liczbę w tej postaci. Aby zmienić postać liczby, wybierz odpowiedni przycisk.

Ćwiczenie 2.3.6 Model OSI i model TCP/IP

Cele

- Opisanie czterech warstw modelu TCP/IP.
- Powiązanie siedmiu warstw modelu OSI z czterema warstwami modelu TCP/IP.
- Określenie głównych protokołów TCP/IP i narzędzi, które działają w poszczególnych warstwach.

Wprowadzenie

To ćwiczenie pomoże w lepszym poznaniu siedmiu warstw modelu OSI. Szczególny nacisk położono na sposób, w jaki są one powiązane z najpopularniejszym istniejącym modelem sieciowym — modelem TCP/IP. Internet opiera się na protokole TCP/IP, który jest standardowym językiem sieci komputerowych. Jednak to siedem warstw modelu OSI jest najczęściej wykorzystywane do opisywania i porównywania oprogramowania i sprzętu sieciowego pochodzącego od różnych producentów. Znajomość obu modeli i umiejętność wzajemnego powiązania warstw tych modeli jest bardzo ważna. Rozumienie modelu TCP/IP oraz protokołów i narzędzi funkcjonujących w każdej warstwie jest bardzo istotne w przypadku rozwiązywania problemów.

Kroki

1. Skorzystaj z poniższych tabel, aby porównać warstwy OSI ze stosem protokołów TCP/IP. W kolumnie drugiej wskaż właściwą nazwę dla każdej z siedmiu warstw modelu OSI odpowiadającą numerowi warstwy. Wypisz numer warstwy TCP/IP i jej prawidłową nazwę w kolejnych dwóch kolumnach. Wypisz także pojęcia określające jednostki enkapsulacji, powiązane z nimi protokoły TCP/IP i narzędzia funkcjonujące w każdej warstwie TCP/IP. Z niektórymi warstwami TCP/IP będzie powiązanych kilka warstw OSI.

Porównanie modelu OSI ze stosem protokołów TCP/IP

Nr warstwy OSI	Nazwa warstwy OSI	Nr warstwy TCP/IP	Nazwa warstwy TCP/IP	Jednostki enkapsul.	Protokoły TCP/IP w każdej warstwie TCP/IP	Narzędzia TCP
7						
6						
5						
4						
3						
2						
1						

Ćwiczenie 2.3.7 Charakterystyka modelu OSI i urządzenia z nim związane

Cele

- Określenie siedmiu kolejnych warstw modelu OSI. Użycie skrótów.
- Opisanie cech, funkcji i słów kluczowych związanych z każdą z warstw.
- Opisanie jednostek pakietów używanych do enkapsulacji poszczególnych warstw.
- Określenie fizycznych urządzeń lub komponentów, które działają w każdej warstwie.

Wprowadzenie

To ćwiczenie pomoże w lepszym poznaniu siedmiu warstw modelu OSI. Szczególny nacisk położono na sposób, w jaki są one powiązane z najpopularniejszym istniejącym modelem sieciowym — modelem TCP/IP. Internet opiera się na protokole TCP/IP, który jest standardowym językiem sieci komputerowych. Jednak to siedem warstw modelu OSI jest najczęściej wykorzystywane do opisywania i porównywania oprogramowania i sprzętu sieciowego pochodzącego od różnych producentów. Znajomość obu modeli i umiejętność wzajemnego powiązania warstw tych modeli jest bardzo ważna. Rozumienie modelu TCP/IP oraz protokołów i narzędzi funkcjonujących w każdej warstwie jest bardzo istotne w przypadku rozwiązywania problemów.

Kroki

1. Wypisz siedem warstw modelu OSI od najwyższej do najniższej. Podaj skrót dla każdej warstwy, który pomoże w jej zapamiętaniu. Następnie wypisz słowa kluczowe i frazy, które opisują cechy i funkcje poszczególnych warstw.

Nr warstwy	Nazwa	Skrót	Słowa kluczowe i opis funkcji
7			
6			
5			
4			
3			
2			
1			

2. Wypisz siedem warstw modelu OSI i jednostki enkapsulacji używane do opisu grup danych w poszczególnych warstwach. Wypisz również nazwy urządzeń sieciowych, które działają w poszczególnych warstwach, jeśli takie są.

Nr warstwy	Nazwa	Jednostka enkapsulacji lub grupa logiczna	Urządzenia lub składniki działające w tej warstwie
7			
6			
5			
4			
3			
2			
1			

Ćwiczenie 3.1.1 Bezpieczna obsługa i użytkowanie multimetru



Cele

- Zapoznanie się ze sposobem właściwego użytkowania i obsługi multimetru.

Wprowadzenie

Multimetr jest uniwersalnym elektrycznym przyrządem pomiarowym służącym do badania poziomu napięć, rezystancji oraz zwarcia lub rozwarcia obwodów. Za jego pomocą można badać zarówno prąd zmienny (AC), jak i stały (DC). Obwody zwarte i rozwarne są wykrywane przez pomiar rezystancji mierzonej w omach. Każdy komputer i urządzenie sieciowe składa się z milionów obwodów i małych układów elektrycznych. Multimetr może być używany do badania problemów elektrycznych występujących w komputerze, urządzeniu sieciowym lub w medium pomiędzy urządzeniami sieciowymi.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć jeden multimetr dla każdej grupy oraz różne baterie do testowania. Praca przebiega w grupach dwuosobowych. Potrzebne będą następujące elementy:

- Multimetr cyfrowy. Urządzenie z serii Fluke 110, 12B lub podobne, po jednym dla każdej grupy.
- Instrukcja obsługi multimetru.
- Bateria do testowania dla każdej grupy. Na przykład bateria o napięciu 9 V, 1,5 V lub bateria do latarki.

Uwaga: Multimetr to delikatne elektroniczne urządzenie pomiarowe. Nie wolno go upuścić ani obchodzić się z nim niedbale. Należy uważać, aby przypadkiem nie naciąć lub nie przeciąć czerwonego i czarnego przewodu, zwanych sondami. Ponieważ istnieje możliwość badania wysokich napięć, należy zachować szczególną ostrożność aby uniknąć porażenia prądem elektrycznym.

Krok 1

Włóż czerwony i czarny przewód do odpowiednich gniazd w mierniku.

a. Czarna sonda powinna być podłączona do gniazda COM, a czerwona do gniazda + (plus).

Krok 2

Włącz multimetr. Naciśnij przycisk lub przełącz w pozycję włączenia.

a. Jaki to model multimetru?

b. Jakie czynności należy wykonać, aby włączyć multimetr?

Krok 3

Ustaw przełącznik na pozycji odpowiadającej pomiarowi. Na przykład pomiar woltów i omów.

a. Ile różnych pozycji przełączenia ma multimetr? _____

b. Jakie to pozycje?

Krok 4

Ustaw przełącznik multimetru na pozycji pomiaru napięcia.

a. Jaki to symbol? _____

Krok 5

Umieść końcówkę czerwonej, dodatniej sondy na dodatnim biegunie baterii. Umieść końcówkę czarnej, ujemnej sondy na drugim biegunie baterii.

a. Czy na multimetrze wyświetlane są jakieś liczby? _____ Jeśli nie, upewnij się, czy jest on przełączony na właściwy typ pomiaru (na przykład Vol, voltage lub V). Jeśli napięcie jest ujemne, zamień miejscami sondy.

Do przemyślenia

1. Wymień jedną czynność, której nie należy robić z multimetrem. _____

2. Wymień jedną istotną funkcję multimetru. _____

3. Jeśli podczas pomiaru napięcia baterii jest ono ujemne, co wykonano niewłaściwie? _____

Ćwiczenie 3.1.2 Pomiar napięcia



Cele

- Demonstracja możliwości bezpiecznego pomiaru napięcia za pomocą multimetru.

Wprowadzenie

Multimetr cyfrowy jest uniwersalnym przyrządem służącym do testowania i rozwiązywania problemów. To ćwiczenie obejmuje zarówno pomiar napięcia stałego (DC), jak i zmiennego (AC). Napięcie stałe i zmienne jest mierzone w voltach, oznaczanych literą V. Napięcie to ciśnienie, z jakim elektrony poruszają się w obwodzie z jednego miejsca na inne. Różnica napięć jest warunkiem koniecznym przepływu elektryczności. Różnica napięć pomiędzy chmurą na niebie a ziemią jest przyczyną powstawania błyskawic.

Uwaga: Podczas dokonywania pomiaru napięcia ważne jest zachowanie ostrożności, aby uniknąć porażenia prądem elektrycznym.

Prąd stały (DC): Napięcie stałe rośnie do określonego poziomu, na którym pozostaje, a prąd płynie w jednym kierunku, dodatnim lub ujemnym. Baterie wytwarzają napięcie stałe, najczęściej o wartościach 1,5 V, 9 V lub 6 V. Typowy akumulator w samochodzie lub ciężarówce to bateria o napięciu 12 V. Gdy „obciążenie” elektryczne, takie jak żarówka lub silnik, zostanie umieszczone pomiędzy biegunem dodatnim (+) a ujemnym (-) baterii, zaczyna płynąć prąd.

Prąd zmienny (AC): Napięcie zmienne rośnie powyżej wartości zerowej, stając się dodatnie, a następnie spada poniżej wartości zerowej, stając się ujemne. Napięcie AC zmienia swój kierunek bardzo szybko. Najbardziej znanym przykładem źródła napięcia AC jest gniazdko sieciowe w domu

lub w pracy. W Europie gniazdka dostarczają około 230 V (do niedawna 220 V) napięcia zmiennego bezpośrednio do podłączonego do nich urządzenia elektrycznego. Przykładem takiego urządzenia jest komputer, toster czy telewizor. Niektóre urządzenia, takie jak małe drukarki i komputery przenośne, są wyposażone w małe czarne pudełko nazywane zasilaczem, które dołącza się do gniazdka 230 V AC. Zasilacze przekształcają napięcie zmienne (AC) na stałe (DC), które może być wykorzystane przez inne urządzenia. Niektóre gniazda AC dostarczają wyższego napięcia trójfazowego, równego 380 V, które jest używane w bardziej energochłonnych urządzeniach, takich jak duże silniki czy spawarki łukowe.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć jeden multimetr dla każdej grupy uczestników oraz rozmaite elementy do testowania napięcia. Praca przebiega w grupach dwuosobowych. Potrzebne będą następujące elementy:

- Multimetr Fluke 110, 12B lub podobny.
- Zestaw baterii: R6 (nazywana też A), R14 (C), R20 (D), 9-woltowa, 4,5-woltowa bateria do latarki.
- Podwójne gniazdko sieciowe, zazwyczaj 230 V.
- Zasilacz do komputera przenośnego lub innego urządzenia elektrycznego.

Następujące elementy są opcjonalne:

- Cytryna z galwanizowanym gwoździem wbitym po jednej stronie i kawałkiem nieizolowanego drutu miedzianego wbitym po przeciwnej stronie.
- Ogniwko słoneczne z podłączonymi przewodami.
- Generator zrobiony własnoręcznie z przewodu owiniętego na ołówku 50 razy i magnesu.

Krok 1 Wybierz odpowiedni zakres napięcia

Metoda wyboru zakresu napięcia będzie się różnić w zależności od typu miernika. Multimetr Fluke 110 ma dwie oddzielne pozycje pomiaru napięcia: nad jedną z nich znajduje się znak fali, oznaczający napięcie zmienne, a nad drugą linie ciągła i przerywana, co oznacza napięcie stałe. W przypadku multimetru Fluke 12B ustaw pokrętkę na pozycji pomiaru napięcia oznaczonej czarnym symbolem V, aby móc dokonywać pomiarów napięcia. Naciśnij przycisk z oznaczeniem VDC i VAC, aby wybrać pomiar napięcia stałego (DC) lub zmiennego (AC).

Pomiary napięcia stałego: Na ekranie zostanie wyświetlony symbol V, oznaczający napięcie, oraz seria kropek i linii w jego górnej części. W zależności od tego, jakie napięcie ma być mierzone, dostępnych jest kilka zakresów. Zakresy zaczynają się od miliwoltów, przez wolty, aż do setek woltów. Miliwolt, który oznacza się skrótem mV, jest równy jednej tysięcznej wolta. Użyj przycisku zakresu (Range), aby zmienić zakres napięcia DC na odpowiedni dla napięcia, które będzie mierzone. Baterie o napięciu poniżej 15 woltów mogą być na ogół dokładnie mierzone na skali VDC i zakresie 0.0. Pomiary napięcia stałego mogą być wykorzystane do określenia, czy baterie są naładowane lub czy zasilacz AC dostarcza napięcia. Zasilacze są często używane do zasilania koncentratorów, modemów, komputerów przenośnych, drukarek i innych urządzeń peryferyjnych. Te zasilacze mogą przetwarzać napięcie zmienne z gniazdka ściennego na niższe napięcia zmienne przeznaczone dla podłączonych urządzeń lub mogą przetwarzać napięcie zmienne na napięcie stałe i zmniejszać jego poziom. Sprawdź z tyłu zasilacza, jakie powinno być napięcie wejściowe (AC) i wyjściowe (AC lub DC).

Pomiary napięcia zmiennego: Na ekranie zostanie wyświetlony symbol V, oznaczający napięcie, a za nim znak fali (~). Oznacza on prąd zmienny. W zależności od tego, jakie napięcie ma być mierzone, dostępnych jest kilka zakresów. Zakresy zaczynają się od miliwoltów, przez wolty, aż do setek woltów. Miliwolt, który oznacza się skrótem mV, jest równy jednej tysięcznej wolta. Użyj przycisku zakresu (Range), aby zmienić zakres napięcia AC na odpowiedni dla napięcia, które będzie mierzone. Napięcie z gniazdka sieciowego 230 V lub wyższe można na ogół dokładnie zmierzyć na skali VAC i zakresie 0.0. Pomiary napięcia AC są przydatne przy określaniu, czy z gniazdka AC dostarczane jest napięcie odpowiednie dla podłączonego sprzętu.

Krok 2

Do wykonania każdego z poniższych pomiarów napięć należy użyć multimetru Fluke 110, 12B lub podobnego. Po zakończeniu pomiaru należy upewnić się, że multimetr został wyłączony.

Element, którego napięcie należy zmierzyć	Ustawienie skali i zakresu	Odczyt napięcia
Baterie: typu R6 (lub mniejsze), R14, R20, 9-woltowa, 4,5-woltowa do latarki		
Podwójne gniazdko sieciowe (zazwyczaj 230 V)		
Zasilacz (przetwarza napięcie AC na niższe AC lub DC) do komputera przenośnego, telefonu komórkowego lub innego elektrycznego urządzenia sieciowego		
(Opcjonalnie) Cytryna z galwanizowanym gwoździem wbitym z jednej strony i kawałkiem nieizolowanego drutu miedzianego wbitym z drugiej strony		

Do przemyślenia

Dlaczego podczas rozwiązywania problemów z siecią istotny jest pomiar napięcia?

Ćwiczenie 3.1.3 Pomiar rezystancji



Cele

- Demonstracja możliwości bezpiecznego pomiaru rezystancji i ciągłości obwodu za pomocą multimetru.

Wprowadzenie

Multimetr cyfrowy jest uniwersalnym przyrządem służącym do testowania i rozwiązywania problemów. To ćwiczenie obejmuje pomiary rezystancji i pomiary pokrewne, zwane pomiarami ciągłości obwodu. Rezystancję mierzy się w omach, oznaczanych grecką literą omega Ω . Przewodniki miedziane, takie jak używane powszechnie w okablowaniu sieciowym, mają zazwyczaj bardzo małą rezystancję lub dobrą ciągłość, gdy bada się je z obu końców. Jeśli w przewodzie jest przerwa, czyli obwód jest „rozarty”, rezystancja jest bardzo wysoka. Powietrze ma praktycznie nieskończoną rezystancję, co oznacza się symbolem nieskończoności ∞

Multimetr ma w środku baterię. Jest ona używana do testowania rezystancji przewodnika lub izolacji przewodu. Gdy do dwóch końców przewodnika przyłożone zostaną sondy, zaczyna płynąć prąd z baterii, a miernik wskazuje napotkaną rezystancję. Jeśli bateria w multimetrze jest słaba lub wyczerpana, należy ją wymienić, gdyż w przeciwnym wypadku multimetr nie będzie mógł dokonywać pomiarów rezystancji.

W tym ćwiczeniu należy przetestować popularne materiały sieciowe, aby zaznajomić się z nimi i z ich rezystancją. Najpierw należy nauczyć się ustawiać pomiar rezystancji w multimetrze. Należy

zwrócić uwagę na funkcję ciągłości podczas pomiaru małych rezystancji. Wraz z multimetrami Fluke 110 i 12B dostarczana jest instrukcja. Inne mierniki działają w podobny sposób.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć jeden multimetr dla każdej grupy oraz różne urządzenia związane z siecią w celu przetestowania ich rezystancji. Praca przebiega w grupach dwuosobowych. Potrzebne będą następujące elementy:

- Multimetr Fluke serii 110 lub 12B (lub podobny).
- Rezystor 1000 omów.
- Rezystor 10 000 omów.
- Ołówek do rysowania grafitowych ścieżek na papierze.
- Wtyczka kategorii 5.
- Odcinek kabla kategorii 5 UTP o długości 0,2 m.
- Kabel koncentryczny zakończony wtyczką BNC.
- Przejściówka z DB9 na RJ-45.
- Zakończony kabel połączeniowy kategorii 5 UTP.

Krok 1 Wybór zakresu rezystancji na multimetrze

Fluke 110:

Pomiar rezystancji: Aby dokonać pomiaru rezystancji, ustaw pokrętko na pozycji oznaczonej symbolem omegi, która oznacza omy (Ω). Użyj przycisku zakresu (Range), aby zmienić zakres rezystancji na odpowiedni dla oczekiwanej rezystancji. Na ekranie zostanie wyświetlony symbol omów (Ω), kiloomów ($K\Omega$ = tysiące omów) lub megaomów ($M\Omega$ = miliony omów).

Pomiar ciągłości obwodu: Ustaw pokrętko na pozycji sygnału dźwiękowego znajdującej się po lewej stronie oznaczenia omów. Symbol sygnału dźwiękowego oznacza ustawienie pomiaru ciągłości obwodu. Gdy rezystancja będzie mniejsza niż 20 omów, słyszalny będzie sygnał dźwiękowy. Sygnał oznacza, że ciągłość obwodu jest prawidłowa. Ustawienie pomiaru ciągłości obwodu jest przydatne wtedy, gdy wymagana jest dobra ścieżka przewodząca, ale nie jest wymagana dokładna znajomość rezystancji.

Fluke 12B:

Pomiar rezystancji: Ustaw pokrętko na pozycji oznaczonej symbolem omegi, która oznacza omy (Ω). Symbol omegi świadczy o ustawieniu pomiaru rezystancji. Wciśnij przycisk oznaczony symbolem omów, aby wybrać tryb pomiaru rezystancji, a nie ciągłości obwodu. Na ekranie nie powinien zostać wyświetlony symbol diody, mały czarny trójkąt wskazujący pionowy pasek. Użyj przycisku zakresu (Range), aby zmienić zakres rezystancji na odpowiedni dla oczekiwanej rezystancji.

Pomiar ciągłości obwodu: Ustaw pokrętko na pozycji oznaczonej symbolem omegi, która oznacza omy (Ω). Symbol omegi świadczy o ustawieniu pomiaru rezystancji. Wciśnij przycisk oznaczony symbolem omów, aby wybrać tryb ciągłości obwodu. Na ekranie powinien zostać wyświetlony symbol diody, mały czarny trójkąt wskazujący pionowy pasek. Dioda to element elektroniczny, który przepuszcza lub blokuje prąd elektryczny. Gdy ciągłość będzie prawidłowa, słyszalny będzie sygnał dźwiękowy. Poprawna ciągłość oznacza niską rezystancję. Ustawienie pomiaru ciągłości obwodu jest potrzebne, gdy wymagana jest dobra ścieżka przewodząca, ale nie jest wymagana dokładna znajomość rezystancji.

Krok 2

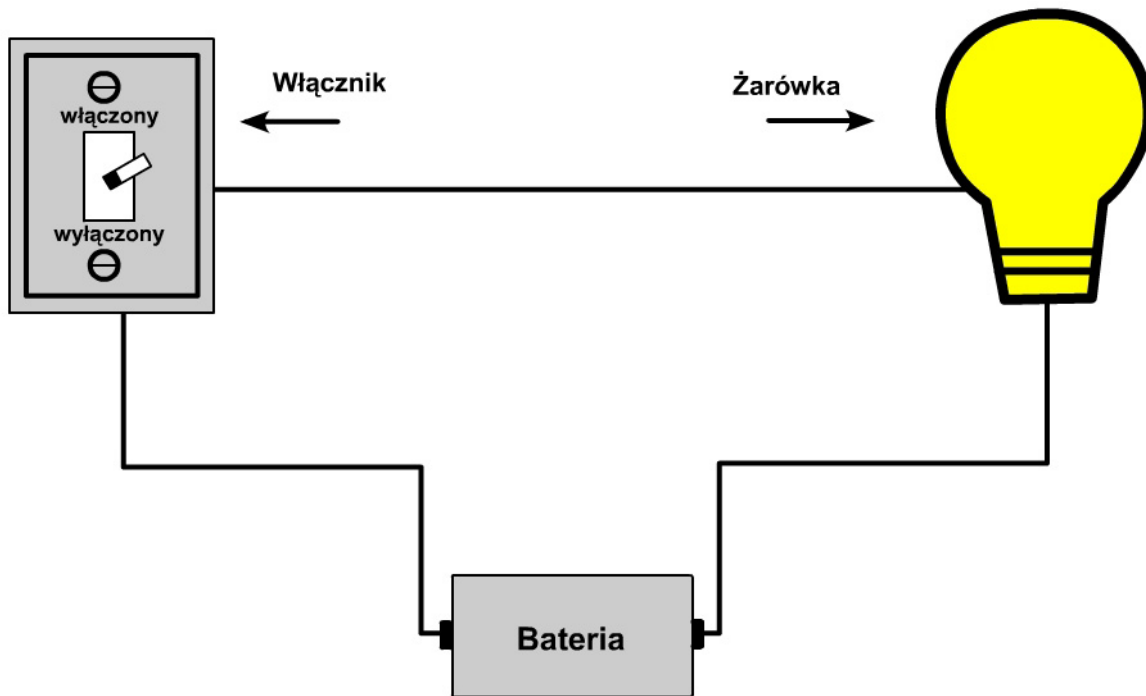
Zmierz rezystancje poniższych elementów. Po zakończeniu pomiarów wyłącz multimetr, gdyż w przeciwnym razie bateria się wyczerpie.

Mierzony element	Ustawienie skali i zakresu	Odczyt rezystancji
Rezystor 1000 Ω		
Rezystor 10 k Ω		
Grafitowa ścieżka narysowana ołówkiem na kawałku papieru		
Wtyczka kategorii 5		
0,2 m kabla kategorii 5 UTP		
Zetknięcie końcówek sondy czerwonej i czarnej		
Ludzkie ciało (dotknij końcówek sond palcami)		
Kabel koncentryczny zakończony wtyczką BNC		
Prześciówka z DB9 na RJ-45		
Zakończony kabel połączeniowy kategorii 5 UTP		

Do przemyślenia

Jaką rolę może spełniać multimetr w konserwacji sieci komputerowej i rozwiązywaniu występujących w niej problemów?

Ćwiczenie 3.1.5 Obwody szeregowe



Cele

- Tworzenie obwodów szeregowych.
- Zapoznanie się z podstawowymi właściwościami obwodów szeregowych.

Wprowadzenie

Jedną z podstawowych koncepcji w elektronice jest obwód. Obwód to ciągła pętla, przez którą płyną elektrony. W technice sieciowej, oprócz rzeczywistych obwodów tworzonych przez medium sieciowe i urządzenia sieciowe, występują również takie pojęcia, jak obwody pętli uziemiających, obwody przełączania pakietów i obwody wirtualne. Jednym z podstawowych obwodów elektrycznych jest obwód szeregowy. Większość urządzeń sieciowych i sieci jest zbudowanych na bazie bardzo skomplikowanych obwodów, których opis znacznie wykracza poza ramy ćwiczeń zawartych w tym kursie. Jednak proces tworzenia niektórych obwodów szeregowych będzie pomocny w zrozumieniu założeń i terminologii sieci komputerowych. To ćwiczenie pomoże także zwiększyć ogólną wiedzę na temat niektórych podstawowych elementów tworzących obwód elektryczny.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć jeden multimetr dla każdej grupy uczestników oraz rozmaite elementy służące do tworzenia obwodów. Praca przebiega w grupach dwuosobowych. Potrzebne będą następujące elementy:

- Multimetr Fluke 110, 12B lub podobny.
- Włącznik światła.
- Kleszcze do cięcia kabli lub kleszcze do ściągania izolacji.

- Drut miedziany.
- Dwie 6-woltowe żarówki z podstawkami lub diody LED z rezystorami.
- Bateria do latarki 6 V.

Krok 1 Pomiar rezystancji wszystkich elementów

Zmierz rezystancję wszystkich urządzeń i komponentów, z wyjątkiem baterii do latarki. Wszystkie rezystancje, z wyjątkiem rezystancji żarówek, powinny być mniejsze niż jeden om (Ω). W przypadku wszystkich elementów, z wyjątkiem baterii, sygnał powinien być ciągły, wskazujący zwarcie lub ścieżkę przewodzącą.

Sprawdź poniższe rezystancje. Po zakończeniu pomiarów wyłącz multimetr, gdyż w przeciwnym razie bateria się wyczerpie.

Element, którego rezystancję należy zmierzyć	Ustawienie skali i zakresu	Odczyt rezystancji
Odcinki przewodów łączących komponenty		
Włącznik światła		
Żarówki		

Krok 2

Pomiar napięcia baterii bez podłączonych elementów, nieobciążonej.

Element, którego napięcie należy zmierzyć	Ustawienie skali i zakresu	Odczyt napięcia
4,5-woltowa bateria do latarki, bez obciążenia		

Krok 3 Tworzenie obwodów szeregowych

Zbuduj obwód szeregowy, dodając za każdym razem jedno urządzenie. Użyj jednej baterii, jednego włącznika, jednej żarówki i przewodów łączących.

Podłącz dodatni biegun baterii do końca jednego z przewodów. Podłącz ujemny biegun do drugiego przewodu. Jeśli włącznik jest włączony, żarówka powinna się świecić.

Odłącz jeden element i zobacz, że obwód został przerwany. Czy żarówka zgasła?

Krok 4 Pomiar napięcia baterii

Zmierz napięcie przyłożone na żarówce, gdy obwód działa.

Włącznik powinien być włączony, a żarówka powinna się świecić.

Czy na żarówce było napięcie, gdy była ona włączona? _____

Krok 5 Dodanie drugiej żarówki

Dodaj drugą żarówkę szeregowo i ponownie zmierz napięcie przyłożone do żarówki.

Czy na żarówce było przyłożone napięcie, gdy była ona włączona? _____

Do przemyślenia

Jaki wpływ mają układy szeregowo na sieć?

Ćwiczenie 3.1.9a Obwody komunikacyjne

Cele

- Zaprojektowanie prostego systemu komunikacyjnego, odznaczającego się szybkością i niezawodnością.
- Zbudowanie systemu przy użyciu ogólnie dostępnych materiałów.
- Przetestowanie systemu.

Wprowadzenie i przygotowanie

Aby w sieci mogła odbywać się niezawodna komunikacja, należy wcześniej rozstrzygnąć takie zagadnienia, jak fizyczna metoda sygnalizacji oraz znaczenie każdego sygnału lub serii sygnałów. Utwórz prostą fizyczną sieć i opracuj podstawowe reguły komunikacji, umożliwiające wysyłanie i odbieranie danych. Będzie to sieć cyfrowa oparta na standardzie ASCII (American Standard Code for Information Interchange). Będzie ona przypominać stare telegrafy wykorzystujące alfabet Morse'a. W takich systemach jedynym sposobem komunikacji na duże odległości było wysyłanie serii kropek i kresek w postaci sygnałów elektrycznych za pośrednictwem przewodów. Mimo iż użyta technologia będzie prostsza niż w systemach rzeczywistych, pojawi się wiele kluczowych zagadnień związanych z przesyłaniem danych pomiędzy komputerami. W tym ćwiczeniu wyjaśnione również zostaną funkcje warstw modelu OSI.

Każda grupa musi zaprojektować, zbudować i przetestować obwód komunikacyjny łączący ją z inną grupą. Celem jest wymiana możliwie największej ilości danych w możliwie najkrótszym czasie i z możliwie małą ilością błędów. Podczas wymiany danych jest zabroniona wszelka komunikacja mówiona, pisana czy pozawerbalna. Jedyna dozwolona komunikacja to komunikacja przewodowa. Zespół musi uzgodnić, jakie połączenia fizyczne i jaka metoda kodowania zostaną użyte. Jeden zespół wyśle wiadomość do drugiego zespołu. Drugi zespół musi zinterpretować treść wiadomości, nie wiedząc wcześniej, jaka wiadomość została przesłana. Podczas projektowania systemu należy pamiętać o modelu OSI.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć jeden multimetr dla każdej grupy uczestników oraz rozmaite elementy służące do zbudowania prostej sieci komunikacyjnej. Praca przebiega w grupach dwu-, maksymalnie czteroosobowych.

Potrzebne będą następujące elementy. Należy zapoznać się z przeznaczeniem każdego elementu, ponieważ pomoże to zaprojektować sieć.

Wymagany element konstrukcyjny sieci	Cel
Multimetr Fluke 110, 12B lub podobny	Do testowania połączeń komunikacyjnych
Kabel kategorii 5 UTP o długości 6 metrów	Do poprowadzenia linii komunikacyjnej. Medium transmisyjne.
Tabela kodu ASCII	Pomaga w kodowaniu i interpretowaniu sygnałów. Jeśli brak jest wydrukowanej tabeli 7-bitowego kodu ASCII, należy poszukać słowa „ASCII chart” w Internecie.
Włącznik światła	Do aktywacji urządzenia sygnalizującego w celu tworzenia cyfrowych sygnałów binarnych włączone/wyłączone
4,5-woltowe żarówki z podstawkami lub diody LED z rezystorami	Działające jako urządzenie sygnalizujące
Bateria 4,5 V do latarki	Do zasilania urządzenia sygnalizującego
Kleszcze do cięcia kabli lub kleszcze do ściągania izolacji	Do dostosowania długości linii komunikacyjnych i przygotowania ich końcówek

Zagadnienia warstwy 1

Połącz dwie pary przewodów w celu umożliwienia komunikacji w obu kierunkach, w półduplesie lub pełnym duplexie.

Zagadnienia warstwy 2

Opracuj sekwencję początku i końca ramki. Jest to sekwencja bitów, która różni się od wysyłanych bitów znaków i liczb.

Zagadnienia warstwy 3

Opracuj schemat adresowania hostów i sieci, jeśli tworzona jest komunikacja bardziej skomplikowana, niż w układzie punkt-punkt.

Zagadnienia warstwy 4

Zastosuj mechanizm kontroli w celu nadzorowania jakości usługi. Na przykład może to być korygowanie błędów, potwierdzanie, okna lub kontrola przepływu.

Zagadnienia warstwy 5

Zaimplementuj mechanizm synchronizacji lub pauz w trakcie długotrwałej wymiany danych.

Zagadnienia warstwy 6

Wybierz sposób przedstawiania danych. Na przykład może to być kod ASCII zakodowany jako bity optyczne.

Zagadnienia warstwy 7

Prześlij wiadomość dostarczoną przez instruktora lub własną.

Do przemyślenia

1. Jakie problemy dotyczące komunikacji pomiędzy komputerami pojawiły się podczas tworzenia systemu komunikacyjnego?

2. Przeanalizuj system komunikacyjny z punktu widzenia warstw OSI.

Ćwiczenie 3.1.9b Proste testowanie kabla za pomocą urządzenia Fluke 620



Cele

- Użycie prostego testera okablowania w celu sprawdzenia, czy kabel prosty lub z przeplotem jest sprawny, czy nie.
- Użycie zaawansowanego testera okablowania Fluke 620 do sprawdzania długości kabla i łączności.

Wprowadzenie

Należy wykorzystać kilka kabli, które zostały uprzednio przygotowane. Korzystając z prostego testera okablowania, trzeba sprawdzić ich ciągłość, występowanie przerw w żyłach oraz zwarcie dwóch lub większej ilości żył. W trakcie następnych ćwiczeń przygotowane zostaną podobne kable.

Proste testery okablowania: Istnieje wiele prostych testerów okablowania, które dostępne są w cenie poniżej 500 zł. Składają się one zazwyczaj z jednego lub dwóch małych pudełek z gniazdami RJ-45. Testowane kable należy podłączyć do gniazd RJ-45. Wiele modeli przeznaczonych jest wyłącznie do testowania kabli UTP sieci Ethernet.

Oba końce kabla należy podłączyć do odpowiednich gniazd. Tester okablowania zbada wszystkie osiem żył i określi, czy kabel jest prawidłowy, czy uszkodzony. Proste testery okablowania mogą mieć wyłącznie pojedynczą lampkę wskazującą, czy kabel jest prawidłowy, czy wadliwy. Inne

przyrządy mogą mieć osiem lampek określających, która żyła jest wadliwa. Przyrządy do testowania kabli mają wewnętrzne baterie służące do badania ciągłości przewodów.

Zaawansowane testery okablowania: Zaawansowane przyrządy do testowania kabli, takie jak Fluke 620 LAN CableMeter®, oprócz podstawowych funkcji testowania kabli wykonują wiele innych zadań. Przyrządy Fluke 620 mogą kosztować od kilkuset do kilku tysięcy dolarów amerykańskich. Zaawansowane przyrządy do testowania kabli będą używane w kolejnych ćwiczeniach do wykonywania mapy połączeń i innych zadań. Fluke 20 LAN CableMeter jest przyrządem do testowania kabli przeznaczonym do sprawdzania połączeń we wszystkich rodzajach kabli spotykanych w sieciach LAN. To wytrzymałe urządzenie może mierzyć długość kabla, sprawdzać występowanie awarii oraz pokazywać odległość do miejsca uszkodzenia. Wykrywane są przerwy w obwodzie, zwarcia, odwrócenie kolejności żył, skrzyżowane żyły i rozdzielenie par. Każde urządzenie 620 LAN CableMeter jest dostarczane z identyfikatorem kabli.

Urządzenie Fluke 620 jest bardziej zaawansowane, ponieważ wykonuje więcej funkcji:

- Wymaga zaledwie jednoosobowej obsługi.
- Testuje wszystkie rodzaje kabli używanych w sieciach LAN - UTP, STP, FTP, koncentryczny.
- Wykrywa wiele problemów z okablowaniem, w tym przerwy w obwodzie, zwarcia, skrzyżowania, odwrócenie kolejności, rozdzielenie par.
- Umożliwia zlokalizowanie problemów z okablowaniem lub połączeniami.
- Mierzy długość kabla.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien dostarczyć każdej grupie podstawowy tester okablowania lub tester firmy Fluke. Dostarczone powinny zostać również uszkodzone kable o różnej długości. Praca przebiega w grupach dwuosobowych. Potrzebne będą następujące elementy:

- Podstawowy tester okablowania.
- Zaawansowany tester okablowania Fluke 620 lub podobne.
- Dwa prawidłowe kable kategorii 5 lub wyższej, jeden kabel z przeplotem i jeden prosty.
- Dwa uszkodzone kable kategorii 5 lub wyższej, jeden z przerwą, a drugi ze zwarcie. Kable powinny różnić się kolorem lub etykietą.

Krok 1 Testowanie kabli

Prosty tester okablowania: Zapoznaj się z instrukcjami producenta. Włóż oba końce testowanego kabla do gniazd, postępując zgodnie z instrukcją.

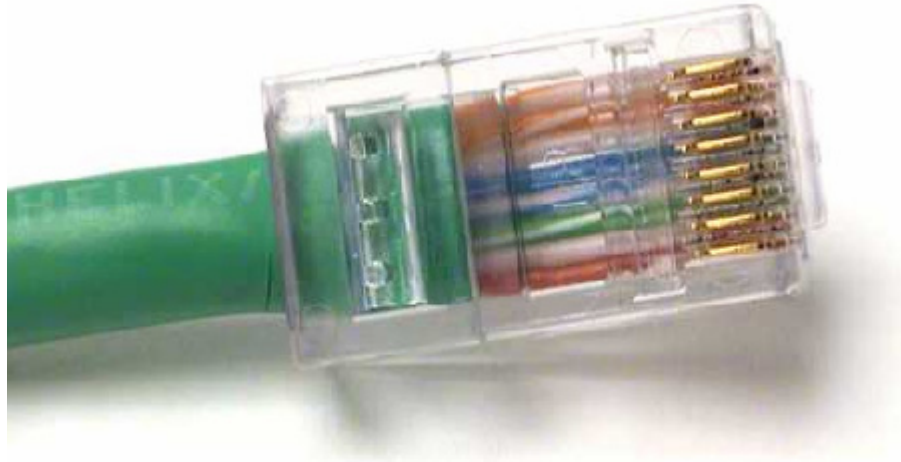
Fluke 620: Włóż wtyczkę RJ-45 z jednego końca kabla do gniazda UTP/FTP w testerze. Ustaw pokrętkę na pozycję „TEST”. Wszystkie żyły zostaną przetestowane w celu sprawdzenia, czy nie są przerwane lub nie mają zwarć.

Uwaga: Ten test nie umożliwi sprawdzenia, czy styki są poprawnie podłączone po obu stronach.

W przypadku każdego testu należy wkładać kabel do gniazd RJ-45 w testerze okablowania. Zapisz wyniki w poniższej tabeli.

	Kolor lub numer kabla	Typ kategorii	Prosty czy z przeplotem?	Długość kabla	Wyniki testu PASS/FAIL
Kabel nr 1					
Kabel nr 2					
Kabel nr 3					
Kabel nr 4					

Ćwiczenie 3.1.9c Budowa kabla prostego



Cele

- Zbudowanie kabla połączeniowego sieci Ethernet ze skrętki nieekranowanej (UTP) kategorii 5 lub 5e (CAT 5 lub 5e).
- Przetestowanie ciągłości kabla i poprawności wyprowadzenia styków.

Wprowadzenie

Zadaniem jest utworzenie składającego się z czterech par (ośmiu żył) kabla prostego, czyli takiego, w którym kolor przewodu na styku 1 po jednym końcu kabla będzie taki sam, jak kolor przewodu na styku 1 na drugim końcu. Styk 2 na jednym końcu będzie taki sam, jak styk 2 na drugim itd. Kabel będzie utworzony na podstawie standardów TIA/EIA T568B lub T568A sieci Ethernet 10BASE-T, które określają kolor przewodu na każdym styku. Standard T568B, zwany również specyfikacją AT&T, jest bardziej popularny w Stanach Zjednoczonych, ale wiele instalacji jest tworzonych na podstawie standardu okablowania T568A, zwanego również standardem ISDN.

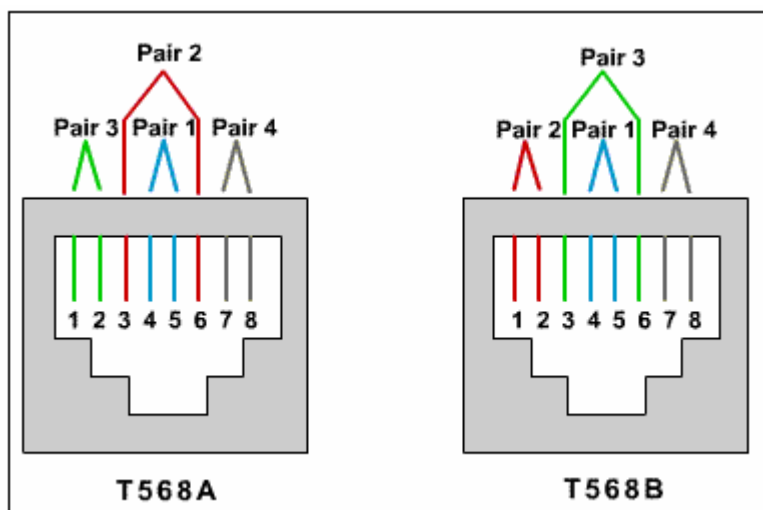
Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien zaopatrzyć się w szpulę skrętki nieekranowanej UTP kategorii 5, złącza RJ-45 (8-stykowe), narzędzie do zaciskania złączy RJ-45 oraz przyrząd do testowania ciągłości kabli Ethernet/RJ-45. Praca odbywa się indywidualnie lub w grupach. Potrzebne będą następujące elementy:

- Odcinek kabla kategorii 5 o długości od 0,6 do 0,9 m na każdą osobę lub zespół.
- Cztery złącza RJ-45, w tym dwa zapasowe.
- Narzędzie do zaciskania złączy RJ-45 na końcach kabla.
- Przyrząd do testowania ciągłości okablowania sieci Ethernet, służący do badania kabli prostych i z przeplotem, T568A lub T568B.
- Kleszcze do cięcia kabli.

Informacje o stykach okablowania w standardzie T568B

Nr styku	Nr pary	Funkcja	Kolor przewodu	Używany w sieci Ethernet 10/100 BASE-T?	Używany w sieci Ethernet 100BASE-T4 i 1000BASE-T?
1	2	Nadawanie	Biało-pomarańczowy	Tak	Tak
2	2	Nadawanie	Pomarańczowy	Tak	Tak
3	3	Odbiór	Biało-zielony	Tak	Tak
4	1	Nie używany	Niebieski	Nie	Tak
5	1	Nie używany	Biało-niebieski	Nie	Tak
6	3	Odbiór	Zielony	Tak	Tak
7	4	Nie używany	Biało-brązowy	Nie	Tak
8	4	Nie używany	Brązowy	Nie	Tak

Diagram showing both T568A and T568B cabling wire colors



Użyj przedstawionej tabeli i rysunku do zbudowania kabla T568B używanego w panelach połączeniowych. Patrząc od strony przewodów, oba końce kabla powinny być podłączone w taki sam sposób.

Krok 1

Określ długość pomiędzy urządzeniami lub urządzeniem i wtyczką. Do tej długości dodaj przynajmniej 30 cm. Maksymalna długość tego typu kabla, zgodnie ze standardami okablowania strukturalnego TIA/EIA, to 3 m, chociaż ta wartość może się zmieniać. Standardowe długości to 1,8 m i 3 m.

Krok 2

Odetnij kawałek linki UTP o żądanej długości. Do utworzenia kabli przyłączeniowych należy używać linki, ponieważ jest ona bardziej wytrzymała na wielokrotne wyginanie. Gdy kable mają zostać zakończone gniazdami, trzeba zastosować kable z litym rdzeniem (drutem).

Krok 3

Zdejmij izolację na długości 5 cm na jednym końcu kabla.

Krok 4

Podczas zdejmowania izolacji trzymaj mocno cztery pary skrętki. Zmień kolejność par kabli tak, aby była zgodna ze standardem okablowania T568B. Należy zwrócić uwagę, aby zachować tyle skręceń, ile jest możliwe, ponieważ zapewniają one tłumienie szumów.

Krok 5

Przytrzymaj izolację i kabel w jednej ręce i odkręć pary zieloną i niebieską na krótkim odcinku. Zmień kolejność par zgodnie ze standardem okablowania T568B. Odkręć i uporządkuj resztę przewodów zgodnie ze schematem kolorów.

Krok 6

Splaszcz, wyprostuj i ułóż przewody. Przytnij je w prostej linii w odległości od 1,25 do 1,9 cm od krawędzi izolacji. Uważaj, aby nie wypuścić izolacji i przewodów, które są teraz właściwie ułożone. Zminimalizuj długość nieskręconych przewodów, ponieważ zbyt długie odcinki znajdujące się w pobliżu złączy są główną przyczyną szumu elektrycznego.

Krok 7

Umieść wtyczkę RJ-45 na jednym końcu kabla, zaczepem skierowanym do dołu i tak, aby pomarańczowa para znalazła się po lewej stronie złącza.

Krok 8

Delikatnie zakładaj wtyczkę na przewody, aż ich miedziane końce będą widoczne na drugim jej końcu. Upewnij się, że koniec izolacji znajduje się wewnątrz wtyczki. Umożliwi to łagodzenie naprężeń i zapewni ułożenie przewodów we właściwej kolejności. Jeśli izolacja nie będzie znajdować się wewnątrz wtyczki, wtyczka nie zostanie właściwie zaciśnięta i w konsekwencji może spowodować problemy. Jeśli wszystko przebiegnie prawidłowo, zaciśnij wtyczkę na tyle mocno, aby styki przebiły izolację na przewodach, tworząc w ten sposób ścieżkę przewodzącą.



Krok 9

Powtórz kroki od 3 do 8, aby zakończyć drugi koniec kabla. Użyj tego samego schematu do zakończenia kabla prostego.

Krok 10

Przetestuj wykonany kabel. Instruktor powinien sprawdzić wykonanie kabla. Na jakiej podstawie można stwierdzić, że kabel działa prawidłowo?

Ćwiczenie 3.1.9d Budowa kabla do konsoli (rollover)

Cele

- Zbudowanie kabla do konsoli (rollover) ze skrętki nieekranowanej (UTP) kategorii 5 lub 5e.
- Przetestowanie ciągłości kabla i poprawności wyprowadzenia styków oraz poprawności doprowadzenia przewodu do właściwego styku.

Wprowadzenie

Będzie to składający się z 4 par przewodów kabel „rollover”. Ten typ kabla ma zazwyczaj długość 3 m, ale może mieć długość do 7,62 m. Kabel tego typu (nazywany kablem rollover lub kablem do konsoli) może być używany do podłączania stacji roboczej lub terminala do portu konsoli znajdującego się z tyłu routera lub przełącznika Cisco. Na obu końcach budowanego kabla znajdować się będą złącza RJ-45. Jeden koniec należy włożyć bezpośrednio do portu zarządzania konsoli RJ-45 z tyłu routera lub przełącznika. Drugi koniec należy włożyć do przejściówki terminala z RJ-45 na DB9. Ta przejściówka zmienia złącze RJ-45 na 9-stykowe złącze żeńskie typu D w celu podłączenia do komputera PC lub portu szeregowego (COM) terminala. Przejściówka terminala DB25 umożliwi również podłączenie do komputera PC lub terminala. Ta przejściówka używa złącza 25-stykowego. Poniższe zdjęcie przedstawia zestaw kabla konsolowego, który jest dostarczany z większością urządzeń Cisco.



Kabel ten nosi nazwę rollover, ponieważ styki na jednym jego końcu są ułożone w odwrotnej kolejności, niż styki na drugim jego końcu, jak gdyby jeden koniec kabla został obrócony. Podczas ostatniego ćwiczenia, gdy tworzony był kabel prosty, umieszczenie drugiego złącza RJ-45 w pozycji odwrotnej spowodowałoby właśnie utworzenie kabla do konsoli (rollover).

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien zaopatrzyć się w szpulę kabla UTP Cat 5 lub Cat 5, złącza RJ-45 (8-stykowe), narzędzie do zaciskania złączy RJ-45 i przyrząd do testowania ciągłości kabli. Praca odbywa się indywidualnie lub w grupach. Potrzebne będą następujące elementy:

- Odcinek kabla kategorii 5 o długości od 3 do 6 m na każdą osobę lub zespół.
- Cztery złącza RJ-45, w tym dwa zapasowe.
- Narzędzie do zaciskania złączy RJ-45 na końcach kabla.
- Przejściówka terminala ze złącza RJ-45 na żeńskie złącze DB9 dostarczana przez firmę Cisco.
- Przyrząd do testowania ciągłości kabli.
- Kleszcze do cięcia kabli.

Krok 1

Użyj poniższej tabeli jako pomocy w przygotowaniu kabla konsolowego.

Router or switch Console port (DTE)	RJ-45 to RJ-45 Rollover Cable (left end)	RJ-45 to RJ-45 Rollover Cable (right end)	RJ-45 to DB9 Adapter	Console Device (PC workstation serial port)
Signal	From RJ-45 Pin No.	To RJ-45 Pin No.	DB9 Pin No.	Signal
RTS	1	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

Opis sygnałów: RTS = żądanie wysłania, DTR = gotowość terminala danych, TxD = dane wysyłane, GND = uziemienie (jedno dla TxD, a drugie dla RxD), RxD = dane odbierane, DSR = gotowość danych, CTS = gotowość do nadawania.

Krok 2

Określ odległość pomiędzy urządzeniami, a następnie dodaj do niej przynajmniej 30 cm. Przygotuj kabel o długości 3 m, chyba że odległość do routera lub przełącznika jest większa. Maksymalna długość kabla tego typu to 8 m.

Krok 3

Zdejmij izolację na długości 5 cm na jednym końcu kabla.

Krok 4

Podczas zdejmowania izolacji trzymaj mocno cztery pary skrętki. Zmień kolejność par kabli i przewodów tak, aby była zgodna ze standardem T568B. Kable mogą być ułożone w dowolnej kolejności, ale należy użyć kolejności standardu T568B, aby się z nim zapoznać.

Krok 5

Splaszcz, wyprostuj i wyrównaj przewody, a następnie przytnij je w prostej linii w odległości od 1,25 do 1,9 cm od krawędzi izolacji. Uważaj, aby nie wypuścić izolacji i przewodów, które są teraz właściwie ułożone.

Krok 6

Umieść wtyczkę RJ-45 na jednym końcu kabla, zaczepem skierowanym do dołu i tak, aby pomarańczowa para znalazła się po lewej stronie złącza.

Krok 7

Delikatnie zakładaj wtyczkę na przewody, aż ich miedziane końce będą widoczne na drugim jej końcu. Upewnij się, że koniec izolacji znajduje się wewnątrz wtyczki i że wszystkie przewody umieszczone są we właściwej kolejności. Jeśli izolacja nie będzie znajdować się wewnątrz wtyczki, wtyczka nie zostanie właściwie zaciśnięta, co może powodować problemy.

Krok 8

Jeśli wszystko przebiegnie prawidłowo, zaciśnij wtyczkę na tyle mocno, aby styki przebiły izolację na przewodach, tworząc w ten sposób ścieżkę przewodzącą.

Krok 9

Powtórz kroki od 2 do 6, aby zakończyć drugi koniec kabla, ale odwracając przy tym kolejność wszystkich przewodów zgodnie z powyższą tabelą. Zamień styk 1 ze stykiem 8, styk 2 ze stykiem 7, styk 3 ze stykiem 6 itd.

a. **Metoda alternatywna** – Ułóż przewody zgodnie ze standardem okablowania T568B. Umieść wtyczkę RJ-45 na jednym końcu kabla, zaczepem skierowanym do góry. Ta metoda pozwoli uzyskać właściwe odwrócenie każdej pary przewodów.

Krok 10

Przetestuj wykonany kabel. Instruktor powinien sprawdzić wykonanie kabla. Na jakiej podstawie można stwierdzić, że kabel działa prawidłowo?

Ćwiczenie 3.1.9e Budowa kabla z przeplotem

Cele

- Zbudowanie kabla z przeplotem sieci Ethernet ze skrętki nieekranowanej (UTP) kategorii 5 lub 5e (CAT 5 lub 5e) zgodnie ze standardami T568B i T568A.
- Przetestowanie ciągłości kabla i poprawności wyprowadzenia styków oraz poprawności doprowadzenia przewodu do właściwego styku.

Wprowadzenie

Będzie to składający się z 4 par przewodów kabel „z przeplotem”. Kabel z przeplotem oznacza kabel, w którym pierwsza i trzecia para na jednym końcu kabla jest odwrócona na drugim jego końcu. Wyjścia styków na jednym końcu kabla będą zgodne ze standardem T568A, a na drugim ze standardem T568B. Wszystkie 8 przewodów (żył) powinny być zakończone złączem modułowym RJ-45.

Ten kabel z przeplotem będzie odpowiadał standardom okablowania strukturalnego. Jeśli kabel z przeplotem jest używany pomiędzy koncentratorami lub przełącznikami, jest uważany za część okablowania „pionowego”. Okablowanie pionowe jest również nazywane okablowaniem strukturalnym. Kabel z przeplotem może być wykorzystywany jako kabel szkieletowy łączący dwa lub więcej koncentratorów lub przełączników w sieci LAN, lub łączący dwie odseparowane stacje robocze w celu utworzenia minisieci LAN. Umożliwi to połączenie dwóch stacji roboczych lub serwera i stacji roboczej bez potrzeby umieszczania pomiędzy nimi koncentratora. Może to być bardzo przydatne do celów szkoleniowych i testowania. Aby połączyć kilka stacji roboczych, potrzebny będzie koncentrator lub przełącznik.

Przed rozpoczęciem ćwiczenia nauczyciel lub asystent powinien zaopatrzyć się w szpulę kabla UTP Cat 5 lub Cat 5e, złącza RJ-45 (8-stykowe), narzędzie do zaciskania złączy RJ-45 oraz przyrząd do testowania ciągłości kabli Ethernet/RJ-45. Praca odbywa się indywidualnie lub w grupach. Potrzebne będą następujące elementy:

- Odcinek kabla kategorii 5 o długości od 0,6 do 0,9 m na każdą osobę lub zespół.
- Cztery złącza RJ-45, w tym dwa zapasowe.
- Narzędzie do zaciskania złączy RJ-45 na końcach kabla.
- Przyrząd do testowania ciągłości okablowania sieci Ethernet, służący do badania kabli z przeplotem w standardzie T568A lub T568B.
- Kleszcze do cięcia kabli.

Krok 1

Zbuduj kabel z przeplotem, korzystając z poniższych tabel i diagramów. Jeden koniec kabla powinien być podłączony zgodnie ze standardem T568A. Drugi koniec kabla powinien być podłączony zgodnie ze standardem T568B. Powoduje to odwrócenie par transmisji i odbioru, pary drugiej i trzeciej, w celu umożliwienia komunikacji.

W sieci 10BASE-T lub 100BASE-TX Ethernet wykorzystywane są tylko cztery przewody.

Okablowanie T568A

Nr styku	Nr pary	Funkcja	Kolor przewodu	Używany w sieci Ethernet 10/100 BASE-T?	Używany w sieci Ethernet 1000BASE-T4 i 1000BASE-T?
1	3	Nadawanie	Biało-zielony	Tak	Tak
2	3	Nadawanie	Zielony	Tak	Tak
3	2	Odbiór	Biało-pomarańczowy	Tak	Tak
4	1	Nie używany	Niebieski	Nie	Tak
5	1	Nieużywany	Biało-niebieski	Nie	Tak
6	2	Odbiór	Pomarańczowy	Tak	Tak
7	4	Nieużywany	Biało-brązowy	Nie	Tak
8	4	Nieużywany	Brązowy	Nie	Tak

Okablowanie T568B

Nr styku	Nr pary	Funkcja	Kolor przewodu	Używany w sieci Ethernet 10/100 BASE-T?	Używany w sieci Ethernet 1000BASE-T4 i 1000BASE-T?
1	2	Nadawanie	Biało-pomarańczowy	Tak	Tak
2	2	Nadawanie	Pomarańczowy	Tak	Tak
3	3	Odbiór	Biało-zielony	Tak	Tak
4	1	Nieużywany	Niebieski	Nie	Tak
5	1	Nieużywany	Biało-niebieski	Nie	Tak
6	3	Odbiór	Zielony	Tak	Tak
7	4	Nieużywany	Biało-brązowy	Nie	Tak
8	4	Nieużywany	Brązowy	Nie	Tak

Krok 2

Określ odległość pomiędzy urządzeniami lub pomiędzy urządzeniem a wtyczką, a następnie dodaj do niej przynajmniej 30 cm. Standardowa długość kabla tego typu to 1,8 m i 3 m.

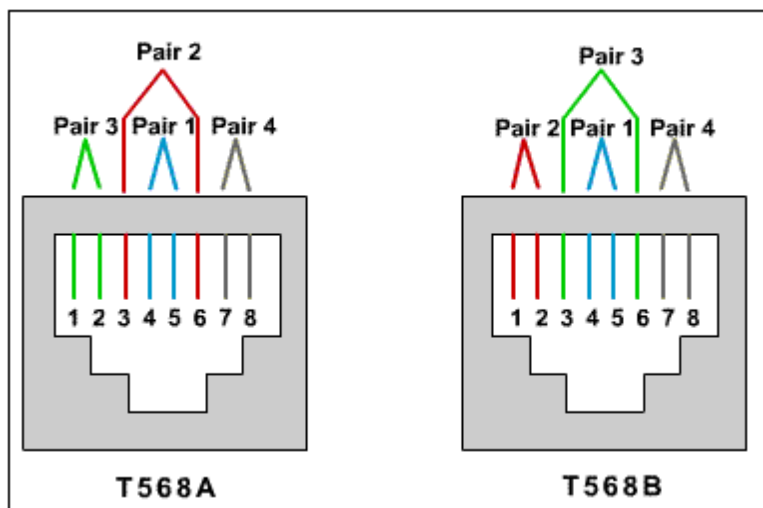
Krok 3

Odetnij kawałek linki UTP o żądanej długości. Do utworzenia kabli przyłączeniowych należy używać linki, ponieważ jest ona bardziej wytrzymała na wielokrotne wyginanie. Gdy kable mają zostać zakończone gniazdami, trzeba zastosować kable z litym rdzeniem (drutem).

Krok 4

Zdejmij izolację na długości 5 cm na jednym końcu kabla.

Diagram showing both T568A and T568B cabling wire colors



Krok 5

Podczas zdejmowania izolacji trzymaj mocno cztery pary skrętki. Zmień kolejność par kabli tak, aby była zgodna ze standardem okablowania **T568B**. Należy zwrócić uwagę, aby zachować skręcenia, ponieważ zapewniają one tłumienie szumów.

Krok 6

Przytrzymaj izolację i kabel w jednej ręce. Rozwiń na krótkim odcinku parę zieloną i niebieską, aby zmienić ich kolejność na zgodną ze schematem kolorów standardu okablowania **T568B**. Odkręć i uporządkuj resztę przewodów zgodnie ze schematem kolorów.

Krok 7

Splaszcz, wyprostuj i ułóż przewody. Przytnij je w prostej linii w odległości od 1,25 do 1,9 cm od krawędzi izolacji. Uważaj, aby nie wypuścić izolacji i przewodów, które są teraz właściwie ułożone. Zminimalizuj długość nieskręconych przewodów, ponieważ zbyt długie odcinki znajdujące się w pobliżu złącza są główną przyczyną szumu elektrycznego.

Krok 8

Umieść wtyczkę RJ-45 na jednym końcu kabla zaczepem do dołu. Na końcu zgodnym ze standardem T568A zielona para powinna się znajdować po lewej stronie złącza. Na końcu zgodnym ze standardem T568B po lewej stronie powinna się znajdować para pomarańczowa.

Krok 9

Delikatnie zakładaj wtyczkę na przewody, aż ich miedziane końce będą widoczne na drugim jej końcu. Upewnij się, że koniec izolacji znajduje się wewnątrz wtyczki i że wszystkie przewody umieszczone są we właściwej kolejności. Jeśli izolacja nie będzie znajdować się wewnątrz wtyczki, wtyczka nie zostanie właściwie zaciśnięta, co może powodować problemy. Jeśli wszystko przebiegnie prawidłowo, zaciśnij wtyczkę na tyle mocno, aby styki przebiły izolację na przewodach, tworząc w ten sposób ścieżkę przewodzącą.

Krok 10

Powtórz kroki od 4 do 8, aby zakończyć drugi koniec kabla, korzystając ze schematu standardu **T568A** do zakończenia kabla z przeplotem.

Krok 11

Przetestuj wykonany kabel. Instruktor powinien sprawdzić wykonanie kabla. Na jakiej podstawie można stwierdzić, że kabel działa prawidłowo?

Ćwiczenie 3.1.9f Zakup kabli UTP

Cele

- Zapoznanie się z różnorodnością cen okablowania sieciowego i komponentów dostępnych na rynku.
- Zebranie informacji o cenach kabli połączeniowych UTP i kabli sprzedawanych luzem.

Wprowadzenie

Zbierz listę cen dla przygotowywanego projektu okablowania. Zbierz informacje o cenach okablowania poziomego (UTP). Jeśli kable UTP nie są używane na danym obszarze, należy zastąpić je kablami ekranowanymi. Elementy obejmują:

- 24 kable połączeniowe UTP kategorii 5 lub wyższej o długości 1 m
- 24 kable połączeniowe UTP kategorii 5 lub wyższej o długości 3 m
- 2 kable połączeniowe UTP kategorii 5 lub wyższej o długości 15 m
- Linka UTP o długości 100 m, której cenę należy porównać z ceną skrętki ekranowanej
- Drut UTP o długości 100 m

Krok 1 Zbieranie informacji o cenach kabli

Należy wykorzystać co najmniej trzy źródła cen. W sieci WWW można sprawdzić adresy <http://www.cdw.com/> i <http://www.google.com/>. Należy przeszukać te strony pod kątem występowania słów **cat 5 jumpers**, **cat 5 patch** oraz **cat 5 bulk**. Na stronie CDW zostaną wyświetlone ceny, natomiast wyszukiwarka Google wyświetli wiele interesujących stron, począwszy od firm kładących okablowanie, aż do instrukcji dotyczących montażu kabli. Należy również skorzystać z katalogów sprzętu sieciowego i materiałów sieciowych.

Krok 2 Utworzenie tabeli z wynikami

Witryna, katalog lub sklep			
24 kable kategorii 5 lub wyższej o			
24 kable kategorii 5 lub wyższej o			
2 kable kategorii 5 lub wyższej o długości			
Linka UTP o długości 100 m			
Linka ekranowana o długości 100 m			
Drut UTP o długości 100 m			

Ćwiczenie 3.2.8 Zakup kabli światłowodowych

Cele

- Zapoznanie się z różnorodnością cen okablowania sieciowego i komponentów dostępnych na rynku.
- Zebranie informacji o cenach światłowodowych kabli połączeniowych i światłowodowych kabli sprzedawanych luzem.

Wprowadzenie

Zbierz listę cen dla przygotowywanego projektu okablowania. Zbierz informacje o cenach okablowania pionowego lub światłowodowego. Użyj światłowodu wielomodowego (MM). Elementy obejmują:

- 24 kable połączeniowe MM o długości 2 m
- 24 kable połączeniowe o długości 5 m
- 2 kable połączeniowe MM o długości 15 m
- Kabel światłowodowy MM o długości 304,8 m

Krok 1 Zbieranie informacji o cenach kabli

Należy wykorzystać co najmniej trzy źródła cen. W sieci WWW można sprawdzić adresy <http://www.cdw.com> i <http://www.google.com>. Należy przeszukać te strony pod kątem występowania słów **optic jumpers**, **fiber optic patch** oraz **fiber optic bulk**. Na stronie CDW zostaną wyświetlone ceny, natomiast wyszukiwarka Google wyświetli wiele interesujących stron, począwszy od firm kładących okablowanie, aż do instrukcji dotyczących montażu kabli. Należy również skorzystać z katalogów sprzętu sieciowego i materiałów sieciowych.

Krok 2 Utworzenie tabeli z wynikami

Witryna, katalog lub sklep			
24 kable połączeniowe MM o długości 2 m			
24 kable połączeniowe o długości 5 m			
2 kable połączeniowe MM o długości 15 m			
Kabel światłowodowy MM o długości 304,8 m			

Ćwiczenie 4.2.9a Tester okablowania Fluke 620 — mapowanie połączeń



Cele

- Zapoznanie się z funkcjami mapowania połączeń dostępnymi w urządzeniu Fluke 620 LAN CableMeter lub jego odpowiedniku.
- Zapoznanie się ze sposobami korzystania z testera okablowania w celu sprawdzenia prawidłowości instalacji skrętki nieekranowanej kategorii 5 zgodnie ze standardami okablowania TIA/EIA-568 dotyczącymi sieci Ethernet.

Wprowadzenie i przygotowanie

Mapy połączeń są często bardzo przydatne przy rozwiązywaniu problemów z kablami UTP. Mapa połączeń umożliwia technikowi instalacji sieciowych sprawdzenie, które styki na jednym końcu kabla są połączone, z którymi stykami na drugim jego końcu.

Przed rozpoczęciem zajęć nauczyciel lub asystent powinien w celu przeprowadzenia testów przygotować kilka prawidłowo połączonych kabli kategorii 5. Należy użyć zarówno kabli z przeplotem, jak i prostych. Trzeba też przygotować kilka kabli kategorii 5, w których występują

usterki, na przykład niedokładnie połączonych i z rozdzielonymi parami. Aby uprościć i usprawnić procedurę testowania, kable należy ponumerować. Demonstrowany tester okablowania powinien umożliwiać przynajmniej testowanie ciągłości i długości kabla oraz kontrolę mapy połączeń. Praca odbywa się indywidualnie lub w grupach. Potrzebne będą następujące zasoby:

- kable proste kategorii 5, w różnych kolorach;
- kabel krosowy kategorii 5 z końcówką T568A na jednym końcu i T568B — na drugim;
- kable proste kategorii 5, w różnych kolorach i o różnej długości, z przerwami w połowie lub zwarciami przewodów na jednym końcu;
- kable proste kategorii 5 z rozdzielonymi parami;
- urządzenie Fluke 620 LAN CableMeter lub podobne — do przetestowania długości kabli i ich ciągłości oraz skontrolowania mapy połączeń.

Krok 1

Obróć pokrętko testera do pozycji WIRE MAP (Mapa połączeń). Naciśnij przycisk **SETUP** (Konfiguracja), aby przejść do trybu konfiguracji, następnie przyjrzyj się wyświetlaczowi testera. Pierwszą opcją powinna być opcja CABLE (Kabel). Naciskaj przyciski ze strzałkami **w górę** lub **w dół**, aż zostanie wybrany odpowiedni rodzaj kabla (w tym przypadku UTP). Wciśnij przycisk **ENTER**, aby potwierdzić wybór, i przejdź do następnej opcji. Postępując się przyciskami ze strzałkami i przyciskiem **ENTER**, wprowadź następującą charakterystykę okablowania:

Opcja testera	Odpowiednie ustawienie — UTP
CABLE:	UTP
WIRING (Połączenie):	10BASE-T lub EIA/TIA 4PR
CATEGORY (Kategoria):	CAT 5
WIRE SIZE (Rozmiar kabla):	AWG 24
CAL to CABLE? (Kalibracja względem kabla?)	NO (Nie)
BEEPING (Sygnał dźwiękowy):	ON (Włączony) lub OFF (Wyłączony)
LCD CONTRAST LCD CONTRAST (Kontrast wyświetlacza):	Od 1 do 10 (najjaśniejszy)

Krok 2

Po dokonaniu ustawień testera należy nacisnąć przycisk SETUP aby wyjść z trybu konfiguracji. Przy testowaniu każdego z kabli skorzystaj z opisanej poniżej procedury. Włóż bliższy koniec kabla do gniazda RJ-45 w testerze oznaczonego UTP/FTP. Na drugi koniec kabla załóż przejściówkę RJ-45-RJ-45 (żeński), a następnie z drugiej strony przejściówki włóż identyfikator kabli. Przejściówka i identyfikator kabli są akcesoriami dołączonymi do urządzenia Fluke 620 LAN CableMeter.



Krok 3

Za pomocą funkcji Wire Map i identyfikatora kabli można sprawdzić połączenia przewodów na obu końcach kabla. Liczby wyświetlane w górnej części wyświetlacza opisują bliższy koniec, a liczby u dołu — dalszy. Opracuj mapy połączeń wszystkich kabli przeznaczonych do testowania. Dla każdego z przetestowanych kabli kategorii 5 wypełnij poniższą tabelę, wpisując wyniki testu. Każdy kabel opisz następującymi informacjami: numer, kolor, rodzaj połączenia (proste lub z przeplotem), wyświetlone na ekranie wyniki testu oraz wykryty problem.

Nr kabla	Kolor kabla	Rodzaj kabla (prosty czy krosowy)	Wyświetlone wyniki testu (Uwaga: Szczegółowy opis wyników wskazań testera Fluke dotyczących mapowania połączeń znajduje się w podręczniku do testera).	Opis problemu
1			Góra: Dół:	
2			Góra: Dół:	
3			Góra: Dół:	
4			Góra: Dół:	
5			Góra: Dół:	

Ćwiczenie 4.2.9b Tester okablowania Fluke 620 — defekty



Cele

- Zapoznanie się z funkcjami testowania kabli (zaliczenie/niezaliczenie testu) dostępnymi w urządzeniu Fluke 620 LAN CableMeter lub jego odpowiedniku.
- Zapoznanie się ze sposobami korzystania z testera okablowania w celu sprawdzenia prawidłowości instalacji skrętki nieekranowanej w sieci Ethernet.
- Opanowanie umiejętności testowania różnych typów kabli w celu stwierdzenia problemów, które mogą wynikać z nieprawidłowego połączenia i zakończenia przewodów.

Wprowadzenie i przygotowanie

Podstawowe testy okablowania są często bardzo przydatne przy rozwiązywaniu problemów z kablami UTP. Zakłada się, że infrastruktura lub system okablowania w budynku ma sprawnie działać przez co najmniej dziesięć lat. Problemy związane z instalacją okablowania są najczęstszymi przyczynami awarii sieci. Niezawodność instalacji zależy przede wszystkim od takich czynników, jak

jakość użytych elementów okablowania, wybór torów przebiegu kabli i sposoby ich zamocowania, a także jakość złączy.

Przed rozpoczęciem zajęć nauczyciel lub instruktor powinien w celu przeprowadzenia testów przygotować kilka prawidłowo połączonych kabli kategorii 5. Należy użyć zarówno kabli z przeplotem, jak i prostych. Trzeba także przygotować kilka kabli kategorii 5, w których wystąpią problemy. Aby uprościć i usprawnić procedurę testowania, kable należy ponumerować. Potrzebne będą następujące zasoby:

- kable proste i z przeplotem kategorii 5 w różnych kolorach: niektóre sprawne, niektóre nie;
- kable proste i z przeplotem kategorii 5 w różnych kolorach i o różnej długości, z przerwami w połowie lub zwarciami przewodów na jednym końcu;
- tester okablowania Fluke 620 LAN CableMeter lub podobny — w celu przetestowania długości kabla.

Krok 1

Obróć pokrętko testera do pozycji **TEST**. Naciśnij przycisk **SETUP** (Konfiguracja), aby przejść do trybu konfiguracji, następnie przyjrzyj się wyświetlaczowi testera. Pierwszą opcją powinna być opcja **CABLE** (Kabel). Naciskaj przyciski ze strzałkami **w górę** lub **w dół**, aż zostanie wybrany odpowiedni rodzaj kabla (w tym przypadku UTP). Naciśnij przycisk **ENTER**, aby potwierdzić wybór, i przejdź do następnej opcji. Posługując się przyciskami ze strzałkami i przyciskiem **ENTER**, wprowadź ustawienia opisane w poniższej tabeli. Kiedy już wszystkie opcje zostaną prawidłowo ustawione, należy nacisnąć **SETUP** aby wyjść z trybu konfiguracji.

Opcja testera	Odpowiednie ustawienie — UTP
CABLE:	UTP
WIRING (Połączenie):	10BASE-T lub EIA/TIA 4PR
CATEGORY (Kategoria):	CAT 5
WIRE SIZE (Rozmiar kabla):	AWG 24
CAL to CABLE? (Kalibracja względem kabla?)	NO (Nie)
BEEPING (Sygnał dźwiękowy):	ON (Włączony) lub OFF (Wyłączony)
LCD CONTRAST (Kontrast wyświetlacza):	Od 1 do 10 (najjaśniejszy)

Krok 2

Przy testowaniu każdego z kabli skorzystaj z opisanej poniżej procedury. Włóż bliższy koniec kabla do gniazda RJ-45 w testerze oznaczonego UTP/FTP. Na drugi koniec kabla załóż przejściówkę RJ-45-RJ-45 (żeński). Następnie z drugiej strony przejściówki włóż identyfikator kabli. Przejściówka i identyfikator kabli są akcesoriami dołączonymi do urządzenia Fluke 620 LAN CableMeter.



Krok 3

Za pomocą funkcji TEST i identyfikatora kabli UTP można określić, czy kabel jest sprawny. Wykonaj test podstawowy wszystkich dostępnych kabli. Dla każdego z przetestowanych kabli kategorii 5 wypełnij poniższą tabelę, wpisując wyniki testu. Każdy kabel opisz następującymi informacjami: numer, kolor, rodzaj (połączenia proste lub z przeplotem albo kabel koncentryczny), wyświetlone na ekranie wyniki testu oraz wykryty problem. Aby wyświetlić informacje o wszystkich parach w przypadku skrętki nieekranowanej (UTP), posłuż się przyciskami ze strzałkami **w dół** lub **w górę**.

Nr kabla	Kolor kabla	Wyniki testu	Problem
1			
2			
3			
4			

Ćwiczenie 4.2.9c Tester okablowania Fluke 620 — długość kabla



Cele

- Zapoznanie się z funkcją pomiaru długości kabla dostępną w urządzeniu Fluke 620 LAN CableMeter lub jego odpowiedniku.
- Zapoznanie się ze sposobami korzystania z testera okablowania w celu sprawdzenia, czy długość kabli w sieci Ethernet jest zgodna z odpowiednimi standardami i czy przewody w kablu mają taką samą długość.

Wprowadzenie i przygotowanie

Testy długości kabli są często bardzo przydatne przy rozwiązywaniu problemów z kablami UTP. Zakłada się, że infrastruktura lub system okablowania w budynku ma sprawnie działać przez co najmniej dziesięć lat. Problemy związane z instalacją okablowania są najczęstszymi przyczynami awarii sieci. Niezawodność instalacji zależy przede wszystkim od takich czynników, jak jakość użytych elementów okablowania, wybór torów przebiegu kabli i sposoby ich zamocowania, a także jakość złączy.

Przed rozpoczęciem zajęć nauczyciel lub instruktor powinien w celu przeprowadzenia testów przygotować kilka prawidłowo połączonych kabli kategorii 5. Należy użyć zarówno kabli z przeplotem, jak i prostych. Aby uprościć i usprawnić procedurę testowania, kable należy ponumerować. Demonstracyjny tester okablowania powinien umożliwiać przynajmniej pomiar długości kabla UTP. Praca odbywa się indywidualnie lub w grupach. Potrzebne będą następujące zasoby:

- kable proste i kable z przeplotem kategorii 5 w różnych kolorach: niektóre sprawne, niektóre nie;
- tester okablowania Fluke 620 LAN CableMeter lub podobny — w celu przetestowania długości kabla.

Krok 1

Obróć pokrętko testera do pozycji LENGTH (Długość). Naciśnij przycisk SETUP (Konfiguracja), aby przejść do trybu konfiguracji, następnie przyjrzyj się wyświetlaczowi testera. Pierwszą opcją powinna być opcja CABLE (Kabel). Naciskaj przyciski ze strzałkami w górę lub w dół, do momentu aż zostanie wybrany odpowiedni rodzaj kabla (w tym przypadku UTP). Naciśnij przycisk ENTER, aby potwierdzić wybór, i przejdź do następnej opcji. Postępując się przyciskami ze strzałkami i przyciskiem ENTER, wprowadź ustawienia opisane w poniższej tabeli. Kiedy już wszystkie opcje zostaną prawidłowo ustawione, należy nacisnąć SETUP aby wyjść z trybu konfiguracji.

Opcja testera	Odpowiednie ustawienie — UTP
CABLE:	UTP
WIRING (Połączenie):	10BASE-T lub EIA/TIA 4PR
CATEGORY (Kategoria):	CAT 5
WIRE SIZE (Rozmiar kabla):	AWG 24
CAL to CABLE? (Kalibracja względem kabla?)	NO (Nie)
BEEPING (Sygnał dźwiękowy):	ON (Włączony) lub OFF (Wyłączony)
LCD CONTRAST (Kontrast wyświetlacza):	Od 1 do 10 (najjaśniejszy)

Krok 2

Przy testowaniu każdego z kabli skorzystaj z opisanej poniżej procedury. Włóż bliższy koniec kabla do gniazda RJ-45 w testerze oznaczonego UTP/FTP. Na drugi koniec kabla załóż przejściówkę RJ-45-RJ-45 (żeński), a następnie z drugiej strony przejściówki włóż identyfikator kabli. Przejściówka i identyfikator kabli są akcesoriami dołączonymi do urządzenia Fluke 620 LAN CableMeter.



Krok 3

Za pomocą funkcji **LENGTH** (długość) i identyfikatora kabli UTP można określić, długość kabla. Wykonaj test podstawowy wszystkich dostępnych kabli. Dla każdego z przetestowanych kabli wypełnij poniższą tabelę, wpisując wyniki testu. Każdy kabel opisz następującymi informacjami: numer, kolor, długość, wyświetlone na ekranie wyniki testu oraz ewentualny wykryty problem. Aby wyświetlić informacje o wszystkich parach w przypadku skrętki nieekranowanej (UTP), posłuż się przyciskami ze strzałkami **w dół** lub **w górę**.

Nr kabla	Kolor kabla	Długość kabla	Wyniki testu	Problem
1				
2				
3				
4				

Ćwiczenie 4.2.9d Fluke LinkRunner — testy sieci LAN

LinkRunner™



Cele

- Zapoznanie się z możliwościami urządzenia Fluke LinkRunner.
- Opanowanie umiejętności sprawdzania, czy przyłączenie kablowe jest aktywne.
- Opanowanie umiejętności określania szybkości danego przyłączenia kablowego oraz zapewnianej przez nie obsługi duplexu i rodzaju usług.
- Opanowanie umiejętności kontrolowania komunikacji w warstwie sieci za pomocą polecenia **ping**.

Wprowadzenie i przygotowanie

Podczas tego ćwiczenia uczestnicy szkolenia będą pracować z przyłączeniami kablowymi Ethernet podłączonymi do urządzeń sieciowych, takich jak koncentratory i przełączniki. Zadaniem jest określenie charakterystyki urządzeń i instalacji okablowania oraz rozpoznanie potencjalnych problemów z siecią. Podczas analizy zostaną wykorzystane niektóre z najważniejszych funkcji urządzenia Fluke LinkRunner, takie jak badanie aktywności przyłączenia i polecenie ping.

Ponieważ sieci działają z coraz większą szybkością i stają się coraz bardziej złożone, okablowanie i urządzenia muszą działać z coraz większą dokładnością i wydajnością. W związku z tym prawie 80% awarii sieci wynika z prostych problemów z okablowaniem i połączeniami. Potrzebne będą następujące zasoby:

- przełącznik i koncentrator Ethernet;
- kilka kabli prostych Ethernet;

- ciąg kablowy od gniazdka ściennego przez panel połączeniowy do przełącznika.

Informacje dotyczące urządzenia Fluke LinkRunner można znaleźć pod podanymi niżej adresami URL. Pierwszy adres odsyła do wirtualnej demonstracji możliwości tego urządzenia, a drugi umożliwia pobranie podręcznika „LinkRunner Quick Reference Guide” w różnych wersjach językowych.

<http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/see+it+live.htm>

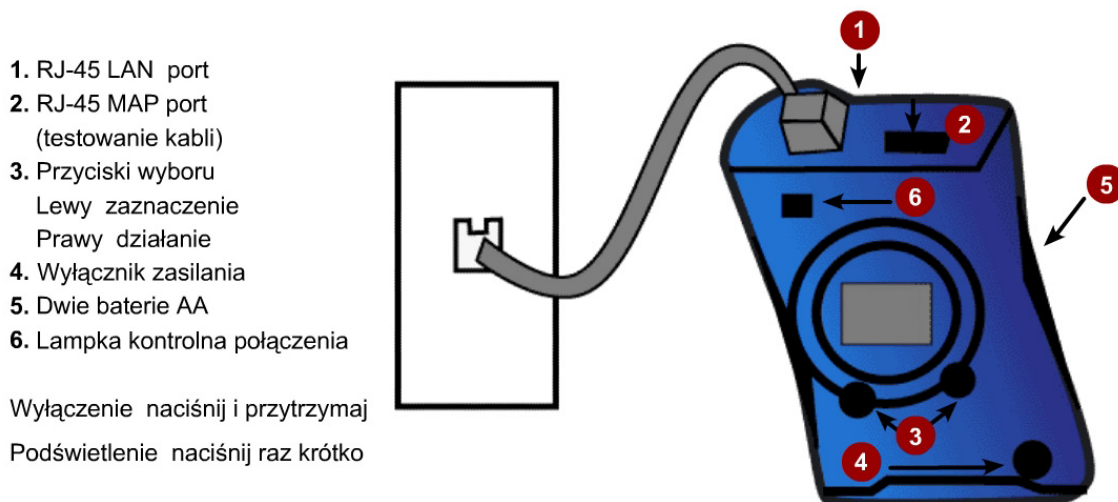
<http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/manuals.htm>

Krok 1 Zapoznanie się z możliwościami urządzenia Fluke LinkRunner

Użyj wirtualnej demonstracji urządzenia LinkRunner znajdującej się pod podanym wyżej adresem. Aby zapoznać się z możliwościami urządzenia, spróbuj wykonać różne testy.

Krok 2 Zapoznanie się z podręcznikiem LinkRunner Quick Reference Guide

Wyświetl podręcznik „Quick Reference Guide” bezpośrednio ze strony WWW lub pobierz go spod podanego wyżej adresu. Instruktor może również dysponować egzemplarzami tego podręcznika. Opis tego ćwiczenia zawiera fragmenty podręcznika „Quick Reference Guide”. Poniższa ilustracja przedstawia złącza i przyciski urządzenia LinkRunner.



Krok 3 Skonfigurowanie urządzenia LinkRunner

- a. Z poziomu dowolnego ekranu wyświetl główne menu konfiguracyjne, naciskając jednocześnie oba przyciski. Możliwa jest zmiana konfiguracji urządzenia LinkRunner lub przejście do polecenia ping.
- b. Po naciśnięciu lewego przycisku zostają wyświetlone ustawienia konfiguracyjne urządzenia LinkRunner, zawierające adres MAC tego urządzenia oraz oferujące możliwość przełączania między wyświetlaniem wskazań w stopach i w metrach.

Jaki jest adres MAC urządzenia? _____

- c. Po naciśnięciu prawego przycisku zostają wyświetlone ustawienia konfiguracyjne polecenia ping.

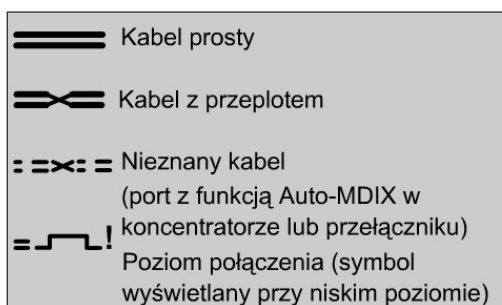
Krok 4 Sprawdzenie aktywnych połączeń stacji roboczych z przełącznikiem

- Urządzenie LinkRunner umożliwia sprawdzenie typu usługi, z którą połączony jest użytkownik: Ethernet, Token Ring czy sieć telefoniczna. W przypadku segmentów Ethernet można określić, czy połączenie jest aktywne, określić jego szybkość, tryb duplexu oraz ustawienia autonegocjacji.
- Ten test umożliwia ustalenie, czy łącze jest aktywne oraz określenie jego szybkości, trybu duplexu i rodzaju usługi (10 lub 10/100 oznacza Ethernet).
- Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
- Odłącz kabel połączeniowy łączący stację roboczą z siecią LAN i podłącz go do portu RJ-45 LAN urządzenia LinkRunner. Test ten nie zakłóca pracy sieci i można go wykonywać w rzeczywistości funkcjonującym środowisku sieciowym. Kabel powinien być podłączony do gniazdka ściennego, które z kolei jest podłączone do przełącznika przez panel połączeniowy w węźle dystrybucji okablowania. Okablowanie powinno być zgodne z obowiązującymi standardami okablowania strukturalnego.
- Odczytaj informacje o połączeniu nr 1 wyświetlane przez urządzenie LinkRunner i zapisz je w poniższej tabeli. Pod tabelą zamieszczono ilustrację pokazującą przykładowy wygląd ekranu, pochodzącą z podręcznika Quick Reference Guide.
- Weź inny kabel połączeniowy dowolnej długości i podłącz jeden koniec bezpośrednio do przełącznika. Drugi koniec tego kabla podłącz do portu LAN urządzenia LinkRunner. W poniższej tabeli zapisz informacje o połączeniu nr 2.

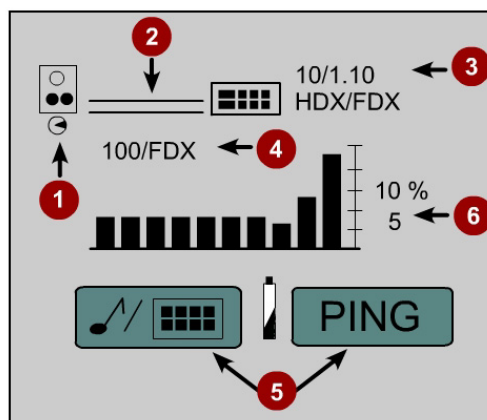
	Połączenie aktywne?	Rodzaj kabla/stan połączenia	Wykrycie autonegocjacji szybkości/trybu duplexu	Faktyczna szybkość połączenia/tryb duplexu	Wykorzystanie sieci
Połączenie nr 1					
Połączenie nr 2					

Czy jest to aktywny port Ethernet?

- Wskaźnik aktywności
- Stan kabla/połączenia:



- Szybkość nominalna/duplex
- Faktyczna szybkość połączenia/duplex
- Przyciski obsługowe (odpowiadają lewemu i prawemu przyciskowi wyboru).
- Wykorzystanie sieci



! Wskaźnik niskiego poziomu baterii (symbol wyświetlany przy niskim poziomie)

- g. Odłącz koniec kabla podłączony do przełącznika i odczytaj informacje na wyświetlaczu. Jaki był wynik?
-

Krok 5 Sprawdzenie bezpośredniego połączenia z koncentratorem

- a. Weź inny kabel połączeniowy dowolnej długości i podłącz jeden koniec bezpośrednio do zwykłego portu koncentratora aktywnego. Drugi koniec tego kabla podłącz do portu LAN urządzenia LinkRunner. Opisz wyniki.
-
- b. Jaka jest różnica między wskazaniem urządzenia w tym przypadku a wskazaniem w przypadku kabla podłączonego do przełącznika?
-
- c. Odłącz zasilanie koncentratora i opisz wskazania urządzenia po wykonaniu tej czynności.
-
- d. Ponownie podłącz koncentrator.
- e. Odłącz kabel od portu zwykłego i podłącz go do portu połączenia nadrzędnego (uplink) w koncentratorze. Upewnij się, że połączenie nadrzędne nie jest aktywne: przycisk nie powinien być wciśnięty. Opisz wyniki.
-
- f. Uaktywnij port połączenia nadrzędnego (uplink), wciskając przycisk. Jak zmieniły się wyświetlane wskazania dotyczące przewodów?
-
- g. Dlaczego tak się stało?
-

Krok 6 Zastosowanie funkcji DHCP Ping w celu sprawdzenia komunikacji w warstwie sieci

Jeśli port LAN zostanie podłączony do środowiska sieciowego DHCP, urządzenie LinkRunner będzie zachowywało się jak klient DHCP. Uzyska adres IP i sprawdzi połączenie z najważniejszymi urządzeniami, wysyłając pakiety ping do domyślnej bramy lub routera oraz do serwera DNS. Poniżej znajduje się ilustracja ukazująca przykładowe wskazania, które mogą pojawić się na wyświetlaczu.

- a. Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
- b. Weź kabel połączeniowy dowolnej długości i podłącz jeden koniec bezpośrednio do przełącznika w sieci LAN, w której dostępny jest serwer DHCP. Drugi koniec tego kabla podłącz do portu LAN urządzenia LinkRunner.
- c. Urządzenie LinkRunner musi być w trybie DHCP, aby wykonać ten test. Naciśnij prawy klawisz (Ping) by zobaczyć czy wyświetlany jest symbol lupy. Jeśli nie, naciśnij dwukrotnie lewy przycisk i zaznacz pole przy opcji DHCP. Zaczekaj, aż urządzenie LinkRunner otrzyma adres IP od serwera DHCP i naciśnij prawy przycisk, który umożliwia skorzystanie z polecenia ping.
- d. Jaki adres IP otrzymało urządzenie LinkRunner? _____
- e. Naciśnij lewy przycisk (lupa). Zostaną wyświetlone szczegółowe informacje o poleceniu ping.
- f. Jaki jest adres IP domyślnej bramy lub routera?
- g. Jaki jest czas wędrówki pakietu ping do routera domyślnego i z powrotem?
-
- h. Jaki jest adres IP serwera DNS?

- i. Jaki jest czas wędrówki pakietu ping do serwera DNS i z powrotem?

- j. Jeśli jeden z czasów odpowiedzi jest dłuższy, dlaczego tak się dzieje?

Uwaga: Jeśli LinkRunner nie otrzymał adresu IP, sprawdź czy opcja DHCP jest zaznaczona oraz czy w sieci dostępny jest aktywny serwer DHCP.

Czy można wykonać polecenie ping?

- Aby wykonać polecenie **ping** w środowisku protokołu DHCP, naciśnij przycisk Urządzenie LinkRunner wyśle pakiet ping zgodnie z poniższymi oznaczeniami:

do routera domyślnego

do serwera DNS

do urządzenia określonego przez użytkownika (ostatnio wybranego)

Krok 7 Wysłanie pakietu ping na adres IP określony przez użytkownika

Urządzenie LinkRunner może wysyłać pakiety ping na dowolny z czterech określanych przez użytkownika adresów IP. Poniższa ilustracja pokazuje przykładowe wskazania wyświetlacza podczas edycji adresu IP dla komputera 1. W tym teście przyjęto założenie, że urządzenie LinkRunner jako klient DHCP otrzymało w poprzednim kroku odpowiedni adres IP, maskę podsieci i adres bramy domyślnej. Jeśli nie, zapoznaj się z uwagą zamieszczoną poniżej w podpunkcie j.

- a. Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
- b. Odłącz od urządzenia wszystkie kable.
- c. Naciśnij prawy przycisk (klucz), aby uzyskać dostęp do opcji konfiguracyjnych.
- d. Ponownie naciśnij prawy przycisk (ping i klucz). Pracując w sieci z serwerem DHCP, wyłącz klienta DHCP w urządzeniu LinkRunner, usuwając znacznik wyboru z pola wyboru DHCP. Aby usunąć zaznaczenie, naciśnij prawy przycisk (znacznik wyboru).
- e. Naciśnij lewy przycisk (strzałka w dół), aby przejść do ikony komputera. Następnie naciśnij prawy przycisk (komputer, IP i klucz), aby uruchomić funkcję konfigurowania adresu IP.
- f. Naciskaj prawy przycisk (strzałka w dół i komputer), aby wybrać jeden z czterech docelowych adresów IP. Zero oznacza, że nie zostanie wykonane polecenie ping. Wybierz docelowy adres IP numer 1.
- g. Naciśnij lewy przycisk (strzałka w dół), aby uzyskać dostęp do ustawienia adresu IP, a następnie prawy (IP x.x.x.x) — aby rozpocząć konfigurowanie adresu IP komputera docelowego numer 1. Patrz ilustracja poniżej.
- h. Dowiedz się, jaki jest adres IP sąsiedniej stacji roboczej lub serwera laboratoryjnego i zapisz go tutaj. _____
- i. Naciskaj lewy przycisk (strzałka w prawo), aby przejść kursorem do kolejnej liczby w adresie IP. Naciskaj prawy przycisk (IP i strzałka w górę), aby zmienić liczbę. Należy podać wszystkie 12 cyfr (w systemie dziesiętnym), również zera. Wpisując pierwszą cyfrę dowolnego z czterech

oktetów, naciśnij przycisk ze strzałką w górę cztery lub pięć razy. Jaka jest największa cyfra, którą można wprowadzić na pierwszej pozycji w okciecie w urządzeniu LinkRunner?

-
- j. Po zakończeniu wprowadzania cyfr obok, na lewym przycisku, zostanie wyświetlona strzałka w dół. Naciskaj lewy przycisk, aż zostanie wyświetlona litera X (wyjście — eXit), a następnie naciśnij prawy przycisk (X). Aby zakończyć działanie funkcji konfigurowania, naciskaj lewy przycisk (strzałka w dół), aż zostanie wyświetlona litera X, a następnie ponownie naciśnij prawy przycisk.

Uwaga: Jeśli w kroku 6 urządzenie LinkRunner nie otrzymało od serwera DHCP poprawnego adresu IP ani maski podsieci, należy je teraz skonfigurować. Podczas konfigurowania zamiast ikony komputera wybierz ikonę urządzenia LinkRunner i wykonaj opisane powyżej czynności, tym razem w celu skonfigurowania adresu IP i maski podsieci urządzenia. Na tym etapie należy także określić adres IP bramy domyślnej dla urządzenia LinkRunner.

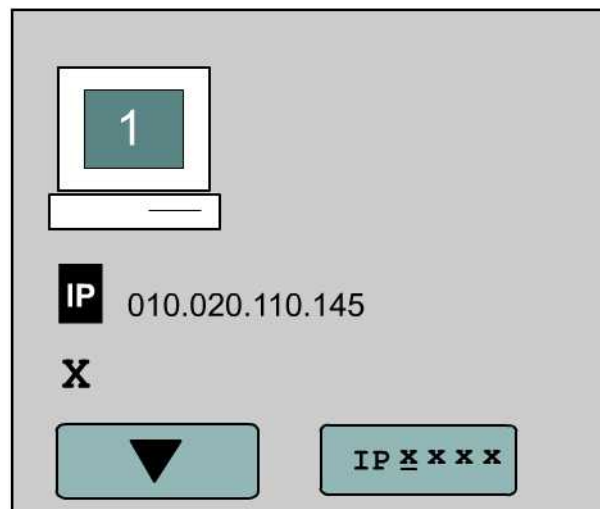
- k. Po skonfigurowaniu adresu IP, na który mają zostać wysłane pakiety ping, podłącz kabel do portu LAN urządzenia LinkRunner i do gniazdka ściennego, koncentratora lub przełącznika sieci, w której mają zostać wysłane pakiety ping. Jakie są wskazania wyświetlacza?

-
- l. Aby uruchomić funkcję ping, naciśnij prawy przycisk (ping). Na wyświetlaczu powinna pojawić się ikona docelowej stacji roboczej numer 1. Czy linia wyświetlana dla tej stacji roboczej jest ciągła, czy też przerywana? _____

Co to oznacza?

-
- m. Naciśnij lewy przycisk (lupa), aby wyświetlić adresy IP wszystkich urządzeń, do których wysyłane są pakiety ping, oraz podany w milisekundach czas wędrówki pakietów w obie strony.
- n. Które urządzenia zostały odpytane i jakie były czasy wędrówki pakietów w przypadku każdego z nich?

-
- o. Aby zakończyć wyświetlanie widoku szczegółowego i korzystanie z funkcji ping, dwukrotnie naciśnij prawy przycisk (X).



Krok 8 Rozłączenie sprzętu oraz schowanie kabli i urządzeń

Ćwiczenie 4.2.9e Urządzenie Fluke LinkRunner — testy okablowania i kart sieciowych

LinkRunner™



Cele

- Zapoznanie się z możliwościami urządzenia Fluke LinkRunner.
- Opanowanie umiejętności sprawdzania długości i integralności kabli.
- Opanowanie umiejętności znajdowania zakończeń kabli.
- Opanowanie umiejętności kontroli działania kart sieciowych w komputerach PC.

Wprowadzenie i przygotowanie

W tym ćwiczeniu uczestnicy szkolenia będą pracować z kablami Ethernet, określając ich charakterystykę i znajdując potencjalne problemy. Zajęcia będą wymagały wykorzystania niektórych najważniejszych funkcji urządzenia Fluke LinkRunner, takich jak mapowanie połączeń i testowanie kart sieciowych.

Ponieważ sieci działają z coraz większą szybkością i stają się coraz bardziej złożone, okablowanie i urządzenia muszą działać z coraz większą dokładnością i wydajnością. W związku z tym prawie 80% awarii sieci wynika z prostych problemów z okablowaniem i połączeniami. Potrzebne będą następujące zasoby:

- kable proste Ethernet: niektóre sprawne, inne — nie;
- kable z przeplotem Ethernet;
- kabel Ethernet od gniazdka ściennego RJ-45 do panelu połączeniowego;

- koncentrator i/lub przełącznik Ethernet;
- komputer z kartą sieciową.

Informacje dotyczące urządzenia Fluke LinkRunner można znaleźć pod podanymi niżej adresami URL. Pierwszy adres odsyła do wirtualnej demonstracji możliwości tego urządzenia, a drugi umożliwia pobranie podręcznika „LinkRunner Quick Reference Guide” w różnych wersjach językowych.

http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_see+it+live.htm

http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_manuals.htm

Krok 1 Zapoznanie się z możliwościami urządzenia Fluke LinkRunner

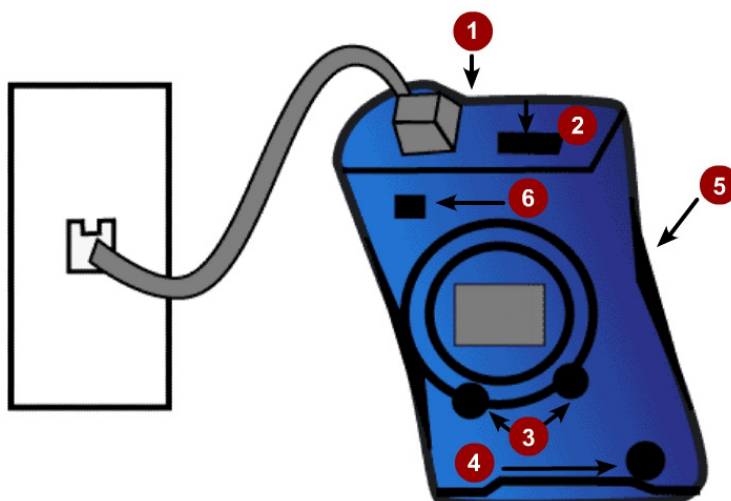
Użyj wirtualnej demonstracji urządzenia LinkRunner znajdującej się pod podanym wyżej adresem. Aby zapoznać się z możliwościami urządzenia, spróbuj wykonać różne testy.

Krok 2 Zapoznanie się z podręcznikiem LinkRunner Quick Reference Guide

Podręcznik Quick Reference Guide można wyświetlić bezpośrednio ze strony WWW lub pobrać spod podanego wyżej adresu. Instruktor może również dysponować egzemplarzami tego podręcznika. Opis tego ćwiczenia zawiera fragmenty podręcznika „Quick Reference Guide”. Poniższa ilustracja przedstawia złącza i przyciski urządzenia LinkRunner.

1. RJ-45 LAN port
2. RJ-45 MAP port (testowanie kabli)
3. Przyciski wyboru
Lewy zaznaczenie
Prawy działanie
4. Wyłącznik zasilania
5. Dwie baterie AA
6. Lampka kontrolna połączenia

Wyłączenie naciśnij i przytrzymaj
Podświetlenie naciśnij raz krótko



Krok 3 Skonfigurowanie urządzenia LinkRunner

- a. Główne menu konfiguracyjne można wyświetlić z poziomu dowolnego ekranu, naciskając jednocześnie oba przyciski. Można teraz zmienić konfigurację urządzenia LinkRunner lub przejść do polecenia ping.
- b. Po naciśnięciu lewego przycisku zostają wyświetlone ustawienia konfiguracyjne urządzenia LinkRunner, zawierające adres MAC tego urządzenia oraz oferujące możliwość przełączania między wyświetlaniem wskazań w stopach i w metrach.

Jaki jest adres MAC urządzenia?

- c. Po naciśnięciu prawego przycisku zostają wyświetlone ustawienia konfiguracyjne polecenia ping, które zostały opisane w poprzednim ćwiczeniu.

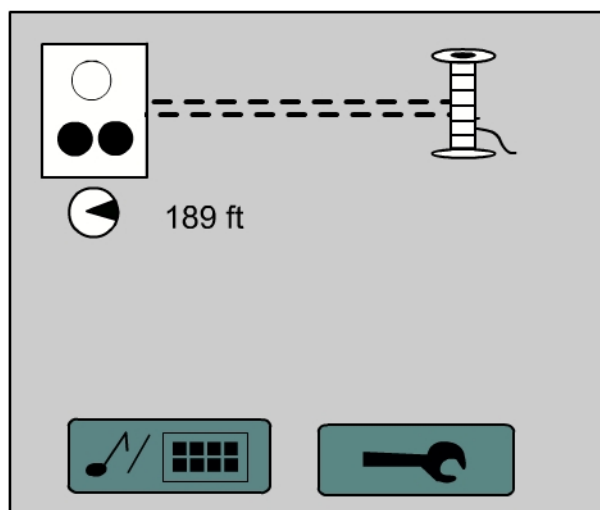
Krok 4 Testowanie długości i ciągłości długiego ciągu kablowego

Funkcja testowania okablowania urządzenia LinkRunner pomaga stwierdzić, czy długość kabla odpowiada specyfikacjom. Jest to podstawowy test stosowany w przypadku długich kabli. Umożliwia on określenie, czy wszystkie cztery pary przewodów są w dobrym stanie i czy mają tę samą długość. Na ilustracji poniżej przedstawiono pomyślny wynik testowania kabla.

Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu. Jakie są wskazania wyświetlacza?

- a. Użyj długiego kabla prostego, który na drugim końcu nie jest podłączony do panelu połączeniowego, koncentratora ani przełącznika. Włóż jeden koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego jako LAN. Jakie są wskazania wyświetlacza?

- b. Jaka jest długość testowanego kabla? _____



Krok 5 Testowanie długości i mapowanie połączeń w kablach połączeniowych

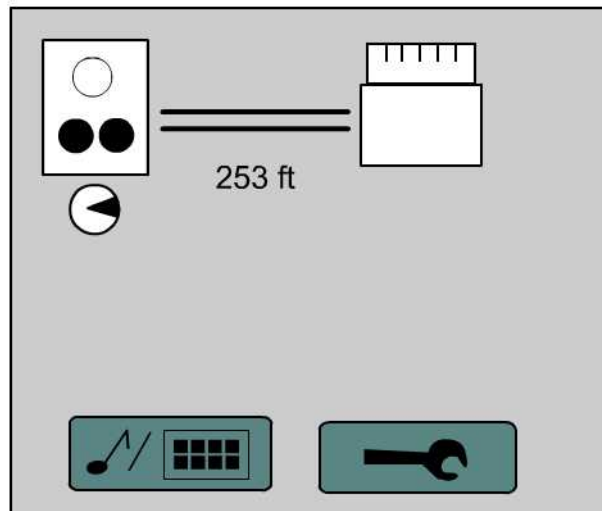
Funkcja testowania okablowania pomaga stwierdzić, czy długość kabla jest zgodna ze specyfikacją, czy jest to kabel z przeplotem czy prosty, a także — czy nie jest uszkodzony. Testy te są skuteczne zarówno w przypadku kabli strukturalnych, jak i połączeniowych. Podczas testu integralność kabla jest sprawdzana pod względem nadmiernej długości oraz rozwarcia, zwarcia, skrzyżowania i rozdzielania par.

- a. Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
- b. Użyj sprawnego prostego kabla połączeniowego Ethernet. Włóż jeden koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego LAN, a drugi — do gniazda RJ-45 oznaczonego jako MAP. Na ilustracji poniżej przedstawiono wskazanie po przetestowaniu sprawnego kabla prostego. Jaka jest długość kabla? _____

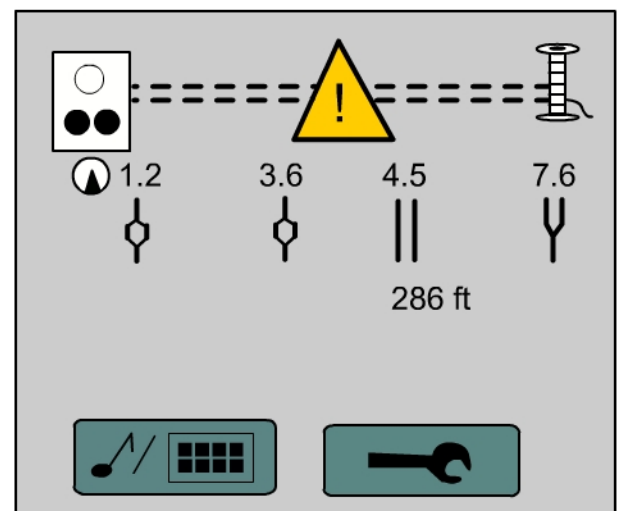
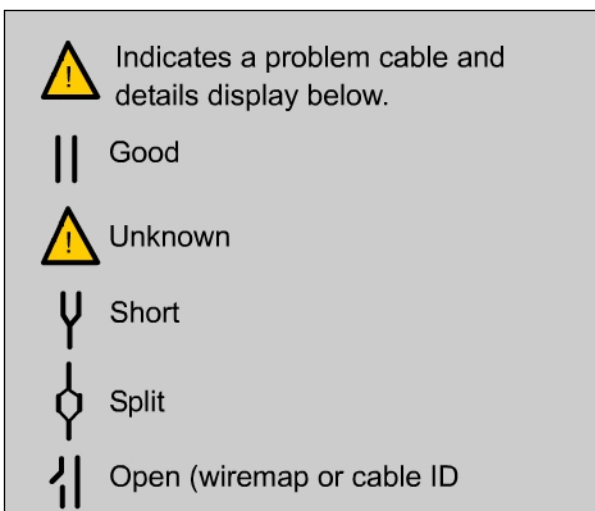
Wyjaśnij, jak odróżnić kabel prosty od kabla z przeplotem. _____

- c. Użyj sprawnego kabla z przeplotem. Włóż jeden koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego LAN, a drugi — do gniazda RJ-45 oznaczonego jako MAP. Jaka jest długość kabla? _____

Wyjaśnij, jak odróżnić kabel prosty od kabla z przeplotem. _____



- d. Użyj kabla prostego z nieprawidłowo połączonymi lub uszkodzonymi przewodami. Włóż jeden koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego LAN, a drugi — do gniazda RJ-45 oznaczonego jako MAP. Na ilustracji poniżej zamieszczono symbole oznaczające różne rodzaje problemów z kablem, które mogą wystąpić. Na czym polegał problem?



Krok 6 Testowanie długości i mapowanie połączeń długiego ciągu kablowego

- Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
- Zastosuj sprawny kabel połączeniowy podłączony do gniazdka ściennego, które jest połączone z panelem połączeniowym, ale nie z koncentratorem ani przełącznikiem. Włóż wolny koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego jako LAN. Do odpowiedniego portu na panelu połączeniowym podłącz przejściówkę do mapowania połączeń. Umożliwi to przetestowanie ciągu kablowego od końcówki kabla połączeniowego w pomieszczeniu przez całe okablowanie poziome aż do panelu połączeniowego w węźle dystrybucji okablowania.
- Jaka jest długość kabla? _____
- Czy test kabla przebiegł pomyślnie? _____
- Jeśli nie, opisz napotkane problemy.

Krok 7 Zastosowanie sygnału Link Pulse do testowania połączenia z koncentratorem/przełącznikiem oraz określania lokalizacji kabla

Sygnał Link Pulse powoduje miganie lampki kontrolnej połączenia przy porcie w koncentratorze lub przełączniku oraz jednocześnie przesłanie przez przewód sygnału dźwiękowego ułatwiającego odnalezienie kabla. Aby odebrać ten dźwięk i dzięki temu znaleźć kabel „na słuch”, należy użyć opcjonalnego urządzenia Microprobe Tone Receiver. Do identyfikowania nieoznaczonych segmentów kabla można użyć opcjonalnego zestawu identyfikatora kabli.

- a. Zastosuj sprawny kabel połączeniowy dowolnej długości. Podłącz jeden jego koniec bezpośrednio do zwykłego portu przełącznika lub koncentratora aktywnego. Drugi koniec tego kabla podłącz do portu LAN urządzenia LinkRunner.
-

- b. Naciśnij lewy przycisk (nuta i symbol koncentratora). Jak zachowuje się lampka kontrolna połączenia w koncentratorze lub przełączniku?
-

- c. Na czym polega ten test i w jaki sposób można by go wykorzystać do identyfikacji kabli i ich zakończeń?
-

Krok 8 Sprawdzenie działania karty sieciowej

- a. Włącz urządzenie LinkRunner, naciskając mały przycisk w prawym dolnym rogu.
 - b. Włóż jeden koniec kabla do gniazda RJ-45 urządzenia LinkRunner oznaczonego LAN, a drugi — do karty sieciowej komputera PC. Jeśli lampka kontrolna połączenia na karcie zacznie świecić, oznacza to, że karta jest sprawna. Czy test karty przebiegł pomyślnie?
-

Krok 9 Rozłączenie sprzętu oraz schowanie kabli i urządzeń

Ćwiczenie 5.1.5 Zaciskanie przewodów w gnieździe RJ-45

Cele

- Opanowanie prawidłowego sposobu zaciskania przewodów w gnieździe RJ-45.
- Opanowanie prawidłowej procedury umieszczania gniazda w gniazdku ściennym.

Wprowadzenie i przygotowanie

Na tych zajęciach uczestnicy mogą się nauczyć, jak za pomocą wciskarki przygotować gniazdo RJ-45 do instalacji w gniazdku ściennym. Umiejętności te są przydatne w przypadku instalowania niewielkiej liczby kabli w biurze lub w mieszkaniu. Wciskarka (nazywana też narzędziem uderzeniowym) jest wyposażona w mechanizm sprężynowy, który umożliwia wciśnięcie przewodów między metalowe styki przy jednoczesnym ściągnięciu izolacji z przewodów. Pozwala to na uzyskanie dobrego połączenia elektrycznego między przewodami a stykami w gnieździe. Wciskarka obcina także zbyt długie odcinki przewodów.

Używane będą kable kategorii 5 lub kategorii 5e oraz gniazda T568B kategorii 5 lub 5e. Gniazda takie służą zwykle do przyłączenia komputera PC do sieci. W tym celu stosowane są przeważnie połączeniowe kable proste kategorii 5 lub 5e ze złączami RJ-45. W przypadku sieci Fast Ethernet (100 Mb/s) i Gigabit Ethernet (1000 Mb/s) istotne jest zastosowanie gniazd kategorii 5 lub 5e i paneli połączeniowych z okablowaniem kategorii 5 lub 5e. Wciskanie przewodów do gniazda umieszczanego przy komputerze (np. w biurze) przebiega tak samo jak w panelu połączeniowym w węźle dystrybucji okablowania. Potrzebne będą następujące elementy:

- kabel kategorii 5 lub 5e o długości 60–90 cm: jeden na osobę lub jeden na zespół;
- dwa gniazda RJ-45 kategorii 5/5e (oraz jedno zapasowe); jeśli po obu stronach kabla zostaną zainstalowane złącza RJ-45, instalację można przetestować przy użyciu kabla ze złączem RJ-45 i zwykłego testera ciągłości połączeń kablowych;
- gniazdko ścienne kategorii 5 lub 5e;
- wciskarka typu 110;
- kleszcze do cięcia kabli.

Poniżej zamieszczono procedurę i diagram, z których należy skorzystać, aby wcisnąć przewody do gniazda RJ-45 i zainstalować to gniazdo w gniazdku ściennym.

Krok 1

Zdejmij izolację z końcówki kabla na odcinku około 2,5 cm.

Krok 2

Umieść przewody we właściwych kanałach w gnieździe. Staraj się zachować skręcenie przewodów maksymalnie blisko gniazda. Sposób rozmieszczenia przewodów w gnieździe jednego typu przedstawiono na diagramie poniżej. W przypadku większości gniazd kanały są oznaczone kolorami wskazującymi, gdzie należy umieścić który przewód. Fotografia znajdująca się na następnej stronie przedstawia jeden z rodzajów gniazd. Gniazda są zwykle oznaczone jako T568A lub B, co można zaobserwować na fotografii.

Krok 3

Przy użyciu pokazanej poniżej wciskarki typu 110 wciśnij przewody do kanałów. Upewnij się, że tnąca strona wciskarki jest skierowana na zewnątrz gniazda. Jeśli tak nie jest, zostanie ucięty wciskany przewód. Wychylenie uchwytu wciskarki nieco na zewnątrz może spowodować, że będzie ona lepiej cięła. Jeśli w wyniku użycia wciskarki nie wszystkie przewody zostaną odcięte, należy po prostu lekko pokręcić końcówkami i delikatnie je oderwać. Kolejną czynnością jest zatrzasknięcie klipsów gniazda i ściśnięcie ich. Między końcem izolacji kabla i kanałami w gnieździe nie powinno znajdować się więcej niż 13 mm nieskręconego przewodu.

Krok 4

Umieść gniazdo w obudowie, wciskając je od tyłu. Gdy to zrobisz, upewnij się, że gniazdo jest skierowane właściwą stroną w górę — tak, aby po zamontowaniu całości klips był skierowany w dół.

Krok 5

Użyj wkrętów, aby przymocować gniazdko do pudełka lub uchwytu. W przypadku pudełka montowanego powierzchniowo należy wziąć pod uwagę, że może się w nim zmieścić od 30 do 60 cm nadmiarowego kabla. Może zatem zaistnieć konieczność przesunięcia kabla w opaskach kablowych albo wciśnięcia pozostałego kabla do korytka kablowego w ścianie po zdjęciu pokrywy z korytka. W przypadku gniazda podtynkowego wystarczy wcisnąć nadmiar kabla do kanału w ścianie.

Schemat kolorów przewodów w gnieździe T568B kategorii 5

Trzymając gniazdo 8-stykowe skierowane do góry lub na zewnątrz, spójrz na kanały przewodów. Gniazdo 8-stykowe to ten fragment gniazda, w który należy włożyć złącze RJ-45. Po każdej stronie powinny być cztery kanały. Dopasuj kolory przewodów do oznaczeń w gnieździe.



Wciskarka typu 110



Gniazdo 8-stykowe	
biało-zielony	biało-niebieski
zielony	niebieski
biało-brązowy	biało-pomarańczowy
brązowy	pomarańczowy

biało-zielony	biało-niebieski
zielony	niebieski
biało-brązowy	biało-pomarańczowy
brązowy	pomarańczowy

Ćwiczenie 5.1.7 Zakup koncentratora i karty sieciowej

Cele

- Zapoznanie się z różnorodnością cen urządzeń sieciowych dostępnych na rynku.
- Zgromadzenie informacji o cenach koncentratorów i kart Ethernet przeznaczonych dla małej sieci.

Wprowadzenie i przygotowanie

Przyjaciół poprosił Cię o pomoc przy tworzeniu listy cen elementów potrzebnych do utworzenia małej sieci LAN przeznaczonej do obsługi niewielkiej firmy. Gwałtowny rozwój firmy, a co za tym idzie, konieczność rozbudowy sieci są mało prawdopodobne. Firma jest wyposażona w komputery, ale nie są one połączone siecią. Firma postanowiła uzyskać dostęp do Internetu przez łącze DSL. Powiedziano im, że wystarczy mały koncentrator i połączenia ze wszystkimi komputerami, aby sieć była gotowa. Każdy z komputerów działa pod kontrolą systemu Windows zapewniającego obsługę sieci węzłów równorzędnych. W opisie ćwiczenia wykorzystano stronę WWW www.cdw.com, ale można także użyć dowolnego lokalnego źródła, katalogu lub strony WWW. Wymagania obejmują następujące elementy:

1. koncentrator Ethernet,
2. karty sieciowe Ethernet do używanych w firmie laptopów,
3. karty sieciowe Ethernet do używanych w firmie komputerów stacjonarnych,
4. kable sieciowe Ethernet kategorii 5e o długości 6,1 m.

Krok 1 Zbieranie informacji o cenach urządzeń

Sprawdź informacje o technikach i cenach z przynajmniej trzech źródeł. W celu odnalezienia informacji w sieci WWW użyj wyszukiwarki w witrynie www.cdw.com, wyszukiwarki internetowej www.google.com lub dowolnej innej. Zapoznaj się z cenami małych koncentratorów i sprawdź, o ile więcej trzeba by zapłacić za mały przełącznik. Porównaj ustalony koszt z kosztem implementacji sieci bezprzewodowej.

Step 2 Utworzenie krótkiego podsumowania wyników

Użyj programu Microsoft Excel, Microsoft Word lub innego podobnego w celu utworzenia podsumowania wyników mieszczącego się na jednej stronie. Tabela porównawcza powinna zawierać możliwe opcje oraz parametry, które były porównywane, takie jak liczba portów, funkcje, cena, wydajność itd.

Ćwiczenie 5.1.10 Zakup przełączników LAN



Cele

- Zapoznanie się z różnorodnością cen urządzeń sieciowych dostępnych na rynku.
- Zgromadzenie informacji o cenach przełączników i kart Ethernet.

Wprowadzenie i przygotowanie

Twoim zadaniem jest przygotowanie przeznaczonej dla biura terenowego propozycji zastąpienia koncentratorów przełącznikami oraz rozważenie co najmniej dwóch różnych rozwiązań i szczegółowe opracowanie propozycji. Szczegółowe założenia są następujące:

- Firma posiada oddział terenowy, w którym działa sieć Ethernet oparta na koncentratorach. Ponieważ liczba usług dostępnych w sieci rośnie, przeciążenia stają się poważnym problemem. Aktualnie na każdym z trzech pięter w węźle dystrybucji okablowania jest jeden lub kilka koncentratorów, które obsługują 30–35 komputerów, natomiast na parterze jest 65 komputerów.
- Wszystkie cztery kondygnacje są dołączone do przełącznika mającego 8 portów o szybkości 10 Mb/s, który został dodany wcześniej w celu zmniejszenia problemów z przeciążeniami. Chociaż to rozwiązanie przyniosło znaczną poprawę, teraz już nie wystarcza. Do tego 8-portowego przełącznika dołączone są również dwa serwery i router połączone z Internetem.
- Okablowanie oddziału jest względnie nowe i zgodne ze standardami kategorii 5. Aktualnie firma nie jest zainteresowana żadnymi większymi zmianami w okablowaniu.
- Co najmniej 75% ze 160 stacji roboczych jest wyposażone w karty sieciowe o szybkości 10/100 Mb/s, działające w trybie pełnego duplexu. Wszystkie laptopy mają nowsze karty sieciowe. Wszystkie nowe komputery są wyposażone w podobne karty sieciowe.

- Zastanów się, co zrobić z aktualnie wykorzystywanym przełącznikiem. Czy możliwe jest uzyskanie większej szerokości pasma połączenia obu serwerów?

Wymagania obejmują następujące elementy:

- Zastąpienie wszystkich koncentratorów przełącznikami.
- Wymiana kart sieciowych o szybkości 10 Mb/s w komputerach stacjonarnych.
- Każde połączenie z hostem powinno obsługiwać co najmniej szybkość 10/100 Mb/s.

Krok 1 Zbieranie informacji o cenach urządzeń

Zacznij od strony www.cisco.com i wybrania łącza „Products & Solutions” (Produkty i Rozwiązania), a następnie łączy do strony „Switches” (Przełączniki), aby zgromadzić podstawowe informacje. Przyjrzyj się szczególnie modelom Catalyst 29xx i 35xx.

Sprawdź informacje o technikach i cenach z przynajmniej trzech innych źródeł. W celu odnalezienia informacji w sieci WWW użyj wyszukiwarki w witrynie www.cdw.com, wyszukiwarki internetowej www.google.com lub dowolnej innej.

Krok 2 Utworzenie tabeli z wynikami

Użyj programu Microsoft Excel, Microsoft Word lub innego podobnego w celu utworzenia tabeli z wynikami.

Na pierwszej stronie powinien znaleźć się opis implementacji, który będzie zawierał wykaz zalecanych produktów i całkowity koszt inwestycji. Należy w nim również zamieścić krótkie (8–15 wierszy) uzasadnienie powodu wyboru danej implementacji.

Na drugiej stronie powinna znaleźć się tabela zawierająca rozpatrywane opcje i porównywane funkcje i parametry, takie jak cena, wydajność itd.

Trzecia strona powinna objaśniać wszelkie kwestie związane z zabezpieczeniami, które pojawiły się podczas opracowywania prezentowanego rozwiązania. Należy je wypunktować. Należy także wskazać, czy te kwestie stwarzają poważne zagrożenia i czy można rozwiązać związane z nimi problemy.

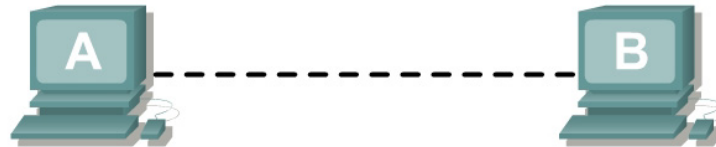
Opcjonalny krok 2 Utworzenie krótkiej prezentacji w programie PowerPoint




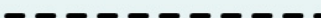
Zamiast przygotowywać powyższe dokumenty programu Excel lub Word, przy użyciu aplikacji PowerPoint utwórz od 4 do 8 slajdów prezentacji opisującej te same zagadnienia.

Podczas przygotowywania materiałów przyjmij założenie, że będą one musiały zostać zaprezentowane.

Jeśli czas na to pozwoli, należy wykonać oba warianty. Najczęściej tak właśnie się robi.

Ćwiczenie 5.1.12 Budowanie sieci węzłów równorzędnych



Kabel prosty	
Kabel szeregowy	
Kabel do konsoli (rollover)	
Kabel z przeplotem	

Cele

- Utworzenie prostej sieci węzłów równorzędnych między dwoma komputerami PC.
- Wybór właściwego kabla do połączenia dwóch komputerów PC.
- Skonfigurowanie adresowania IP na stacjach roboczych.
- Przetestowanie połączenia przy użyciu polecenia `ping`.

Wprowadzenie i przygotowanie

To ćwiczenie umożliwia nabycie umiejętności łączenia dwóch komputerów PC. Polega ono na utworzeniu prostej lokalnej sieci węzłów równorzędnych Ethernet między dwoma stacjami roboczymi. Stacje robocze będą połączone ze sobą bezpośrednio, bez użycia koncentratora lub przełącznika. Oprócz wykonania połączenia fizycznego w warstwie 1 i połączenia łącza danych w warstwie 2, aby możliwa była komunikacja między komputerami, należy w nich również skonfigurować właściwe ustawienia IP, które należą do warstwy 3. Do wykonania połączenia wykorzystany zostanie jedynie kabel z przeplotem wykonany ze skrętki nieekranowanej kategorii 5 lub 5e. Kabel z przeplotem to taki sam kabel, jak te używane w sieci szkieletowej lub w okablowaniu pionowym do łączenia przełączników. Ten sposób połączenia komputerów może być bardzo przydatny przy przesyłaniu plików z dużą szybkością i rozwiązywaniu problemów związanych z urządzeniami połączeniowymi znajdującymi się między tymi komputerami. Jeśli dwa komputery połączone za pomocą jednego kabla mogą się ze sobą komunikować, oznacza to, że przyczyna problemów z siecią nie dotyczy samych komputerów. Ćwiczenie to należy rozpocząć przy wyłączonych urządzeniach i rozłączonym okablowaniu. Praca przebiega w zespołach dwuosobowych; na każdą osobę powinien przypadać jeden komputer. Wykorzystane będą następujące przedmioty:

- dwie stacje robocze z zainstalowanymi kartami sieciowymi Ethernet 10/100;
- kilka kabli prostych i kabli z przeplotem dla sieci Ethernet (w celu wybrania spośród nich kabla właściwego do połączenia dwóch stacji roboczych).

Krok 1 Wybór właściwego kabla Ethernet i połączenie dwóch komputerów PC

- a. Połączenie między dwoma komputerami PC zostanie wykonane przy użyciu kabla z przeplotem kategorii 5 lub 5e. Wybierz kabel, którego długość umożliwi połączenie obu komputerów, i podłącz końce kabla do kart sieciowych komputerów. Pamiętaj, aby uważnie sprawdzić końce kabla i wybrać kabel z przeplotem.
- b. Jakiego kabla należy użyć do połączenia kart sieciowych? _____
- c. Jaka jest kategoria tego kabla? _____
- d. Jakie jest oznaczenie AWG rozmiaru przewodu kabla? _____

Krok 2 Sprawdzenie połączenia fizycznego

- a. Podłącz komputery do zasilania i włącz je. Aby sprawdzić połączenia komputerów, upewnij się, że w obu kartach sieciowych świecą się diody LED wskazujące stan łącza. Czy świecą się obie diody LED łącza? _____

Krok 3 Otwarcie okna ustawień adresu IP

Uwaga: Pamiętaj o zapisaniu istniejących ustawień IP, aby możliwe było ich odtworzenie po zakończeniu ćwiczenia. Ustawienia te obejmują: adres IP, maskę podsieci, domyślną bramę i serwery DNS. Jeśli stacja robocza jest klientem DHCP, nie trzeba zapisywać tych informacji.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie ikonę **Network (Sieć)**.
- Wybierz ikonę protokołu TCP/IP, która jest powiązana z kartą sieciową tego komputera, i kliknij opcję **Properties (Właściwości)**.
- Kliknij zakładkę **IP Address (Adres IP)** i zakładkę **Gateway (Brama)**.

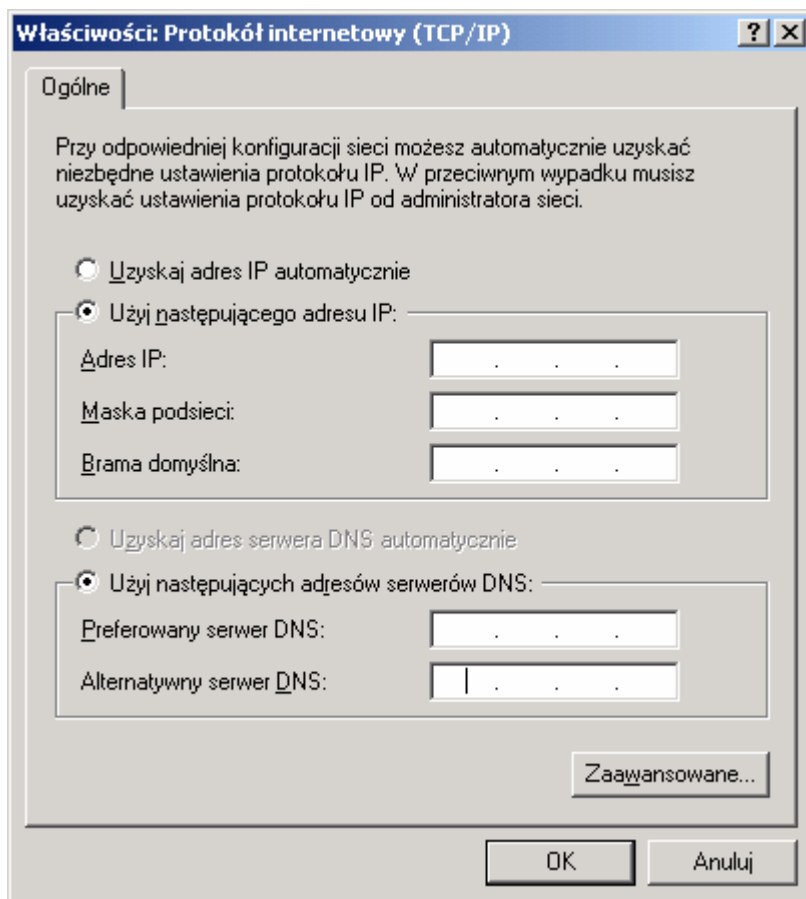
Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie otwórz folder **Network and Dial-up Connections (Połączenia sieciowe i telefoniczne)**.
- Kliknij i otwórz ikonę **Local Area Connection (Połączenie lokalne)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie ikonę **Network Connection (Połączenie sieciowe)**.
- Wybierz opcję **Local Area Network Connection (Połączenie LAN)**, a następnie kliknij opcję **Change settings of this connection (Zmień ustawienia tego połączenia)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Spójrz na poniższy przykład:



Krok 4 Konfiguracja ustawień TCP/IP w komputerach

- Ustaw informacje o adresie IP w każdym z komputerów zgodnie z informacjami podanymi w tabeli.
- Zauważ, że adres IP domyślnej bramy nie jest wymagany, ponieważ komputery te są połączone bezpośrednio. Domyślna brama jest potrzebna tylko w przypadku sieci lokalnych podłączonych do routera.

Komputer	Adres IP	Maska podsieci	Domyślna brama
Komputer A	192.168.1.1	255.255.255.0	Niewymagana
Komputer B	192.168.1.2	255.255.255.0	Niewymagana

Krok 5 Otwarcie okna wiersza poleceń

- Skorzystaj z menu Start, aby otworzyć okno wiersza poleceń, przypominające okno systemu MS-DOS.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS).**

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń).**

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

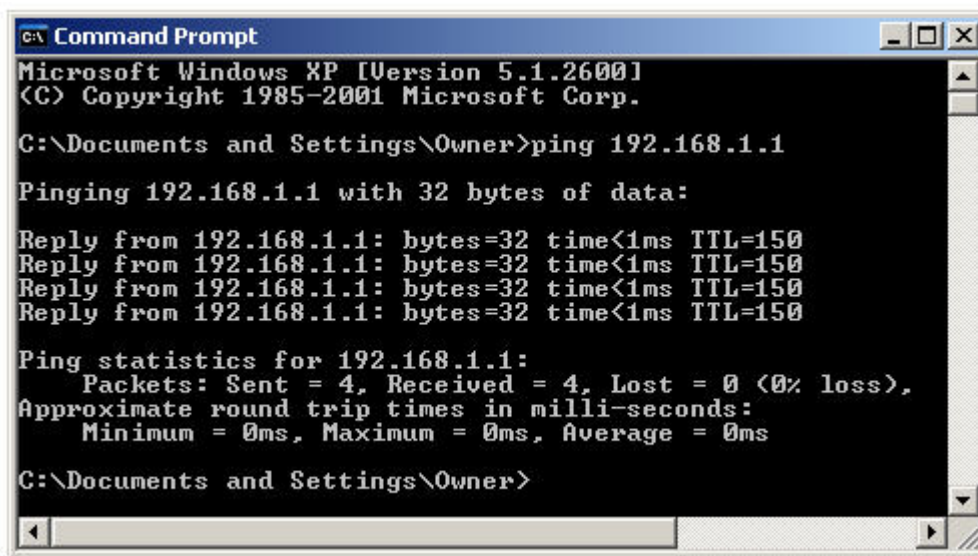
Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń).**

Krok 6 Sprawdzenie komunikacji między komputerami

- a. Sprawdź połączenie utworzone między komputerami, wydając polecenie ping pod adresem IP komputera znajdującego się po drugiej stronie łącza. Użyj następującego polecenia w wierszu poleceń:

```
C:>ping 192.168.1.1 (lub 192.168.1.2)
```

- b. Sprawdź, czy wyniki są podobne do przedstawionych poniżej. Jeśli nie, sprawdź połączenia komputerów i ich ustawienia TCP/IP. Jaki był wynik działania polecenia ping?



```
c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Owner>
```

Krok 7 Potwierdzenie ustawień sieciowych TCP/IP

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

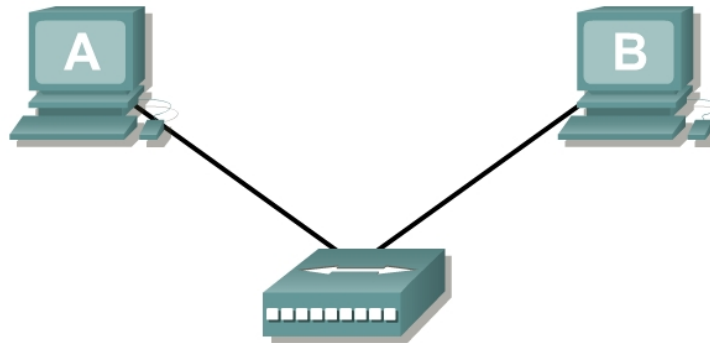
- a. W wierszu poleceń wpisz polecenie **winipcfg**. Zapisz wyniki:



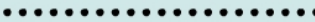
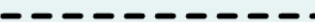
Użytkownicy systemu Windows NT/2000/XP powinni wykonać następujące czynności:

- b. W wierszu poleceń wpisz polecenie **ipconfig**. Zapisz wyniki:

Krok 8 Przywrócenie oryginalnych ustawień IP w komputerach, rozłączenie urządzeń i zwinięcie kabli

Ćwiczenie 5.1.13a Budowanie sieci z wykorzystaniem koncentratorów



Kabel prosty	
Kabel szeregowy	
Kabel do konsoli (rollover)	
Kabel z przeplotem	

Cele

- Utworzenie prostej sieci między dwoma komputerami przy użyciu koncentratora.
- Wybór właściwego kabla do podłączenia komputerów do koncentratora.
- Skonfigurowanie informacji o adresach IP stacji roboczych.
- Przetestowanie połączenia przy użyciu polecenia `ping`.

Wprowadzenie i przygotowanie

To ćwiczenie umożliwia nabycie umiejętności łączenia dwóch komputerów PC. Polega na utworzeniu prostej lokalnej sieci Ethernet między dwoma stacjami roboczymi z użyciem koncentratora. Koncentrator jest koncentrującym łącza urządzeniem sieciowym. Czasami jest nazywany wieloportowym wtórnikiem (ang. multiport repeater). Koncentratory są tanie i łatwe do zainstalowania, ale nie zapobiegają występowaniu kolizji. Są dobrym rozwiązaniem w przypadku niewielkich sieci LAN o małym ruchu.

Oprócz wykonania połączenia fizycznego w warstwie 1 i połączenia łącza danych w warstwie 2, aby możliwa była komunikacja między komputerami, należy w nich również skonfigurować właściwe ustawienia IP, które należą do warstwy 3. Ponieważ w tym ćwiczeniu jest używany koncentrator, do podłączenia obu komputerów do koncentratora potrzebny będzie kabel prosty ze skrętki nieekranowanej o kategorii 5 lub 5e. Kabel taki nazywa się kablem połączeniowym (jest on elementem okablowania poziomego). Służy on do łączenia stacji roboczych z typową siecią LAN. Ćwiczenie to należy rozpocząć przy wyłączonych urządzeniach i rozłączonym okablowaniu. Praca przebiega w zespołach dwuosobowych; na każdą osobę powinien przypadać jeden komputer. Potrzebne będą następujące materiały:

- dwie stacje robocze z zainstalowanymi kartami sieciowymi Ethernet 10/100;
- koncentrator Ethernet 10BaseT lub Fast Ethernet;
- kilka kabli prostych i kabli z przeplotem dla sieci Ethernet, aby można było spośród nich wybrać właściwe do podłączenia obu stacji roboczych.

Krok 1 Wybór właściwego kabla Ethernet i podłączenie dwóch komputerów PC do koncentratora

- a. Połączenie między komputerami i koncentratorom zostanie wykonane przy użyciu kabla połączeniowego kategorii 5 lub 5e. Wybierz dwa kable, których długość umożliwi połączenie każdego z komputerów z koncentratorom. Jeden koniec kabla należy podłączyć do karty sieciowej, a drugi — do portu w koncentratorze. Pamiętaj, aby uważnie sprawdzić końce kabla i wybrać kabel prosty.
- b. Jakiego kabla należy użyć do połączenia karty sieciowej i koncentratora? _____
- c. Jakiej kategorii jest ten kabel? _____
- d. Jakie jest oznaczenie AWG rozmiaru przewodu kabla? _____

Krok 2 Sprawdzenie połączenia fizycznego

- a. Podłącz komputery do zasilania i włącz je. Aby sprawdzić połączenia komputerów, upewnij się, że w obu kartach sieciowych i przy interfejsach koncentratora świecą się diody LED wskazujące stan łącza. Czy świecą się wszystkie diody LED łącza? _____

Krok 3 Otwarcie okna ustawień adresu IP

Uwaga: Pamiętaj o zapisaniu istniejących ustawień IP, aby możliwe było ich odtworzenie po zakończeniu ćwiczenia. Ustawienia te obejmują: adres IP, maskę podsieci, domyślną bramę i serwery DNS. Jeśli stacja robocza jest klientem DHCP, nie trzeba zapisywać tych informacji.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network (Sieć)**.
- Wybierz ikonę protokołu TCP/IP, która jest powiązana z kartą sieciową tego komputera, i kliknij opcję **Properties (Właściwości)**.
- Kliknij zakładkę **IP Address (Adres IP)** i zakładkę **Gateway (Brama)**.

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

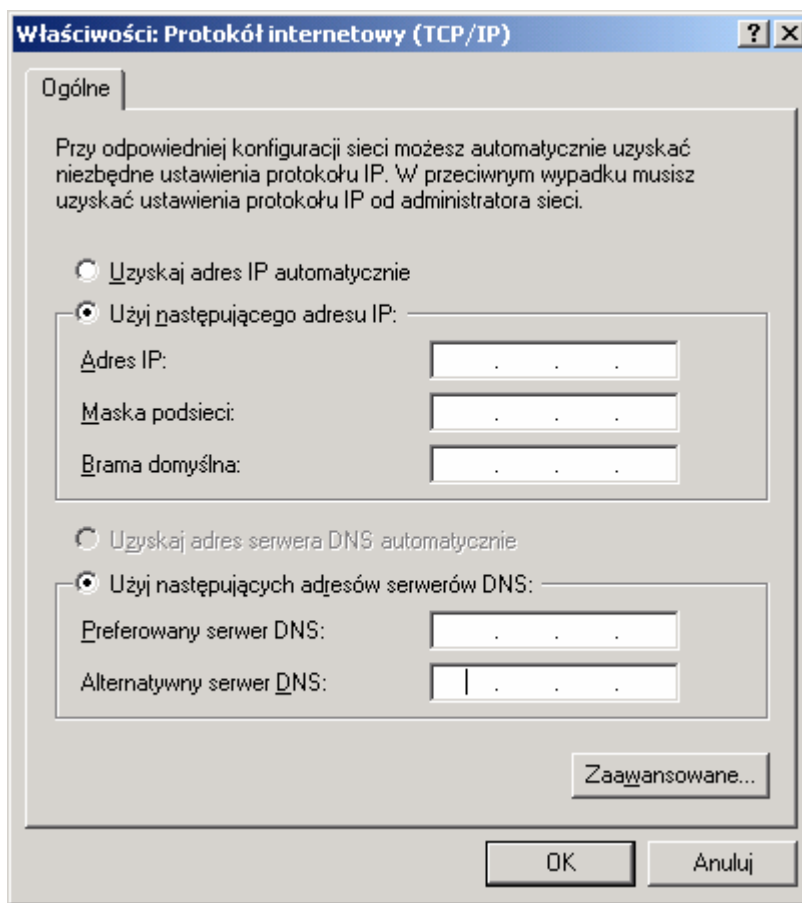
- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie otwórz folder **Network and Dial-up Connections (Połączenia sieciowe i telefoniczne)**.
- Kliknij i otwórz ikonę **Local Area Connection (Połączenie lokalne)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network Connection (Połączenie sieciowe)**.

- Wybierz opcję **Local Area Network Connection (Połączenie LAN)**, a następnie kliknij opcję **Change settings of this connection (Zmień ustawienia tego połączenia)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Spójrz na poniższy przykład:



Krok 4 Konfiguracja ustawień TCP/IP w komputerach

- Ustaw informacje o adresie IP w każdym z komputerów zgodnie z informacjami podanymi w tabeli.
- Zauważ, że adres IP domyślnej bramy nie jest wymagany, ponieważ komputery te są połączone bezpośrednio. Domyślna brama jest potrzebna tylko w przypadku sieci lokalnych podłączonych do routera.

Komputer	Adres IP	Maska podsieci	Domyślna brama
Komputer A	192.168.1.1	255.255.255.0	Niewymagana
Komputer B	192.168.1.2	255.255.255.0	Niewymagana

Krok 5 Otwarcie okna wiersza poleceń

- Skorzystaj z menu Start, aby otworzyć okno wiersza poleceń, przypominające okno systemu MS-DOS.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS)**.

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

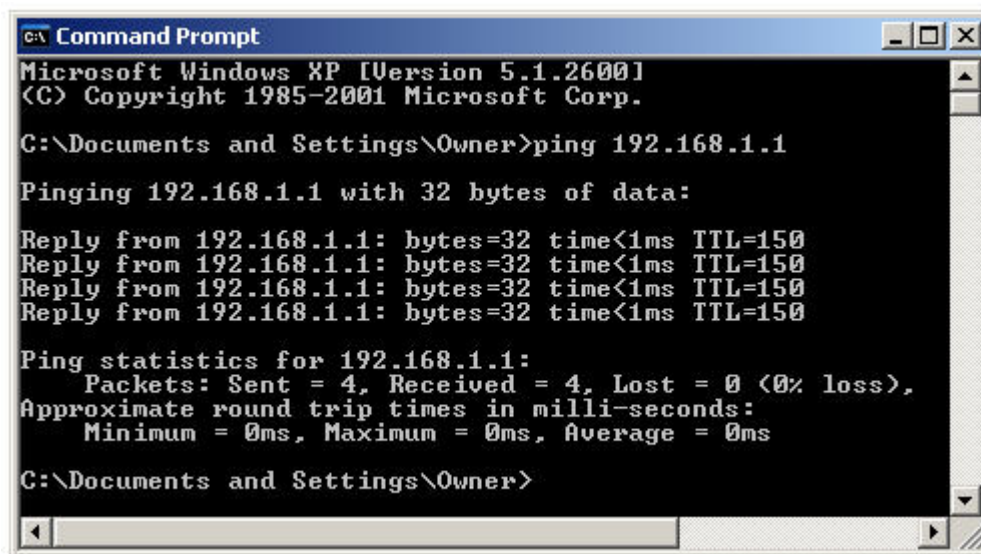
Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)**.

Krok 6 Sprawdzenie komunikacji między komputerami

- Sprawdź, czy działa połączenie utworzone między komputerami przy użyciu koncentratora, wydając polecenie ping pod adresem IP komputera znajdującego się po drugiej stronie łącza. Użyj następującego polecenia w wierszu poleceń:

```
C:>ping 192.168.1.1 (lub 192.168.1.2)
```

- Sprawdź, czy wyniki są podobne do przedstawionych poniżej. Jeśli nie, sprawdź połączenia komputerów i ich ustawienia TCP/IP. Jaki był wynik działania polecenia ping?



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Owner>
```

Krok 7 Potwierdzenie ustawień sieciowych TCP/IP

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

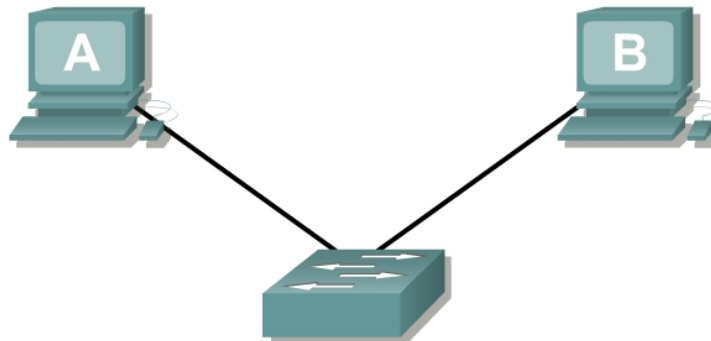
- W wierszu poleceń wpisz polecenie **winipcfg**. Zapisz wyniki:




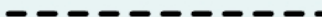
Użytkownicy systemu Windows NT/2000/XP powinni wykonać następujące czynności:

b. W wierszu poleceń wpisz polecenie `ipconfig`. Zapisz wyniki:

Krok 8 Przywrócenie oryginalnych ustawień IP w komputerach, rozłączenie urządzeń i zwinięcie kabli

Ćwiczenie 5.1.13b Budowanie sieci z wykorzystaniem przełączników



Kabel prosty	
Kabel szeregowy	
Kabel do konsoli (rollover)	
Kabel z przeplotem	

Cele

- Utworzenie prostej sieci między dwoma komputerami przy użyciu przełącznika.
- Wybór właściwego kabla do podłączenia komputerów do przełącznika.
- Skonfigurowanie informacji o adresach IP stacji roboczych.
- Przetestowanie połączenia przy użyciu polecenia `ping`.

Wprowadzenie i przygotowanie

To ćwiczenie umożliwia nabycie umiejętności łączenia dwóch komputerów PC. Polega na utworzeniu prostej lokalnej sieci Ethernet między dwoma stacjami roboczymi z użyciem przełącznika. Przełącznik jest urządzeniem sieciowym koncentrującym łącza. Czasami jest nazywany wieloportowym mostem (ang. multiport bridge). Przełączniki są względnie tanie i łatwe do zainstalowania. Działając w trybie pełnego duplexu, umożliwiają wydzielenie pasma dla poszczególnych stacji roboczych. Przełączniki uniemożliwiają powstawanie kolizji, tworząc mikrosegmenty między portami, do których są podłączone stacje robocze. Przełączniki są dobrym rozwiązaniem w przypadku małych i dużych sieci LAN o średnim lub dużym ruchu.

Oprócz wykonania połączenia fizycznego w warstwie 1 i połączenia łącza danych w warstwie 2, aby możliwa była komunikacja między komputerami, należy w nich również skonfigurować właściwe ustawienia IP, które należą do warstwy 3. Ponieważ w tym ćwiczeniu jest używany przełącznik, do podłączenia obu komputerów do koncentratora potrzebny będzie kabel prosty ze skrętki

nieekranowanej o kategorii 5 lub 5e. Kabel taki nazywa się kablem połączeniowym (jest on elementem okablowania poziomego). Służy on do łączenia stacji roboczych z typową siecią LAN. Ćwiczenie to należy rozpocząć przy wyłączonych urządzeniach i rozłączonym okablowaniu. Praca przebiega w zespołach dwuosobowych; na każdą osobę powinien przypadać jeden komputer. Potrzebne będą następujące materiały:

- dwie stacje robocze z zainstalowanymi kartami sieciowymi Ethernet 10/100;
- przełącznik Ethernet 10BaseT lub Fast Ethernet;
- kilka kabli prostych i kabli z przeplotem dla sieci Ethernet, aby można było spośród nich wybrać właściwe do podłączenia obu stacji roboczych.

Krok 1 Wybór właściwego kabla Ethernet i podłączenie dwóch komputerów PC do przełącznika

- a. Połączenie między komputerami i przełącznikiem zostanie wykonane przy użyciu kabla połączeniowego kategorii 5 lub 5e. Wybierz dwa kable, których długość umożliwi połączenie każdego z komputerów z przełącznikiem. Jeden koniec kabla należy podłączyć do karty sieciowej a drugi — do portu w przełączniku. Pamiętaj, aby uważnie sprawdzić końce kabla i wybrać kabel prosty.
- b. Jakiego kabla należy użyć do połączenia karty sieciowej i przełącznika? _____
- c. Jaka jest kategoria tego kabla? _____
- d. Jakie jest oznaczenie AWG rozmiaru przewodu kabla? _____

Krok 2 Sprawdzenie połączenia fizycznego

- a. Podłącz komputery do zasilania i włącz je. Aby sprawdzić połączenia komputerów, upewnij się, że w obu kartach sieciowych i przy interfejsach przełącznika świecą się diody LED wskazujące stan łącza. Czy świecą się wszystkie diody LED łączy? _____

Krok 3 Otwarcie okna ustawień adresu IP

Uwaga: Pamiętaj o zapisaniu istniejących ustawień IP, aby możliwe było ich odtworzenie po zakończeniu ćwiczenia. Ustawienia te obejmują: adres IP, maskę podsieci, domyślną bramę i serwery DNS. Jeśli stacja robocza jest klientem DHCP, nie trzeba zapisywać tych informacji.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network (Sieć)**.
- Wybierz ikonę protokołu TCP/IP, która jest powiązana z kartą sieciową tego komputera, i kliknij opcję **Properties (Właściwości)**.
- Kliknij zakładkę **IP Address (Adres IP)** i zakładkę **Gateway (Brama)**.

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

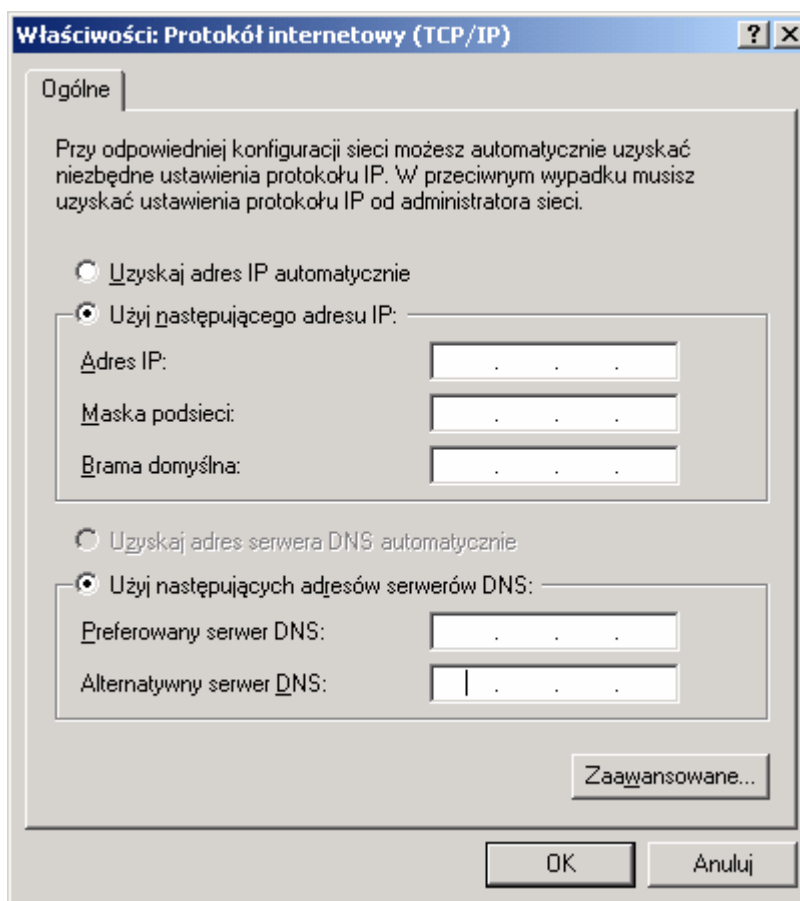
- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie otwórz folder **Network and Dial-up Connections (Połączenia sieciowe i telefoniczne)**.
- Kliknij i otwórz ikonę **Local Area Connection (Połączenie lokalne)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.

- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network Connection (Połączenie sieciowe)**.
- Wybierz opcję **Local Area Network Connection (Połączenie LAN)**, a następnie kliknij opcję **Change settings of this connection (Zmień ustawienia tego połączenia)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Spójrz na poniższy przykład:



Krok 4 Konfiguracja ustawień TCP/IP w komputerach

- a. Ustaw informacje o adresie IP w każdym z komputerów zgodnie z informacjami podanymi w tabeli.
- b. Zauważ, że adres IP domyślnej bramy nie jest wymagany, ponieważ komputery te są połączone bezpośrednio. Domyślna brama jest potrzebna tylko w przypadku sieci lokalnych podłączonych do routera.

Komputer	Adres IP	Maska podsieci	Domyślna brama
Komputer A	192.168.1.1	255.255.255.0	Niewymagana
Komputer B	192.168.1.2	255.255.255.0	Niewymagana

Krok 5 Otwarcie okna wiersza poleceń

- a. Skorzystaj z menu Start, aby otworzyć okno wiersza poleceń, przypominające okno systemu MS-DOS.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS)**.

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)**.

Krok 6 Sprawdzenie komunikacji między komputerami

- a. Sprawdź, czy działa połączenie utworzone między komputerami przy użyciu przełącznika, wydając polecenie ping pod adresem IP komputera znajdującego się po drugiej stronie łącza. Użyj następującego polecenia w wierszu poleceń:

```
C:>ping 192.168.1.1 (lub 192.168.1.2)
```

- b. Sprawdź, czy wyniki są podobne do przedstawionych poniżej. Jeśli nie, sprawdź połączenia komputerów i ich ustawienia TCP/IP. Jaki był wynik działania polecenia ping?

```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Owner>

```

Krok 7 Potwierdzenie ustawień sieciowych TCP/IP

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

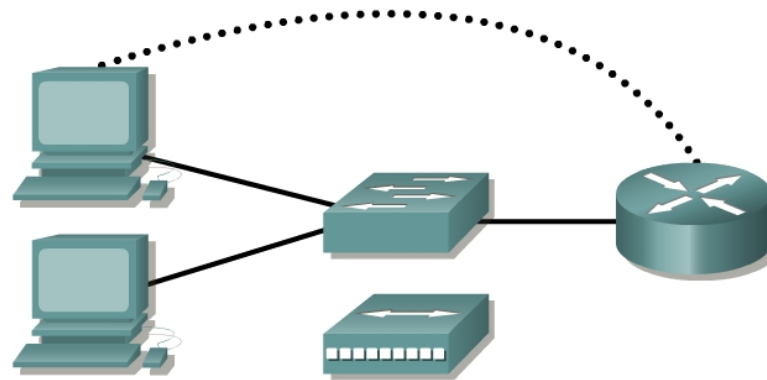
- a. W wierszu poleceń wpisz polecenie `winipcfg`. Zapisz wyniki:
-




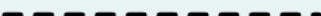
Użytkownicy systemu Windows NT/2000/XP powinni wykonać następujące czynności:

- b. W wierszu poleceń wpisz polecenie `ipconfig`. Zapisz wyniki:
-

Krok 8 Przywrócenie oryginalnych ustawień IP w komputerach, rozłączenie urządzeń i zwinięcie kabli

Ćwiczenie 5.2.3a Łączenie interfejsów LAN routera



Kabel prosty	
Kabel szeregowy	
Kabel do konsoli (rollover)	
Kabel z przeplotem	

Cele

- Opanowanie umiejętności rozpoznawania interfejsu Ethernet i Fast Ethernet w routerze.
- Wybór właściwych kabli w celu podłączenia routera i komputera PC do koncentratora lub przełącznika.
- Podłączenie routera i komputera do koncentratora lub przełącznika przy użyciu wybranych kabli.

Wprowadzenie i przygotowanie

To ćwiczenie umożliwia nabycie umiejętności wykonywania fizycznego okablowania między urządzeniami lokalnej sieci Ethernet, takimi jak koncentratory i przełączniki, oraz odpowiednim interfejsem Ethernet w routerze. W komputerach i w routerze powinny być określone poprawne ustawienia sieciowe IP. Ćwiczenie to należy rozpocząć przy wyłączonych oraz niepodłączonych komputerach (komputerze), routerze i koncentratorze lub przełączniku. Potrzebne będą następujące elementy:

- co najmniej jedna stacja robocza z zainstalowaną kartą sieciową Ethernet 10/100;
- jeden przełącznik lub koncentrator Ethernet;
- jeden router z interfejsem RJ-45 sieci Ethernet lub Fast Ethernet lub z interfejsem AUI;
- transceiver z interfejsem AUI 10BASE-T (DB-15 do RJ-45) do routera z interfejsem AUI sieci Ethernet (seria 2500);

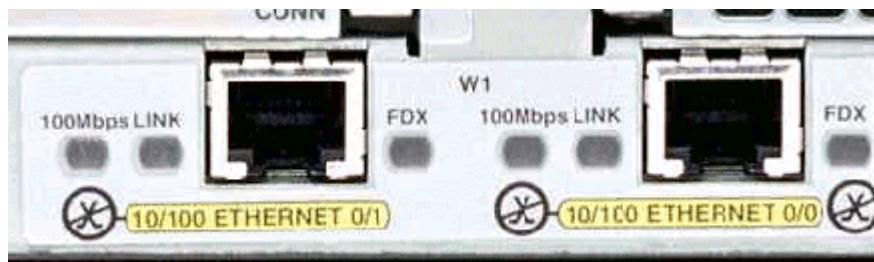
- kilka kabli prostych i kabli z przeplotem dla sieci Ethernet, aby można było spośród nich wybrać właściwe do połączenia stacji roboczej i routera do koncentratora lub przełącznika.

Krok 1 Rozpoznanie interfejsów Ethernet i Fast Ethernet w routerze

- Przyjrzyj się routerowi.

Jaki jest numer jego modelu? _____

- Znajdź na routerze jedno lub więcej złączy RJ-45 oznaczonych „Ethernet0” lub „Ethernet1”. Oznaczenie to może być inne — zależnie od typu używanego routera. Na ilustracji znajduje się router z serii 2600. Router z serii 2500 jest wyposażony w port Ethernet AUI DB-15 oznaczony „AUI 0”. W takim przypadku w celu podłączenia do kabla RJ-45 potrzebny będzie transceiver 10BASE-T.



- Znajdź porty Ethernet, które można wykorzystać do podłączenia routerów. Zapisz poniższe informacje. Zapisz numery portów AUI, jeśli używany jest router Cisco serii 2500.

Router	Port	Port

Krok 2 Wybór właściwych kabli i podłączenie routera

- Połączenie między routerem i koncentratorem lub przełącznikiem zostanie wykonane przy użyciu prostego kabla połączeniowego kategorii 5. Wybierz kabel połączeniowy, którego długość umożliwi połączenie routera z koncentratorem. Pamiętaj, aby uważnie sprawdzić końce kabli i wybrać tylko kable proste.
- Przy użyciu kabla połącz interfejs Ethernet routera oznaczony zerem z portem koncentratora lub przełącznika. Oznaczenie na routerze może być inne — zależnie od typu używanego routera. Na ilustracji znajduje się router z serii 2600.

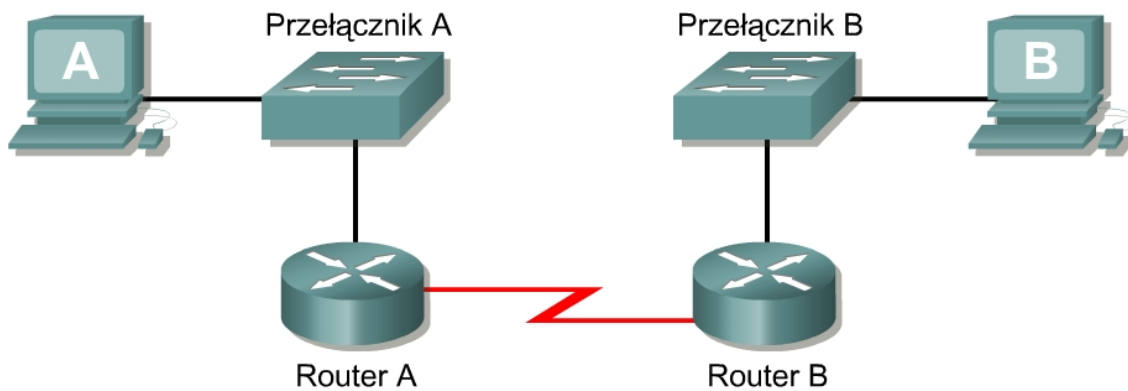
Krok 3 Instalacja okablowania Ethernet stacji roboczej

- Komputery również zostaną podłączone do koncentratora przy użyciu prostego kabla połączeniowego. Między komputerami a koncentratorem lub przełącznikiem należy położyć kable połączeniowe kategorii 5. Jeden koniec kabla należy podłączyć do złącza RJ-45 karty sieciowej komputera, a drugi — do portu koncentratora lub przełącznika. Pamiętaj, aby uważnie sprawdzić końce kabli i wybrać tylko kable proste.

Krok 4 Sprawdzenie połączenia

- Podłącz do zasilania i włącz router, komputery oraz koncentrator lub przełącznik.
- Aby sprawdzić połączenia z routerem, upewnij się, że przy interfejsie routera oraz przy interfejsie koncentratora lub przełącznika świecą się diody LED wskazujące stan łącza.
- Aby sprawdzić połączenia komputerów, upewnij się, że w obu kartach sieciowych i przy interfejsie koncentratora lub przełącznika świecą się diody LED wskazujące stan łącza.

Ćwiczenie 5.2.3b Budowanie prostej sieci WAN z routingiem



Kabel prosty	—————
Kabel szeregowy	————— ⚡ —————
Kabel do konsoli (rollover)
Kabel z przeplotem	- - - - -

Cele

- Utworzenie prostej sieci WAN z routingiem: dwa komputery PC, dwa przełączniki lub koncentratory i dwa routery.
- Wybór właściwych kabli w celu podłączenia komputera i routera do przełącznika.
- Wybór właściwych kabli w celu połączenia routerów i utworzenia łącza WAN.
- Skonfigurowanie informacji o adresach IP stacji roboczych.
- Przetestowanie połączenia przy użyciu polecenia `ping`.

Wprowadzenie i przygotowanie

To ćwiczenie umożliwi nabycie umiejętności połączenia dwóch prostych sieci LAN (z których każda składa się ze stacji roboczej oraz przełącznika lub koncentratora) w celu utworzenia prostej sieci WAN o konstrukcji router-router. Router jest urządzeniem sieciowym, którego można użyć do połączenia dwóch sieci LAN. Urządzenie to realizuje routing pakietów między różnymi sieciami przy wykorzystaniu adresowania IP w warstwie 3. Typowym zastosowaniem routerów jest tworzenie łącza w Internecie.

Oprócz wykonania połączenia fizycznego w warstwie 1 i połączenia łącza danych w warstwie 2, aby możliwa była komunikacja między komputerami i routerami, należy w tych urządzeniach

skonfigurować właściwe ustawienia IP, które należą do warstwy 3. Do podłączania komputerów i routerów do przełącznika lub koncentratora używane są proste kable połączeniowe. Do utworzenia symulowanego łącza WAN między routerami zostaną wykorzystane dwa specjalne kable V.35.

Uwaga: Zadaniem instruktora jest ustawienie prawidłowych adresów IP w interfejsach LAN i WAN obu routerów. Router A będzie generował sygnał taktujący jako urządzenie DCE.

Ćwiczenie to należy rozpocząć przy wyłączonych urządzeniach i rozłączonym okablowaniu. Praca przebiega w zespołach dwuosobowych; na każdą osobę powinna przypadać jedna sieć LAN. Potrzebne będą następujące elementy:

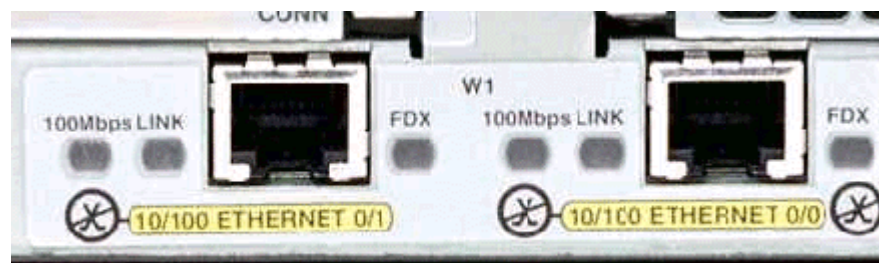
- dwie stacje robocze z zainstalowanymi kartami sieciowymi Ethernet 10/100;
- dwa przełączniki lub koncentratory Ethernet 10BaseT lub Fast Ethernet;
- dwa routery z interfejsem RJ-45 Ethernet lub Fast Ethernet (lub interfejsem AUI) i co najmniej jednym interfejsem szeregowym;
- transceiver z interfejsem AUI 10BASE-T (DB-15 do RJ-45) do routera z interfejsem AUI sieci Ethernet (seria 2500);
- cztery proste kable dla sieci Ethernet w celu podłączenia stacji roboczych i routerów do koncentratora lub przełącznika;
- jeden kabel V.35 żeński (DCE) i jeden męski (DTE) do połączenia routerów.

Krok 1 Wybór właściwego kabla Ethernet i połączenie komputera z przełącznikiem

- a. Połączenie między komputerem i przełącznikiem zostanie wykonane przy użyciu kabla połączeniowego kategorii 5 lub 5e. Jeden koniec kabla należy podłączyć do karty sieciowej, a drugi — do portu w przełączniku lub koncentratorze. Pamiętaj, aby uważnie sprawdzić końce kabla i wybrać kabel prosty.
- b. Przyjrzyj się przełącznikowi lub koncentratorowi.
Jaki jest numer modelu przełącznika lub koncentratora?

Krok 2 Rozpoznanie interfejsów Ethernet i Fast Ethernet w routerach

- a. Przyjrzyj się routerom.
- b. Jaki jest numer modelu routera A? _____
- c. Jaki jest numer modelu routera B? _____
- d. Znajdź jedno lub więcej złączy RJ-45 w każdym routerze. Są one oznaczone jako „10/100 Ethernet”, co przedstawiono poniżej. Oznaczenie może być inne — zależnie od typu używanego routera. Na ilustracji znajduje się router z serii 2600. Router serii 2500 jest wyposażony w port Ethernet AUI DB-15 oznaczony jako „AUI 0”. Przy zastosowaniu tego routera do podłączenia go do kabla RJ-45 potrzebny jest transceiver 10Base-T.



- e. Znajdź porty Ethernet, które można wykorzystać do podłączenia routerów. Zapisz poniższe informacje. Zapisz numery portów AUI w przypadku korzystania z routera Cisco serii 2500.

Router	Port	Port

Krok 3 Okablowanie łączy LAN routera

- a. Konfiguracja routera.

Routery powinny zostać skonfigurowane przez instruktora tak, aby dla interfejsu Ethernet 0 każdego routera był prawidłowo ustawiony adres IP i maska podsieci, zgodnie ze wskazówkami zawartymi w poniższej tabeli. Dzięki temu możliwy będzie routing pakietów między lokalnymi sieciami 192.168.1.0 i 192.168.2.0.

Router	Adres IP interfejsu E0	Maska podsieci
Router A	192.168.1.1	255.255.255.0
Router B	192.168.2.1	255.255.255.0

- b. Łączenie kabli.

Połączenie między routerem i koncentratorem lub przełącznikiem zostanie wykonane przy użyciu prostego kabla połączeniowego kategorii 5. Wybierz kabel połączeniowy, którego długość umożliwi połączenie routera z koncentratorem. Pamiętaj, aby uważnie sprawdzić końce kabli i wybrać tylko kable proste. Połącz interfejs Ethernet routera oznaczony zerem (0) z portem koncentratora lub przełącznika. W przypadku połączenia z routerami z serii 2500 należy użyć transceivera 10BASE-T AUI.

Step 4 Sprawdzenie fizycznych połączeń Ethernet

- a. Podłącz do zasilania i włącz komputery, przełączniki/koncentratory oraz routery. Aby sprawdzić połączenia, upewnij się, że w obu kartach sieciowych, przy interfejsach przełączników/koncentratorów i interfejsach routerów Ethernet świecą się diody LED wskazujące stan łącza. Czy świecą się wszystkie diody LED łączy? _____ Jeśli nie, sprawdź połączenia i typy kabli.

Krok 5 Rozpoznanie interfejsów szeregowych routera

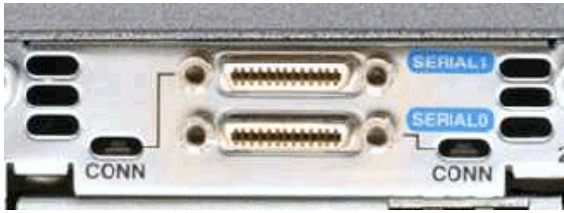

- a. Przyjrzyj się routerom.
- b. W każdym z routerów określ porty szeregowo, których można użyć do połączenia routerów w celu przeprowadzenia symulacji łącza WAN. Zapisz poniższe informacje. Jeśli interfejsów szeregowych jest więcej niż jeden, w każdym routerze należy użyć interfejsu oznaczonego jako „0”.

Nazwa routera	Port szeregowy routera	Port szeregowy routera
Router A		
Router B		

Krok 6 Wybór właściwych kabli V.35

- Przejrzyj kable szeregowo dostępne w laboratorium. Router może być wyposażony w różne złącza w zależności od typu routera i/lub karty szeregowo.
- Charakterystyka portu szeregowo routera.

Najczęściej używane są złącza typu DB-60 i typu „smart serial”. Posługując się poniższą tabelą, wskaż używane typy routerów.

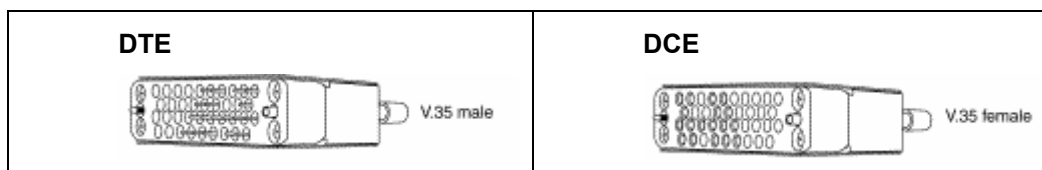
Router	Smart Serial	DB60
		
RTR A	<input type="checkbox"/>	<input type="checkbox"/>
RTR B	<input type="checkbox"/>	<input type="checkbox"/>

- Symulowanie łącza WAN — urządzenia DCE/DTE oraz sygnał taktujący.

Ponieważ w ćwiczeniu nie będzie wykorzystywana faktyczna linia dzierżawiona, jeden z routerów musi generować sygnał taktujący dla obwodu. Zwykle sygnał taki zapewnia routerom urządzenie DCE, takie jak jednostka CSU/DSU. Z tego powodu jeden z routerów musi być podłączony przy użyciu kabla DCE, a nie zwykłego kabla DTE, przy użyciu którego będzie podłączony drugi router. Połączenie między routerami należy zatem wykonać przy użyciu jednego kabla DCE i jednego kabla DTE. Do symulacji połączenia WAN zostaną użyte kable DCE V.35 oraz kable DTE V.35.

- Charakterystyka kabla V.35.

Złącze DCE V.35 to duże (34-stykowe) złącze żeńskie V.35. Kabel DTE jest wyposażony w duże złącze męskie V.35. Kable są także oznaczone jako „DCE” lub „DTE” na tym końcu kabla, który jest podłączany do routera. Kabel DCE należy podłączyć do routera A, ponieważ to on będzie generował sygnał taktujący.



Krok 7 Okablowanie łącza WAN routera

a. Konfiguracja routera.

Router A powinien zostać skonfigurowany przez instruktora tak, aby podawał sygnał taktujący DCE poprzez interfejs szeregowy 0. W przypadku interfejsu szeregowego 0 każdego z routerów należy ustawić prawidłowy adres IP i maskę podsieci zgodnie ze wskazówkami znajdującymi się w poniższej tabeli. Adresem sieci łączącej interfejsy szeregowo routerów jest 192.168.3.0.

Router	Taktowanie	Adres IP interfejsu S0	Maska podsieci
Router A	DCE	192.168.3.1	255.255.255.0
Router B	DTE	192.168.3.2	255.255.255.0

b. Łączenie kabli.

Kabel DCE zostanie podłączony do interfejsu szeregowego 0 routera A. Kabel DTE zostanie podłączony do interfejsu szeregowego 0 routera B. Najpierw należy połączyć oba kable V.35. Kable można podłączyć tylko w jeden – prawidłowy – sposób. Dopasuj styki na kablu męskim do styków na kablu żeńskim i delikatnie je wciśnij. Po złączeniu styków wkręć śruby zgodnie z ruchem wskazówek zegara, aby zapewnić trwałe połączenie złącza.

Podłącz kabel do obu routerów. Trzymając złącze jedną ręką, ustaw odpowiednio złącze kabla i złącze routera tak, aby styki do siebie pasowały. Wciśnij złącze kabla częściowo w złącze routera, a następnie dokręć śruby, aby kabel został całkowicie wsunięty do złącza.

Krok 8 Konfiguracja ustawień IP stacji roboczej

Uwaga: Pamiętaj o zapisaniu istniejących ustawień IP, aby możliwe było ich odtworzenie po zakończeniu ćwiczenia. Ustawienia te obejmują: adres IP, maskę podsieci, domyślną bramę i serwery DNS. Jeśli stacja robocza jest klientem DHCP, nie trzeba zapisywać tych informacji.

Otwarcie okna ustawień IP.

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network (Sieć)**.
- Wybierz ikonę protokołu TCP/IP, która jest powiązana z kartą sieciową tego komputera, i kliknij opcję **Properties (Właściwości)**.
- Kliknij zakładkę **IP Address (Adres IP)** i zakładkę **Gateway (Brama)**.

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

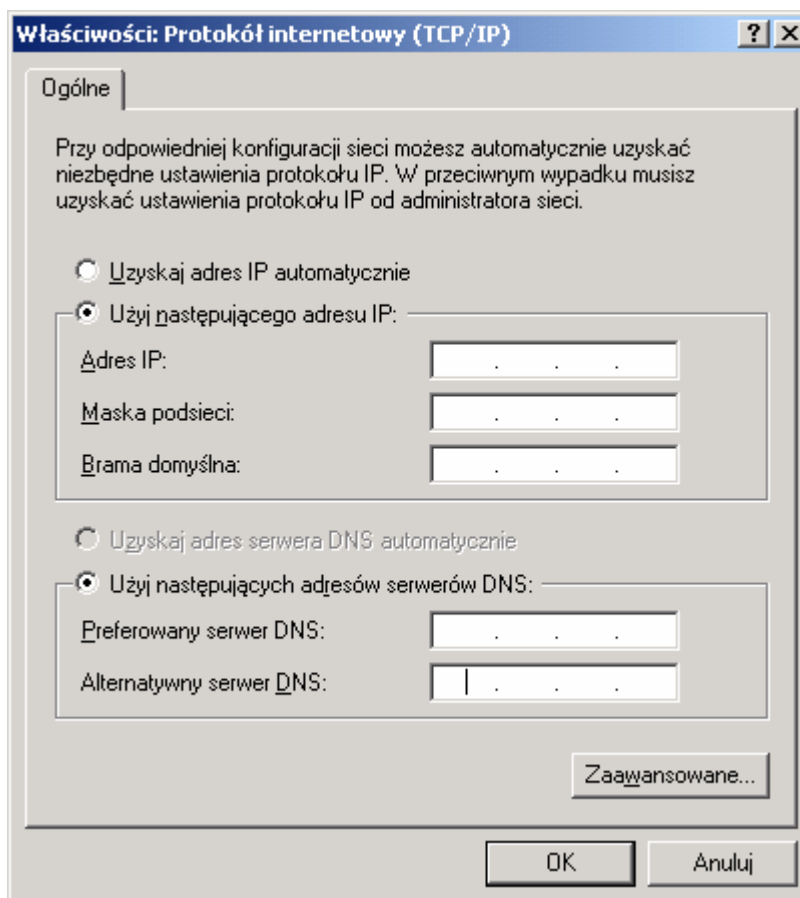
- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie otwórz folder **Network and Dial-up Connections (Połączenia sieciowe i telefoniczne)**.
- Kliknij i otwórz ikonę **Local Area Connection (Połączenie lokalne)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

- Kliknij kolejno opcje: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**, a następnie kliknij ikonę **Network Connection (Połączenie sieciowe)**.

- Wybierz opcję **Local Area Network Connection (Połączenie LAN)**, a następnie kliknij opcję **Change settings of this connection (Zmień ustawienia tego połączenia)**.
- Wybierz ikonę **Internet Protocol (TCP/IP) (Protokół internetowy (TCP/IP))**, która dotyczy karty sieciowej używanego komputera.
- Kliknij przycisk **Properties (Właściwości)**, a następnie kliknij opcję **Use the following IP address (Użyj następującego adresu IP)**.

Spójrz na poniższy przykład:



Ustaw informacje o adresie IP w każdym z komputerów zgodnie z informacjami podanymi w tabeli.

Zwróć uwagę, że adres IP każdego z komputerów należy do tej samej sieci, co adres domyślnej bramy, którą jest interfejs Ethernet routera podłączonego do danego komputera. Domyślna brama jest potrzebna w przypadku sieci lokalnych podłączonych do routera.

Komputer	Adres IP	Maska podsieci	Domyślna brama
Komputer A	192.168.1.2	255.255.255.0	192.168.1.1
Komputer B	192.168.2.2	255.255.255.0	192.168.2.1

Krok 9 Sprawdzenie, czy komputery mogą komunikować się poprzez sieć WAN

- a. Otwórz okno wiersza poleceń (podobne do okna systemu MS-DOS):

Użytkownicy systemu Windows 95/98/Me powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS).**

Użytkownicy systemu Windows NT/2000 powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń).**

Użytkownicy systemu Windows XP powinni wykonać następujące czynności:

Kliknij kolejno opcje: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń).**

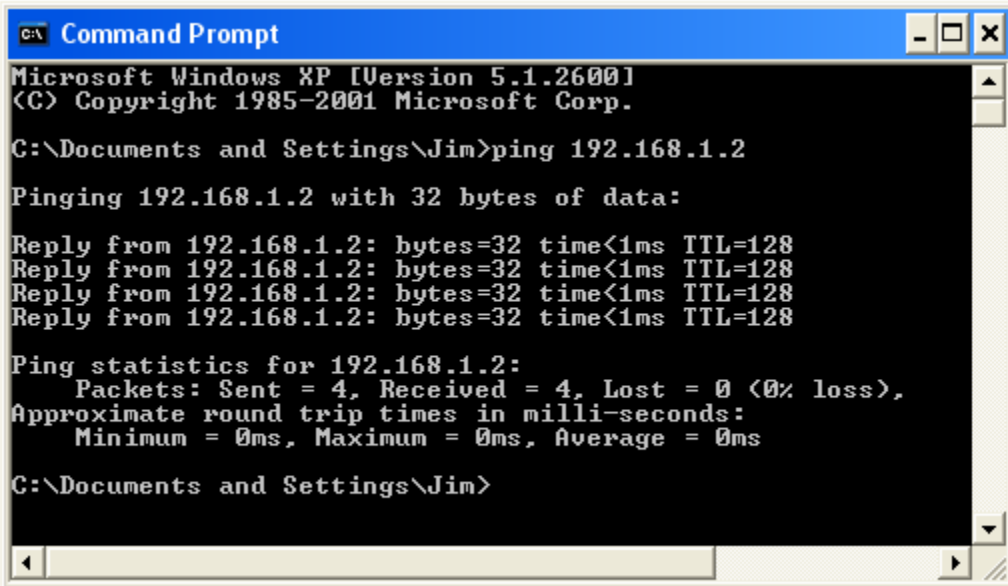
- b. Przeprowadź test połączenia.

Wykonaj polecenie ping, podając jako argument adres IP komputera w drugiej sieci LAN. W wierszu poleceń wpisz następujące polecenie:

```
C:>ping 192.168.1.2
```

W ten sposób zostanie przetestowana łączność IP między komputerami: poprzez przełącznik i router pierwszego komputera, łącze sieci WAN oraz przełącznik i router drugiego komputera.

- c. Sprawdź, czy wyniki są podobne do przedstawionych poniżej. Jeśli nie, sprawdź połączenia komputerów i ich ustawienia TCP/IP. Jaki był wynik działania polecenia ping?



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jim>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

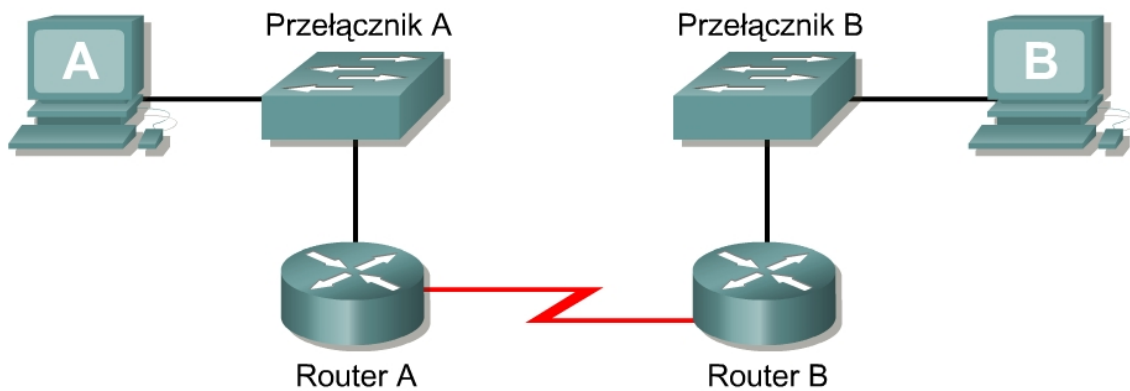
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Jim>
```

Krok 10 Przywrócenie oryginalnych ustawień IP w komputerach, rozłączenie urządzeń i zwinięcie kabli

Ćwiczenie 5.2.3c Rozwiązywanie problemów z połączonymi urządzeniami



Kabel prosty	—————
Kabel szeregowy	————— ⚡
Kabel do konsoli (rollover)
Kabel z przeplotem	- - - - -

Cele

- Utworzenie prostej sieci WAN z routingiem: dwa komputery PC, dwa przełączniki lub koncentratory i dwa routery.
- Skonfigurowanie informacji o adresach IP stacji roboczych.
- Rozpoznanie i rozwiązywanie problemów sieciowych związanych z okablowaniem.
- Rozpoznanie i rozwiązywanie problemów sieciowych związanych z adresami IP stacji roboczych.

Wprowadzenie i przygotowanie

To ćwiczenie obejmuje konfigurowanie prostej sieci WAN o konstrukcji router-router oraz rozwiązywanie problemów związanych z okablowaniem (problemy w warstwie 1) i adresami IP stacji roboczych (problemy w warstwie 3).

Uwaga: Zadaniem instruktora jest ustawienie prawidłowych adresów IP w interfejsach LAN i WAN obu routerów. Router A będzie generował sygnał taktujący jako urządzenie DCE.

Przed rozpoczęciem rozwiązywania problemów należy przygotować sieć do tego ćwiczenia, posługując się materiałami z poprzedniego ćwiczenia „Prosta sieć WAN z routingiem”. Po utworzeniu przedstawionej konfiguracji należy wprowadzić do sieci usterki związane z okablowaniem i adresami IP stacji roboczych. Jeśli praca przebiega w zespołach dwuosobowych, jedna osoba

może ustawić konfigurację i wprowadzić do niej usterki, a druga może spróbować je wykryć i rozwiązać.

Do tego ćwiczenia potrzebne będą następujące elementy:

- dwa przełączniki lub koncentratory typu Ethernet 10BASE-T lub Fast Ethernet;
- dwa routery z interfejsem RJ-45 Ethernet lub Fast Ethernet (lub interfejsem AUI) i co najmniej jednym interfejsem szeregowym;
- transceiver z interfejsem AUI 10BASE-T (DB-15 do RJ-45) do routera z interfejsem AUI sieci Ethernet (seria 2500);
- kilka prostych, z przeplotem oraz nieprawidłowo skonstruowanych lub uszkodzonych kabli w celu podłączenia stacji roboczych i routerów do koncentratora lub przełącznika;
- jeden kabel V.35 żeński (DCE) i jeden męski (DTE) do połączenia routerów.

Krok 1 Ustawienie konfiguracji ćwiczenia (wykonuje uczestnik A)

- Przygotuj ćwiczenie zgodnie ze wskazówkami zawartymi w ćwiczeniu „Budowanie prostej sieci WAN z routingiem”.
- Łącząc urządzenia, używaj różnych kabli kategorii 5, w tym co najmniej jednego kabla z przeplotem i kabla z nieprawidłowymi połączeniami przewodów.
- Konfigurując stacje robocze, na każdym komputerze wprowadź przynajmniej jeden błąd w informacjach dotyczących adresów IP.
- Zapisz wprowadzone usterki w poniższej tabeli. Przewidziano w niej miejsce na maksymalnie trzy problemy związane z okablowaniem i trzy problemy związane z adresami IP. Opisując problem z okablowaniem, określ miejsce, gdzie występuje — na przykład połączenie komputera A z przełącznikiem A. Jeśli problem dotyczy adresu IP, określ, na którym komputerze występuje. W trzeciej kolumnie opisz wprowadzoną usterkę, na przykład użycie kabla z przeplotem, niewłaściwy adres IP lub niewłaściwa domyślna brama.

Rodzaj problemu	Miejsce wystąpienia problemu	Opis problemu
Związany z okablowaniem		
Związany z okablowaniem		
Związany z okablowaniem		
Związany z adresem IP		
Związany z adresem IP		
Związany z adresem IP		

Krok 2 Rozwiązanie przygotowanych problemów (wykonuje uczestnik B)

- a. Sprawdź łączność między stacjami roboczymi.

Za pomocą wiersza poleceń stacji roboczej A wykonaj polecenie ping, podając jako argument adres IP stacji roboczej B. Jeśli zostały wprowadzone usterki, wykonanie tego polecenia nie powinno zakończyć się powodzeniem.

- b. Sprawdź integralność warstwy fizycznej.

Rozpocznij od zagadnień dotyczących warstwy 1 i sprawdź okablowanie między komputerami i przełącznikiem. Sprawdź, czy użyto właściwego typu kabla oraz czy połączenia przewodów są prawidłowe. Sprawdź, czy okablowanie między routerami i przełącznikami jest dobrze połączone. W razie potrzeby wymień kable i popraw połączenia.

- c. Sprawdź integralność warstwy sieciowej.

Sprawdź, czy nie występują problemy z konfiguracją warstwy 3 stacji roboczych. Weź pod uwagę, że router powinien zostać wstępnie skonfigurowany i nie powinien być źródłem problemów. W wierszu poleceń użyj polecenia `winiipcfg` (Windows 95/98/ME) lub polecenia `ipconfig` (Windows NT/2000), aby sprawdzić konfigurację protokołu IP na obu stacjach roboczych. Do sprawdzenia ustawień IP można także użyć aplikacji Network (Sieć) Panelu sterowania. Na obu stacjach roboczych sprawdź adres IP, maskę podsieci i domyślną bramę.

Krok 3 Zapisanie znalezionych problemów w poniższej tabeli (wykonuje uczestnik B)

Rodzaj problemu	Miejsce wystąpienia problemu	Wykonane czynności naprawcze
Związany z okablowaniem		
Związany z okablowaniem		
Związany z okablowaniem		
Związany z adresem IP		
Związany z adresem IP		
Związany z adresem IP		

Krok 4 Zamiana ról w zespole: uczestnicy A i B zamieniają się zadaniami i powtarzają ćwiczenie

Krok 5 Przywrócenie oryginalnych ustawień IP w komputerach, rozłączenie urządzeń i zwinięcie kabli

Ćwiczenie 5.2.7 Ustanawianie połączenia konsoli z routerem lub przełącznikiem



Kabel prosty	—————
Kabel szeregowy	——— ⚡
Kabel do konsoli (rollover)
Kabel z przeplotem	- - - - -

Cele

- Utworzenie połączenia konsoli z komputera PC do routera lub przełącznika przy użyciu właściwego kabla.
- Skonfigurowanie terminala HyperTerminal na komputerze PC.
- Zapoznanie się z interfejsami użytkownika routera i przełącznika.

Wprowadzenie i przygotowanie

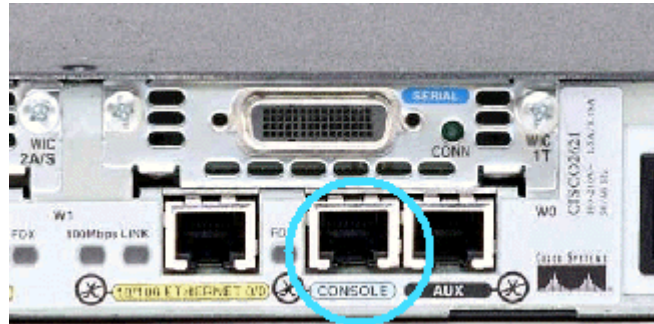
To ćwiczenie umożliwia nabycie umiejętności podłączania komputera PC do routera lub przełącznika w celu ustanowienia sesji konsoli i uzyskania dostępu do interfejsu użytkownika urządzenia sieciowego. Sesja konsoli umożliwia użytkownikowi sprawdzenie i zmianę konfiguracji przełącznika lub routera. Jest to najprostsza metoda podłączania się do jednego z tych urządzeń.

To ćwiczenie należy wykonać dwukrotnie, raz przy użyciu routera i drugi raz — przełącznika, aby móc stwierdzić różnice między interfejsami użytkownika tych urządzeń. Ćwiczenie to należy rozpocząć przy wyłączonych urządzeniach i rozłączonym okablowaniu. Praca przebiega w zespołach dwuosobowych; jedna osoba powinna zająć się routerem, a druga przełącznikiem. Potrzebne będą następujące elementy:

- stacja robocza ze złączem szeregowym i zainstalowanym terminalem HyperTerminal;
- przełącznik Ethernet 10BASE-T lub Fast Ethernet;
- router Cisco;
- kabel rollover lub kabel konsolowy do podłączenia stacji roboczej do routera lub przełącznika.

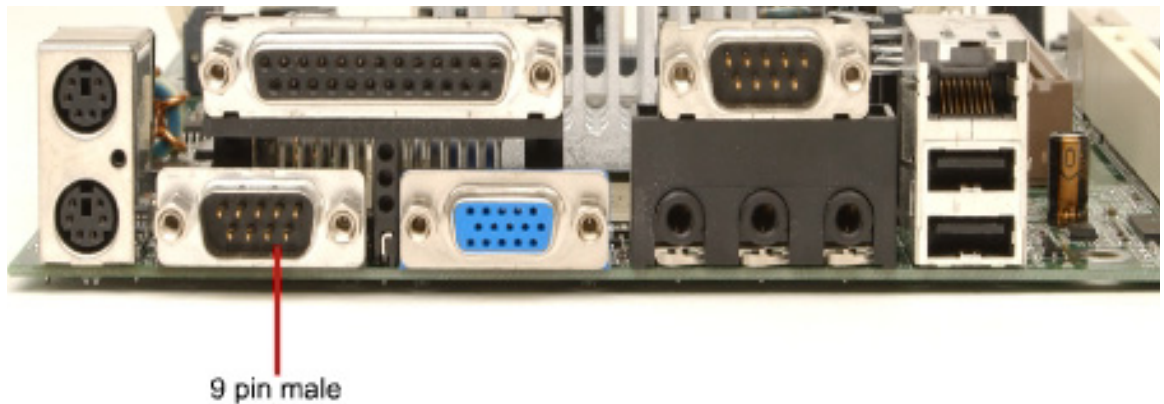
Krok 1 Zapoznanie się ze złączami konsoli routera i przełącznika

- a. Obejrzyj router lub przełącznik i znajdź złącze RJ-45 oznaczone jako „Console”.



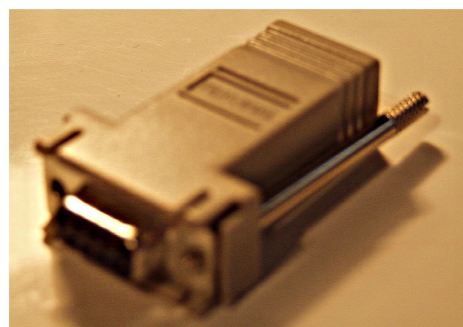
Krok 2 Rozpoznanie złącza szeregowego komputera — może to być COM 1 lub COM 2

- a. Powinno to być złącze męskie z 9 lub 25 stykami, oznaczone jako „serial” lub „COM1”. Może ono być oznaczone, ale nie musi.



Krok 3 Założenie przejściówki RJ-45-DB-9

Jedną stronę przejściówki należy podłączyć do złącza szeregowego komputera, a drugą — do złącza RJ-45 kabla rollover. Jeśli złącze szeregowe w komputerze lub terminalu jest typu DB-25, potrzebna będzie przejściówka RJ-45-DB-25. Przejściówki obu typów są zwykle dostarczane razem z routerem lub przełącznikiem firmy Cisco.

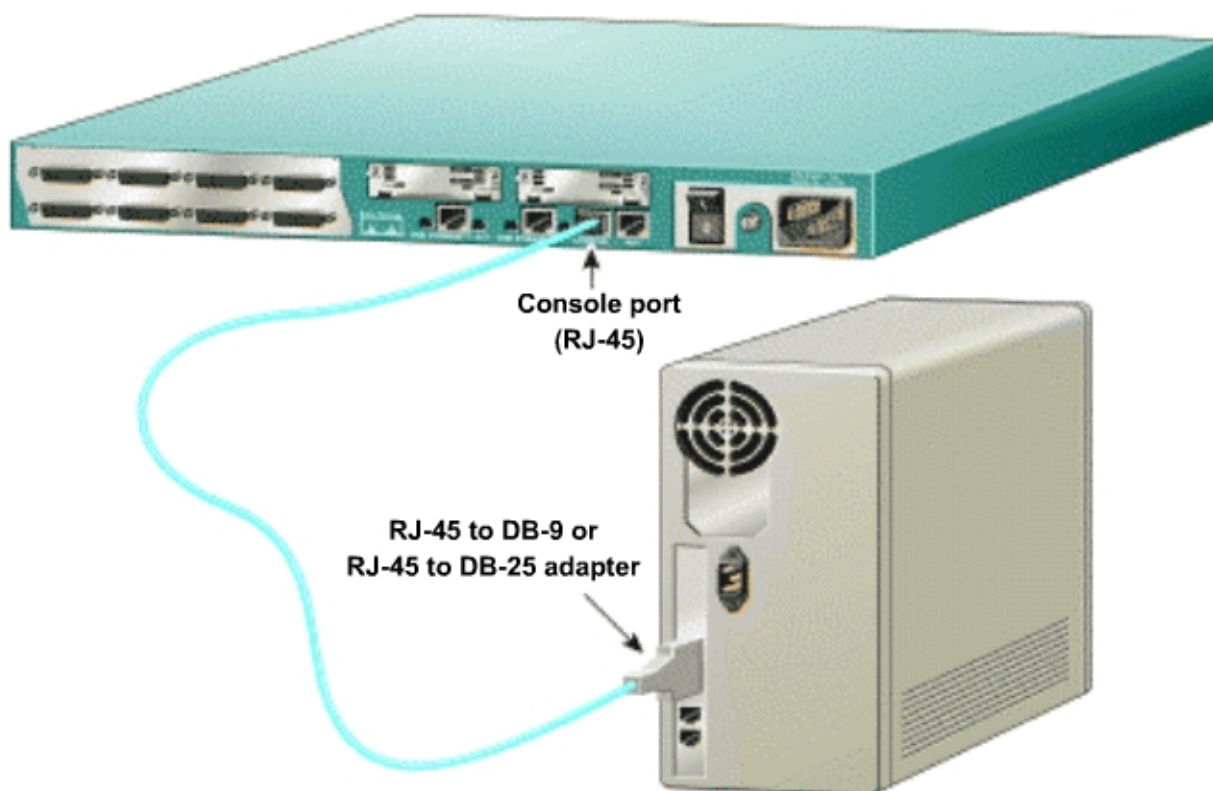


Krok 4 Znalezienie lub wykonanie kabla rollover

Użyj kabla rollover. W razie potrzeby wykonaj taki kabel, tak aby jego długość umożliwiła podłączenie routera lub przełącznika do stacji roboczej.

Krok 5 Połączenie składników okablowania

Podłącz kabel rollover do złącza RJ-45 portu konsoli routera lub przełącznika. Podłącz drugi koniec kabla rollover do przejściówki RJ-45-DB-9 lub RJ-45-DB-25. Podłącz przejściówkę do złącza DB-9 lub DB-25 portu szeregowego komputera (w zależności od tego, które złącze jest dostępne w komputerze).

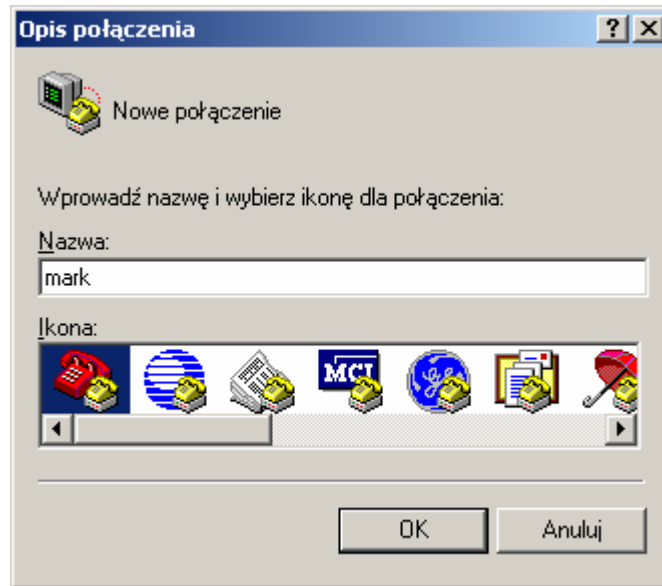


Krok 6 Uruchomienie programu HyperTerminal na komputerze

- a. Włącz komputer.
- b. Na pasku zadań systemu Windows znajdź program **HyperTerminal**:
Kliknij kolejno opcje **Start > Programs (Programy) > Accessories (Akcesoria) > Communications (Komunikacja) > Hyper Terminal**.

Krok 7 Nazwanie sesji programu HyperTerminal

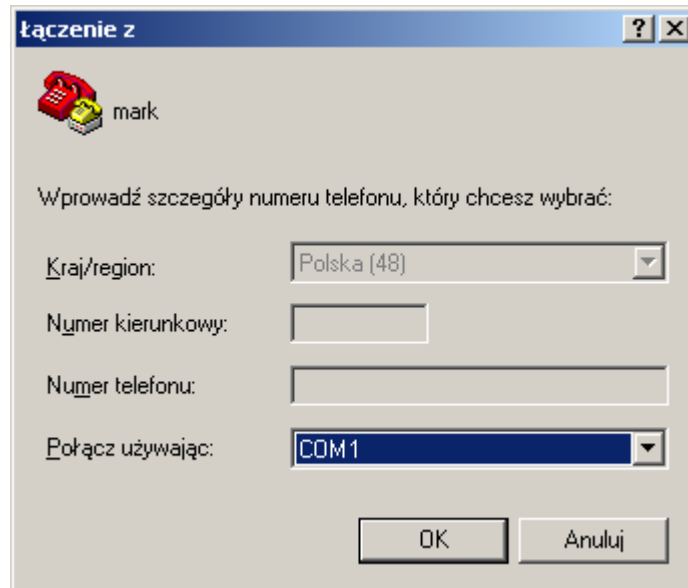
W oknie podręcznym „Connection Description” („Opis połączenia”) w polu Name (Nazwa) wprowadź nazwę sesji i kliknij przycisk **OK**.



Krok 8 Określenie interfejsu łączącego z komputerem

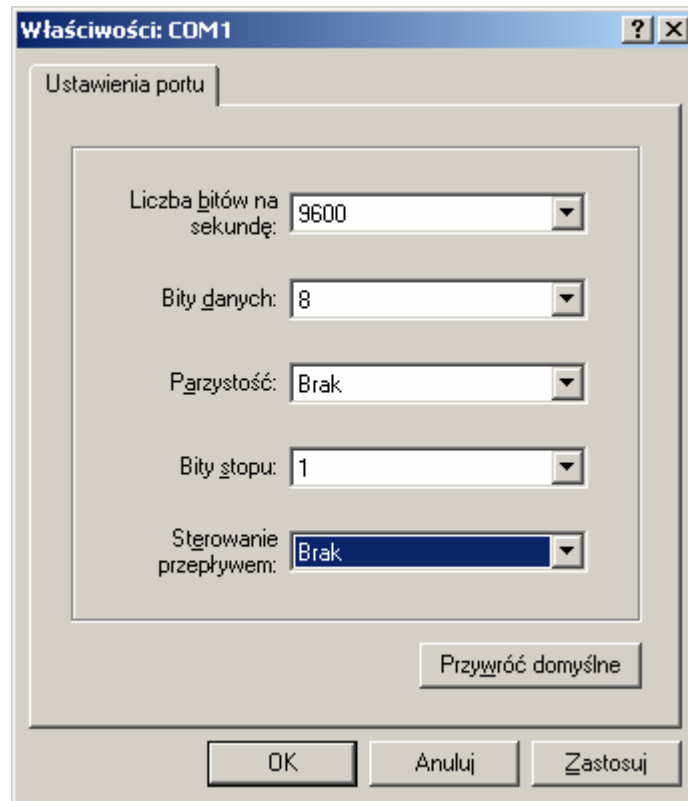
W oknie podręcznym „Connect To” („Połącz z”) użyj strzałki w polu Connect using (Połącz używając), aby wybrać opcję **COM1**, a następnie kliknij przycisk **OK**.

Uwaga: Może zaistnieć konieczność ustawienia wartości **COM2** — w zależności od tego, który port w komputerze jest używany.



Krok 9 Określenie właściwości połączenia interfejsu

- a. W oknie podręcznym „COM1 Properties” („Właściwości COM1”) użyj strzałek, aby wybrać następujące wartości:
 - Bits per second (Liczba bitów na sekundę) = **9600**
 - Data bits (Bity danych) = **8**
 - Parity (Parzystość) = **Brak**
 - Stop bits (Bity stopu) = **1**
 - Flow control (Sterowanie przepływem) = **Brak**
- b. Kliknij przycisk **OK**.



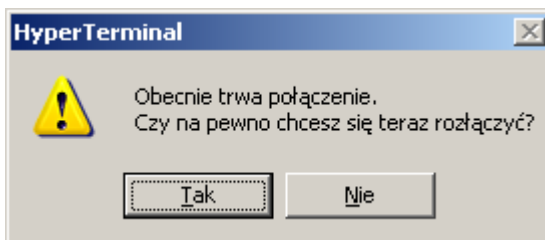
- c. Gdy pojawi się okno sesji programu HyperTerminal, włącz router lub przełącznik. Jeśli router lub przełącznik jest już włączony, naciśnij klawisz **Enter**. Powinna pojawić się odpowiedź routera lub przełącznika. Jeśli odpowiedź się pojawi, oznacza to, że połączenie zostało wykonane prawidłowo.

Krok 10 Zapoznanie się z interfejsami użytkownika routera i przełącznika

- a. Zapoznaj się z interfejsem użytkownika.
- b. Jeśli używany jest router, jaki jest znak zachęty? _____
- c. Jeśli używany jest przełącznik, jaki jest znak zachęty? _____

Krok 11 Zamknięcie okna sesji

- a. Aby zakończyć sesję konsoli w sesji programu HyperTerminal, wybierz kolejno opcje:
File (Plik) > Exit (Zakończ).
- b. Gdy pojawi się okno podręczne programu HyperTerminal z ostrzeżeniem o rozłączeniu, kliknij przycisk **Yes (Tak)**.



- c. Zostanie wyświetlone pytanie o to, czy sesja ma zostać zapisana. Wybierz opcję **No (Nie)**.

Krok 12 Wyłączenie routera lub przełącznika i zwinięcie kabli

Ćwiczenie 7.1.2 Dekodowanie przebiegu

Cele

Uporządkowanie wiadomości na temat mediów sieciowych, warstw 1, 2 i 3 modelu OSI oraz sieci Ethernet. Cel ten zostanie zrealizowany poprzez zapisanie kształtu przebiegu cyfrowego odpowiadającego ramce Ethernet i zdekodowanie go. Uczestnicy kursu wykonają następujące czynności:

- Powtórzenie wiadomości o systemach liczbowych, warstwach OSI i metodach kodowania (materiał z modułu 1).
- Zapoznanie się ze sposobem dekodowania kształtu przebiegu z powrotem na postać binarną, uporządkowanie danych binarnych i zidentyfikowanie granic między polami ramki Ethernet (materiał z modułu 2).
- Zdekodowanie pola Długość/Typ ramki Ethernet, zlokalizowanie oraz odczytanie danych RFC i zdekodowanie warstwy 3 na podstawie kształtu przebiegu (materiał z modułu 3).
- Użycie analizatora protokołów (materiał z modułu 4).

Wprowadzenie i przygotowanie

Uczestnik kursu sieciowego ma okazję zapoznać się z następującymi nowymi pojęciami:

- model OSI,
- media sieciowe i sygnały,
- sieć Ethernet,
- protokoły TCP/IP.

Administratorzy sieci, technicy i inżynierowie mogą nauczyć się, jak rozwiązywać problemy sieciowe za pomocą oprogramowania do analizy protokołów. Oprogramowanie do analizy protokołów umożliwia przechwytywanie i interpretację danych na poziomie ramki, dzięki czemu możliwe jest zrozumienie, co dzieje się w badanej, sprawiającej kłopoty sieci. Ręczne dekodowanie sygnału umożliwia lepszy wgląd w czynności wykonywane automatycznie przez oprogramowanie. Z tego powodu ćwiczenie to stanowi solidną podstawę do dalszej nauki rozwiązywania problemów sieciowych.

W celu przechwycenia sygnałów przesyłanych w sieci Ethernet do kabla koncentrycznego sieci Ethernet 10BASE2 został podłączony oscyloskop cyfrowy. Istnieje co prawda możliwość przechwycenia sygnału w skrętkach sieci 10BASE-T i 100BASE-TX, jednak kabel koncentryczny pozwala uzyskać najmniej zakłócone i najbardziej czytelne informacje o kształcie przebiegu. Te dane są dostępne u instruktora. Dekodowanie kształtu przebiegu jest ważnym krokiem na drodze do zrozumienia sposobu działania sieci.

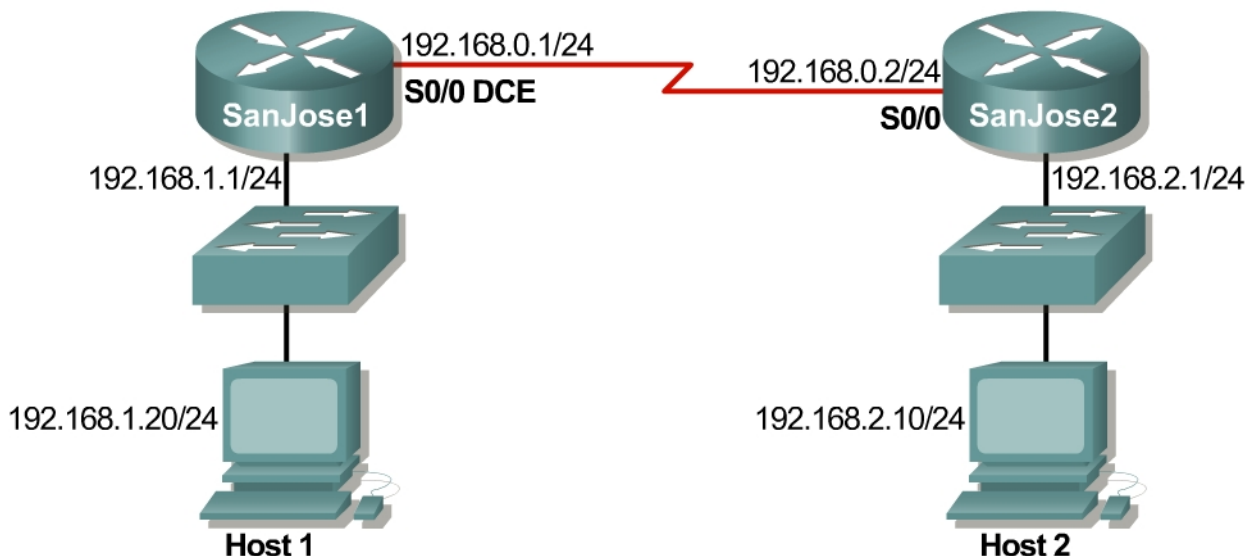
Do wykonania pierwszej części ćwiczenia niezbędna jest niniejsza instrukcja i wydruk przebiegu sygnału, na którym uczestnicy będą mogli zapisywać uwagi podczas jego dekodowania. Ostatnim zadaniem w tym ćwiczeniu jest użycie analizatora protokołów Fluke Protocol Inspector lub podobnego.

Uwaga: Instrukcja do tego ćwiczenia liczy ponad 20 stron i zawiera doskonały materiał uzupełniający związany z następującymi zagadnieniami:

- systemy liczbowe, w tym dwójkowy, dziesiętny i szesnastkowy;
- 7-warstwowy model OSI z (z przykładami);
- metody sygnalizacji i kodowania (kodowanie Manchester w sieciach Ethernet).

Instrukcję do ćwiczenia można pobrać z lokalnego serwera Akademii w instytucji realizującej wersję 3.0 programu nauczania lub z witryny Cisco Academy Connection. Należy także pobrać przebieg sygnału, który ma być dekodowany, w sieci Ethernet. Instruktor udzieli pomocy dotyczącej uzyskania instrukcji i przebiegu sygnału.

Ćwiczenie 7.1.9a Wprowadzenie do programu Fluke Network Inspector



Cele

To ćwiczenie ma na celu zapoznanie się z programem Network Inspector (NI) firmy Fluke Networks, służącym do wykrywania urządzeń sieciowych w domenie rozgłoszeniowej i analizowania ich pracy. W tym ćwiczeniu zostaną przedstawione podstawowe funkcje programu. Mogą one często znaleźć zastosowanie podczas rozwiązywania problemów w pozostałych ćwiczeniach.

Wprowadzenie i przygotowanie

Oprogramowanie Network Inspector rozróżnia stacje robocze, serwery, drukarki sieciowe, przełączniki i zarządzane koncentratory, jeśli zostały im przypisane adresy sieciowe.

Wskazówki dotyczące przeprowadzenia tego ćwiczenia.

- 1) Użyj programu Network Inspector w małej, kontrolowanej sieci LAN. Sieć ta została skonfigurowana przez instruktora w zamkniętym środowisku laboratoryjnym w sposób przedstawiony na powyższym rysunku. Minimalna konfiguracja powinna składać się ze stacji roboczej, przełącznika i routera.
- 2) Aby zapoznać się z innymi, bardziej zróżnicowanymi sytuacjami, wykonaj opisane czynności w większym środowisku, takim jak sieć klasowa lub szkolna. Przed próbą uruchomienia programu NI w szkolnej sieci LAN uzyskaj zgodę instruktora i administratora sieci.

Poniżej znajduje się lista punktów, które należy uwzględnić:

1. Program Network Inspector wykrywa urządzenia w podsieci lub w sieci VLAN. Nie są wykrywane urządzenia znajdujące się poza routerem. Zatem nie zostanie sporządzony spis wszystkich urządzeń znajdujących się w sieci szkoły, chyba że cała sieć znajduje się w jednej podsieci.
2. Program Network Inspector nie jest produktem firmy Cisco ani też jego działanie nie ogranicza się do wykrywania urządzeń firmy Cisco.

3. Program Network Inspector służy do wykrywania urządzeń, ale nie umożliwia ich konfigurowania. Nie można go używać do zmiany konfiguracji jakichkolwiek urządzeń.

Wyniki przedstawione w tej instrukcji służą wyłącznie jako przykład. Uzyskane rzeczywiste wyniki będą się różnić w zależności od liczby urządzeń, ich adresów MAC, nazw hostów oraz podłączonej sieci LAN.

Przedstawiony w tym ćwiczeniu program Network Inspector firmy Fluke Networks może być przydatny w kolejnych ćwiczeniach dotyczących rozwiązywania problemów, a także w rzeczywistych sytuacjach. Oprogramowanie Network Inspector jest cennym uzupełnieniem programu nauczania Akademii. Prezentuje przy tym typowe funkcje dostępne w innych produktach znajdujących się na rynku.

Program Network Inspector musi być zainstalowany przynajmniej na jednym hoście. Jeśli ćwiczenie wykonywane jest w parach, zainstalowanie programu na obu komputerach powoduje, że każda osoba może samodzielnie wykonywać wszystkie czynności opisane w tej instrukcji. Upewnij się, że podczas instalacji programu Network Inspector został wybrany zarówno moduł konsoli, jak i agenta.

Program Console może znajdować się na dowolnym komputerze, którego konfiguracja IP oraz ustawienia zabezpieczeń umożliwiają połączenie z modułem agenta. Ciekawym ćwiczeniem mogłoby być uzyskanie dostępu przez program Console za pośrednictwem łącza szeregowego i załadowanie bazy danych z innego programu Agent. Przy użyciu programu Console uczestnik kursu może odczytać inną bazę danych niż ta, która jest aktualnie używana na komputerze lokalnym.

Krok 1 Konfigurowanie sieci wydzielonej lub podłączenie stacji roboczej do szkolnej sieci LAN

Opcja 1. Jeśli wybrane jest zamknięte środowisko laboratoryjne, podłącz sprzęt w sposób pokazany powyżej i załaduj pliki konfiguracyjne na odpowiednie routery. Te pliki mogą być już załadowane na routerach. W przeciwnym wypadku uzyskaj je od instruktora. Ustawienia zawarte w plikach powinny być zgodne ze schematem adresowania IP przedstawionym na powyższym rysunku i w poniższej tabeli.

Skonfiguruj stację roboczą zgodnie ze specyfikacjami podanymi w poniższej tabeli.

Host nr 1	Host nr 2
Adres IP: 192.168.1.20	Adres IP: 192.168.2.10
Maska podsieci: 255.255.255.0	Maska podsieci: 255.255.255.0
Domyślna brama: 192.168.1.1	Domyślna brama: 192.168.2.1

Ponieważ oprogramowanie wykrywa urządzenia w sieci, im więcej urządzeń zostanie dołączonych do sieci, tym obszerniejsza będzie prezentacja.

Jeśli jest to możliwe, dodaj kolejne hosty do obu sieci LAN.

Opcja 2. Jeśli wybrano opcję 2, podłączenie do szkolnej sieci LAN, podłącz po prostu stację roboczą, na której zainstalowano program Network Inspector lub Protocol Expert, bezpośrednio do znajdującego się w klasie przełącznika lub do gniazdka szkolnej sieci LAN.

Krok 2 Uruchomienie programów Network Inspector i Agent

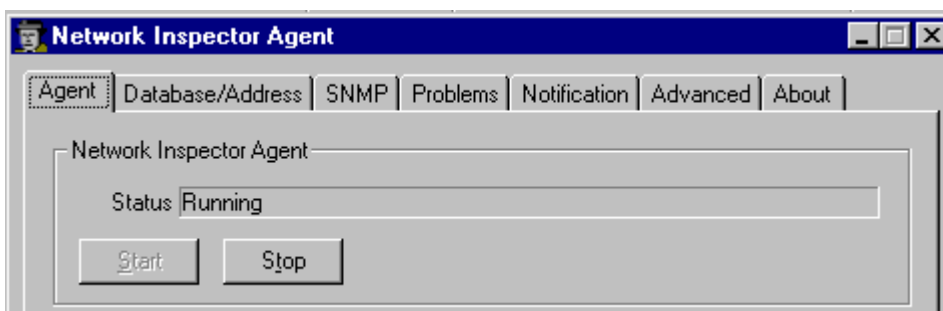
Z menu Start uruchom program Network Inspector Console.

Kliknij przycisk **Agent** znajdujący się po lewej stronie paska narzędzi, aby uruchomić program Agent.



Jeśli jest to konieczne, wybierz w oknie zakładkę **Agent**, a następnie kliknij przycisk **Start**, po czym obserwuj pole **Status (Stan)**, dopóki nie zostanie wyświetlony komunikat o uruchomieniu programu Agent (patrz poniższy rysunek). Uruchamianie może potrwać kilka minut.

Zwróć uwagę na stan programu Agent wyświetlany w dolnej części okna programu Console. Przyjrzyj się uważnie fragmentowi ekranu zamieszczonemu w kroku 3 i zauważ, że program Agent został uruchomiony o godzinie 9:57 PM.

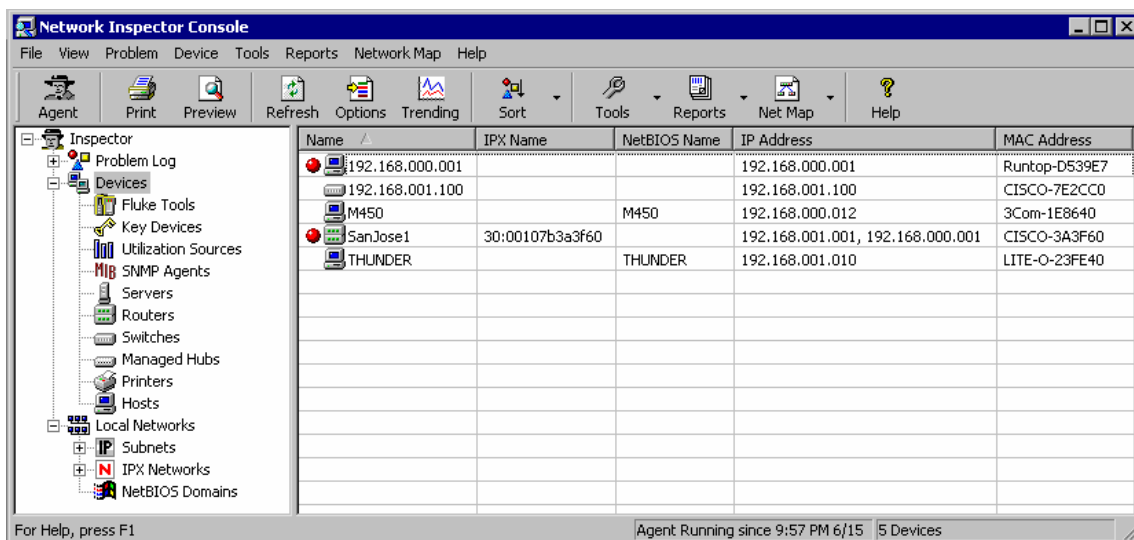


Użyj przycisku **Close (Zamknij)** w prawym dolnym rogu okna programu Agent, aby go zamknąć. W niektórych wersjach może to być przycisk **Hide (Ukryj)**. Nie należy używać przycisku **Stop (Zatrzymaj)**, gdyż w takim przypadku proces wykrywania zostanie przerwany.

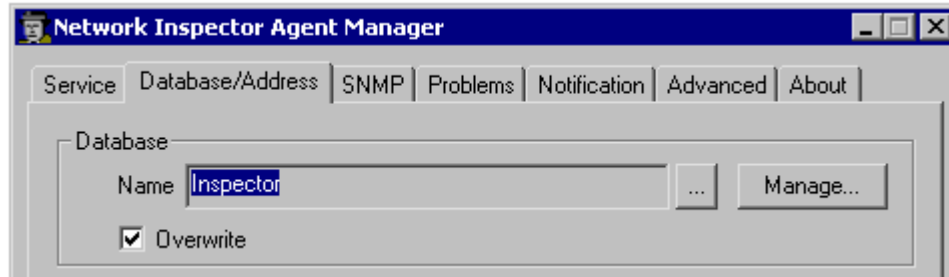
Krok 3 Wykrywanie urządzeń w sieci

Program Network Inspector służy do zbierania danych o sieci, zarówno w sposób pasywny, jak i aktywny. Zanim zostaną wyświetlone informacje o urządzeniu, musi upłynąć pewien czas. Tak mała sieć powinna zostać wykryta w przeciągu minuty lub dwóch minut. Aktywne zbieranie danych statystycznych rozpoczyna się po 10 minutach. Zebranie większości danych z rzeczywistej sieci produkcyjnej może potrwać 30 minut lub więcej.

Po kilku minutach w oknie programu Console powinno rozpocząć się wyświetlanie informacji o sieci. W poniższym przykładzie dodano dwie dodatkowe stacje robocze.



Uwaga: W oknie mogą być wyświetlane wpisy pochodzące z poprzednich sesji. Minie kilka minut, zanim wpisy będą odzwierciedlać konfigurację sieci. W oknie programu Agent na zakładce **Database/Address (Baza danych/Adres)** znajduje się pole wyboru **Overwrite (Zastąp)**. Jeśli to pole jest zaznaczone, bieżąca zawartość bazy danych zostanie usunięta, a nowy zestaw danych będzie ładowany w miarę upływu czasu, po rozpoczęciu wykrywania przez program Agent. W przeciwnym wypadku, nowe dane będą w miarę wykrywania dołączane do danych już znajdujących się w bazie danych.

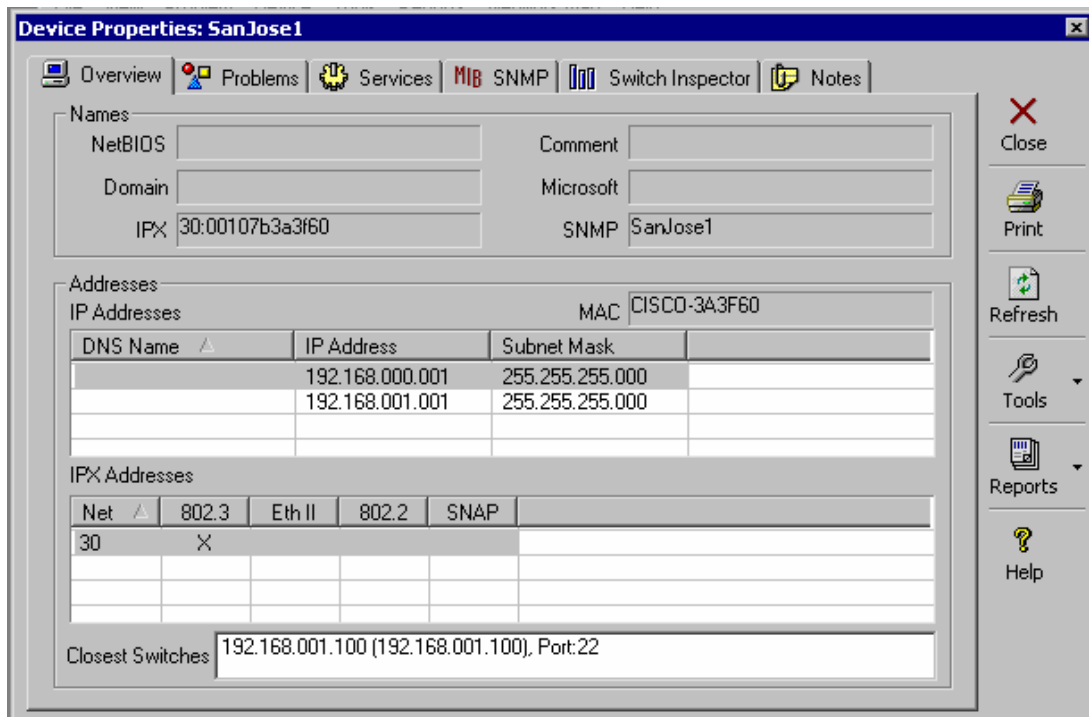


W powyższym przykładzie zwróć uwagę na nazwy hostów: M450, SanJose1 i Thunder. W trakcie ćwiczenia zostaną wykryte hosty o innych nazwach. Zwróć także uwagę na adresy IP i adresy MAC każdego wykrytego urządzenia. Jest oczywiste, że zarówno komputer SanJose1, jak i SanJose2 mają dwa adresy IP przypisane do interfejsu sieci LAN.

Zauważ również, że program NI nie bada sieci poza granicami interfejsu routera. Program zbiera informacje tylko z urządzeń współdzielących domenę rozgłoszeniową z komputerem, na którym uruchomiono program NIC.

Krok 4 Badanie właściwości urządzenia

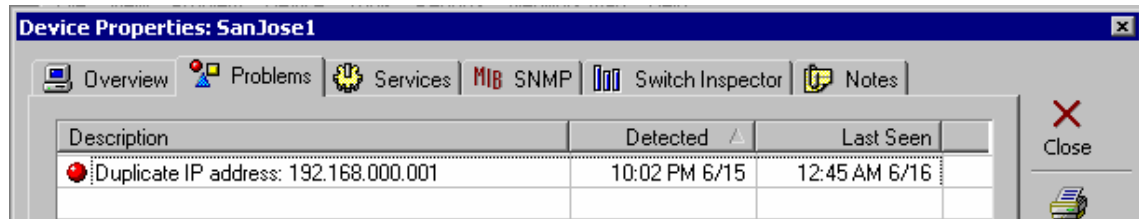
Kliknij dwukrotnie nazwę routera i przejrzyj dostępne właściwości urządzenia (Device Properties). Pamiętaj, że wyniki zależeć będą od urządzeń znajdujących się w podsieci sieci LAN.



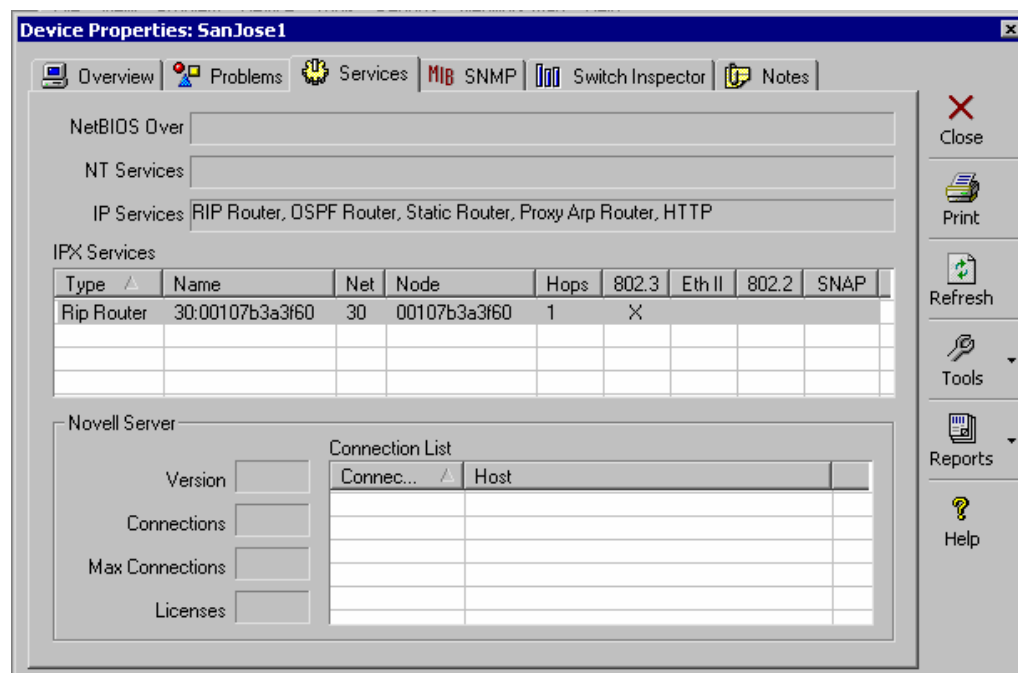
Zakładka **Overview (Przegląd)** na powyższym rysunku przedstawia adresy IP, adres IPX, podłączone sieci IPX, typ używanej ramki w sieci IPX (w tym przypadku 802.3) i adres MAC. Zauważ, że identyfikator OUI w powyższym przykładzie został zastąpiony nazwą producenta.

Najbliższe przełączniki zostaną wyświetlone tylko wtedy, gdy w programie Network Inspector podano prawidłowy dla nich łańcuch wspólnoty (Community String) SNMP.

Na zakładce **Problems (Problemy)** widać, że jeden z adresów IP został w sieci użyty dwukrotnie. Dzieje się tak, jeśli opcjonalny host został skonfigurowany przez uczestnika kursu zgodnie z opisem z kroku 1. Czerwona kropka po lewej stronie opisu wskazuje, że wystąpił problem.



Na zakładce **Services (Usługi)** przedstawione są usługi IP i IPX uruchomione na routerach.

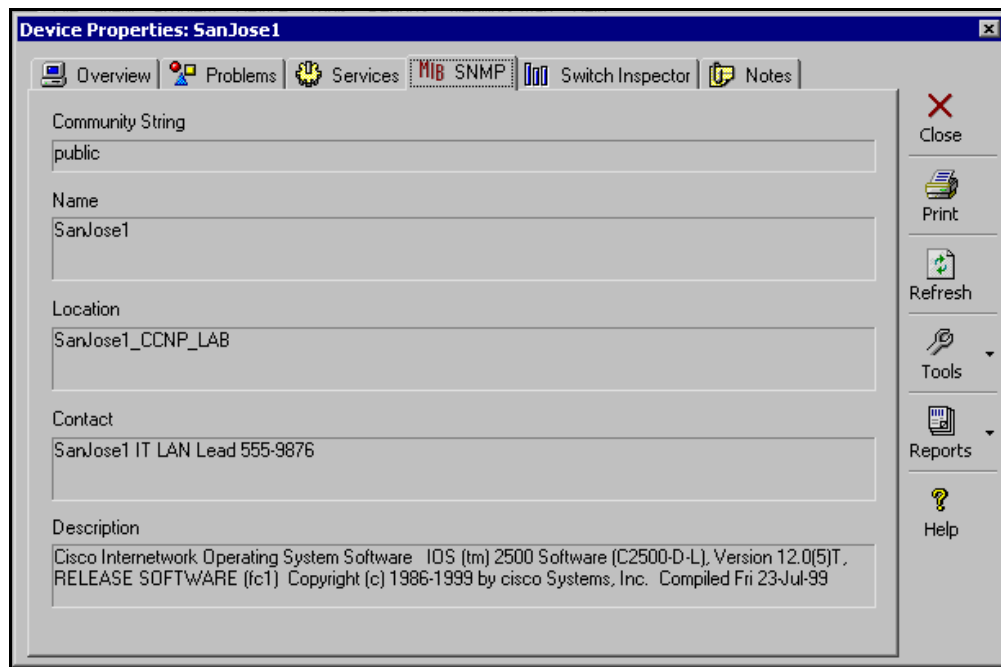


Wśród usług IP (IP Services) na powyższym przykładowym ekranie znajduje się usługa **serwera HTTP dla protokołu IP**. Oznacza to, że dostęp do routera można uzyskać za pośrednictwem przeglądarki sieci WWW.


W polu IPX Services jest podany identyfikator sieci IPX (30), adres węzła (MAC), typ ramki i to, że uruchomiona jest usługa IPX RIP.

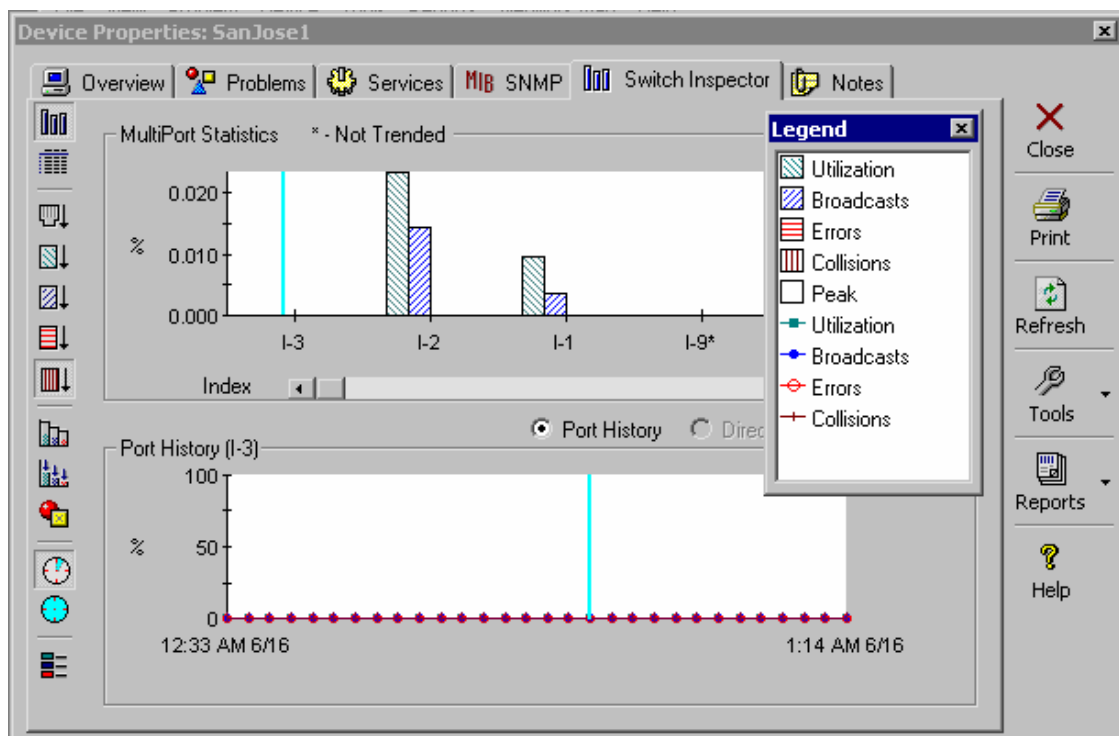
Dolna część okna przedstawia informacje, które zostałyby przedstawione, gdyby urządzenie było serwerem Novell. Serwer wyposażony w kilka kart sieciowych przyłączonych do odrębnych sieci działa jako router lub most.


Zakładka **MIB SNMP** zawiera informacje dotyczące protokołu SNMP, a także informacje o systemie IOS routera.

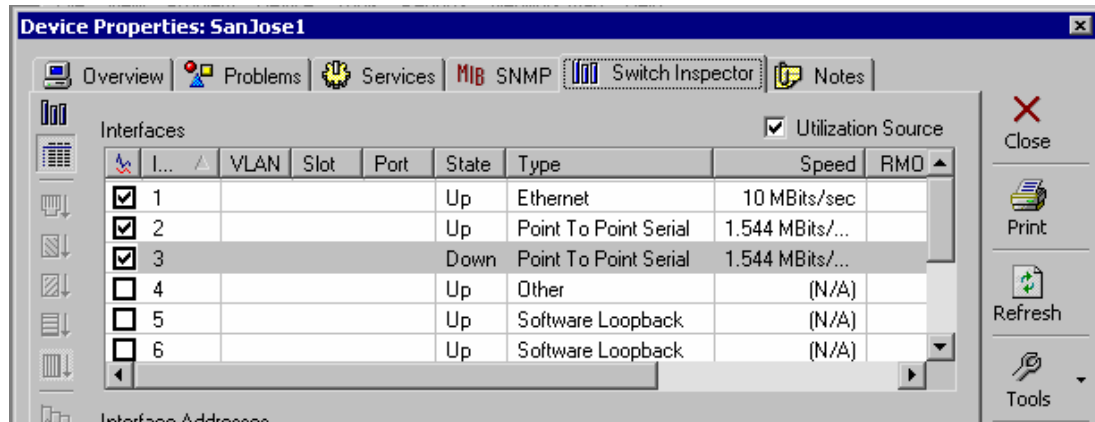



Zakładka **Switch Inspector (Inspektor przełącznika)** tworzy szereg wykresów danych zebranych przez interfejsy wybranego urządzenia. Dane nie są zbierane przez pierwszych 10 minut. Testy wykonywane przez funkcję Switch Inspector (Inspektor przełącznika) umożliwiają utworzenie prostych wykresów obrazujących wykorzystanie każdego urządzenia obsługującego protokół SNMP. Szczegółowość informacji dostarczanych przez ten test zależy od tego, które zmienne MIB są obsługiwane przez wybrane urządzenie. Na przykład SanJose1 jest routerem, i dlatego uczestnik kursu nie może wyświetlić adresu żadnego urządzenia podłączonego bezpośrednio do wybranego portu. Przyciski po lewej stronie okna służą do zmiany formatu wykresów. Kliknięcie przycisku

Graph Legend (Legenda wykresu)  w lewym dolnym rogu powoduje wyświetlenie legendy w oknie przestawnym, co widać na zamieszczonym poniżej rysunku.



Po kliknięciu przycisku **TabularView**  (**Widok tabelaryczny**) zostają wyświetlone szczegóły dotyczące każdego interfejsu w wybranym urządzeniu, z uwzględnieniem tego, czy interfejs jest włączony, czy wyłączony. Pole wyboru po lewej stronie każdego wiersza określa, czy dla danego interfejsu są zbierane statystyki dotyczące trendów długookresowych. Przewinięcie okna w prawo pozwala uzyskać informacje o wielkości MTU oraz opis (FastEthernet0/0 lub Token-Ring 0/1).

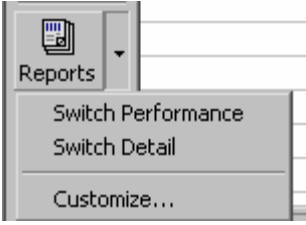




Dwa przyciski wyglądające jak zegary służą do przełączania pomiędzy historią 1- i 24-godzinną. Jeśli program NI był uruchomiony przez dłuższy czas, można dzięki tej opcji uzyskać interesujące porównanie. Ze względu na krótki czas trwania tego ćwiczenia, wyniki przy obu ustawieniach będą w nim miały tę samą wartość.

Kliknięcie przycisku **Reports (Raporty)** znajdującego się na karcie **Switch Inspector (Inspektor przełącznika)** po prawej stronie ekranu powoduje wyświetlenie dwóch opcji. Wybierz opcję **Switch Performance (Wydajność przełącznika)**, aby wyświetlić na ekranie wielostronicowy raport zawierający różne wykresy. Zapoznaj się z wynikami.

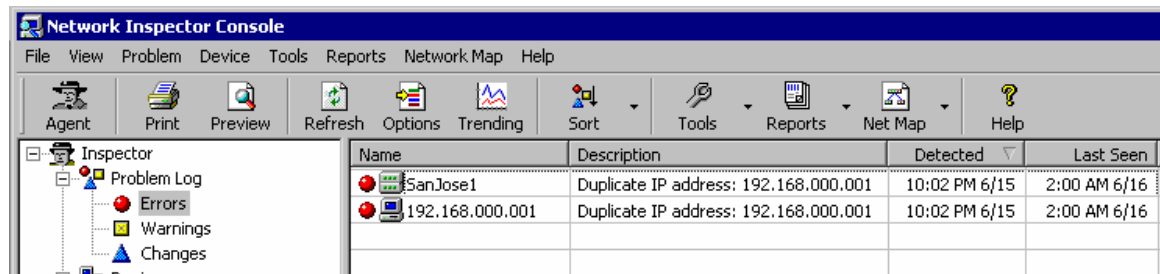
Opcja **Switch Detail (Szczegóły dla przełącznika)** działa tylko w przypadku przełącznika.



Po zapoznaniu się z oknem Device Properties (Właściwości urządzenia) kliknij przycisk **Close (Zamknij)** w prawym górnym rogu, aby wrócić do programu Network Inspector Console.

Krok 5 Zapoznanie się z opcjami dostępnymi na lewym panelu

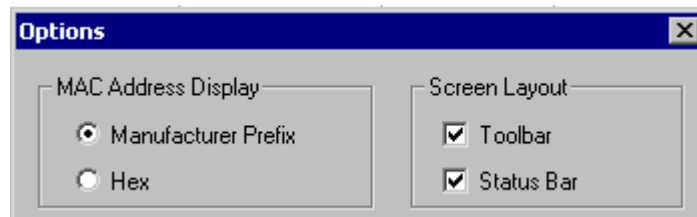
Poeksperymentuj z rozwijaniem i zwijaniem opcji dostępnych w lewym panelu programu Network Inspector Console. Podobnie jak w Eksploratorze, wybranie elementu po lewej stronie powoduje wyświetlenie po prawej stronie dotyczących go szczegółów. W poniższym przykładzie rozwinięcie opcji **Problems Log (Rejestr problemów)** i wybranie opcji **Errors (Błędy)** spowoduje wyświetlenie po prawej stronie urządzeń, w których wystąpiły błędy. Ułatwia to wykrycie urządzenia o zduplikowanym adresie IP.



Wypróbuj różne opcje lewego panelu i zwróć uwagę na informacje wyświetlane w prawym panelu. Z powodu ograniczonej liczby urządzeń niektóre pola będą puste. Spróbuj wykonać te operacje później na większej liczbie urządzeń.

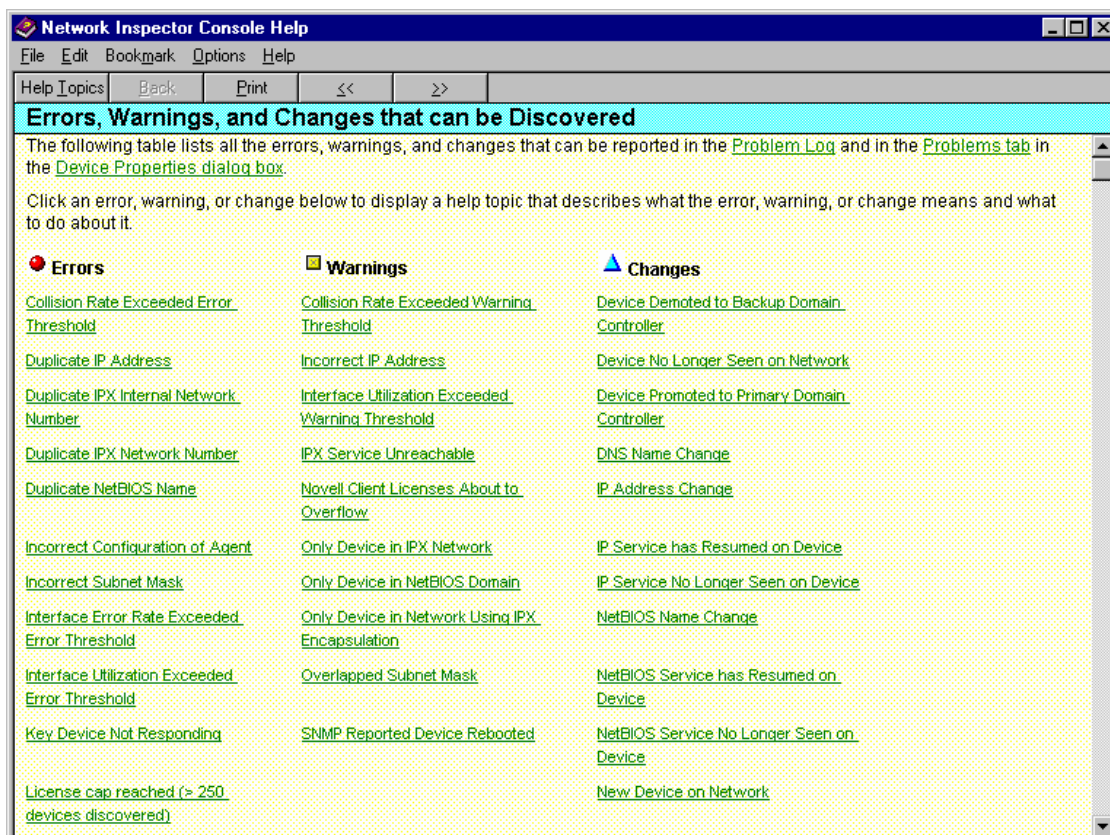
W lewym panelu wybierz opcję **Devices (Urządzenia)**, aby wyświetlić wszystkie urządzenia w prawym panelu. Zwróć uwagę na format adresu MAC.

Kliknij przycisk **Options (Opcje)** na pasku narzędzi lub w menu View (Widok) wybierz Options (Opcje). Zwróć uwagę, że można wybrać opcję **Manufacturer Prefix (Prefiks producenta)** lub **Hex (Szesnastkowo)**. Wybierz inną opcję niż aktualnie wybrana, przejrzyj inne opcje, a następnie kliknij przycisk OK. Zapoznaj się z wynikiem.

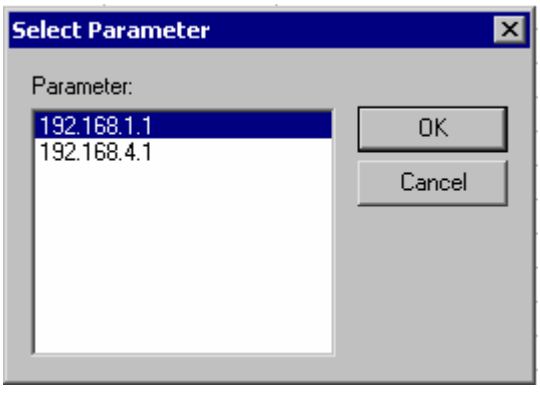


Uzyskiwanie pomocy. W głównym ekranie programu Console sprawdź, czy wybrana jest opcja **Problem Log (Rejestr problemów)** i czy urządzenie wyświetlane w oknie szczegółów zostało podświetlone. Naciśnij klawisz F1, który jest klawiszem funkcji pomocy, aby wyświetlić listę problemów uporządkowanych według kategorii.

Na przykład, jednym z problemów występujących w bieżącej konfiguracji laboratoryjnej zgodnej z przedstawionym wyżej rysunkiem jest zduplikowany adres IP. Aby dowiedzieć się więcej na temat zduplikowanych adresów IP, objawów i czynności, jakie można podjąć, wybierz z listy łącze **Duplicate IP Address (Zduplikowany adres IP)**. W pomocy dołączonej do tego programu znajduje się wiele użytecznych informacji.



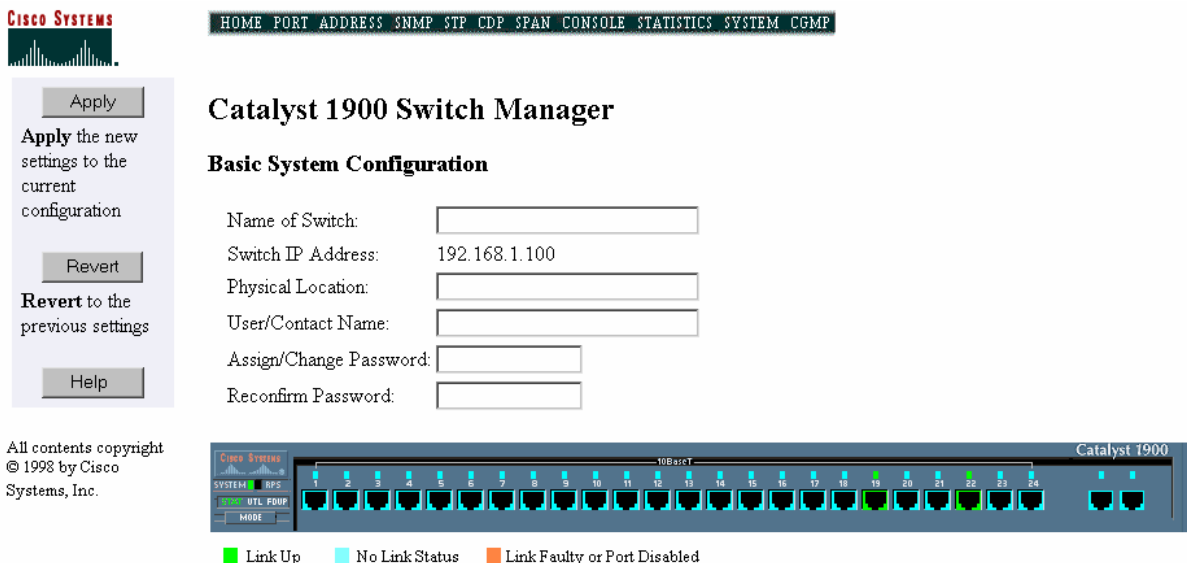
Poświęć chwilę na poeksperymentowanie z przyciskami paska narzędzi **Preview (Podgląd)**, **Sort (Sortowanie)** i **Reports (Raporty)**, znajdującymi się na pasku narzędzi. Działanie tych funkcji powinno być oczywiste. Zwróć szczególną uwagę na możliwości rozwiązywania problemów i możliwości dokumentacyjne, jakie dają te raporty.

<p>Wybierz hosta, a następnie kliknij przycisk Tools (Narzędzia) znajdujący się na pasku narzędzi i wybierz opcję Ping.</p> <p>Zostanie wyświetlone okno Select Parameter (Wybierz parametr) zawierające adresy IP sieci LAN, dla których uczestnik kursu może wywołać funkcję ping. Wybierz adres i kliknij przycisk OK.</p> <p>Zostanie wyświetlone okno wiersza poleceń (MS-DOS) zawierające wyniki.</p> <p>Aby zamknąć nowe okno po zakończeniu pracy, wpisz exit.</p>	
---	--

Spróbuj użyć opcji **Telnet** i **Traceroute**. W oknie programu Console wybierz router lub przełącznik, a następnie z menu Tools (Narzędzia) wybierz polecenie Telnet. Spowoduje to wyświetlenie okna sesji programu Telnet. Opcja Traceroute działa w ten sam sposób.

Wybór opcji **Web** przycisku **Tools (Narzędzia)** spowoduje otwarcie sesji WWW z urządzeniem, jeśli jest na nim włączona funkcja serwera HTTP. W przypadku korzystania z tej opcji nazwą użytkownika jest nazwa hosta, czyli SanJose1 lub SanJose2, a hasłem jest cisco.

W powyższym przykładzie przełącznikiem jest Catalyst 1924 z przypisanym adresem IP. Dlatego po zaznaczeniu przełącznika i wybraniu opcji **Web** zostanie wyświetlone poniższe okno.

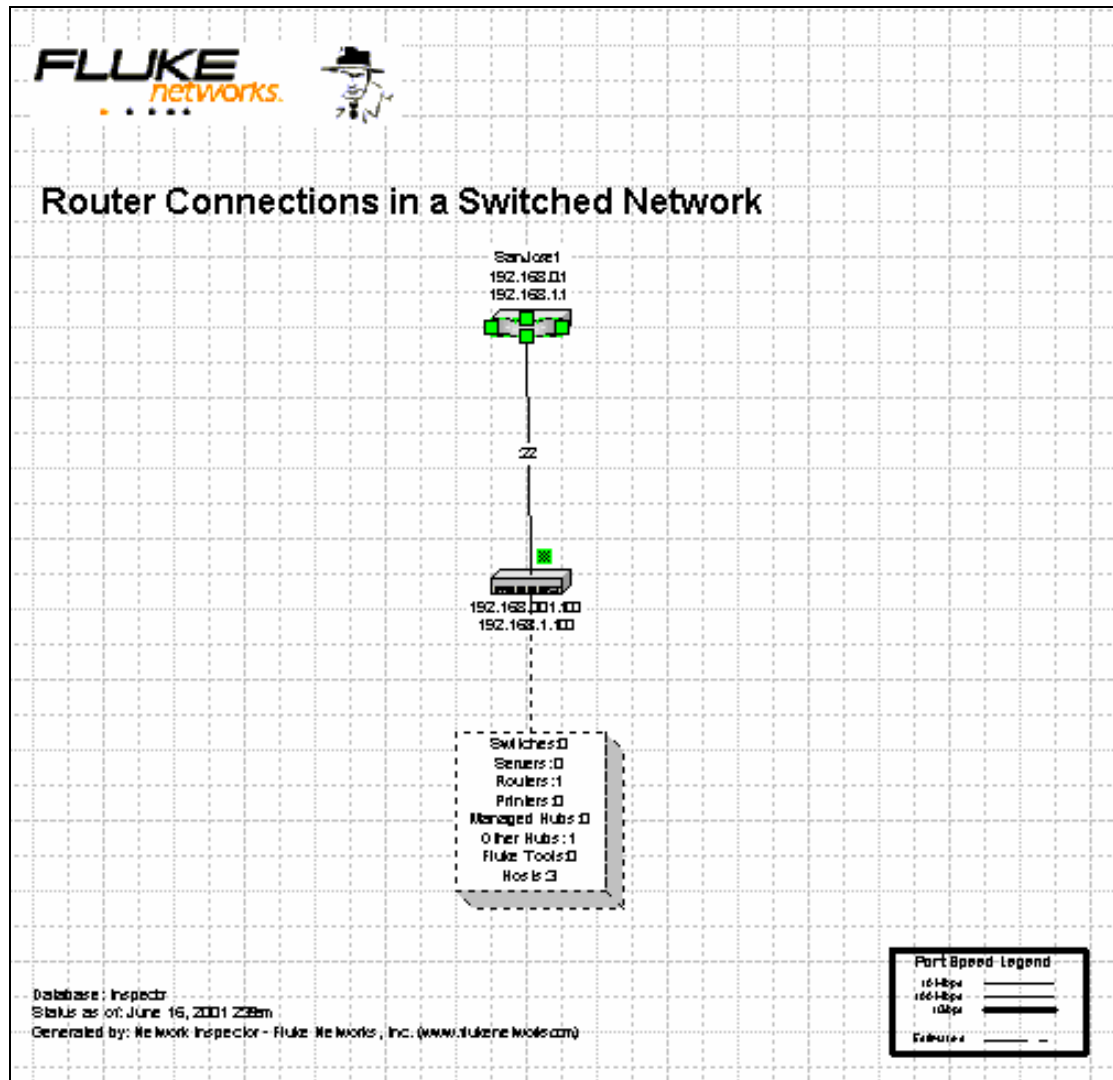


Poeksperymentuj z powyższymi opcjami paska narzędzi, aby zapoznać się z nimi.

Krok 6 Użycie funkcji Net Map (Mapa sieci) i programu Visio do rysowania schematu sieci

Jeśli na komputerze zainstalowany jest program Visio, użycie przycisku **Net Map (Mapa sieci)** spowoduje uaktywnienie programu Visio i utworzenie mapy sieci domeny rozgłoszeniowej. W poniższym przykładzie wybrano opcję „Router Connections in a Switched Network” („Połączenia

routera w sieci przełączanej”) przycisku Net Map (Mapa sieci). Spowoduje to narysowanie sieci niezależnie od tego, czy zawiera ona przełącznik.



Program Visio jest w pełni zintegrowany z programem NI. Oznacza to, że dwukrotne kliknięcie jednego z urządzeń na rysunku wywoła okno Device Properties (Właściwości urządzenia), które było używane w kroku 4.

Krok 7 Dokumentowanie informacji o routerze

Korzystając z umiejętności nabytych wcześniej, wybierz router i spisz następujące informacje, jeśli są one dostępne:

- Jak nazywa się urządzenie? _____
- Jakie usługi IP są uruchomione w urządzeniu?

- Jakie usługi IPX są uruchomione w urządzeniu?

- Jaki jest łańcuch wspólnoty SNMP? _____
- Jaka jest lokalizacja? _____

f. Kto jest osobą kontaktową?

g. Jakie interfejsy są dostępne? _____

h. Jakie interfejsy są włączone?

i. Wymień poniżej wszystkie problemy, które zostały wykryte przez oprogramowanie.

Krok 8 Obserwacja wykrywania urządzeń

Jeśli to możliwe, podłącz dwa przełączniki kablem z przeplotem i obserwuj proces wykrywania nowych urządzeń przez program NI. Jeśli kabel z przeplotem nie jest dostępny, usuń jeden przełącznik i podłącz hosty i router do drugiego przełącznika. Choć takich czynności zazwyczaj nie wykonuje się w środowisku produkcyjnym, tym niemniej wykonaj je teraz, aby zobaczyć, jak zareaguje program NI.

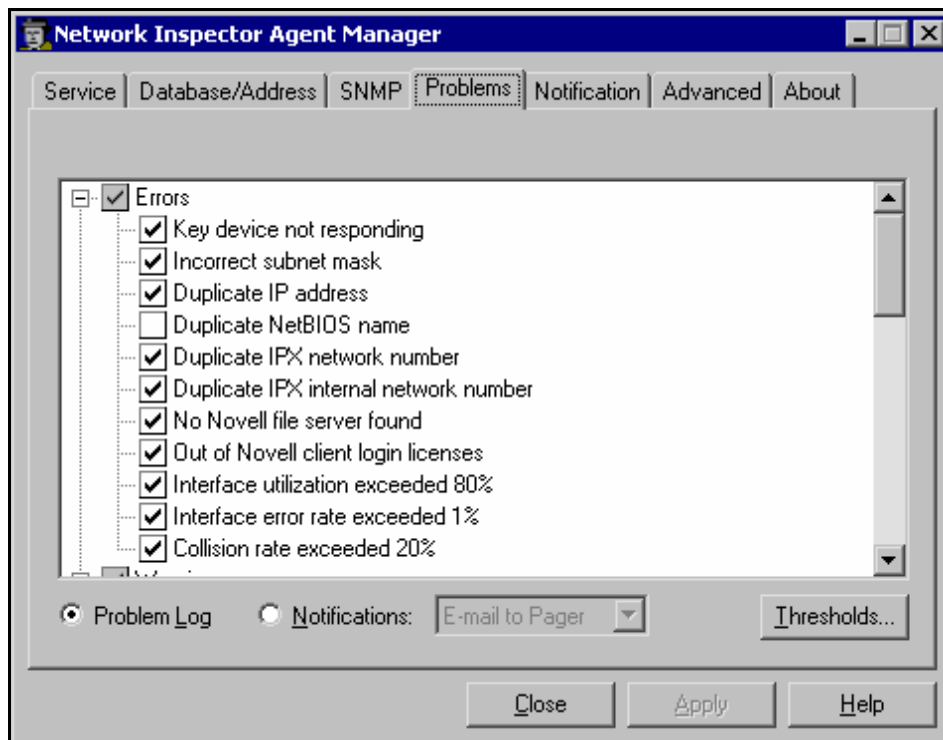
Nowe urządzenia powinny zostać najpierw wyświetlone w postaci niebieskich trójkątów. Wskazuje to, że zostały one właśnie wykryte. W przypadku niektórych urządzeń może zostać wyświetlony żółty prostokąt wskazujący na potencjalny problem. Pamiętaj, że ten proces może potrwać 10 minut lub dłużej.

Na koniec powinny zostać wyświetlone inne podsieci i drugi router.

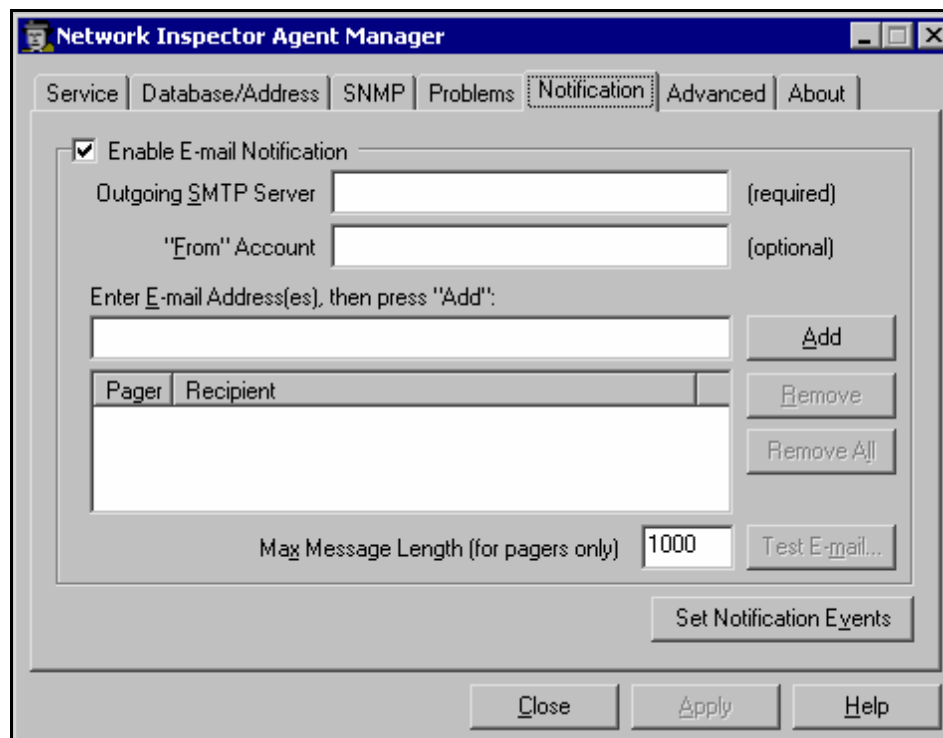
Krok 9 Zatrzymanie przechwytywania i uzyskanie dostępu do zakładki Problems (Problemy) i Notification (Powiadomienie)

Kliknij przycisk **Agent** na pasku narzędzi. Program Agent zbierał dane przez cały ten czas. Kliknij przycisk **Stop (Zatrzymaj)** i potwierdź zamiar, jeśli zostanie wyświetlony monit.

Przejrzyj zakładki, aby zobaczyć, jakie opcje bazy danych mogą zostać ustawione. Zwróć uwagę na zakładkę **Problems (Problemy)** i opcje umożliwiające zawężenie zakresu badania.



Zauważ, że na karcie **Notification (Powiadomienie)** można włączyć opcję wysyłania powiadomień pocztą elektroniczną. Aby użyć tej funkcji, uczestnik kursu będzie potrzebował tych samych informacji, które są wymagane do skonfigurowania internetowego konta pocztowego lub konta pocztowego w programie Outlook.



Jeśli uczestnik kursu ponownie uruchomi program Agent, wykrycie zmian, które zaszły w czasie, gdy program Agent był wyłączony, może potrwać kilka minut.

Krok 10 Eksperymentowanie z programem NI

Poeksperymentuj z programem NI, badając różne urządzenia.

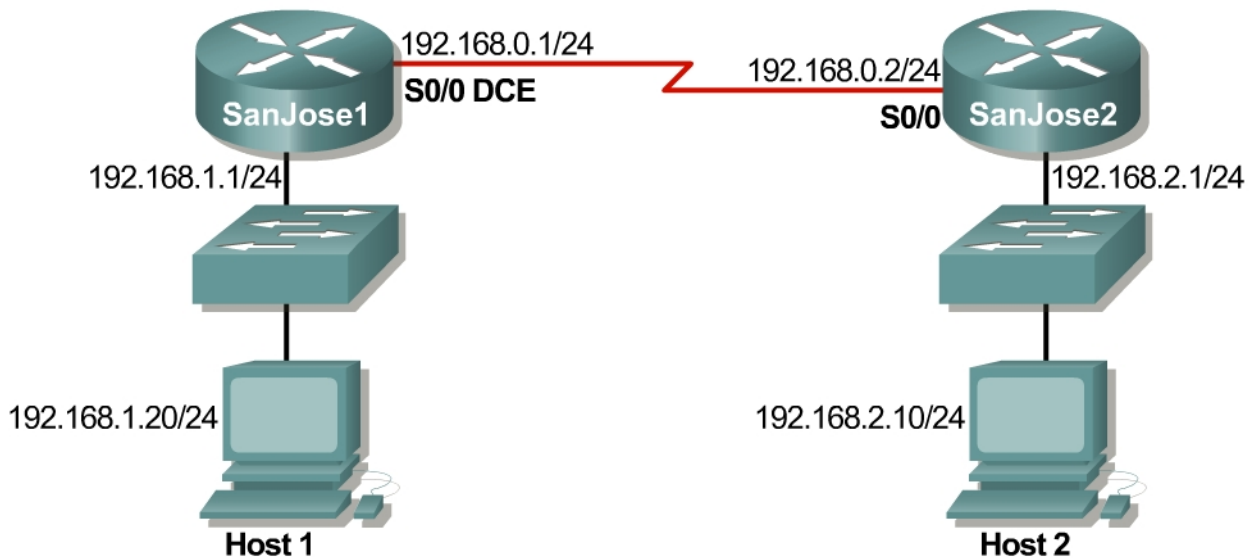
Jeśli program NI jest zainstalowany na komputerach przyłączonych do większej sieci (np. klasy), zbadaj znajdujące się w niej urządzenia.

Do przemyślenia

Jak można wykorzystać te informacje do rozwiązywania problemów?

Jakie zalety przy dokumentowaniu rozwiązywania problemów może mieć program NI w porównaniu z programem HyperTerminal?

Ćwiczenie 7.1.9b Wprowadzenie do programu Fluke Protocol Inspector



Cele

To ćwiczenie ma na celu zapoznanie się z programem Protocol Inspector firmy Fluke Networks, służącym do analizy ruchu sieciowego i ramek danych. W tym ćwiczeniu zostaną przedstawione podstawowe funkcje programu, które mogą być bardzo przydatne podczas rozwiązywania problemów w pozostałych ćwiczeniach

Wprowadzenie i przygotowanie

Wyniki przedstawione w tej instrukcji są wyłącznie przykładowe. Uzyskane rzeczywiste wyniki będą się różnić w zależności od liczby dodanych urządzeń, ich adresów MAC, nazw hostów podłączonej sieci LAN, itd.

Przedstawiony w tym ćwiczeniu program Protocol Inspector będzie przydatny w kolejnych ćwiczeniach dotyczących rozwiązywania problemów, a także w rzeczywistych sytuacjach. Oprogramowanie Protocol Inspector (PI) jest cennym uzupełnieniem programu nauczania Akademii. Prezentuje przy tym typowe funkcje dostępne w innych produktach znajdujących się na rynku.

Wskazówki dotyczące przeprowadzenia tego ćwiczenia.

- 1) Użyj programu Protocol Inspector lub Protocol Expert w małej, kontrolowanej sieci LAN, która została skonfigurowana przez instruktora w zamkniętym środowisku laboratoryjnym w sposób pokazany na powyższym rysunku. Minimalna konfiguracja powinna składać się ze stacji roboczej, przełącznika i routera.
- 2) Aby zapoznać się z innymi, bardziej zróżnicowanymi sytuacjami, wykonaj opisane czynności w większym środowisku, takim jak sieć klasowa lub szkolna. Przed próbą uruchomienia programu PI lub PE w szkolnej sieci LAN uzyskaj zgodę instruktora i administratora sieci.

Przynajmniej na jednym hoście musi być zainstalowany program Protocol Inspector. Jeśli ćwiczenie wykonywane jest w parach, zainstalowanie programu na obu komputerach powoduje, że każda osoba może samodzielnie wykonywać wszystkie czynności opisane w tej instrukcji. Wyniki wyświetlane dla każdego hosta mogą się jednak nieco różnić.

Krok 1 Konfigurowanie sieci wydzielonej lub podłączenie stacji roboczej do szkolnej sieci LAN

Opcja 1. Jeśli wybrane jest zamknięte środowisko laboratoryjne, podłącz sprzęt w sposób pokazany powyżej i załaduj pliki konfiguracyjne na odpowiednie routery. Te pliki mogą być już załadowane na routerach. W przeciwnym wypadku uzyskaj je od instruktora. Ustawienia zawarte w plikach powinny być zgodne ze schematem adresowania IP przedstawionym na powyższym rysunku i w poniższej tabeli.

Skonfiguruj stacje robocze zgodnie ze specyfikacjami podanymi w poniższej tabeli.

Host nr 1	Host nr 2
Adres IP: 192.168.1.20	Adres IP: 192.168.2.10
Maska podsieci: 255.255.255.0	Maska podsieci: 255.255.255.0
Domyślna brama: 192.168.1.1	Domyślna brama: 192.168.2.1

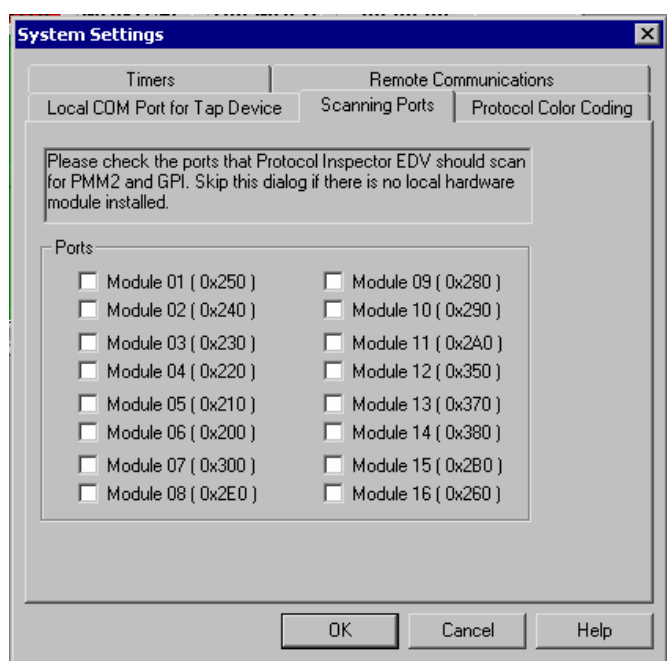
Opcja 2. W przypadku wyboru opcji 2, podłączenia do szkolnej sieci LAN, podłącz po prostu stację roboczą, na której zainstalowano program PI lub PE, bezpośrednio do znajdującego się w klasie przełącznika lub do gniazdka szkolnej sieci LAN.

Krok 2 Uruchomienie programu Protocol Inspector EDV

Z menu Start uruchom program Fluke Protocol Inspector EDV.

Uwaga: Po pierwszym uruchomieniu programu zostanie wyświetlony komunikat „Do you have any Fluke analyzer cards or Fluke taps in your local system?” („Czy w lokalnym systemie znajdują się jakiegokolwiek karty analizatora Fluke lub sondy Fluke?”)

Jeśli korzystasz z wersji edukacyjnej, wybierz opcję **No (Nie)**. Jeśli udzielisz pozytywnej odpowiedzi lub jeśli zostanie wyświetlony ekran przedstawiony obok, kliknij przycisk **OK** bez wybierania jakichkolwiek portów.

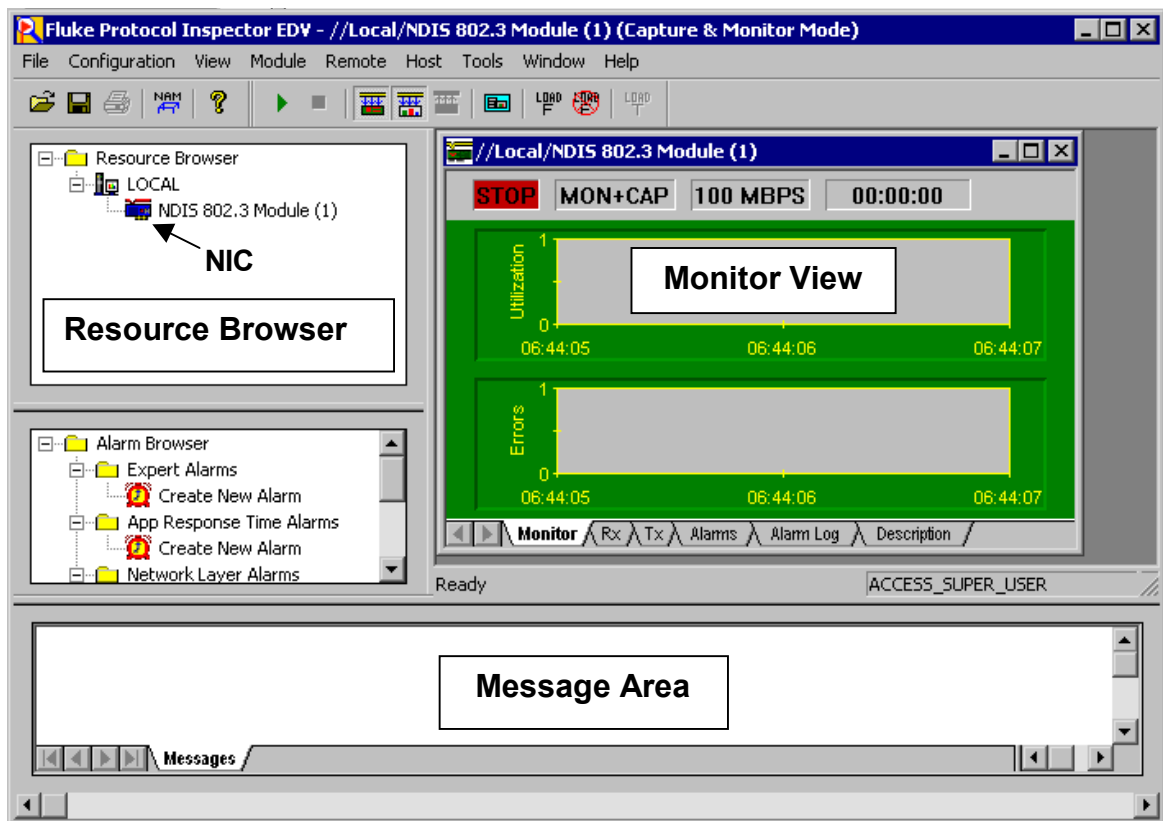


W programie Protocol dostępne są cztery główne widoki:


- Summary View (Widok podsumowania),
- Detail View (Widok szczegółów),
- Capture View of Capture Buffers (Widok przechwytywania buforów przechwytywania),
- Capture View of Capture Files (Widok przechwytywania plików przechwytywania).

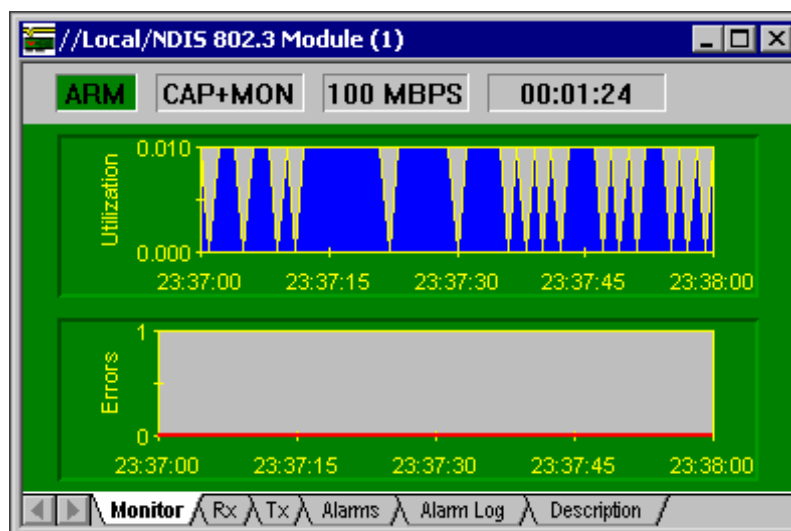
Przy otwarciu programu wyświetlany jest widok **Summary View (Widok podsumowania)**. W widoku tym dostępnych jest kilka okien. Okno **Resource Browser (Przeglądarka zasobów)** w lewym górnym rogu przedstawia jedyne dostępne urządzenie monitorujące, którym jest moduł NDIS 802.3 (karta sieciowa) hosta. Gdyby dostępne były monitory Protocol Media Monitors (Monitory medium protokołu), zostałyby wyświetlone wraz z przypisanymi im urządzeniami hosta. Okna **Alarm Browser (Przeglądarka alarmów)** znajdujące się po lewej stronie i **Message Area (Obszar komunikatów)** umieszczone poniżej zostaną omówione później.

Widok **Monitor View (Widok monitora)**, który jest wyświetlany w prawej górnej części okna głównego, służy do monitorowania każdego zasobu w oddzielnym oknie, przy użyciu różnych wybranych opcji wyświetlania. W poniższym przykładzie i prawdopodobnie na ekranie startowym w oknie Monitor View (Widok monitora) nie są wyświetlane żadne informacje. Napis **Stop** w lewym górnym rogu okna Monitor View (Widok monitora) oznacza, że monitorowanie jest wyłączone.



Krok 3 Uruchomienie procesu monitorowania/przechwytywania

Aby rozpocząć proces monitorowania/przechwytywania, użyj przycisku Start  lub z menu Module (Moduł) wybierz opcję Start. Powinno to spowodować rozpoczęcie wyświetlania aktywności na wykresie Utilization (Wykorzystanie) w sposób przedstawiony na poniższym rysunku.



Tam, gdzie wcześniej było wyświetlane słowo **Stop**, powinno zostać wyświetlone słowo **ARM**. Zauważ, iż po otwarciu menu **Module (Moduł)** dostępna jest opcja **Stop**, a opcja **Start** stała się niedostępna. Nie przerywaj procesu monitorowania. Jeśli uległ przerwaniu, uruchom go ponownie.

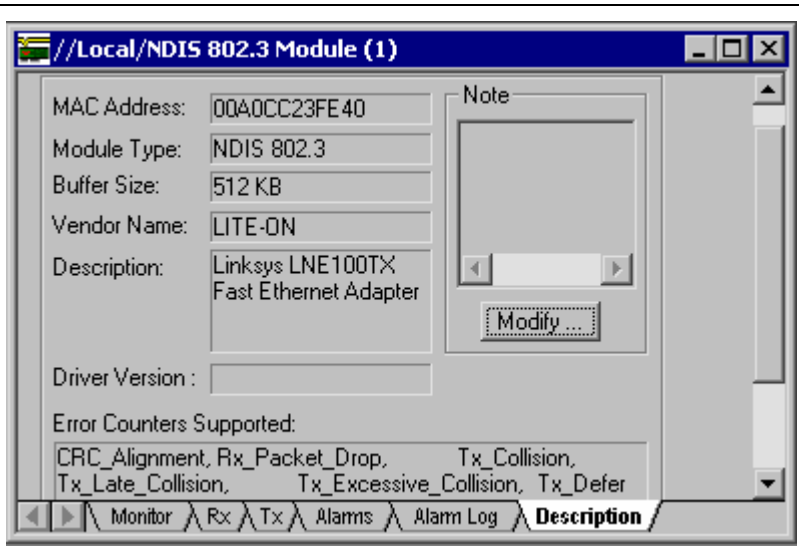
Zakładki dostępne w dolnej części okna przedstawiają dane wynikowe wyświetlane w różnych formularzach. Kliknij każdą z nich, aby obejrzeć wyniki. Karty **Transmitted (Tx) (Wysłano)**, **Alarms (Alarmy)** i **Alarm Log (Rejestr alarmów)** będą puste. Na przedstawionej poniżej karcie **Received (Rx) (Odebrano)** widać, że zarejestrowano jedynie ramki rozgłoszeniowe (**Broadcast**) oraz ramki wysłane w trybie multiemisji (**Multicast**), nie odebrano zaś żadnych ramek wysłanych w trybie emisji pojedynczej (**Unicast**).

MAC Counters	Value	Errors	Value
Frames Captured	463	CRC Alignment	0
Frames Received	463	Undersize	N/A
Broadcast	100	Oversize	N/A
Multicast	363	Fragments	N/A
Unicast	0	Jabbers	N/A
Frames/Second	2	Collision Indication	N/A
Bytes Received	31,400	Packet Dropped	0
Utilization	0	Errors	0


Wykorzystując konsolowe połączenie z routerem, użyj polecenia ping wobec monitorowanego hosta (192.168.1.10 lub 192.168.2.10). Zwróć uwagę, że zostaną wyświetlone ramki **Unicast**. Niestety, błędy wyświetlane w trzeciej kolumnie nie pojawią się w trakcie ćwiczenia, chyba że zostanie dodany generator ruchu, taki jak Fluke Networks OptiView.

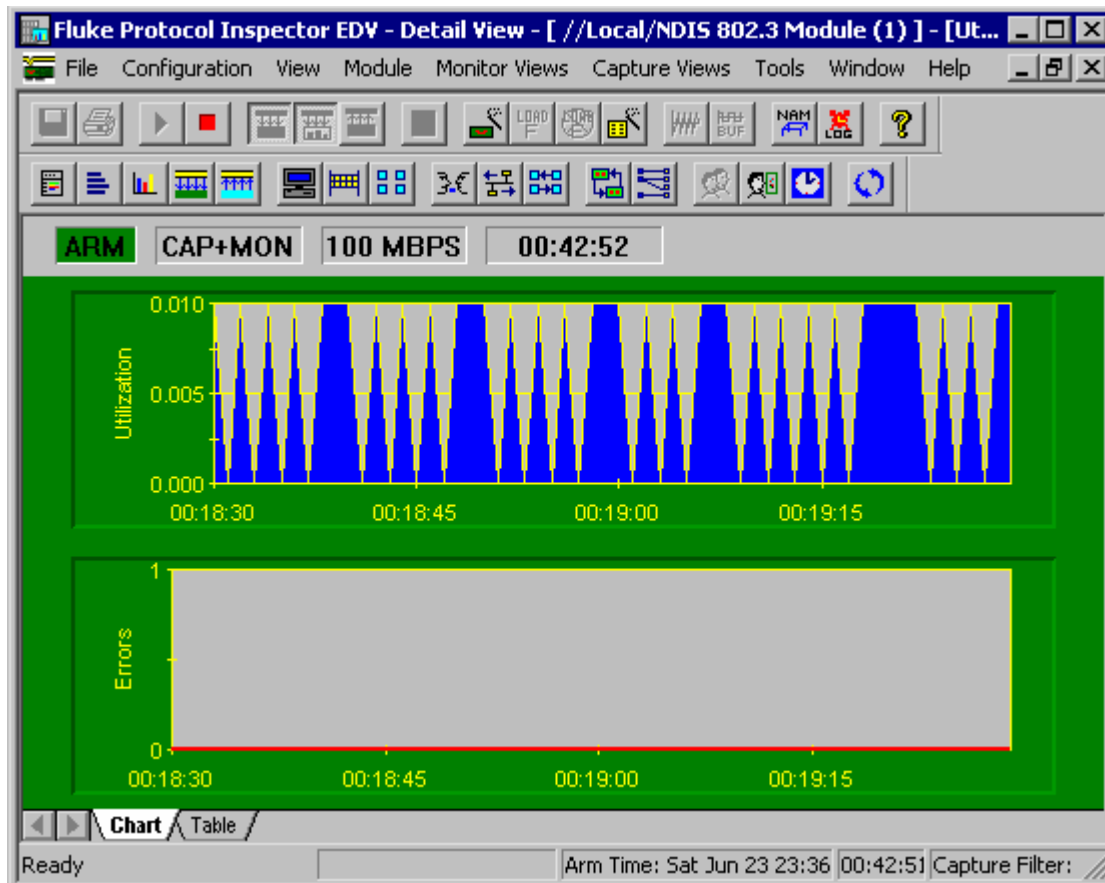
Zakładka **Description (Opis)** pokazuje adres MAC, producenta oraz model karty sieciowej. Wskazuje również, które liczniki błędów są włączone.

Poświęć kilka minut na zaznajomienie się z zakładkami i funkcjami przewijania okna.



Krok 4 Wyświetlenie szczegółów

Aby przejść do okna **Detail View (Widok szczegółów)**, kliknij przycisk **Detail View**  (**Widok szczegółów**) na pasku narzędzi lub kliknij dwukrotnie dowolne miejsce wykresu Monitor View (Widok monitora). Spowoduje to otwarcie drugiego okna, które, po zmaksymalizowaniu okna **Utilization / Errors Strip Chart (RX) (Wykres wykorzystania/błędów RX)**, powinno wyglądać tak jak poniższe.





Uwaga: Jeśli jest to konieczne, uaktywnij wszystkie paski narzędzi w menu View (Widok).

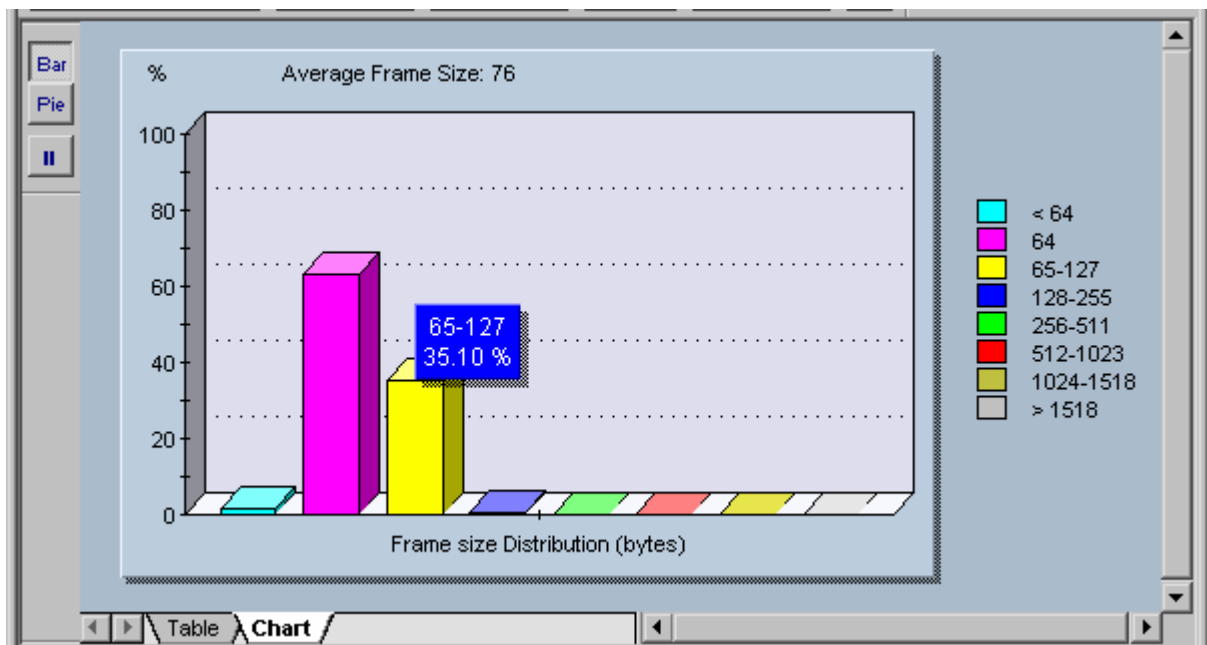
Wykres wygląda tak samo jak w widoku Summary View (Widok podsumowania), jednak w tym przypadku dostępnych jest więcej opcji na pasku narzędzi i w menu. Zanim przyjrzyś się tym funkcjom sprawdź, czy zakładki **Chart (Wykres)** i **Table (Tabela)** pokazują te same informacje, co wcześniej.


Podobnie jak w innych programach zgodnych z systemem Windows, umieszczenie kursora myszy na przycisku powoduje wyświetlenie wskazówki ekranowej z krótkim opisem funkcji przycisku. Przesuwając myszą nad przyciskami, zwróć uwagę, że niektóre z nich są nieaktywne. Oznacza to, że w danej sytuacji funkcja nie ma zastosowania. W przypadku wersji edukacyjnej programu może to również w niektórych przypadkach oznaczać, że taka funkcja nie jest obsługiwana.

Uwaga: W dodatku umieszczonym na końcu tego ćwiczenia znajdują się rysunki wszystkich pasków narzędzi oraz ich opis.

Kliknij przycisk **Mac Statistics**  (**Statystyki adresów MAC**), aby wyświetlić tabelę danych ramek odebranych (Rx) w innym formacie. Znaczenie wyświetlanych wyników powinno być oczywiste. Zmaksymalizuj wyświetlone okno. Nową wyświetlaną informacją jest pole **Speed (Szybkość)**, które przedstawia szybkość transmisji karty sieciowej.


Kliknij przycisk **Frame Size Distribution**  (**Rozkład wielkości ramek**), aby wyświetlić rozkład wielkości ramek odbieranych przez kartę sieciową. Umieszczenie kursora myszy na pasku spowoduje wyświetlenie krótkiego podsumowania, takiego jak przedstawione na poniższym rysunku. Zmaksymalizuj wyświetlone okno.

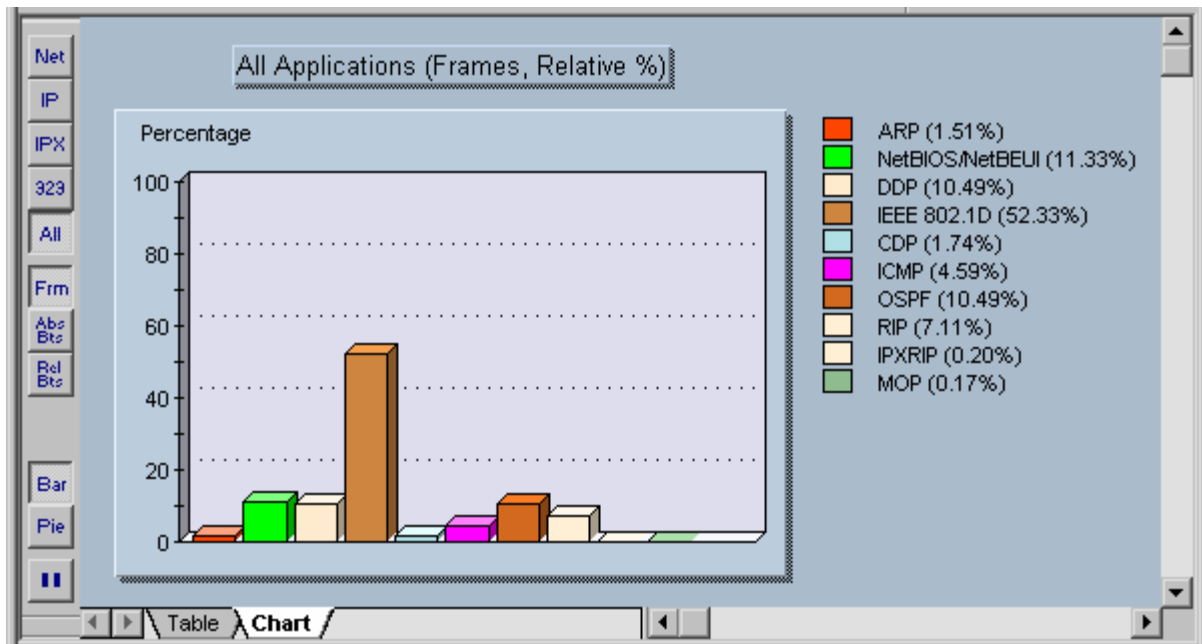


Spróbuj użyć przycisków **Pie (Wykres kołowy)**, **Bar (Wykres słupkowy)** i **Pause**  (**Pauza**), znajdujących się w lewym górnym rogu. Zauważ, że przycisk **Pause (Pauza)** powoduje zatrzymanie przechwytywania, zatem naciśnij go ponownie, aby wznowić przechwytywanie. Obejrzyj zarówno zakładki **Table (Tabela)**, jak i **Chart (Wykres)**.


W przykładowej konfiguracji powinny być odbierane wyłącznie krótkie ramki, ponieważ jedynymi procesami, jakie są wykonywane, są aktualizacje routingu. Łącząc się z routerem poprzez port konsoli, przećwicz stosowanie rozszerzonej funkcji ping przez wysłanie 100 długich pakietów.

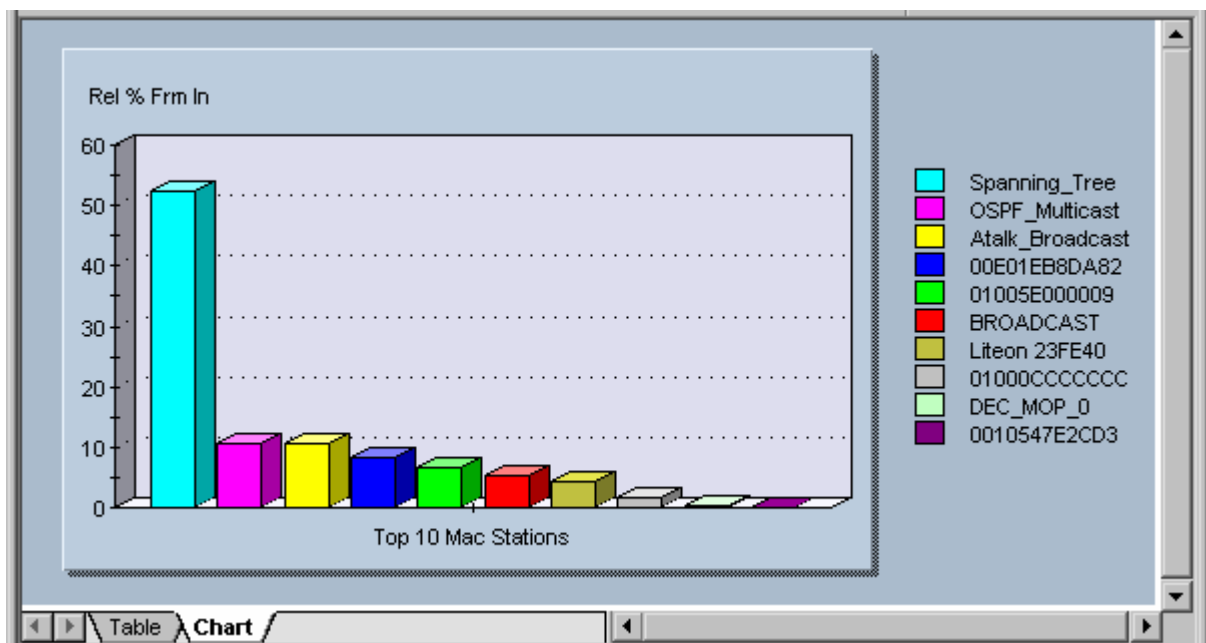
Jeśli każdy nowy ekran jest maksymalizowany, możesz wrócić do poprzedniego widoku, używając opcji Window (Okno) z menu programu. Możesz również rozłożyć okna przy użyciu opcji **Tile (Rozłóż sąsiadująco)**. Poeksperymentuj z menu Window (Okno) i zamknij wszystkie niepotrzebne widoki.

Kliknij przycisk **Protocol Distribution**  (**Rozkład protokołów**), aby wyświetlić rozkład protokołów odebranych przez kartę sieciową. Umieszczenie kursora myszy na pasku spowoduje wyświetlenie małego panelu podsumowania. Zmaksymalizuj wyświetlone okno.



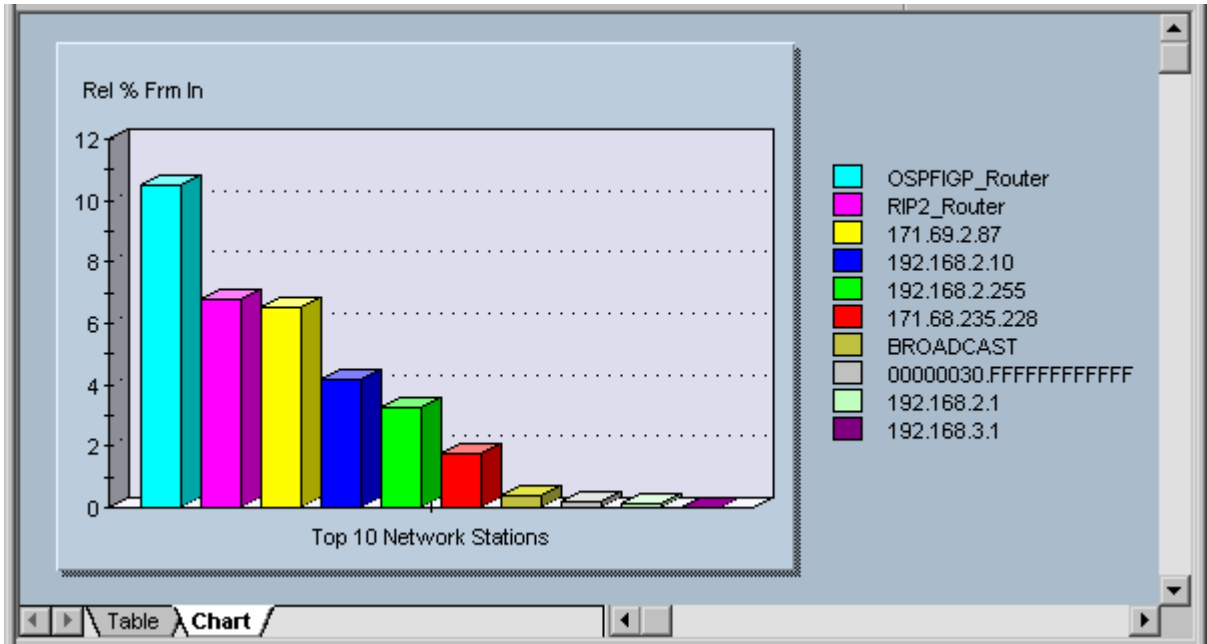
Wypróbuj inne przyciski i inne zakładki, aby zobaczyć wyświetlane wyniki. Po kliknięciu przycisku **Net (Sieć)** zostaną wyświetlone wyłącznie protokoły sieciowe. Przycisk **323** odnosi się do protokołów H323 Voiceover IP (VoIP). Jednakże w zależności od wersji używanego programu, przycisk ten może być opisany również jako VoIP. Aby wyświetlić wyniki, kliknij przyciski **Frm (Ramka)**, **Abs Bts (Bezwzględna liczba bajtów)** i **Rel Bts (Względna liczba bajtów)**. Pamiętaj, że przycisk **Pause (Pauza)** powoduje zatrzymanie przechwytywania.

Kliknij przycisk **Host Table**  (**Tabela hosta**), aby wyświetlić urządzenia z adresami MAC oraz związane z nimi ruch.



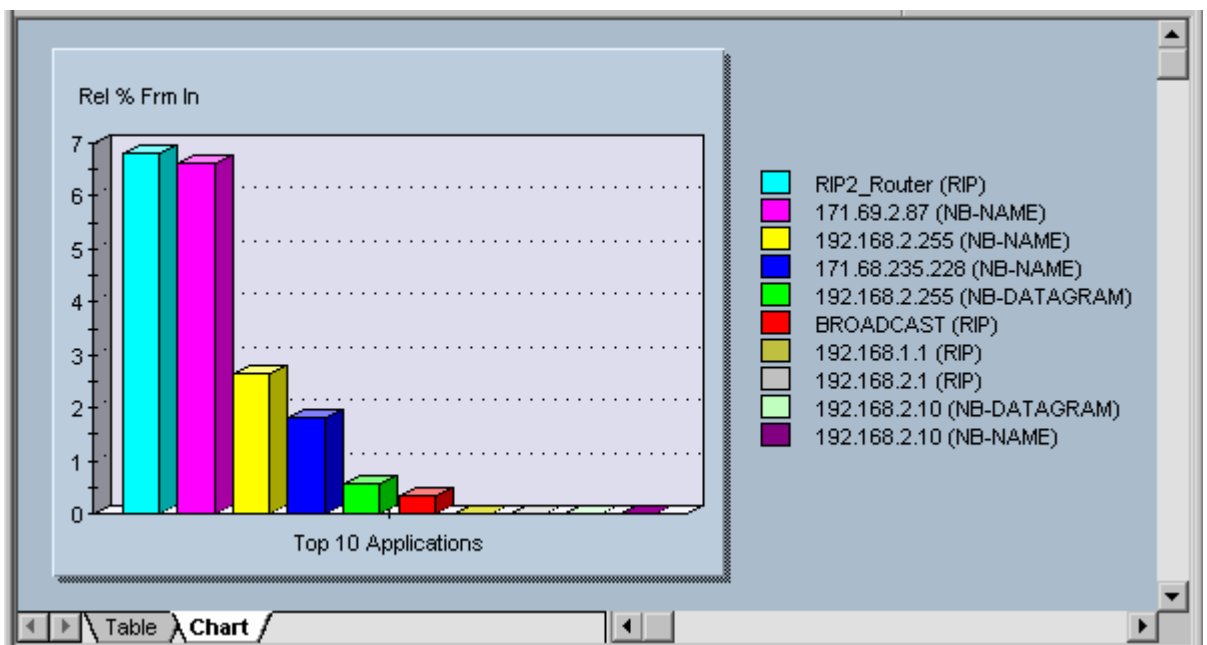
Zwróć uwagę na ruch Spanning Tree, AppleTalk i OSPF. Pamiętaj, aby wyświetlić zakładkę **Table (Tabela)** w celu obejrzenia bieżących wartości.

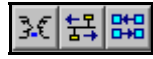
Kliknij przycisk **Network Layer Host Table**  (**Tabela hostów warstwy sieciowej**), aby wyświetlić urządzenia sieciowe (IP/IPX) i związane z nimi ruch.

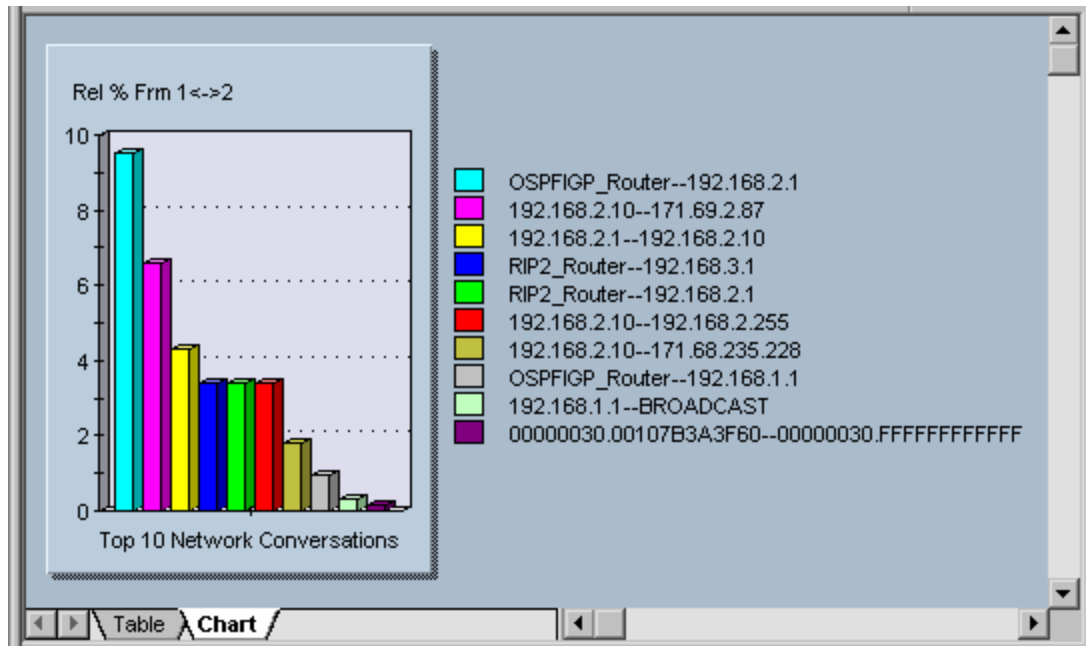



Wszelkie pakiety ping oraz hosty, które zostały dodane do bieżącej konfiguracji, będą miały wpływ na adresy, które zostaną pokazane po prawej stronie.

Kliknij przycisk **Application Layer Host Table**  (**Tabela hostów warstwy aplikacji**), aby wyświetlić ruch pomiędzy urządzeniami sieciowymi uporządkowany według aplikacji.




Poeksperymentuj z kolejnymi trzema przyciskami . Służą one do tworzenia macierzy opisujących konwersacje dla par host-host w warstwach MAC, sieci i aplikacji. Poniżej przedstawiony jest przykład konwersacji w warstwie sieciowej (IP/IPX).




Kolejne dwa przyciski to . Przy użyciu pierwszego z nich, przycisku **VLAN** wyświetlany jest ruch sieciowy w sieciach VLAN. W tym przykładzie sieci VLAN nie są używane. Pamiętaj o tym przycisku podczas późniejszego rozwiązywania problemów występujących w sieciach VLAN.

Za pomocą drugiego przycisku można utworzyć macierz wiążącą adresy MAC i adresy sieciowe stacji z nazwami. W poniższym przykładzie drugi wiersz dotyczy stacji sieci Novell.

MAC Station Name	MAC Station Address	Network Station Name	Network Station Address
00107B3A3F60	00107B3A3F60	192.168.1.1	192.168.1.1
00107B3A3F60	00107B3A3F60	00000030.00107B3A3F60	00000030.00107B3A3F60
Liteon 23FE40	00A0CC23FE40	192.168.2.10	192.168.2.10
00E01EB8DA82	00E01EB8DA82	192.168.2.1	192.168.2.1
00E01EB8DA82	00E01EB8DA82	192.168.3.1	192.168.3.1

Przycisk **Name Table**  (**Tabela nazw**) służy do otwierania bieżącej tabeli nazw w celu jej odczytu lub edycji.

Protocol	Name	Address
MAC	HP_Probe	090009000001
MAC	OSPF_Multicast	01005E000005
IP	IP_Station1	206.132.32.2
IP	BROADCAST	255.255.255.255
IP	IP_Multicast	224.0.0.0
IP	DVMRP_Router	224.0.0.4
IP	OSPFGRP_Router	224.0.0.5
IP	OSPFGRP_Router_0	224.0.0.6

Za pomocą przycisku **Expert View**  (**Widok eksperta**) przedstawiane są wykryte objawy, które mogą mieć znaczenie dla eksperta. Programy PI używają tych statystyk, aby wskazać potencjalne problemy. Podkreślone opcje umożliwiają wyświetlenie dodatkowego okna zawierającego dodatkowe szczegóły, jeśli zarejestrowane zostały jakiegokolwiek wartości. Konfiguracja w tym ćwiczeniu nie zawiera wiele takich informacji. Pozwala natomiast zbadać opcje debugowania ISL, HSRP oraz inne typy problemów, które pojawią się w późniejszych ćwiczeniach.


Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/IP SYN Attack	0	ISL BPDU/CDP Packets	0
TCP/IP RST Packets	0	IP Time to Live Expiring	0
TCP/IP Retransmissions	0	IP Checksum Errors	0
TCP/IP Zero Window	0	Illegal Network Source Address	0
TCP/IP Long Acks	0	Illegal MAC Source Address	0
TCP/IP Frozen Window	0	Total MAC Stations	11
Network Overload	0	Broadcast/Multicast Storm	0
Non Responsive Stations	0	Physical Errors	0
		HSRP Errors	0
		TCP Checksum Errors	0

Krok 5 Zatrzymanie procesu przechwytywania

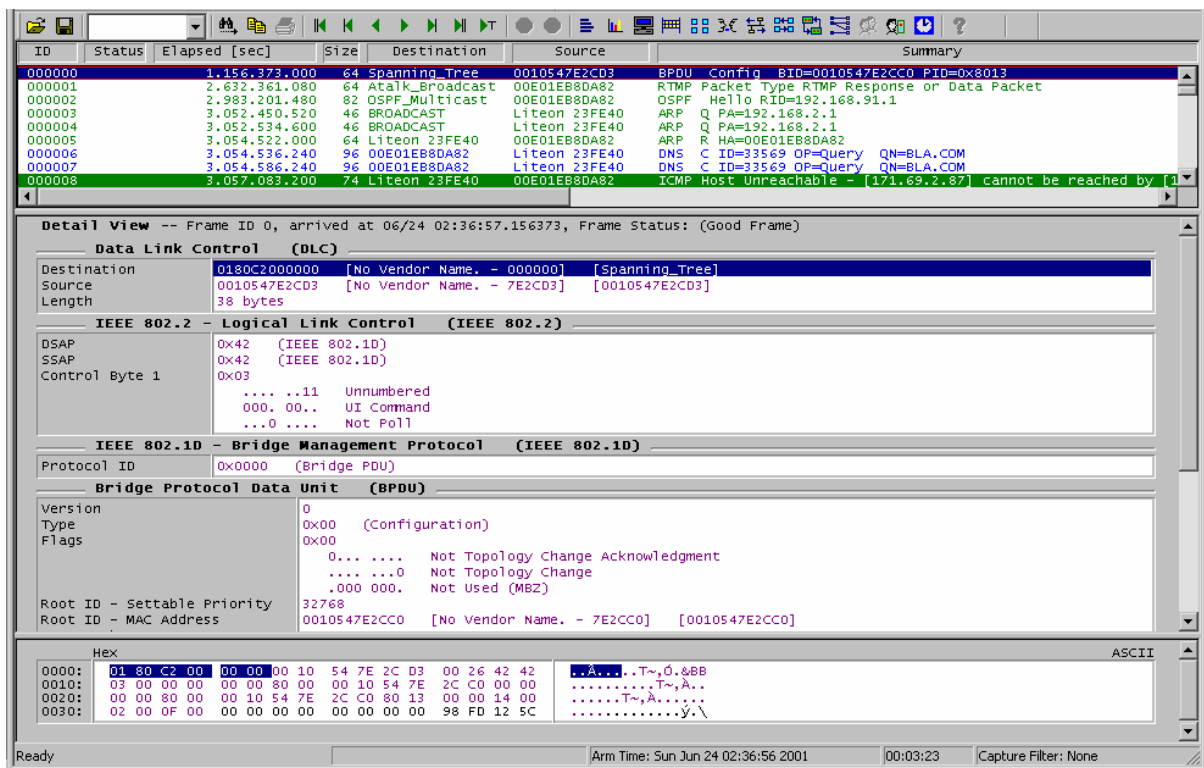
Aby zatrzymać przechwytywanie ramek i przyjrzeć się poszczególnym ramkom, użyj przycisku **Stop**



(**Zatrzymaj**) lub z menu Module (Moduł) wybierz polecenie Stop (Zatrzymaj).

Po zatrzymaniu przechwytywania kliknij przycisk **Capture View**  (**Wyświetlenie przechwytywania**). W tej wersji edukacyjnej zostanie wyświetlone okno informujące, że przechwytywanie jest ograniczone do 250 pakietów. W takim przypadku kliknij przycisk OK.

Wyświetlone okno może na pierwszy rzut oka wydawać się przeładowane informacjami. Zmaksymalizuj je, aby ukryć wszystkie inne okna otwarte w tle.

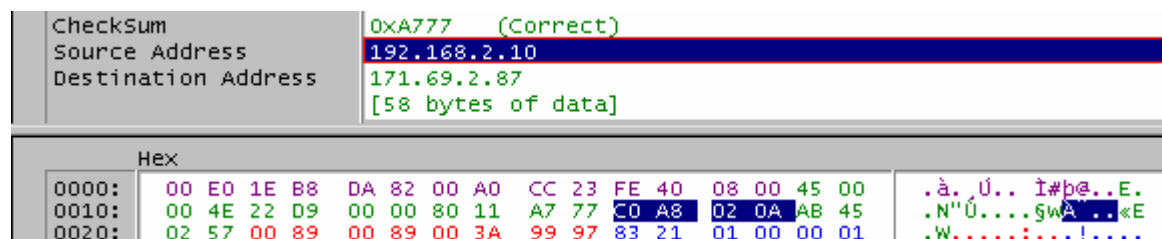


Przeglądając wyniki, zwróć uwagę, że otwarte są trzy okna rozmieszczone w pionie. Okno górne przedstawia listę przechwyconych pakietów. Okno środkowe przedstawia szczegółowe informacje o pakiecie wybranym w oknie górnym, a okno dolne przedstawia wartości szesnastkowe tego pakietu.

Po umieszczeniu myszy na granicy okien kursor zmienia się w ikonę przesuwania linii (dwustronną strzałkę). Umożliwia to zmianę obszaru zajmowanego przez poszczególne okna. Warto maksymalnie powiększyć okno środkowe i pozostawić pięć lub sześć wierszy w pozostałych oknach, tak jak w powyższym przykładzie.

Przejrzyj pakiety znajdujące się w oknie górnym. Powinny w nim znajdować się pakiety DNS, ARP, RTMP oraz pakiety innych typów. W przypadku stosowania przełącznika powinny znajdować się tam pakiety CDP i Spanning Tree. Zwróć uwagę, że wybranie wiersza w górnym oknie powoduje zmianę zawartości dwóch pozostałych okien.

Zaznacz dane w oknie środkowym i zwróć uwagę, że zmianie uległy dane wyświetlane w dolnym oknie (format szesnastkowy), wskazując miejsce, w którym przechowywane są zaznaczone dane. W tym przykładzie wybranie pozycji Source Address (IP) (Adres źródłowy IP) spowoduje wyświetlenie wartości szesnastkowych zawartych w pakiecie.



Zwróć również uwagę, że kolory ułatwiają zlokalizowanie informacji z okna środkowego w oknie danych szesnastkowych. W poniższym przykładzie prezentującym pakiet DNS dane w sekcji Data Link Control (DLC) (Kontrola łącza danych - DLC) w oknie środkowym są fioletowe, a sekcja Internet Protocol (IP) (Protokół IP) jest zielona. Odpowiednie wartości szesnastkowe mają ten sam kolor.

000005	3.054.522.000	64	Liteon 23FE40	00E01EB8DA82	ARP R HA=0C
000006	3.054.536.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33
000007	3.054.586.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33

Data Link Control (DLC)	
Destination	00E01EB8DA82 [No Vendor Name. - B8DA82] [00E01EB8DA82]
Source	00A0CC23FE40 [LITE-ON COMMUNICATIONS, INC. - 23FE40] [Liteon
EtherType	0x0800 (Internet Protocol (IP))

Internet Protocol (IP)	
Version/Header Length	0x45 0100 Version 4 0101 20 bytes - Header Length
Type of Service	0x00

Hex	
0000:	00 E0 1E B8 DA 82 00 A0 CC 23 FE 40 08 00 45 00 .à.ú..I#p@.E.
0010:	00 4E 22 D9 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Ú....\$WA...«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....
0030:	00 00 00 00 00 00 20 45 43 45 40 45 42 43 4F 45ECEMEBCOE
0040:	44 45 50 45 4E 43 41 43 41 43 41 43 41 43 41 43 DEPENCACACACACAC
0050:	41 43 41 43 41 41 41 00 00 20 00 01 67 87 47 13 ACACAAA...g.G.

Zwróć uwagę, że w powyższym przykładzie wartość pola **EtherType** wynosi **0x0800**. Oznacza to, że jest to pakiet IP. Zwróć uwagę na adresy MAC hosta docelowego i źródłowego oraz na miejsce przechowywania danych znajdujących się w oknie zawierającym dane szesnastkowe.

Kolejną sekcją środkowego okna jest w tym przykładzie **User Datagram Protocol (UDP) (Protokół UDP)**, zawierający numery portów UDP.

User Datagram Protocol (UDP)	
Source Port	137 (NETBIOS Name Service)
Destination Port	137 (NETBIOS Name Service)
Length	58 bytes
Checksum	0x9997 (Correct) [50 bytes of data]

Struktura środkowego okna zmienia się w zależności od typu pakietu.

Poświęć kilka minut na wybieranie różnych typów pakietów w górnym oknie i przejrzanie informacji wyświetlanych w pozostałych dwóch oknach. Zwróć szczególną uwagę na typ EtherType i numery portów, a także adresy źródłowe i docelowe, które zawarte są zarówno w warstwie MAC, jak i w warstwie sieciowej. Powinny zostać przechwycone pakiety RIP, OSPF, RTMP oraz AppleTalk. Upewnij się, że można zlokalizować i zinterpretować istotne dane. Zwróć uwagę, że poniższe przechwycone pakiety RIP są w wersji 2. Adresem docelowym multiemisji jest 224.0.0.9 i widoczne są wpisy w bieżącej tablicy routingu. Jaki byłby adres multiemisji w wersji 1? _____

Source Address	192.168.3.1
Destination Address	224.0.0.9 [RIP2_Router] [72 bytes of data]

User Datagram Protocol (UDP)	
Source Port	520 (Routing Information Protocol)
Destination Port	520 (Routing Information Protocol)
Length	72 bytes
Checksum	0x6192 (Correct) [64 bytes of data]

Routing Information Protocol	
Command	2 (Routing Response)
Version	2 (RIP2)
Unused	0 0
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.0.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.90.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.91.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1


Jeśli są dostępne jakiegokolwiek pakiety CDP, spróbuj uzyskać informacje o platformie. Poniższe dane pochodzą z przełącznika Catalyst 1900.

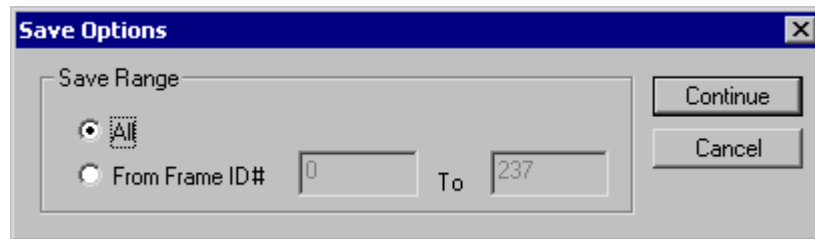
Variable Type	0x0006 (Platform)	
Variable Length	14	
Platform	cisco 1900	

0030:	00 00 01 01 01 CC 00 04 C0 A8 01 64 00 03 00 06	1034 22C0.....
0040:	31 39 00 04 00 08 00 00 00 0A 00 05 00 09 56 38i..A..d....
0050:	2E 30 30 00 06 00 0E 63 69 73 63 6F 20 31 39 30	19.....V8
0060:	30 8A 8B 60 39	..00....Cisco 190

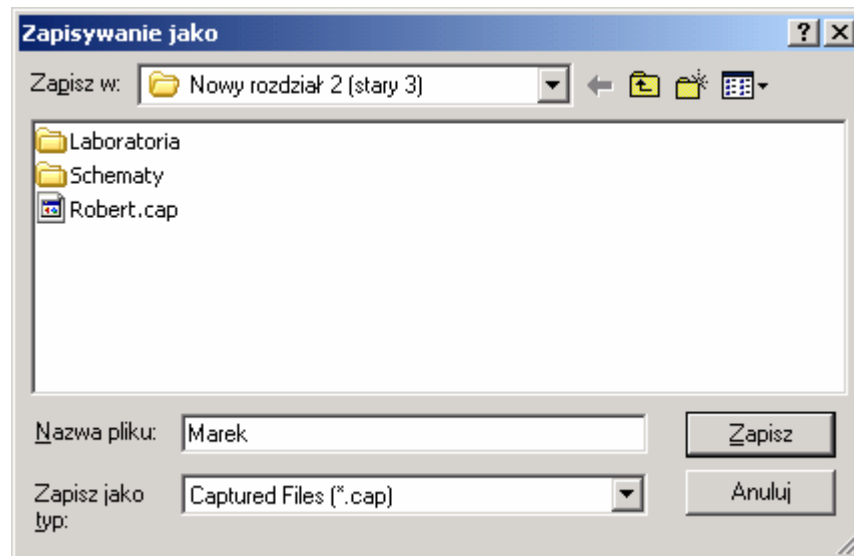
Eksperymentuj tak długo, aż używanie narzędzi nie będzie ci sprawiać problemów.


Krok 6 Zapisanie przechwyconych danych

Aby zapisać przechwycone dane, użyj przycisku **Save Capture**  (**Zapisz przechwycone dane**) lub z menu File (Plik) wybierz polecenie Save Capture (Zapisz przechwycone dane). W zależności od używanej wersji programu w menu File (Plik) opcja Save Capture (Zapisz przechwycone dane) może zostać zastąpiona przez „Save Current Section” (Zapisz aktualnie przeglądany sekcję). Zaakceptuj opcję **All (Wszystkie)** przy użyciu przycisku **Continue (Kontynuuj)**. Uczestnik kursu może w tym oknie wybrać zakres przechwyconych ramek, które mają zostać zapisane.




Podaj odpowiednią nazwę pliku i zapisz plik na wybranym dysku. Jeśli po otwarciu okna wyświetlane jest rozszerzenie CAP, upewnij się, że będzie ono również wyświetlane po wpisaniu nazwy.




Użyj przycisku **Open Capture File**  (**Otwórz plik przechwytywania**) i otwórz plik o nazwie Lab3-2 PI Lab.cap. Jeśli plik ten nie jest dostępny, otwórz plik, który został zapisany.

Użyj teraz funkcji **Capture View of Capture Files (Widok przechwytywania plików przechwytywania)**. Dostępne są te same narzędzia, ale pasek tytułu w górnej części ekranu wskazuje, że wyświetlane są dane z pliku, a nie dane przechwytywania znajdujące się w pamięci.

Krok 7 Badanie ramek

Wybierz ramkę w górnym oknie i użyj przycisków . Strzałki powodują przesunięcie ramek o jedną w górę lub w dół. Za pomocą strzałki z pojedynczą linią można przejść do góry lub na dół bieżącego okna, a za pomocą strzałki z dwoma liniami można przejść do początku lub na koniec całej listy. Strzałka z literą T również służy do przejścia na początek listy.

Użyj przycisku **Search**  (**Wyszukiwanie**), aby wykonać wyszukiwanie. W polu listy wpisz tekst OSPF. Następnie kliknij ikonę lornetki, co spowoduje przejście od jednego wpisu OSPF do drugiego.

Eksperymentuj tak długo, aż używanie narzędzi nie będzie ci sprawiać problemów.

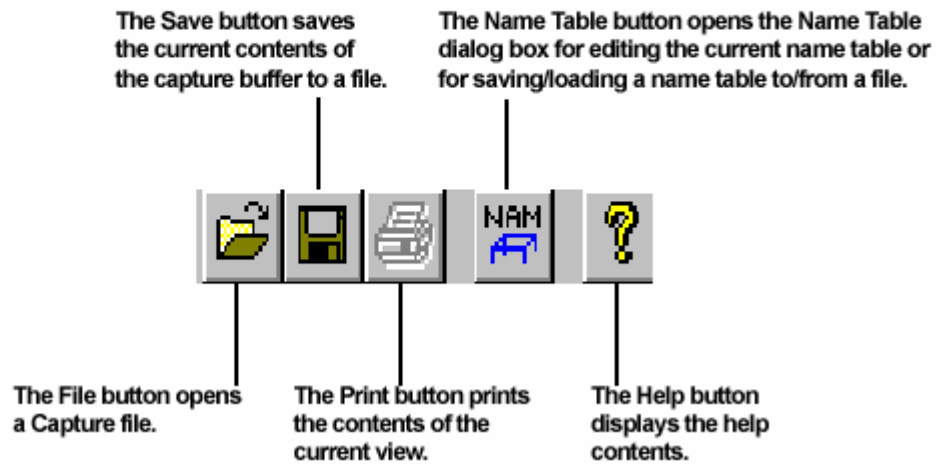
Do przemyślenia

- a. W jaki sposób narzędzie to może być przydatne do rozwiązywania problemów?

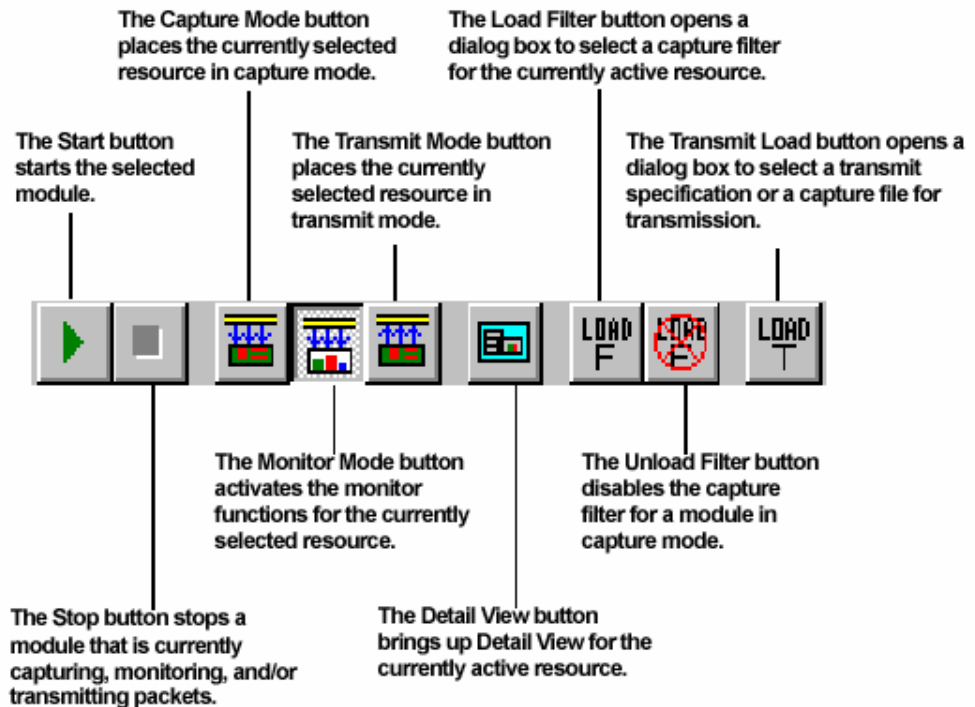
- b. Czy wszystkie dane w sieci są analizowane?

- c. Jaki wpływ ma podłączenie do przełącznika?

Protocol Inspector Toolbar



Module Toolbar (Summary View)



Detail View Toolbar

The Save button saves the current contents of the capture buffer to a file.

The Capture Mode button places the currently selected resource in capture mode.

The Stop button stops a module that is currently capturing, monitoring, and/or transmitting packets.

The Transmit Mode button places the currently selected resource in Transmit mode.

The Capture Filter button displays the Capture Filter window. The window displays a previously opened filter or the default filter.

The Unload Filter button disables the capture filter for a module in capture mode.

The Transmit Specification button opens a dialog box to select a transmit specification or a capture file for transmit.

The Help button displays the help contents.

The Start button starts the selected module. ("Am")

The Capture View Button selects this mode for viewing captured information including protocol decodes.

The Display Filter Button displays the Display Filter window containing the previously opened filter or the default filter.

The Name Table button opens the Name Table dialog box for editing the current name table or for saving/loading a name table to/from a file.

The Print button prints the contents of the current view.

The Monitor Mode button activates the monitor functions for the currently selected resource.

The Load Filter button brings up a dialog box to select a capture filter for the currently active resource.

The Transmit from Buffer Button lets you select a capture file and then load the capture file for transmission.

Data Views Toolbar (Note: Only some of these views are available with GMM cards)

The MAC Statistics button shows packet and error counters, plus module status information.

The Utilization/Error View (Tx) button shows utilization and the number of errors over time.

The Host Matrix button shows captured information including conversations between MAC stations.

The Address Map button shows associations between station names and addresses.

The Refresh button updates the information in all open views.

The Protocol Distribution button shows a chart of the distribution of major protocols and applications.

The Network Layer Host Table button shows Network (IP/IPX) stations and their traffic.

The Application Layer Matrix button shows conversations between applications.

The Expert View button shows all expert symptoms detected and counters of expert symptoms. (Protocol Inspector Pro only)

The Frame Size Distribution button shows the distribution of frame sizes.

The Host Table button shows MAC stations and their traffic.

The Network Layer Matrix button shows all network conversations for IP and IPX traffic.

The Duplicate Address button shows duplicate IP or IPX addresses. (Only in Protocol Inspector Pro)

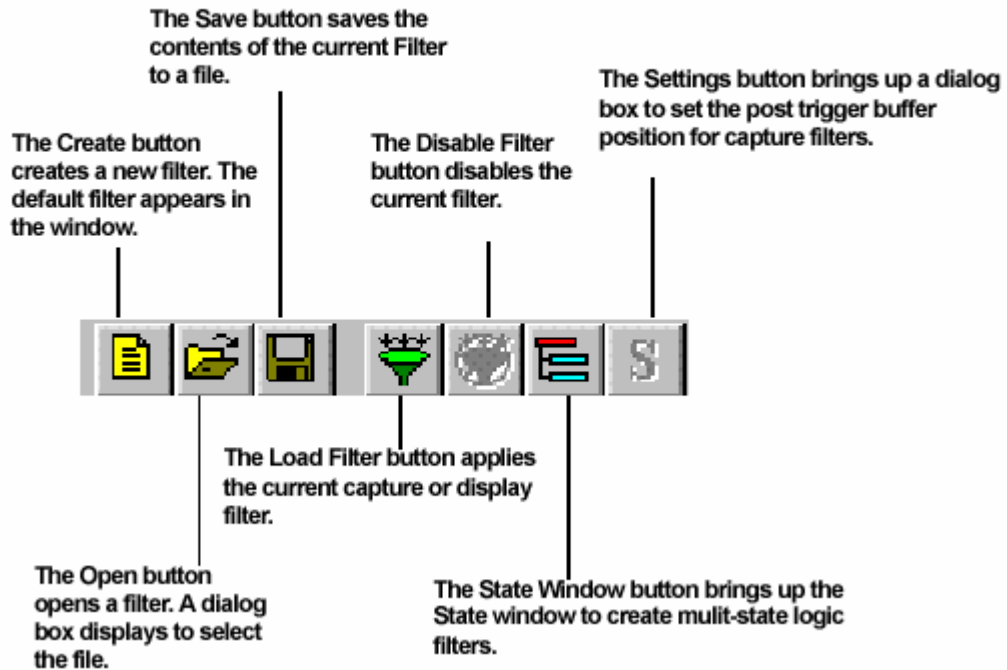
The Utilization/Error View (Rx) button shows utilization and number of errors over time.

The Application Layer Host Table button shows network station traffic by application.

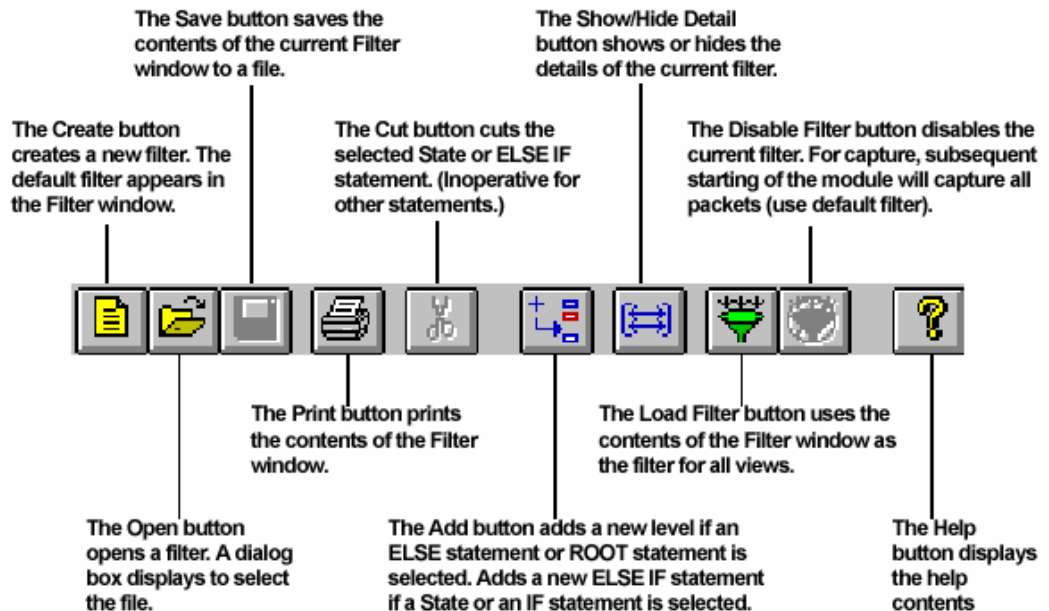
The VLAN button shows network traffic on virtual LANs.

The Application Response Time button shows minimum, maximum, and average application response times. (Protocol Inspector Pro only)

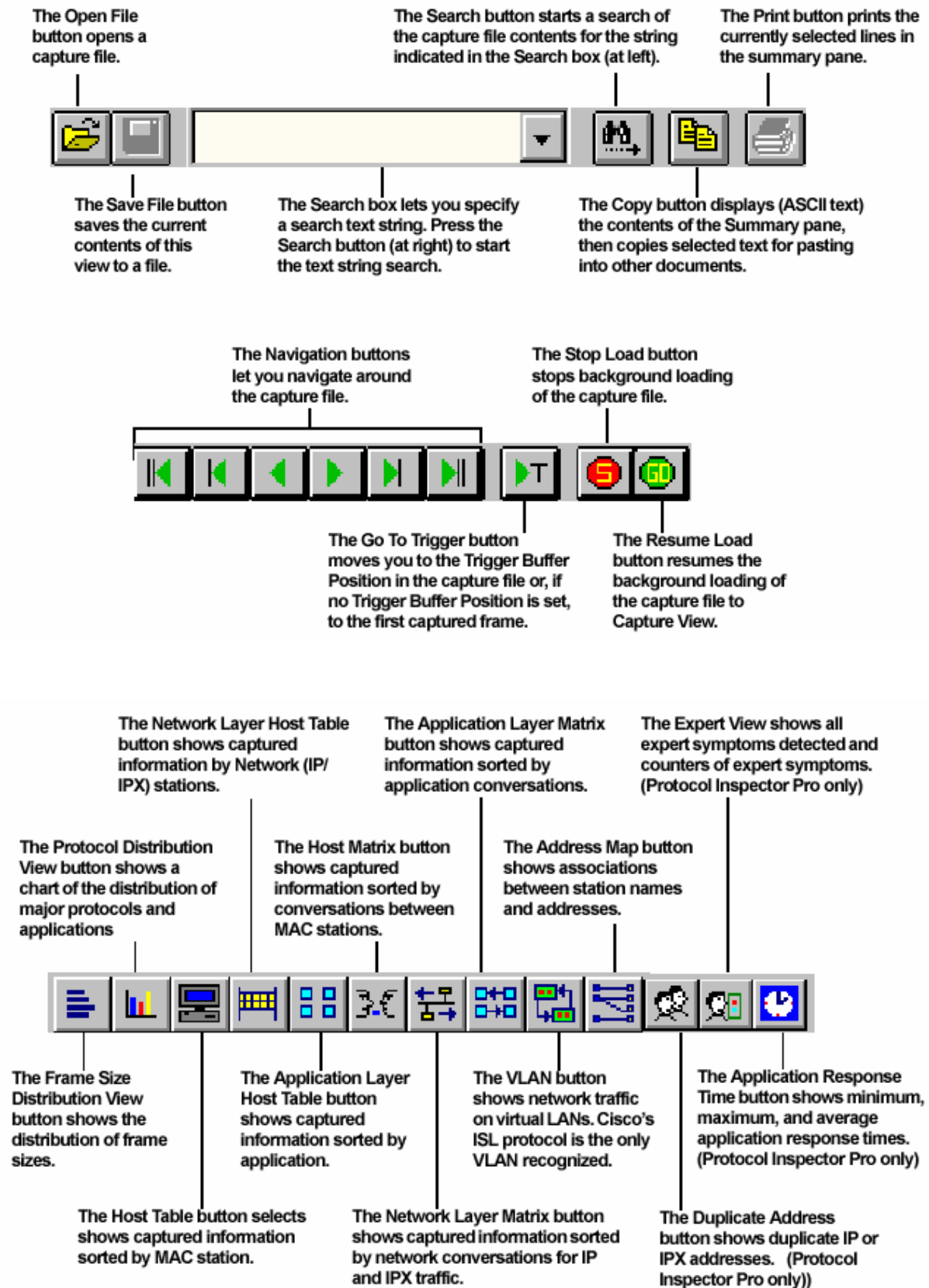
Create/Modify Filter Toolbar



State Toolbar



Capture View Toolbar



Function Keys

Function keys perform different operations within different Protocol Inspector views.

Function Key	Summary View	Detail View
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop
F11	N/A	N/A
F12	N/A	N/A

Other Keyboard Shortcuts...

Key Combination	Action
Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save
Ctrl + T	Start Module
Ctrl + P	Stop Module

Ćwiczenie 9.2.7 Podstawy adresowania IP

Cele

- Poznanie pięciu różnych klas adresów IP.
- Opisanie cech i zastosowań różnych klas adresów IP.
- Poznanie sposobu identyfikacji klasy adresu IP na podstawie numeru sieci.
- Określenie, która część (oktet) adresu IP jest identyfikatorem sieci, a która identyfikatorem hosta.
- Opanowanie umiejętności identyfikowania prawidłowych i nieprawidłowych adresów IP hostów w oparciu o reguły adresowania IP.
- Zdefiniowanie zakresu adresów i domyślnej maski podsieci dla każdej klasy.

Wprowadzenie i przygotowanie

Ćwiczenie pomaga w zrozumieniu struktury adresów IP i działania sieci TCP/IP. Jest to przede wszystkim ćwiczenie pisemne. Warto przy tym jednak przyjrzeć się kilku prawdziwym adresom sieciowym IP, używając do tego celu narzędzia wiersza poleceń `ipconfig` w systemie operacyjnym Windows NT/2000/XP lub `winiptcfg` w systemie Windows 9x/ME. Adresy IP są używane do jednoznacznego identyfikowania sieci TCP/IP i znajdujących się w tych sieciach hostów, takich jak komputery i drukarki, dzięki czemu urządzenia te mogą się ze sobą komunikować. Stacje robocze i serwery w sieci TCP/IP są nazywane hostami. Każde z tych urządzeń ma unikalny adres IP. Adres ten nazywamy adresem hosta. TCP/IP jest najczęściej używanym protokołem na świecie. W Internecie i w sieci WWW używa się wyłącznie adresów IP. Host, aby móc komunikować się z Internetem, musi mieć przydzielony adres IP.

Adres IP w swojej podstawowej formie składa się z dwóch części:

- adresu sieci,
- adresu hosta.

Część adresu IP identyfikująca sieć jest przydzielana firmie lub organizacji przez Internet Network Information Center (InterNIC). Routery używają adresu IP do przenoszenia danych pomiędzy sieciami. Adresy IP zgodne z aktualną wersją IPv4 mają długość 32 bitów i są podzielone na 4 oktety po 8 bitów każdy. Działają one w warstwie sieci (warstwa 3) modelu OSI (ang. *Open System Interconnection*), która odpowiada warstwie Internetu modelu TCP/IP. Adresy IP są nadawane:

- statycznie — czyli ręcznie, przez administratora sieci,
- dynamicznie — czyli automatycznie, np. za pomocą serwera DHCP.

Adres IP stacji roboczej lub hosta jest adresem logicznym, co oznacza, że można go zmieniać. Adres MAC stacji roboczej jest 48-bitowym adresem fizycznym. Adres ten jest związany na stałe z kartą sieciową (NIC) i nie można go zmienić, dopóki nie zmieni się karty sieciowej. Połączenie logicznego adresu IP i fizycznego adresu MAC pomaga routować pakiety do ich miejsc docelowych.

Istnieje pięć różnych klas adresów IP. Adresy należące do różnych klas różnią się między sobą liczbą bitów używanych do przedstawiania części identyfikujących sieć i hosta. Przedmiotem tego ćwiczenia są adresy należące do różnych klas. Ma to służyć poznaniu cech poszczególnych klas

adresów. Zrozumienie działania adresów IP jest niezbędne do zrozumienia działania nie tylko sieci TCP/IP, ale też wszelkich innych intersieci. Wymagane są następujące zasoby:

- stacja robocza PC z zainstalowanym systemem Windows 9x/NT/2000/XP,
- dostęp do programu Kalkulator.

Krok 1 Przypomnienie informacji o klasach adresów IP i ich cechach

Klasy adresów

Istnieje pięć klas adresów IP (od A do E), z których tylko pierwsze trzy są używane komercyjnie. Na wstępie, przy wykorzystaniu poniższej tabeli, zostanie omówiony jeden z adresów — adres sieciowy klasy A. W pierwszej kolumnie przedstawiona jest klasa adresu IP. Druga kolumna zawiera zakres prawidłowych wartości pierwszego oktetu adresu dla danej klasy adresów. Adres klasy A musi zaczynać się od liczby z przedziału od 1 do 126. Pierwszy bit adresu klasy A jest zawsze równy zero, co oznacza, że nie można użyć najbardziej znaczącego bitu (bitu o wartości 128). Adres z pierwszym oktetem równym 127 jest zarezerwowany do testowania wewnętrznego sprzężenia zwrotnego. W przypadku adresu sieci klasy A sieć jest identyfikowana wyłącznie przez pierwszy oktet.

Domyślna maska podsieci

Domyślna maska podsieci składa się z samych jedynek, czyli dziesiętnej liczby 255, i maskuje pierwszych 8 bitów adresu klasy A. Ta domyślna maska podsieci pomaga routerom i hostom określić, czy host docelowy znajduje się w tej samej sieci, czy też w innej. Ponieważ istnieje tylko 126 sieci klasy A, pozostałe 24 bity, czyli 3 oktety, można przeznaczyć na adres hosta. Każda sieć klasy A może zawierać 2^{24} hostów, czyli ponad 16 milionów hostów. Sieć często jest dzielona na mniejsze grupy zwane podsieciami. W tym celu używa się niestandardowej maski podsieci. Zostanie ona omówiona w następnym ćwiczeniu.

Adres sieci i hosta

Część identyfikująca sieć lub hosta w adresie IP nie może składać się z samych jedynek lub samych zer. Na przykład adres klasy A 118.0.0.5 jest prawidłowym adresem IP. Część identyfikująca sieć, czyli pierwsze 8 bitów, jest równa 118, więc nie składa się z samych zer. Część identyfikująca hosta, czyli ostatnie 24 bity, nie składa się ani z samych zer, ani z samych jedynek. Gdyby część identyfikująca hosta składała się z samych zer, byłby to adres samej sieci. Gdyby natomiast część identyfikująca hosta składała się z samych jedynek, byłby to adres rozgłoszeniowy. Wartość każdego oktetu nie może być większa niż dziesiętna liczba 255, czyli 11111111 dwójkowo.

Klasa	Zakres wartości pierwszego oktetu	Najbardziej znaczące bity pierwszego oktetu	Identyfikator sieci/hosta (S=sieć, H=host)	Domyślna maska podsieci	Liczba sieci	Liczba hostów w sieci (możliwych do użycia)
A	1–126 *	0	S.H.H.H	255.0.0.0	126 (2^7-2)	16 777 214 ($2^{24}-2$)
B	128–191	10	S.S.H.H	255.255.0.0	16 382 ($2^{14}-2$)	65 534 ($2^{16}-2$)
C	192–223	110	S.S.S.H	255.255.255.0	2 097 150 ($2^{21}-2$)	254 (2^8-2)
D	224–239	1110	Zarezerwowana dla rozsyłania grupowego.			
E	240–254	11110	Eksperymentalna, używana do celów badawczych.			

Uwaga: Adres sieci klasy A równy 127 jest zarezerwowany dla wewnętrznego sprzężenia zwrotnego i funkcji diagnostycznych, w związku z czym nie można go używać.

Krok 2 Określanie podstawowych cech adresów IP

Posługując się tabelą adresów IP i własną wiedzą na temat klas adresów IP, odpowiedz na następujące pytania:

- Jaki jest zakres wartości (dziesiętnie i dwójkowo) pierwszego oktetu dla wszystkich możliwych adresów IP klasy B?
Dziesiętnie Od: _____ Do: _____
Dwójkowo Od: _____ Do: _____
- Który oktet lub oktety w adresie IP klasy C reprezentują część identyfikującą sieć?

- Który oktet lub oktety w adresie IP klasy A reprezentują część identyfikującą hosta?

- Jaka jest maksymalna liczba możliwych do wykorzystania adresów hostów w adresie sieciowym klasy C? _____
- Ile jest sieci klasy B? _____
- Ile hostów może zawierać każda z sieci klasy B? _____
- Ile oktetów zawiera adres IP? _____ Ile bitów ma oktet? _____

Krok 3 Określanie części identyfikujących sieć i hosta w adresie IP

Dla poniższych adresów IP hostów uzupełnij następujące informacje:

- klasa każdego adresu,
- adres lub identyfikator sieci,
- część identyfikująca hosta,
- adres rozgłoszeniowy dla tej sieci,
- domyślna maska podsieci.

W przypadku adresu sieci część identyfikująca hosta składa się z samych zer. Aby zidentyfikować adres hosta, należy wpisać tylko odpowiednie oktety. W przypadku adresu rozgłoszeniowego część identyfikująca hosta składa się z samych jedynek. W adresie maski podsieci część identyfikująca sieć zawiera same jedyneki. Uzupełnij poniższą tabelę.

Adres IP hosta	Klasa adresu	Adres sieci	Adres hosta	Adres rozgłoszeniowy dla tej sieci	Domyślna maska podsieci
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Krok 4 Odpowiedz na poniższe pytania, biorąc pod uwagę adres IP 142.226.0.15 i maskę podsieci 255.255.255.0:

Jaką wartość binarną ma drugi oktet? _____

Jaka jest klasa tego adresu? _____

Jaki jest adres sieci dla tego adresu IP? _____

Czy jest to prawidłowy adres IP hosta (tak/nie)?

Dlaczego tak sądzisz?

Krok 5 Określ adresy IP hostów, które można użyć dla sieci komercyjnych

Dla poniższych adresów hostów określ, czy można je użyć w sieciach komercyjnych. Uzasadnij swoją opinię. Prawidłowy adres to taki, który można przydzielić następującym urządzeniom:

- stacji roboczej,
- serwerowi,
- drukarce,
- interfejsowi routera,
- innemu zgodnemu urządzeniu.

Uzupełnij poniższą tabelę.

Adres IP hosta	Czy jest to prawidłowy adres? (tak/nie)	Dlaczego tak sądzisz?
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		

Ćwiczenie 9.3.5 Konfigurowanie klienta DHCP

Cele

Zapoznanie się z protokołem dynamicznej konfiguracji hostów (DHCP, ang. *Dynamic Host Configuration Protocol*) i skonfigurowanie komputera jako klienta DHCP tak, aby korzystał z usług DHCP.

Wprowadzenie i przygotowanie

DHCP jest mechanizmem służącym do dynamicznego przypisywania adresów IP i innych informacji. Umieszczony w sieci LAN lub u dostawcy usług internetowych serwer DHCP może odpowiadać na żądania hostów i przekazywać im następujące informacje:

- adres IP,
- maskę podsieci,
- bramę domyślną,
- adres serwera DNS (*Domain Name Service*),
- adresy innych zasobów.

Jeśli usługa DHCP nie jest używana, wszystkie powyższe informacje trzeba skonfigurować ręcznie na każdym hoście.

Urządzeniem DHCP jest zwykle serwer sieciowy.

W małych sieciach usługi DHCP mogą być udostępniane przez mały router. Przykładami takich sieci są między innymi sieci domowe łączące się za pośrednictwem modemów DSL, sieci telewizji kablowej lub łączы bezprzewodowych. Firma Cisco, jak i wielu innych producentów, oferuje niewielkie routery mające następujące możliwości:

- połączenie z Internetem lub połączenie WAN,
- mały, wbudowany koncentrator lub przełącznik,
- serwer usługi DHCP.

Ćwiczenie dotyczy skonfigurowania komputera w taki sposób, by używał dostępnych usług DHCP.

Zakłada się, że na komputerze jest zainstalowana dowolna wersja systemu operacyjnego Windows. Ćwiczenie to powinno być wykonywane w sieci znajdującej się w klasie lub w innej sieci LAN mającej połączenie z Internetem. Można je przeprowadzić, korzystając z pojedynczego połączenia modemowego lub połączenia DSL.

Uwaga: Jeżeli w sieci, do której przyłączony jest ten komputer, używane jest adresowanie statyczne, należy jedynie przeglądać okna dialogowe wskazane w instrukcji. **Nie należy** próbować zmieniać ustawień na tych komputerach. W takim przypadku konfiguracja statyczna zostanie usunięta i trzeba będzie ponownie konfigurować taki komputer.

Krok 1 Ustanawianie połączenia sieciowego

Jeżeli połączenie z Internetem następuje poprzez łącze komutowane, należy połączyć się z dostawcą usług internetowych, aby zapewnić, że komputer będzie posiadał adres IP. W sieci LAN TCP/IP zawierającej serwer DHCP nie ma konieczności wykonywania tego kroku.

Krok 2 Otwieranie okna wiersza poleceń

Użytkownicy systemów Windows NT/2000/XP powinni skorzystać z menu **Start**, aby otworzyć okno **Command Prompt (Wiersz poleceń)**. Okno Command Prompt (Wiersz poleceń) jest podobne do okna MS-DOS Prompt (Tryb MS-DOS), znajdującego się w innych wersjach systemu Windows:

Wybierz kolejno polecenia: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)** lub **Start > Programs (Programy) > Command Prompt (Wiersz poleceń)**.

Aby otworzyć okno MS-DOS Prompt (Tryb MS-DOS), użytkownicy systemów Windows 95, 98 i Windows ME mogą posłużyć się menu Start w następujący sposób:

Wybierz kolejno polecenia: **Start > Programs (Programy) > Accessories (Akcesoria) > MS-DOS Prompt (Tryb MS-DOS)** lub **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS)**.

Krok 3 Wyświetlanie ustawień IP w celu sprawdzenia, czy sieć używa usług DHCP

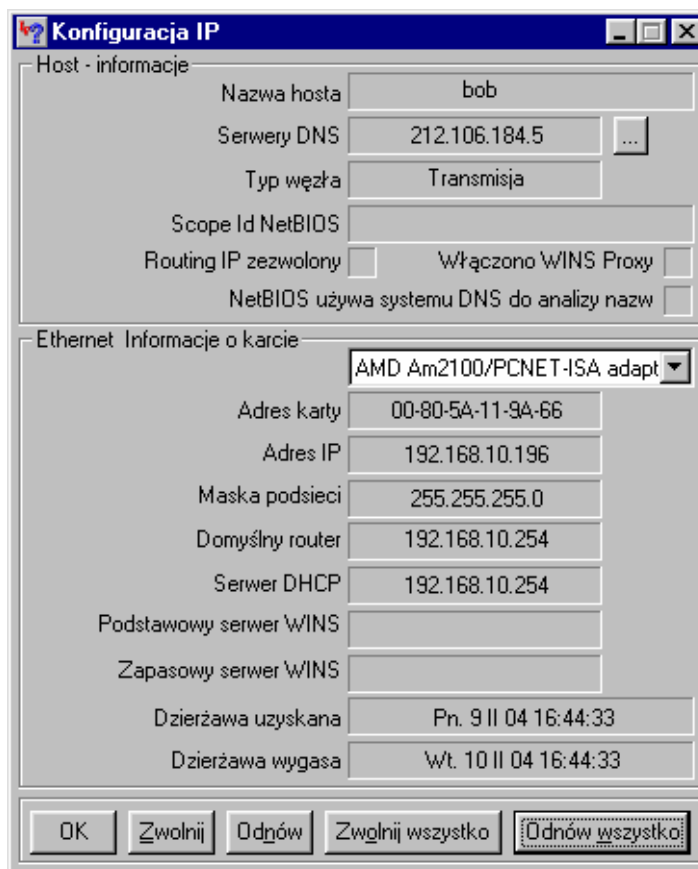
Użytkownicy systemów Windows 95/98/ME:

Wpisz polecenie `wiipcfg` i naciśnij klawisz **Enter**, a następnie przycisk **More Info (Więcej informacji)**.

W poniższym przykładzie fakt korzystania z usługi DHCP można poznać po wartościach znajdujących się w następujących polach:

- **DHCP Server IP address (Serwer DHCP)**
- **Lease Obtained (Dzierżawa uzyskana)**
- **Lease Expires (Dzierżawa wygasa)**

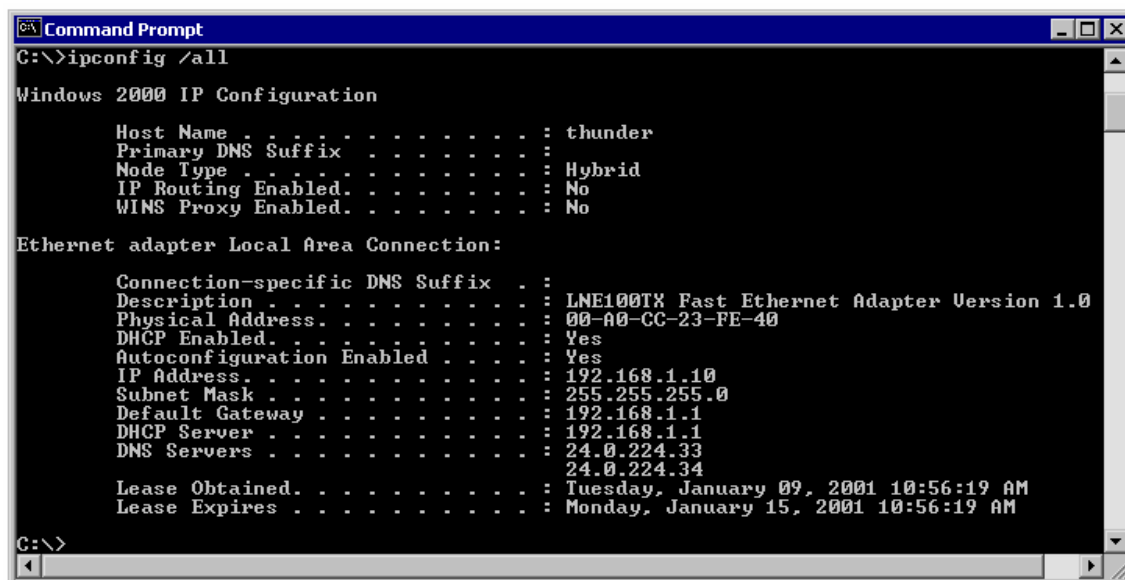
Pola te byłyby puste w przypadku urządzenia skonfigurowanego statycznie. Usługa DHCP dostarcza także informacji o adresie serwera DHCP i WINS. Brak bramy domyślnej oznacza korzystanie z mechanizmu proxy ARP.



Użytkownicy systemów Windows NT/2000/XP:

Należy wpisać polecenie `ipconfig /all` i nacisnąć klawisz **Enter**.

W poniższym przykładzie, dotyczącym systemu Windows NT, 2000 lub XP, widać, że na podstawie wartości pola **DHCP Enabled (DHCP włączone)** można stwierdzić, czy usługa DHCP jest używana. Fakt ten potwierdza zawartość pól **DHCP Server (Serwer DHCP)**, **Lease Obtained (Dzierżawa uzyskana)** i **Lease Expires (Dzierżawa wygasa)**. W przypadku urządzenia skonfigurowanego statycznie ostatnie trzy pozycje nie byłyby widoczne, a pole **DHCP Enabled (DHCP włączone)** miałoby wartość **No (Nie)**.



```
C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : thunder
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . :
Description . . . . . : LNE100TX Fast Ethernet Adapter Version 1.0
Physical Address. . . . . : 00-A0-CC-23-FE-40
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 24.0.224.33
                        24.0.224.34
Lease Obtained. . . . . : Tuesday, January 09, 2001 10:56:19 AM
Lease Expires . . . . . : Monday, January 15, 2001 10:56:19 AM

C:\>
```

Czy w sieci jest uruchomiona usługa DHCP? _____

Jeśli trudno jest stwierdzić, czy usługa DHCP jest uruchomiona, poproś o pomoc instruktora lub asystenta.

Jaka jest długość okresu dzierżawy DHCP? _____

Serwery DHCP przypisują adres IP na określony czas, zazwyczaj na kilka dni. Rzeczywista długość tego okresu może jednak zostać zmieniona przez administratora sieci. Gdy dzierżawa wygasa, adres IP jest zwracany do puli adresów wolnych i może być użyty przez inne hosty. Dzięki temu w ramach usługi DHCP możliwe jest odzyskanie nieaktywnych adresów IP bez konieczności ręcznej aktualizacji danych. Organizacja, która ma zbyt mało adresów IP, żeby przypisać je wszystkim użytkownikom, może używać bardzo krótkich okresów dzierżawy, dzięki czemu adresy są ponownie używane nawet podczas krótkiej nieaktywności.

Komputer włączony i podłączony do sieci będzie automatycznie żądał wydłużenia dzierżawy. Dzięki temu, jeżeli komputer jest używany regularnie, nie następuje wygaśnięcie dzierżawy.

Czasami komputer jest przenoszony z jednej sieci do innej, różniącej się częścią adresu IP identyfikującą sieć. W takiej sytuacji komputer może nadal zachowywać ustawienia dotyczące starej sieci i nie będzie mógł połączyć się z nową siecią. Jednym z rozwiązań jest zwolnienie i odnowienie dzierżawy. Te operacje można przeprowadzić także dla komputerów skonfigurowanych statycznie, ale nie spowoduje to żadnej zmiany. Komputery podłączone bezpośrednio do dostawcy usług internetowych mogą utracić połączenie i trzeba będzie uzyskać je ponownie, ale nie wystąpią żadne trwałe zmiany. Aby zwolnić i odnowić dzierżawę usługi DHCP, należy wykonać poniższe czynności:

Użytkownicy systemów Windows NT/2000/XP:

Wpisz polecenie `ipconfig /release` i naciśnij klawisz **Enter**. Po obejrzeniu wyników wpisz polecenie `ipconfig /renew`.

Po tej procedurze najprawdopodobniej zostaną wyświetlone te same ustawienia, ponieważ w rzeczywistości komputer nie zmienił lokalizacji. Jeżeli komputer zostałby przeniesiony w sposób opisany powyżej, pojawiłyby się nowe ustawienia.

Użytkownicy systemów Windows 95/98/ME:

Naciśnij przycisk **Release All (Zwolnij wszystko)**. Po obejrzeniu wyników naciśnij przycisk **Renew All (Odnów wszystko)**.

Po tej procedurze najprawdopodobniej zostaną wyświetlone te same ustawienia, ponieważ w rzeczywistości komputer nie zmienił lokalizacji. Jeżeli komputer zostałby przeniesiony w sposób opisany powyżej, pojawiłyby się nowe ustawienia.

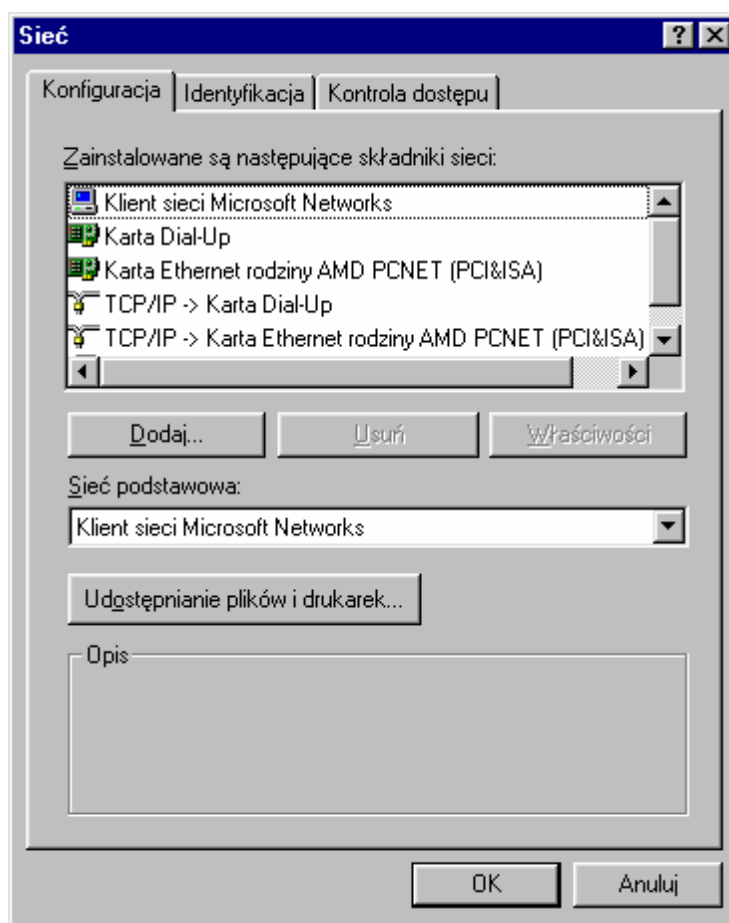
Krok 4 Korzystanie z okna konfiguracji sieci

Kliknij prawym przyciskiem znajdującą się na Pulpicie ikonę **Network Neighborhood (Otoczenie sieciowe)** lub **My Network Places (Moje miejsca sieciowe)** i wybierz polecenie **Properties (Właściwości)**. Jeżeli na komputerze nie widać żadnej z tych ikon, użyj menu Start w następujący sposób:

Wybierz kolejno polecenia: **Start > Settings (Ustawienia) > Control Panel (Panel sterowania)**.

Kliknij dwukrotnie ikonę **Network (Sieć)**.

Na niektórych komputerach zostanie wyświetlone okno właściwości sieci, takie jak przedstawione poniżej.



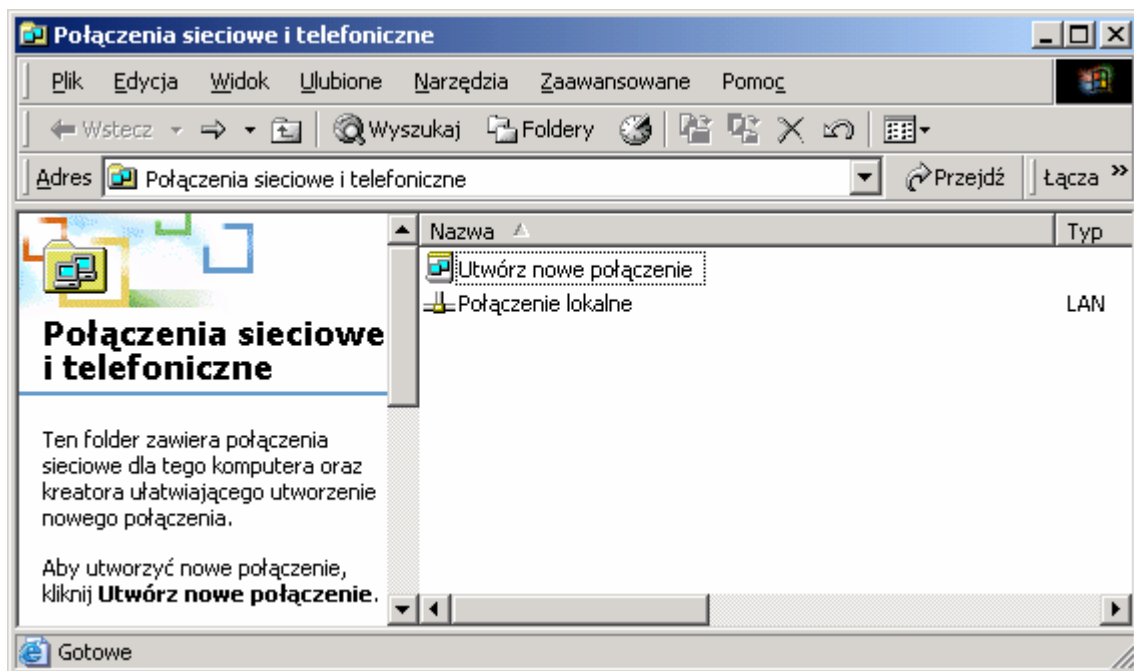
W innych wersjach systemu Windows będą wyświetlane inne zakładki, a zawartość okna zainstalowanych składników sieci będzie zależała od aktualnej konfiguracji danego komputera. Tym niemniej wyświetlone okno powinno być podobne do przedstawionego powyżej.

Większość użytkowników systemów Windows 95, 98 i Windows ME powinna w tym miejscu zobaczyć okno właściwości sieci. Tak więc jeżeli zostanie wyświetlone okno podobne do pokazanego powyżej, należy przejść do następnego kroku.

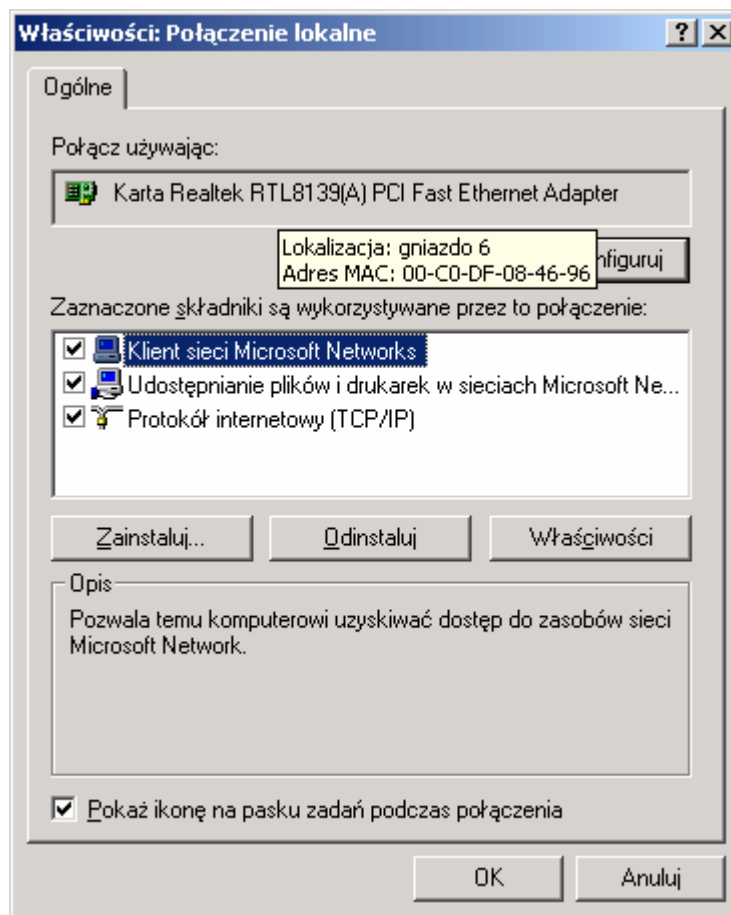
Użytkownicy systemów Windows 2000 i XP muszą wykonać jeszcze dwie dodatkowe czynności:

Najpierw dwukrotnie kliknij ikonę **Local Area Connection (Lokalne połączenia sieciowe)**.

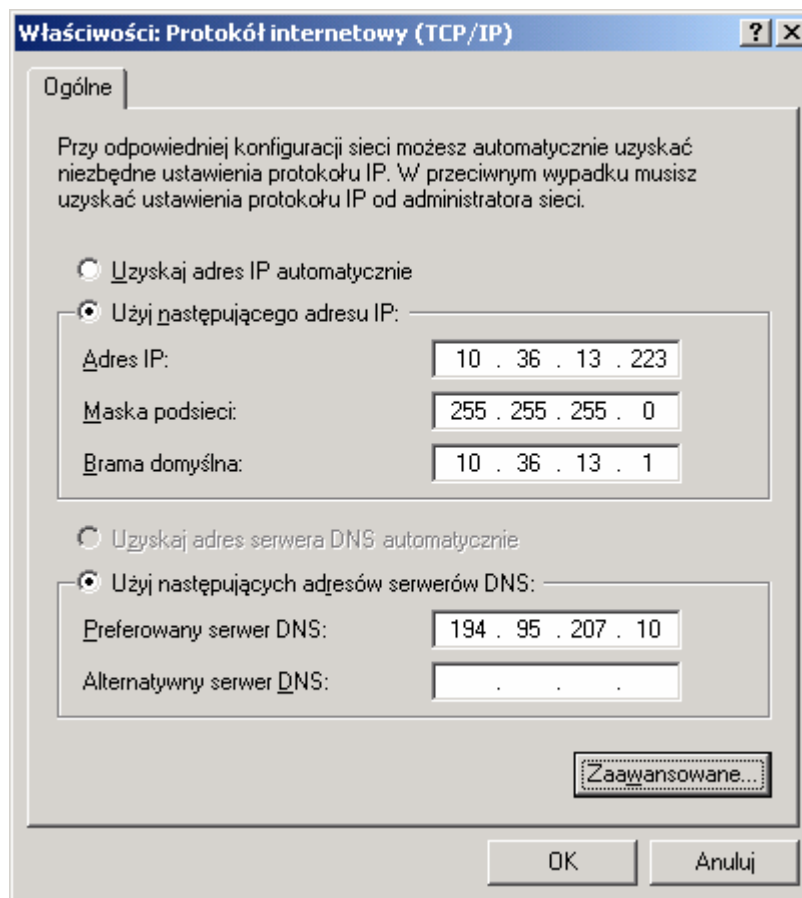
Po pojawieniu się okna **Local Area Connection Status (Stan połączenia LAN)** kliknij przycisk **Properties (Właściwości)**. Spowoduje to wyświetlenie okna **Local Area Connection Properties (Właściwości połączenia LAN)**, takiego jak przedstawione w następnym kroku.



W oknie właściwości sieci znajdź składnik o nazwie TCP/IP. Jeżeli wyświetlany jest więcej niż jeden taki składnik, wybierz ten, który odpowiada za aktualne połączenie sieciowe, na przykład związany z kartą sieciową lub modemem. W systemach Windows 2000 i XP okno to będzie wyglądało następująco:



Wybierz odpowiedni składnik i kliknij przycisk **Properties (Właściwości)** lub dwukrotnie kliknij sam składnik. Wygląd okna, które pojawia się po wykonaniu tej czynności, również zależy od używanej wersji systemu Windows, jednak dostępne czynności i używane pojęcia pozostają takie same. Użytkownicy systemów Windows 2000 i XP powinni zobaczyć okno bardzo podobne do poniższego. Pierwszą rzeczą, na którą należy zwrócić uwagę, jest to, że przykładowy komputer jest skonfigurowany statycznie.



Krok 5 Włączanie usługi DHCP

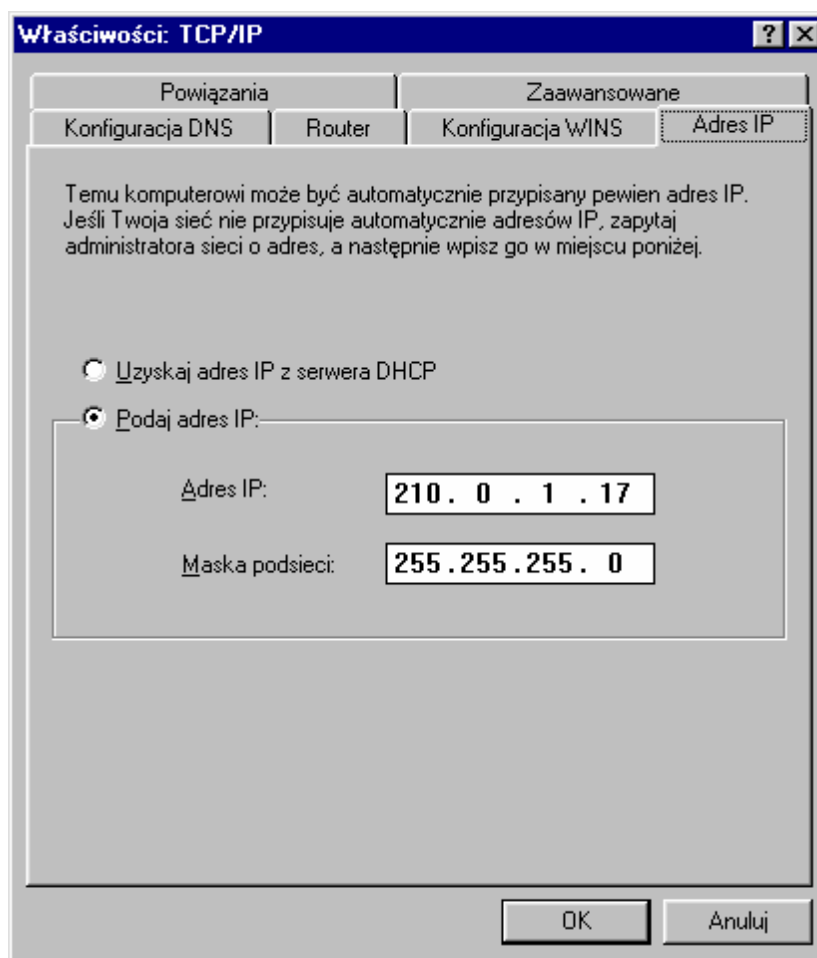
Aby rozpocząć korzystanie z usługi DHCP, wybierz opcję **Obtain an IP address automatically (Automatycznie uzyskaj adres IP)**. Zwykle należy także wybrać opcję **Obtain DNS server address automatically (Automatycznie uzyskaj adres serwera DNS)**. Po wybraniu tych opcji zostanie usunięta zawartość pozostałych pól. Jeżeli komputer używał adresowania statycznego, którego nie należy zmieniać, kliknij przycisk **Cancel (Anuluj)**. Aby zachować zmienione ustawienia, kliknij przycisk **OK**.

W starszych wersjach systemu Windows w tym oknie wyświetlane są różne zakładki. Najpierw na początkowej karcie wybierz opcję **Obtain an IP address automatically (Automatycznie uzyskaj adres IP)**, a następnie przejdź do zakładki **DNS Configuration (Konfiguracja DNS)** i wybierz opcję **Obtain DNS server address automatically (Automatycznie uzyskaj adres serwera DNS)**.

Gdyby zachodziła konieczność zmiany konfiguracji komputera ze statycznej na dynamiczną, należałoby usunąć wszystkie pozycje na zakładkach **Gateway (Brama)** i **WINS Configuration (Konfiguracja WINS)**.

Jeżeli komputer używał adresowania statycznego, którego nie należy zmieniać, kliknij przycisk **Cancel (Anuluj)**.

Aby zachować zmienione ustawienia, kliknij przycisk **OK**.



W starszych wersjach systemu Windows konieczne będzie ponowne uruchomienie komputera. Systemy Windows 2000 i XP zwykle nie będą wymagały ponownego uruchomienia.

W systemie Windows 95 w celu zakończenia tego procesu może okazać się konieczne włożenie instalacyjnej płyty CD-ROM.

Przy rzeczywistej zmianie konfiguracji na obsługę DHCP należałoby powtórzyć krok 3, aby upewnić się, czy konfiguracja jest prawidłowa.

Do przemyślenia

Dlaczego administrator sieci często wyłącza dostęp do przedstawionych wyżej okien i ustawień, przez co uniemożliwia użytkownikom wykonywanie zmian? _____

Jakie potencjalne korzyści może odnieść administrator sieci, używając w swojej sieci serwera DHCP? _____

Uwaga: Wiele małych routerów, przeznaczonych do korzystania z łącza DSL, ISDN lub sieci telewizji kablowej ma włączoną domyślnie obsługę DHCP. Pozwala to na współdzielenie połączenia sieciowego przez dodatkowe komputery przy użyciu koncentratora lub przełącznika. Każdy komputer trzeba skonfigurować tak, jak pokazano w tym ćwiczeniu. Zwykle serwer DHCP przypisuje adresy należące do jednej z sieci prywatnych (takich jak 192.168.1.0), które są do tego przeznaczone. Zwykle można zmienić te ustawienia, jednak najpierw należy przeczytać podręcznik użytkownika i przyswoić sobie zawarte tam informacje. Należy także dowiedzieć się, gdzie znajduje się przycisk przywracania wartości domyślnych **Reset Defaults (Przywróć domyślne)**.

Ćwiczenie 9.3.7 Protokół ARP na stacji roboczej

Cele

- Zapoznanie się z protokołem odwzorowania adresów ARP (ang. *Address Resolution Protocol*) i poleceniem `arp -a`.
- Zapoznanie się z możliwością uzyskania pomocy dla polecenia `arp` przy użyciu opcji `-?`.

Wprowadzenie i przygotowanie

Program ARP służy do sprawdzania, czy adresy sieciowe warstwy 3 są w komputerze prawidłowo przyporządkowywane adresom MAC warstwy 2. Działanie protokołu sieciowego TCP/IP jest oparte na adresach IP (przykład takiego adresu to 192.168.14.211), które identyfikują pojedyncze urządzenia i pomagają kierować pakiety danych do odpowiednich sieci. Chociaż adres IP jest konieczny do przeniesienia danych z jednej sieci LAN do innej, nie wystarcza jednak do dostarczenia tych danych w docelowej sieci LAN. Protokoły sieci lokalnych, takie jak Ethernet lub Token Ring, używają adresów MAC do identyfikowania urządzeń i dostarczania danych. Adres MAC komputera występował już we wcześniejszych ćwiczeniach.

Przykładowy adres MAC wygląda następująco:

- **00-02-A5-9A-63-5C**

Adres MAC jest adresem złożonym z 48 bitów, które przedstawia się w postaci szesnastkowej jako sześć oddzielonych myślnikami grup po dwa znaki kodu szesnastkowego. W tym formacie każdy symbol reprezentuje 4 bity. Niektóre urządzenia mogą pokazywać te dwanaście znaków szesnastkowych w postaci trzech rozdzielonych kropkami lub dwukropkami grup po cztery znaki (0002.A59A.635C).

Usługa ARP zarządza w komputerze tablicą odwzorowań adresów IP i MAC. Inaczej mówiąc, „pamięta” ona, jaki adres MAC jest związany z danym adresem IP. Jeżeli tablica odwzorowań usługi ARP nie zawiera adresu MAC urządzenia lokalnego, wówczas usługa wysyła pakiet rozgłoszeniowy z poszukiwanym adresem IP. Pakiet rozgłoszeniowy szuka adresu MAC odpowiadającego temu adresowi IP. Jeżeli w sieci znajduje się host o takim adresie IP, wyśle on odpowiedź, na podstawie której usługa ARP określi jego adres MAC. Spowoduje to dodanie takiej pary adresów do tablicy ARP na komputerze, z którego zostało wysłane żądanie.

Adresy MAC, a więc i protokół ARP, są używane jedynie wewnątrz sieci LAN. Podczas przygotowywania na komputerze pakietu do transmisji następuje sprawdzenie, czy docelowy adres IP należy do sieci lokalnej. Polega to na skontrolowaniu, czy część adresu IP identyfikująca sieć jest taka sama, jak adres sieci lokalnej. Jeżeli tak, komputer przy pomocy usługi ARP pobiera adres MAC urządzenia docelowego. Znaleziony w ten sposób adres MAC służy jako adres docelowy dla pakietów z danymi.

Jeżeli docelowy adres IP nie jest adresem lokalnym, komputer musi znaleźć adres MAC bramy domyślnej. Brama domyślna jest interfejsem routera, do którego przyłączona jest sieć lokalna, i który zapewnia łączność z innymi sieciami. Adres MAC bramy jest potrzebny dlatego, że pakiety są przesyłane właśnie do niej, a router przesyła je dalej do sieci, dla której są przeznaczone.

Jeżeli komputer w ciągu kilku minut nie otrzyma żadnych pakietów od danego adresu IP, wtedy adres ten, razem z odpowiadającym mu adresem MAC, zostanie usunięty z tabeli usługi ARP, ponieważ sytuacja taka oznacza, że urządzenie zostało wyłączone. Późniejsze próby użycia takiego

adresu IP spowodują ponowne wysłanie pakietu rozgłoszeniowego przez usługę ARP i zaktualizowanie tabeli.

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 sieci znajdującej się w klasie lub w innej sieci LAN mającej połączenie z Internetem. Można je przeprowadzić, korzystając z pojedynczego połączenia modemowego lub połączenia DSL.

Krok 1 Ustawianie połączenia sieciowego

Jeżeli połączenie z Internetem następuje poprzez łącze komutowane, połącz się z dostawcą usług internetowych, aby komputer otrzymał adres IP. W sieci LAN TCP/IP zawierającej serwer DHCP nie ma konieczności wykonywania tego kroku.

Krok 2 Otwieranie okna wiersza poleceń

Użytkownicy systemów Windows NT/2000/XP:

Użyj menu Start, aby otworzyć okno Wiersz poleceń. Okno Wiersz poleceń jest podobne do okna Tryb MS-DOS znajdującego się w innych wersjach systemu Windows.

Wybierz kolejno polecenia: **Start > Programs (Programy) > Accessories (Akcesoria) > Command Prompt (Wiersz poleceń)** lub **Start > Programs (Programy) > Command Prompt (Wiersz poleceń)**.

Użytkownicy systemów Windows 95/98/ME:

Użyj menu Start, aby otworzyć okno MS-DOS Prompt (Tryb MS-DOS).

Wybierz kolejno polecenia: **Start > Programs (Programy) > Accessories (Akcesoria) > MS-DOS Prompt (Tryb MS-DOS)** lub **Start > Programs (Programy) > MS-DOS Prompt (Tryb MS-DOS)**.

Krok 3 Wyświetlanie tabeli ARP

- Wpisz polecenie `arp -a` i naciśnij klawisz **Enter**. Nie dziw się, jeśli nie zostaną wyświetlone żadne pozycje. Zostanie wówczas najprawdopodobniej wyświetlony komunikat „No ARP Entries Found” („Nie znaleziono wpisów ARP”). Komputery z systemem Windows usuwają każdy adres, który nie jest używany przez kilka minut.
- Wyślij pakiety ping na kilka lokalnych adresów oraz na wybrany adres URL strony WWW. Wykonaj ponownie polecenie `arp -a`. Na rysunku przedstawiony jest przykładowy wynik działania polecenia `arp -a`. W tabeli nie ma adresu MAC strony WWW, ponieważ nie jest to adres lokalny, ale próba uzyskania do niego dostępu spowoduje pojawienie się w tabeli adresu bramy domyślnej. W poniższym przykładzie adres 10.36.13.1 jest adresem bramy domyślnej, a adresy 10.36.13.92 i 10.36.13.101 należą do innych komputerów w sieci. Proszę zauważyć, że dla każdego adresu IP wyświetlony jest zarówno adres fizyczny MAC, jak i sposób, w jaki adres ten został znaleziony.
- Z poniższego rysunku można wywnioskować, że sieć ma adres 10.36.13.0, a komputery w tej sieci są identyfikowane poprzez końcówki 223, 1, 92 i 101.

```
C:\>arp -a

Interface: 10.36.13.223 on Interface 0x1000003
 Internet Address      Physical Address      Type
 10.36.13.1            00-00-5e-00-01-0a    dynamic
 10.36.13.92          00-01-02-84-60-85    dynamic
 10.36.13.101         00-50-8b-fa-30-05    dynamic

C:\>_
```

Krok 4 Wysyłanie pakietów ping na kilka adresów URL

- a. Wyślij pakiety ping na poniższe adresy URL i zapisz odpowiadające im adresy IP. Wybierz także jeden dodatkowy adres URL i zapisz go poniżej.

www.cisco.com: _____

www.msn.de: _____

_____:

- b. Ponownie wykonaj polecenie `arp -a`. Spróbuj zapisać adresy MAC każdego z powyższych serwerów obok ich adresów IP. Czy można to zrobić? _____

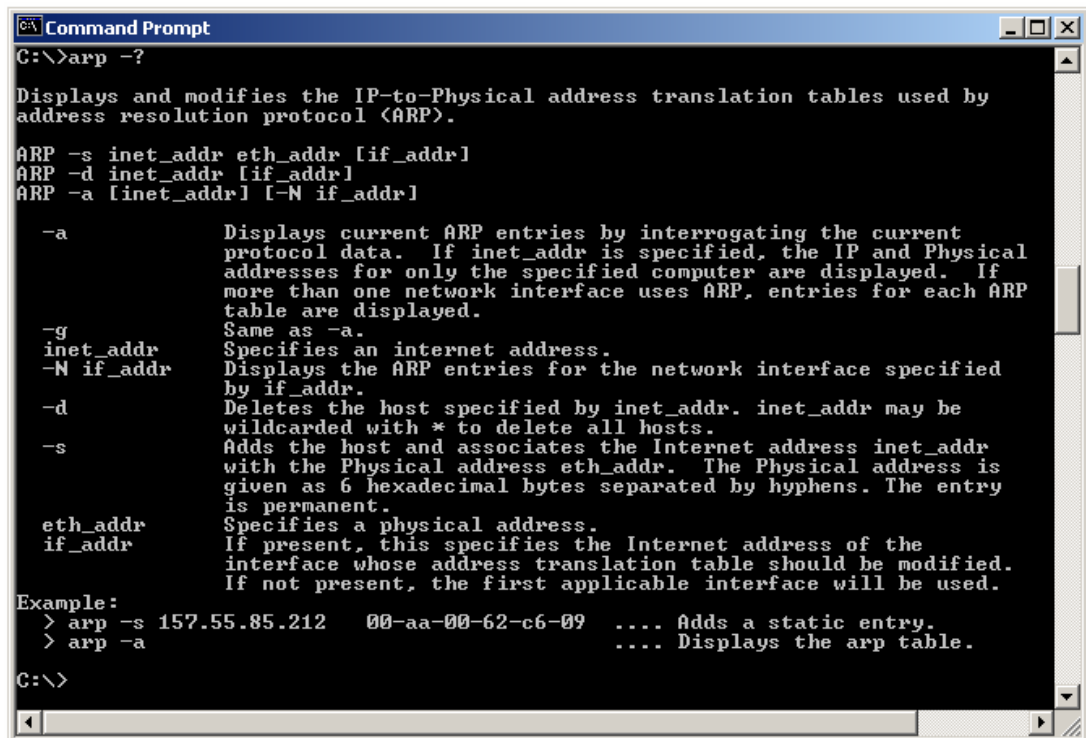
- c. Dlaczego tak sądzisz? _____

- d. Jaki adres MAC był używany przy przesyłaniu pakietów ping do serwerów określonych tymi adresami URL? _____

_____ Dlaczego? _____

Krok 4 Korzystanie z pomocy dla polecenia ARP

Aby wyświetlić pomoc, wykonaj polecenie `arp -?` i przyjrzyj się wyświetlanym opcjom.



```
Command Prompt
C:\>arp -?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

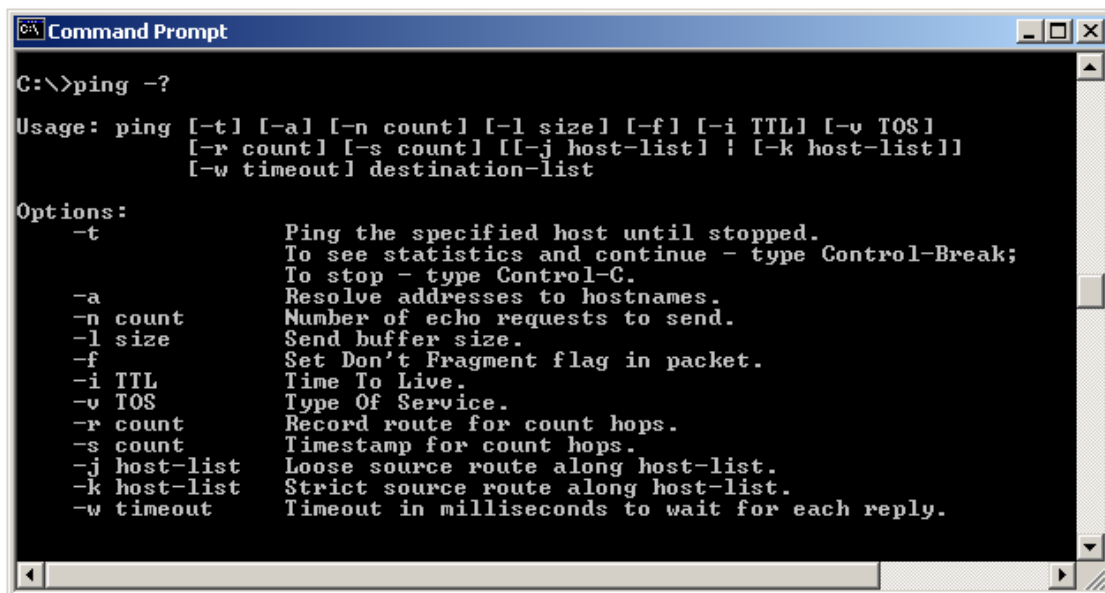
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.

C:\>
```

Celem tego kroku jest nie tyle poznanie opcji usługi ARP, co wskazanie możliwości uzyskania pomocy przy użyciu opcji `?`, jeżeli pomoc ta jest dostępna. Pomoc nie zawsze jest wywoływana w ten sposób. W niektórych poleceniach zamiast opcji `-?` używa się `/?`.

Krok 5 Korzystanie z pomocy do poleceń tracert i ping

Aby poznać dostępne opcje używanych wcześniej poleceń, wykonaj polecenia `tracert -?` i `ping -?`.



```
C:\>ping -?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] destination-list

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.
  -f           Set Don't Fragment flag in packet.
  -i TTL       Time To Live.
  -v TOS       Type Of Service.
  -r count     Record route for count hops.
  -s count     Timestamp for count hops.
  -j host-list Loose source route along host-list.
  -k host-list Strict source route along host-list.
  -w timeout   Timeout in milliseconds to wait for each reply.
```

W pomocy do polecenia ping można zauważyć opcję `-t`, która powoduje ciągłe wysyłanie pakietów ping, bez ograniczania ich liczby do czterech. Ważniejsze jednak są następujące dwa polecenia, które zatrzymują wysyłanie pakietów:

- **Control-Break**
- **Control-C**

Te dwie kombinacje klawiszy są często używane do zatrzymywania działania poleceń. Spróbuj wysłać pakiety ping do sąsiedniego komputera, używając opcji `-t`, a następnie wypróbuj działanie kombinacji klawiszy Control-Break i Control-C. Na przykład dla powyższej sieci można wpisać polecenie `ping 10.36.13.101 -t` i nacisnąć klawisz **Enter**.

Pamiętaj o użyciu kombinacji klawiszy **Control-C** do zakończenia wysyłania pakietów ping.

Do przemyślenia

Co można wywnioskować z poniższych wyników w oparciu o poczynione dziś obserwacje?

Komputer 1

Adres IP: 192.168.12.113

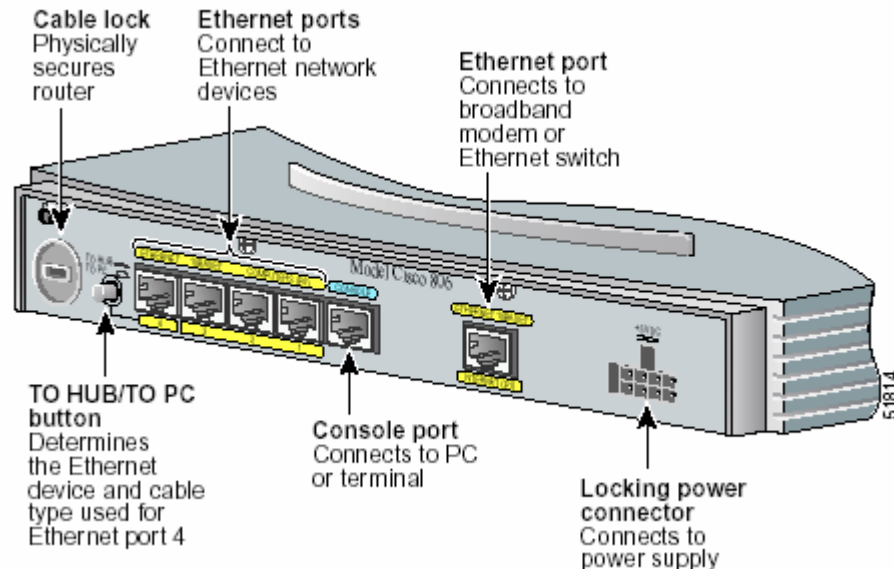
Maska podsieci: 255.255.255.0

Brama domyślna: 192.168.12.1

Pakiety ping i tracert dotarły bez przeszkód do 207.46.28.116.

Jak będzie wyglądała tabela ARP związana z tym adresem. Dlaczego właśnie tak?

Ćwiczenie 10.2.9 Zakup niewielkiego routera



Cele

Przedstawienie różnorodnych komponentów sieciowych dostępnych na rynku oraz ich cen. Ćwiczenie to będzie dotyczyło w szczególności niewielkich routerów używanych przez telepracowników podczas pracy w domu. W opisie wskazano witrynę WWW <http://www.cisco.com>, ale można użyć dowolnego lokalnego źródła, katalogu czy witryny WWW.

Wprowadzenie i przygotowanie

Niektórzy członkowie kierownictwa firmy, pracujący w domu za pośrednictwem połączeń kablowych i DSL, chcieliby, aby ich połączenia były bezpieczniejsze. Zażądali oni opracowania projektu zakupu niewielkich routerów, które można wykorzystać do tego celu. Przedmiotem zadania jest analiza przynajmniej dwóch różnych rozwiązań i opracowanie propozycji. Szczegóły dotyczące projektu są następujące:

- Pracownicy działu informatycznego firmy kładą nacisk na niezawodność rozwiązania.
- Ważne jest, aby nie wykorzystywać i nie obsługiwać zbyt wielu modeli urządzeń.
- Firma w swej sieci korporacyjnej korzysta z routerów Cisco.
- Firma chciałaby móc objąć zdalnych użytkowników takimi funkcjami systemu Cisco IOS, jak VPN i zaporę (firewall).

Podczas rozmów z kierownictwem i personelem wsparcia stało się jasne, że niektórzy pracownicy mieszkają na obszarach, na których usługa transmisji danych poprzez DSL lub telewizję kablową nie jest dostępna. Należy więc także wziąć pod uwagę modele urządzeń obsługujące połączenia ISDN.

Wymagania dotyczące propozycji obejmują następujące elementy:

- 12 routerów obsługujących połączenia DSL lub kablowe,
- 3 routery obsługujące połączenia ISDN,
- wszystkie urządzenia muszą obsługiwać funkcje Cisco IOS.

Zakłada się, że dostawca usług dostarczy każdy wymagany modem oraz że router zostanie z nim połączony poprzez interfejs Ethernet.

Kilku członków kierownictwa wyraziło zainteresowanie możliwością podłączenia 2 lub 3 komputerów do tego samego łącza. Można przyjąć bezpieczne założenie, że takie żądanie będzie dotyczyć większości użytkowników.

Krok 1 Analiza cen sprzętu

Rozpocznij od przejścia do witryny <http://www.cisco.com>, wybrania pozycji **Products & Services** (Produkty i usługi) i kliknięcia łącza **Routers** (Routery) w celu uzyskania podstawowych informacji. Zwróć szczególną uwagę na modele 700 i 800 oraz na modele przeznaczone dla małego biura i biura domowego (SOHO).

W dziale Overview (Przegląd) poszukaj dokumentacji technicznej, prezentacji i broszur. Mogą one zawierać dane i rysunki przydatne podczas finalnej prezentacji.

Porównaj dostępne technologie i ceny z przynajmniej trzema innymi źródłami. Jeśli korzystasz z wyszukiwarek WWW, spróbuj użyć adresów <http://www.cdw.com>, <http://www.google.com> lub dowolnego innego preferowanego mechanizmu wyszukiwania.

Krok 2 Utworzenie jednostronicowego podsumowania wyników poszukiwań

Do przygotowania podsumowania wyników użyj aplikacji Microsoft Excel, Microsoft Word lub dowolnego innego produktu o podobnych możliwościach. Umieść w nim składający się z 8 do 15 wierszy krótki opis przyczyn wyboru danej implementacji. Dołącz również prosty diagram prezentujący następujące elementy:

- router,
- komputery PC,
- przewód zasilania,
- modem kablowy lub DSL.

Krok 2 (opcjonalnie)

Zamiast przygotowywać powyższe dokumenty programu Excel lub Word, przy użyciu aplikacji PowerPoint utwórz od 4 do 8 slajdów prezentacji spełniającej te same wymagania.

Podczas przygotowywania materiałów przyjmij założenie, że będą one musiały zostać zaprezentowane.

Jeśli czas na to pozwoli, wykonaj zarówno krok 2, jak i opcjonalną prezentację. Takie wymagania często pojawiają się w pracy zawodowej.

Ćwiczenie 10.3.5a Podstawy podsieci

Cele

- Określenie przyczyn użycia masek podsieci
- Rozróżnienie domyślnej i niestandardowej maski podsieci
- Określenie maski podsieci, liczby podsieci i liczby hostów przypadających na podsieć w oparciu o podane wymagania
- Przedstawienie niezbędnych informacji o możliwych do użycia podsieciach i liczbie możliwych do użycia hostów
- Opisanie sposobu używania operacji iloczynu logicznego (AND) do określenia, czy docelowy adres IP jest lokalny, czy zdalny
- Opisanie metody identyfikacji prawidłowego i nieprawidłowego adresu IP hosta w oparciu o numer sieci i maskę podsieci

Wprowadzenie i przygotowanie

W tym ćwiczeniu skupiono się na podstawach użycia masek IP podsieci i ich zastosowaniu w sieciach TCP/IP. Maska podsieci może służyć do podzielenia istniejącej sieci na podsieci. Oto niektóre z głównych powodów stosowania podsieci:

- Zmniejszony rozmiar domen rozgłoszeniowych, dzięki czemu tworzone są mniejsze sieci, gdzie ruch jest mniejszy
- Umożliwienie komunikacji między sieciami LAN położonymi w różnych miejscach
- Zapewnienie większego bezpieczeństwa poprzez rozdzielenie sieci LAN

Routerzy rozdzielają podsieci i określają, kiedy pakiet może zostać przesłany z jednej podsieci do drugiej. Każdy router, przez który jest przesyłany pakiet, nazywany jest przeskokiem. Maski podsieci ułatwiają stacjom roboczym, serwerom i routerom w sieci IP określenie, czy host docelowy, do którego ma być wysłany pakiet, znajduje się w tej samej sieci, czy w innej. W tym ćwiczeniu przedstawiono domyślne maski podsieci, a następnie skupiono się na niestandardowych maskach podsieci. Niestandardowe maski podsieci korzystają z większej liczby bitów niż domyślne maski podsieci poprzez „pożyczenie” tych bitów z części hosta adresu IP. Powoduje to powstanie trzyczęściowego adresu składającego się z następujących elementów:

- początkowy adres sieciowy;
- adres podsieci złożony z pożyczonych bitów;
- adres hosta złożony z bitów pozostałych po pożyczeniu pewnej ich części w celu wyznaczenia podsieci.

Krok 1 Przegląd struktury adresów IP

Jeśli dana organizacja dysponuje adresem IP klasy A, pierwszy oktet, czyli 8 bitów, jest wstępnie przypisany i nie zmienia się. Pozostałe 24 bity mogą służyć do zdefiniowania maksymalnie 16 777 214 hostów w danej sieci. To duża liczba hostów. Nie jest możliwe umieszczenie tylu hostów w jednej sieci fizycznej bez rozdzielenia ich routerami i podsieciami.

Często można spotkać się z sytuacją, w której stacja robocza znajduje się w jednej sieci lub podsieci, a serwer w innej. Gdy stacja robocza ma pobrać plik z serwera, używa swojej maski podsieci do określenia, czy serwer znajduje się w tej samej czy innej sieci lub podsieci. Zadaniem masek podsieci jest ułatwienie hostom i routerom określenia lokalizacji sieciowej, w której znajduje się host docelowy. Skorzystaj z poniższej tabeli w celu przejrzania następujących informacji:

- klasy adresu IP;
- domyślne maski podsieci;
- liczba sieci, które mogą być utworzone w ramach każdej klasy adresu sieciowego;
- liczba hostów, które mogą być utworzone w ramach każdej klasy adresu sieciowego.

Klasa adresu	Dziesiętny zakres 1. oktetu	Najbardziej znaczące bity 1. oktetu	Identyfikator sieci/hosta (N=sieć, H=host)	Domyślna maska podsieci	Liczba sieci	Liczba hostów w sieci (adresy użyteczne)
A	1–126 *	0	N.H.H.H	255.0.0.0	126 (2^7-2)	16,777,214 ($2^{24}-2$)
B	128–191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14}-2$)	65,534 ($2^{16}-2$)
C	192–223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21}-2$)	254 (2^8-2)
D	224–239	1110	Zarezerwowane dla transmisji grupowej			
E	240–254	11110	Eksperymentalne, używane w badaniach			

* Adres 127 klasy A nie może być wykorzystywany, ponieważ jest zarezerwowany dla pętli zwrotnej i funkcji diagnostycznych.

Krok 2 Przegląd operacji iloczynu logicznego (AND)

Hosty i routery używają operacji iloczynu logicznego do określenia, czy host docelowy znajduje się w tej samej sieci. Operacja ta jest wykonywana za każdym razem, gdy host ma wysłać pakiet do innego hosta w sieci IP. Aby połączyć się z serwerem, konieczna jest znajomość adresu IP serwera lub nazwy hosta, na przykład <http://www.cisco.com>. Jeśli użyta zostanie nazwa hosta, serwer DNS przekształci ją na adres IP.

Najpierw host źródłowy wykonuje operację porównania (iloczynu logicznego) swojego adresu IP z własną maską podsieci. W wyniku tej operacji możliwa jest identyfikacja sieci, w której znajduje się host źródłowy. Następnie dokonywane jest porównanie docelowego adresu IP z własną maską podsieci. Wynikiem drugiej operacji jest adres sieci, w której znajduje się host docelowy. Jeśli adresy sieci źródłowej i docelowej są takie same, możliwa jest bezpośrednia komunikacja. Jeśli wyniki są różne, oznacza to, że hosty znajdują się w różnych podsieciach. W tym przypadku host źródłowy i docelowy będą musiały komunikować się poprzez routery lub nie będą mogły komunikować się w ogóle.

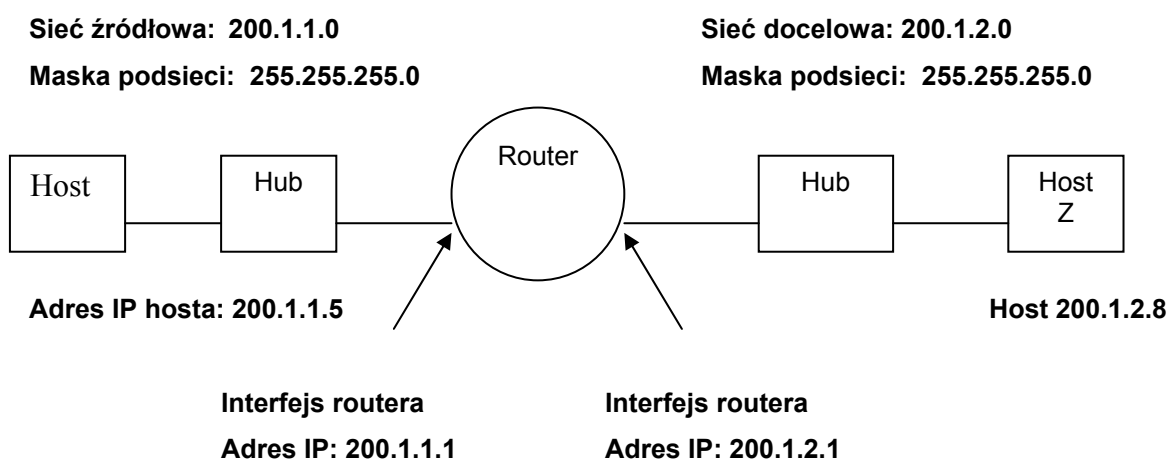
Operacja iloczynu logicznego zależy od maski podsieci. W masce podsieci jedynki logiczne odpowiadają tej części adresu IP, która oznacza sieć lub sieć + podsieć. Domyślna maska podsieci dla sieci klasy C to 255.255.255.0 lub 11111111.11111111.11111111.00000000. Jest ona porównywana z adresem IP nadawcy bit po bicie. Pierwszy bit adresu IP jest porównywany z pierwszym bitem maski podsieci, drugi z drugim itd. Jeśli oba bity są jedynkami, wynikiem iloczynu logicznego jest jedynka. Jeśli jeden z bitów jest zerem, a drugi jedynką, lub oba bity są zerami,

wynikiem jest zero. Oznacza to po prostu, że kombinacja dwóch jedynek da w wyniku jedynekę, a każda inna kombinacja — zero. W wyniku operacji iloczynu logicznego możliwa jest identyfikacja numeru sieci lub podsieci, w której znajduje się adres źródłowy lub docelowy.

Krok 3 Dwie sieci klasy C korzystające z domyślnej maski podsieci

W tym przykładzie pokazano, jak domyślna maska podsieci klasy C może posłużyć do określenia, w której sieci znajduje się host. Domyślna maska podsieci nie dzieli adresu na podsieci. Zastosowanie domyślnej maski podsieci sprawia, że sieć nie zostaje podzielona na podsieci. Host X będący hostem źródłowym w sieci 200.1.1.0 ma adres IP równy 200.1.1.5. Ma zostać z niego wysłany pakiet do hosta Z, będącego hostem docelowym w sieci 200.1.2.0 i mającego adres IP równy 200.1.2.8. Wszystkie hosty w każdej sieci są podłączone do koncentratorów lub przełączników, a następnie do routera. Należy pamiętać, że w adresie sieci klasy C pierwsze 3 oktety (24 bity) są przypisane jako adres sieci. Są to więc dwie różne sieci klasy C. Pozostał jeden oktet (8 bitów) na hosty, czyli każda sieć klasy C może zawierać do 254 hostów:

- $2^8 = 256 - 2 = 254$



Operacja iloczynu logicznego pomaga w przesłaniu pakietu z hosta 200.1.1.5 w sieci 200.1.1.0 do hosta 200.1.2.8 w sieci 200.1.2.0 dzięki zastosowaniu następującej procedury:

1. Host X za pomocą operacji iloczynu logicznego porównuje swój adres IP ze swoją maską podsieci.

Adres IP hosta X: 200.1.1.5	11001000.00000001.00000001.00000101
Maska podsieci: 255.255.255.0	11111111.11111111.11111111.00000000
Wynik operacji iloczynu logicznego (200.1.1.0):	11001000.00000001.00000001.00000000

Uwaga: Wynikiem operacji iloczynu logicznego jest adres sieci hosta X, czyli 200.1.1.0.

2. Następnie host X za pomocą operacji iloczynu logicznego porównuje adres IP docelowego hosta Z z własną maską podsieci.

Adres IP hosta Z: 200.1.2.8	11001000.00000001.00000010.00001000
Maska podsieci: 255.255.255.0	11111111.11111111.11111111.00000000
Wynik operacji iloczynu logicznego (200.1.2.0):	11001000.00000001.00000010.00000000

Uwaga: Wynikiem operacji iloczynu logicznego jest adres sieci hosta Z, czyli 200.1.2.0.

Host X porównuje wyniki operacji iloczynu logicznego z kroku 1 i 2, z czego płynie wniosek, że są one różne. Wiadomo już, że host Z nie znajduje się w tej samej sieci lokalnej (LAN) co host X. Z tego względu pakiet musi zostać wysłany do domyślnej bramy hosta X, to jest na adres IP interfejsu routera 200.1.1.1 w sieci 200.1.1.0. Następnie na routerze powtarza się operację iloczynu logicznego w celu określenia, do którego interfejsu routera ma być wysłany pakiet.

Krok 4 Jedna sieć klasy C z podsieciami korzystająca z niestandardowych masek podsieci

W tym przykładzie użyto jednego adresu sieci klasy C (200.1.1.0) i przedstawiono sposób użycia niestandardowej maski podsieci klasy C do określenia, w której podsieci znajduje się host, oraz do routingu pakietów z jednej podsieci do drugiej. Należy pamiętać, że w adresie sieci klasy C pierwsze 3 oktety (24 bity) odwzorowują adres sieci. Pozostaje jeden oktet (8 bitów) na hosty. Tak więc każda sieć klasy C może zawierać do 254 hostów:

- $2^8 = 256 - 2 = 254$

Przypuśćmy, że w sieci ma istnieć mniej niż 254 hostów, stacji roboczych i serwerów. Może to być spowodowane względami bezpieczeństwa lub potrzebą zmniejszenia ruchu. Efekt taki można osiągnąć poprzez utworzenie dwóch podsieci i rozdzielenie ich routerem. Spowoduje to utworzenie mniejszych, niezależnych domen rozgłoszeniowych, co może zwiększyć wydajność sieci oraz bezpieczeństwo. Jest to możliwe, ponieważ podsieci będą rozdzielone jednym lub kilkoma routerami. Założmy, że potrzebne będą przynajmniej dwie podsieci i że każda będzie zawierać przynajmniej 50 hostów. Ponieważ dostępny jest tylko jeden adres sieci klasy C, jedynie osiem bitów w czwartym okciecie jest dostępnych dla całkowitej liczby 254 hostów. Z tego względu należy utworzyć niestandardową maskę podsieci. Niestandardowa maska podsieci posłuży do „pożyczenia” bitów z części adresu odpowiadającego hostowi. Aby uzyskać taki efekt, należy wykonać poniższą procedurę:

1. Pierwszym krokiem w procesie tworzenia podsieci jest określenie wymaganej liczby podsieci. W tym przypadku wymagane są dwie podsieci. Aby zobaczyć, ile bitów należy pożyczyć z części hosta adresu sieciowego, należy dodać wartości bitów od prawej do lewej, aż uzyska się wartość równą lub większą niż liczba potrzebnych podsieci. Ponieważ potrzebne są dwie podsieci, należy dodać bit pierwszy i drugi, co w wyniku daje liczbę trzy. Wartość ta przekracza liczbę wymaganych podsieci. Aby osiągnąć żądany efekt, należy pożyczyć przynajmniej dwa bity z adresu hosta, począwszy od lewej strony oktetu zawierającego ten adres.

Adres sieci: 200.1.1.0

Bity adresu hosta w czwartym okciecie:	1	1	1	1	1	1	1
	1						
Wartości bitów adresu hosta:	128	64	32	16	8	4	<u>2</u>
	1						
(od prawej)							

Bity należy dodawać począwszy od prawej strony, najpierw 1, następnie 2 itd., aż suma będzie większa od liczby potrzebnych podsieci.

Uwaga: Alternatywnym sposobem obliczenia liczby bitów, które należy pożyczyć w celu utworzenia podsieci, jest podniesienie liczby 2 do potęgi odpowiadającej ilości pożyczonych bitów. Wynik musi być większy niż liczba potrzebnych podsieci. Na przykład jeśli zostaną pożyczone 2 bity, wynikiem podniesienia liczby 2 do potęgi drugiej będzie liczba cztery. Ponieważ liczba potrzebnych podsieci jest równa dwa, powyższy wynik będzie odpowiedni.

2. Gdy wiadomo już, ile bitów należy pożyczyć, należy je pobrać, począwszy od lewej strony adresu hosta w czwartym okciecie. Każdy bit pożyczony z adresu hosta pozostawia mniej bitów przeznaczonych dla hostów. Mimo iż liczba podsieci się zwiększy, liczba hostów przypadających

na każdą sieć ulegnie zmniejszeniu. Ponieważ dwa bity należy pożyczyć od strony lewej, nowa wartość musi być zaprezentowana w masce podsieci. Istniejąca domyślna maska podsieci była równa 255.255.255.0, a nowa niestandardowa maska podsieci jest równa 255.255.255.192. Liczba 192 powstaje w wyniku dodania dwóch pierwszych bitów od lewej strony, $128 + 64 = 192$. Te bity przyjęły wartość 1 i są częścią pełnej maski podsieci. Pozostawia to 6 bitów na adresy IP hostów, czyli $2^6 = 64$ hostów na podsieć.

Bity czwartego oktetu pożyczone na podsieć: 1 1 0 0 0 0 0 0

Wartości bitów podsieci (od lewej strony): 128 64 32 16 8 4 2 1

Dzięki tym informacjom można utworzyć następującą tablicę. Pierwsze dwa bity to binarna wartość podsieci.

Ostatnie sześć bitów to bity hosta. Pożyczając 2 z 8 bitów adresu hosta, można utworzyć 4 podsieci (2 do potęgi 2), z których każda może zawierać 64 hosty. Te cztery sieci tworzy się w następujący sposób:

- Sieć 200.1.1.0
- Sieć 200.1.1.64
- Sieć 200.1.1.128
- Sieć 200.1.1.192

Sieć 200.1.1.0 jest uważana jako bezużyteczna, chyba że urządzenie sieciowe obsługuje komendę IOS `ip subnet-zero`, która umożliwia użycie pierwszej podsieci.

Nr podsieci	Wartość binarna pożyczonych bitów podsieci	Dziesiętna wartość bitów podsieci	Możliwe binarne wartości bitów hosta (zakres) (6 bitów)	Dziesiętny zakres podsieci/hostów	Użyteczna?
Podsieć 0	00	0	000000–111111	0–63	Nie
Podsieć 1	01	64	000000–111111	64–127	Tak
Podsieć 2	10	128	000000–111111	128–191	Tak
Podsieć 3	11	192	000000–111111	192–254	Nie

Należy zwrócić uwagę, że pierwsza podsieć zawsze rozpoczyna się od wartości 0, a wartość odpowiadająca każdej następnej w tym przypadku jest większa od poprzedniej o 64, co jest równe liczbie hostów w każdej podsieci. Jednym ze sposobów określenia liczby hostów w każdej podsieci lub wartości początkowej dla każdej podsieci jest podniesienie liczby 2 do wartości będącej ilością pozostałych bitów hosta. Ponieważ pożyczone zostały dwa bity z ośmiu, pozostało sześć bitów, więc liczba hostów w każdej podsieci wynosi 2^6 , czyli 64. Innym sposobem określenia liczby hostów w każdej podsieci lub przyrostu między kolejnymi podsieciami jest odjęcie od liczby 256, będącej maksymalną liczbą możliwych kombinacji ośmiu bitów, dziesiętnej wartości maski podsieci w czwartym oktecie — 192. Wynikiem jest liczba 64. Oznacza to, że pierwsza sieć rozpoczyna się od wartości 0, a każda następna od wartości powiększonej o 64. Jeśli na przykład zostanie użyta druga podsieć, sieć 200.1.1.64 nie może służyć jako identyfikator hosta, ponieważ identyfikator podsieci o wartości 64 składa się z samych zer w części hosta.

Innym popularnym sposobem przedstawienia maski podsieci jest użycie notacji z ukośnikiem: „/#”, gdzie symbol # znajdujący się po ukośniku to liczba bitów użytych w masce (połączona sieć i podsieć). Na przykład adres sieciowy klasy C, taki jak 200.1.1.0, ze standardową maską podsieci (255.255.255.0) można zapisać jako 200.1.1.0 /24, co wskazuje, że w masce użyte są 24 bity. Ta

sama sieć podzielona na podsieci przez użycie dwóch bitów hosta dla podsieci może być zapisana jako 200.1.1.0 /26. Oznacza to, że 24 bity są użyte dla sieci, a 2 bity określają podsieć. To oznacza niestandardową maskę podsieci równą 255.255.255.192 w notacji dziesiętnej kropkowej.

Sieć klasy A 10.0.0.0 z maską standardową (255.0.0.0) może być zapisana jako 10.0.0.0 /8. Jeśli 8 bitów (następny oktet) zostanie użytych dla określenia podsieci, odpowiadałoby to zapisowi 10.0.0.0 /16. Oznaczać to będzie niestandardową maskę podsieci równą 255.255.0.0 w notacji dziesiętnej kropkowej. Liczba po ukośniku występującym po numerze sieci to skrócona metoda wskazania, jaka maska podsieci została użyta.

Krok 5 Odpowiedz na następujące pytania dotyczące podsieci, opierając się na poniżej przedstawionych informacjach i poprzednich przykładach

Firma wystąpiła o adres sieci klasy C i otrzymała adres 197.15.22.0. Sieć fizyczna musi być podzielona na 4 podsieci, które będą połączone routerami. W każdej podsieci będzie wymaganych przynajmniej 25 hostów. Musi być użyta niestandardowa maska podsieci klasy C oraz wymagany jest router między podsieciami do przeprowadzania routingu pakietów z jednej podsieci do pozostałych. Należy określić liczbę bitów, które należy pożyczyć z części hosta adresu sieci, oraz liczbę bitów, która pozostanie na adresy hostów.

Uwaga: Dostępnych będzie 8 podsieci, z czego 6 będzie nadawało się do użycia.

Wypełnij poniższą tabelę i odpowiedz na następujące pytania:

Nr podsieci	Wartość binarna pożyczonych bitów podsieci	Dziesiętna wartość bitów podsieci i numer podsieci	Możliwe binarne wartości bitów hosta (zakres) (5 bitów)	Dziesiętny zakres podsieci/hostów	Do wykorzystania ?
Podsieć 0					
Podsieć 1					
Podsieć 2					
Podsieć 3					
Podsieć 4					
Podsieć 5					
Podsieć 6					
Podsieć 7					

UWAGI:

Skorzystaj z wypełnionej tabeli jako pomocy podczas odpowiadania na poniższe pytania:

1. Które oktety oznaczają część sieci adresu IP klasy C? _____
2. Które oktety oznaczają część hosta adresu IP klasy C? _____
3. Jaki jest binarny odpowiednik adresu sieci klasy C w tym scenariuszu? **197.15.22.0**
Adres sieci w postaci dziesiętnej: _____
Adres sieci w postaci binarnej: _____
4. Ile najbardziej znaczących bitów zostało pożyczonych z bitów hosta w czwartym oktecie?

5. Która maska podsieci musi być użyta? Przedstaw maskę podsieci w postaci dziesiętnej i binarnej.
Maska podsieci w postaci dziesiętnej: _____
Maska podsieci w postaci binarnej: _____
6. Jaka jest maksymalna liczba podsieci, które można utworzyć przy użyciu tej maski podsieci?

7. Jaka jest maksymalna liczba użytecznych podsieci, które można utworzyć przy użyciu tej maski podsieci? _____
8. Ile bitów pozostało w czwartym oktecie dla identyfikatorów hostów?

9. Ile hostów w każdej podsieci można zdefiniować za pomocą tej maski podsieci?

10. Jaka jest maksymalna liczba hostów, które można zdefiniować dla wszystkich podsieci w tym scenariuszu? Załóż, że nie można wykorzystać najniższego i najwyższego numeru podsieci oraz najniższego i najwyższego identyfikatora hosta w każdej podsieci.

11. Czy adres 197.15.22.63 jest prawidłowym adresem IP hosta w tym scenariuszu?

12. Dlaczego tak sądzisz?

13. Czy adres 197.15.22.160 jest prawidłowym adresem IP hosta w tym scenariuszu?

14. Dlaczego tak sądzisz?

15. Host A ma adres IP równy 197.15.22.126. Host B ma adres IP równy 197.15.22.129. Czy te hosty znajdują się w tej samej podsieci? _____ Dlaczego?



Ćwiczenie 10.3.5b Podsieci w sieci klasy A

Cele

Analiza adresu sieci klasy A z uwzględnieniem liczby określonych bitów sieci w celu określenia następujących czynników:

- maska podsieci
- liczba podsieci
- liczba hostów przypadających na każdą podsieć
- informacja na temat poszczególnych podsieci

Wprowadzenie i przygotowanie

Jest to ćwiczenie pisemne i powinno być wykonywane bez pomocy kalkulatora.

Krok 1 Mając podany adres sieci klasy A równy 10.0.0.0/ 24, odpowiedz na następujące pytania

Ile bitów zostało pożyczonych z części hosta w tym adresie? _____

Jaka jest maska podsieci dla tej sieci?

1. Notacja dziesiętna kropkowa

2. Notacja binarna _____

Ile ta sieć zawiera możliwych do wykorzystania podsieci?

Ile każda z podsieci zawiera możliwych do wykorzystania adresów hostów?

Jaki jest zakres hostów dla możliwej do wykorzystania podsieci numer 16?

Jaki jest adres sieci dla możliwej do wykorzystania podsieci numer 16?

Jaki jest adres rozgłoszeniowy dla możliwej do wykorzystania podsieci numer 16?

Jaki jest adres rozgłoszeniowy dla ostatniej możliwej do wykorzystania podsieci?

Jaki jest adres rozgłoszeniowy sieci głównej?



Ćwiczenie 10.3.5c Podsieci w sieci klasy B

Cele

Dostarczenie schematu tworzenia podsieci w przypadku użycia sieci klasy B

Wprowadzenie i przygotowanie

Jest to ćwiczenie pisemne i powinno być wykonywane bez pomocy kalkulatora.

Firma ABC Manufacturing nabyła adres klasy B — 172.16.0.0. Firma musi utworzyć schemat podsieci złożony z następujących składników:

- 36 podsieci zawierających przynajmniej 100 hostów,
- 24 podsieci zawierające przynajmniej 255 hostów,
- 10 podsieci zawierających przynajmniej 50 hostów.

Nie ma konieczności rezerwowania osobnego adresu dla połączenia WAN, ponieważ został on dostarczony przez dostawcę usług internetowych.

Krok 1 Mając dany adres sieci klasy B i powyższe wymagania, odpowiedz na następujące pytania

Ile podsieci jest wymaganych w tej sieci? _____

Jaka jest minimalna liczba bitów, które można pożyczyć? _____

Jaka jest maska podsieci dla tej sieci? _____

1. Notacja dziesiętna kropkowa _____

2. Notacja binarna _____

3. Format z ukośnikiem _____

Ile ta sieć zawiera możliwych do wykorzystania podsieci?

Ile każda z podsieci zawiera możliwych do wykorzystania adresów hostów?

Krok 2 Wypełnij poniższą tabelę, wpisując pierwsze trzy i ostatnie cztery podsieci

Nr podsieci	Identyfikator podsieci	Zakres hostów	Identyfikator rozgłaszania

Jaki jest zakres hostów dla podsieci numer 2?

Jaki jest adres rozgłoszeniowy dla 126 podsieci?

Jaki jest adres rozgłoszeniowy sieci głównej?



Ćwiczenie 10.3.5d Podsieci w sieci klasy C

Cele

Celem tego ćwiczenia jest dostarczenie schematu tworzenia podsieci w przypadku użycia sieci klasy C.

Wprowadzenie i przygotowanie

Jest to ćwiczenie pisemne i powinno być wykonywane bez pomocy kalkulatora.

Akademia Classical Academy nabyła adres klasy C — 192.168.1.0. Wymagane jest utworzenie podsieci, co zapewni podstawowe zabezpieczenie i kontrolę rozgłoszeń w sieci LAN. Nie ma konieczności rezerwowania osobnego adresu dla połączenia WAN. Jest on dostarczony przez dostawcę usług internetowych.

Sieć LAN składa się z następujących elementów, z których każdy wymaga własnej podsieci:

- Sala zajęć nr 1 28 węzłów
- Sala zajęć nr 2 22 węzły
- Pracownia komputerowa 30 węzłów
- Instruktorzy 12 węzłów
- Administracja 8 węzłów

Krok 1 Mając dany adres sieci klasy C i powyższe wymagania, odpowiedz na następujące pytania

Ile podsieci jest wymaganych w tej sieci? _____

Jaka jest maska podsieci dla tej sieci? _____

1. Notacja dziesiętna kropkowa

2. Notacja binarna _____

3. Format z ukośnikiem

Ile każda z podsieci zawiera możliwych do wykorzystania adresów hostów?

Krok 2 Wypełnij poniższą tabelę

Nr podsieci	Adres IP podsieci	Zakres hostów	Identyfikator rozgłaszania

Jaki jest zakres hostów dla podsieci numer 6?

Jaki jest adres rozgłoszeniowy dla trzeciej podsieci?

Jaki jest adres rozgłoszeniowy sieci głównej?

Ćwiczenie 11.2.4 Program Protocol Inspector, protokoły TCP i HTTP

Cele

Zastosowanie programu Protocol Inspector lub odpowiadającego mu oprogramowania do przeglądania dynamicznych operacji protokołu TCP. Szczególna uwaga zostanie zwrócona na operacje protokołu HTTP związane z dostępem do stron WWW.

Wprowadzenie i przygotowanie

Oprogramowanie służące do analizy protokołu ma funkcję zwaną przechwytywaniem. Jest to funkcja umożliwiająca wychwytywanie wszystkich przepływających przez interfejs ramek w celu ich analizy. Za jej pomocą jest możliwe obserwowanie sposobu, w jaki w ramach protokołu TCP przesyłane są przez sieć segmenty wypełnione danymi użytkowymi. Za pomocą analizatora protokołowego można zaobserwować, jak z pozoru nieco abstrakcyjny protokół TCP jest istotny dla procesów sieciowych, takich jak poczta elektroniczna i przeglądanie stron WWW.

Oprogramowanie Protocol Inspector musi być zainstalowane przynajmniej na jednym z hostów. Jeśli ćwiczenie wykonywane jest w parach, zainstalowanie oprogramowania na obu komputerach umożliwia każdej z osób wykonanie kroków ćwiczenia. Jednakże wyniki wyświetlone na każdym z hostów mogą się nieznacznie różnić.

Krok 1 Uruchom program Protocol Inspector oraz przeglądarkę

Krok 2 Przejdź do widoku szczegółowego

Krok 3 Uruchom przechwytywanie

Krok 4 Wyślij żądanie pobrania strony WWW

Krok 5 Obserwuj widok monitorowania w czasie wysyłania żądania i dostarczania strony WWW

Krok 6 Zatrzymaj przechwytywanie

Krok 7 Przeanalizuj ramki protokołu TCP, ramki protokołu HTTP oraz statystyki, używając różnych widoków, zwłaszcza widoku szczegółowego

Krok 8 Wyjaśnij, co w oparciu o widok szczegółowy można powiedzieć odnośnie następujących zagadnień

- uzgodnienia w protokole TCP,
- potwierdzenia w protokole TCP,
- podział na segmenty i rozmiar segmentów w protokole TCP,
- numery sekwencyjne w protokole TCP,
- okna przesuwne w protokole TCP,
- protokół HTTP.

Do przemyślenia

W jaki sposób ćwiczenie to pomaga w wizualizacji działania protokołu TCP?
