

Rozdział 7: Adresowanie IP

Spis treści

Przegląd zagadnień	1
Adresowanie IP z podziałem na klasy	2
Podział sieci na podsieci	6
Laboratorium A: Ustalanie klas adresów oraz masek podsieci	11
Planowanie adresowania IP	15
Laboratorium B: Rozpoznawanie poprawnych adresów IP	19
Przypisywanie adresów TCP/IP	20
Laboratorium C: Sprawdzanie konfiguracji TCP/IP	25
Podsumowanie	32



Zastrzega się prawo wprowadzania zmian do treści niniejszego dokumentu bez uprzedniego powiadomienia. Wszystkie firmy, produkty, osoby, teksty i/lub dane opisane w przykładach są fikcyjne i jeżeli przypominają jakiegokolwiek rzeczywiste osoby, firmy lub wydarzenia, w żadnym przypadku nie było to zamierzone, o ile nie wspomniano, że jest inaczej. Odpowiedzialność za przestrzeganie wszystkich odnośnych praw autorskich ponosi użytkownik. Niniejszego dokumentu lub jego części nie wolno powielać w żadnej formie ani przekazywać za pomocą jakichkolwiek nośników elektronicznych lub mechanicznych, z wyjątkiem przypadków, w których uzyskano na to pisemną zgodę firmy Microsoft Corporation. Jeżeli użytkownik ma dostęp do niniejszego dokumentu wyłącznie w formie elektronicznej, zezwala się na wydrukowanie jednego egzemplarza tego dokumentu.

Firma Microsoft może mieć patenty lub rozpoczęte postępowania patentowe, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, które odnoszą się do treści zawartej w niniejszym dokumencie. Otrzymanie tego dokumentu nie oznacza udzielenia licencji na te patenty, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, z wyjątkiem wyraźnie określonych przypadków zawartych w pisemnych Umowach Licencyjnych firmy Microsoft.

© 2000 Microsoft Corporation. Wszystkie prawa zastrzeżone.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint i Visual Studio są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w USA i/lub w innych krajach.

Wszystkie inne nazwy firm i producentów wymienione w niniejszym dokumencie mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli.

Inne produkty i nazwy firm używane w treści mogą być nazwami zastrzeżonymi przez ich właścicieli.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.),

Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Symulacje oraz ćwiczenia interaktywne zostały wykonane przez firmę Macromedia Authorware

Opracowanie wersji polskiej: DC Edukacja Sp. z o.o., Al. Niepodległości 659, 81-855 Sopot
e-mail: info@edukacja.com, Internet: <http://www.edukacja.com>

Współpraca: P.S.I. Sp. z o.o., ul. Manifestu Lipcowego 9, 25-323 Kielce
e-mail: psi@edukacja.com, Internet: <http://www.interpsi.ok.pl>

Zespół tłumaczy: Artur Pucek, Sebastian Tobolski

Konsultacja: Waldemar PierścioneK, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
60 minut

Laboratoria:
60 minut

W rozdziale tym słuchacze poznają zagadnienia związane z adresowaniem IP z podziałem na klasy, dzieleniem sieci na podsieci, przypisywaniem adresów IP oraz przeglądaniem konfiguracji TCP/IP. W pierwszej sekcji rozdziału opisane zostały elementy adresu IP oraz klasy adresów IP. W drugiej części objaśniono proces dzielenia na podsieci, akcentując, czym jest podsieć i maska podsieci. Słuchacze, wykonując umieszczone po tych sekcjach laboratorium, określają klasę adresu IP, jego elementy oraz domyślną maskę podsieci. Trzecia sekcja opisuje wytyczne, stosowane przy adresowaniu, oraz zakresy, jakie przyjmują identyfikatory sieci i hosta. Wykonując umieszczone dalej laboratorium, słuchacze będą przydzielać adresy IP i określać poprawność konfiguracji IP.

W ostatniej sekcji omówiono statyczne i dynamiczne adresowanie oraz metody przeglądania informacji TCP/IP i wyjaśniono, kiedy należy stosować poszczególne narzędzia TCP/IP. W umieszczonym dalej laboratorium, słuchacze będą przeglądać informacje TCP/IP swoich komputerów na dwa sposoby—za pomocą narzędzia Ipconfig i okna dialogowego **Internet Protocol (TCP/IP) Properties**. Określą także odpowiednie zastosowanie dla obu metod.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Zdefiniować klasy adresów IP i opisać cechy każdej z klas.
- Opisać proces dzielenia sieci na podsieci.
- Opisać kwestie związane z planowaniem adresów IP dla sieci.
- Opisać metody stosowane do przydzielania adresów IP za pomocą narzędzi, dostępnych w systemie Microsoft® Windows® 2000.

Materiały i sposób przygotowania

W sekcji tej opisano sposób przygotowania wykładowcy oraz materiały niezbędne do właściwej prezentacji rozdziału.

Wymagane materiały

Do przedstawienia tego rozdziału potrzebne będą następujące materiały:

- Plik programu Microsoft PowerPoint® o nazwie 2243A_07.ppt
- Rozdział 7, „Adresowanie IP”

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału, należy:

- Przeczytać całość materiałów poświęconych temu rozdziałowi.
- Przeczytać dokumenty *Introduction to TCP/IP* oraz *TCP/IP Implementation Details for Windows 2000* z płyty kompaktowej Materiały dla wykładowcy.
- Przeczytać temat pomocy systemu Windows 2000 o nazwie IP Addressing .
- Wykonać wszystkie trzy laboratoria.
- Przejrzeć wskazówki i zagadnienia kluczowe kolejnych sekcji i tematów.
- Przejrzeć pytania podsumowujące i podać inne odpowiedzi do dyskusji.
- Przewidzieć możliwe pytania słuchaczy i przygotować na nie odpowiedzi.

Strategia przedstawienia rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Adresowanie IP z podziałem na klasy

Prezentację tego rozdziału należy rozpocząć od przypomnienia pojęcia adresu IP, które zostało wprowadzone w rozdziale 6, „Analiza protokołu TCP/IP” kursu 2243A *Podstawy sieci i systemu operacyjnego Microsoft Windows 2000*. Następnie należy opisać składniki adresu IP, krótko omówić adresowanie IP z podziałem na klasy oraz wytłumaczyć znaczenie klas adresów i ich funkcji w określaniu elementów adresu IP.

- Podział sieci na podsieci

Omawianie tej części należy zacząć od opisanie powodów, dla których sieć dzielona jest na podsieci. Następnie trzeba wyjaśnić koncepcję dzielenia sieci na podsieci, pojęcie maski podsieci oraz przyczyny tworzenia podsieci poprzez zastosowanie niestandardowych masek podsieci. Wreszcie należy opisać procedurę określania, czy dwa hosty są względem siebie lokalne czy też zdalne.

- Planowanie adresowania IP

Opisując tę sekcję, należy podać ograniczenia dotyczące wartości identyfikatorów sieci i identyfikatorów hosta, które muszą być brane pod uwagę w czasie przypisywania adresów IP. Następnie trzeba podać zakresy identyfikatorów sieci i identyfikatorów hosta, które mogą zostać przypisane.

- Przypisywanie adresów TCP/IP

W tej części należy podać różnicę między statycznym i dynamicznym adresowaniem IP. Trzeba zademonstrować sposób przypisywania adresu IP hostowi oraz pokazać dwa sposoby przeglądania informacji TCP/IP. Następnie należy przedstawić sposób korzystania z narzędzia Ipconfig i opisać sytuacje, w których zastosowanie poszczególnych sposobów jest najwłaściwsze.

Informacje uzupełniające

W sekcji tej opisane są wymagania dotyczące instalacji laboratoriów dla tego rozdziału oraz zmiany w konfiguracji, które zachodzą na komputerach słuchaczy w trakcie realizacji laboratoriów. Informacje te będą pomocne w powielaniu lub dostosowywaniu materiałów szkoleniowych MOC (Microsoft Official Curriculum).

Ważne Aby możliwe było wykonanie laboratoriów, zawartych w tym rozdziale, konieczne jest odpowiednie skonfigurowanie pracowni, zgodnie z uwagami znajdującymi się w sekcji Informacje uzupełniające, zamieszczonej w rozdziale Przygotowanie pracowni do kursu 2243A, *Podstawy sieci i systemu operacyjnego Microsoft Windows 2000*.

Rezultaty laboratorium

Nie ma żadnych zmian w konfiguracji komputerów słuchaczy, wpływających na powielanie lub dostosowywanie materiałów szkoleniowych.

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

W trakcie omawiania tego rozdziału przedstawione zostaną sposoby określania klasy adresu komputera na podstawie jego adresu IP, metody dzielenia sieci na podsieci oraz wytyczne dotyczące planowania i przypisywania adresów IP.

- Adresowanie IP z podziałem na klasy
- Podział sieci na podsieci
- Planowanie adresowania IP
- Przypisywanie adresów TCP/IP

Podstawowa funkcja protokołu IP (Internet Protocol) polega na dodawaniu informacji o adresie do pakietów danych i przesyłaniu ich poprzez sieć do właściwych miejsc docelowych. Aby zrozumieć, w jaki sposób protokół IP realizuje to zadanie, konieczne jest poznanie pojęć, które pozwalają określić pośrednie i ostateczne miejsca docelowe pakietów danych.

Aby umożliwić określanie położenia docelowego hosta względem komputera źródłowego, adresy IP zostały podzielone na klasy. Taki sposób organizacji nosi nazwę adresowania IP z podziałem na klasy. Każdemu komputerowi podłączonemu do sieci musi zostać przypisany adres IP. Segmenty sieci połączone przez ruter noszą nazwę podsieci. Dzielenie sieci na podsieci związane z przypisywaniem adresów IP nazywane jest *tworzeniem podsieci*.

Korzystając z narzędzi zawartych w systemie Microsoft® Windows® 2000 można zaplanować i przypisać adres IP każdemu komputerowi w sieci w oparciu o zasady, które rządzą adresowaniem IP z podziałem na klasy.

Uwaga Słowo *host* jest często używane w odniesieniu do dowolnego urządzenia w sieci, które wysyła i odbiera informacje w oparciu o adres IP. Dowolny komputer, drukarka czy ruter w sieci TCP/IP jest hostem i aby mógł się komunikować, musi mu zostać przypisany przynajmniej jeden adres IP.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Powiedzieć, czym jest adresowanie IP z podziałem na klasy i opisać cechy każdej z klas.
- Opisać procedurę dzielenia sieci na podsieci.
- Opisać kwestie związane z planowaniem adresów IP dla sieci.
- Opisać procedurę stosowaną podczas przypisywania adresów IP za pomocą narzędzi, dostępnych w systemie Windows 2000.

◆ Adresowanie IP z podziałem na klasy

Cel slajdu

Wprowadzenie pojęcia klas adresów IP.

Wprowadzenie

Zanim komputer będzie mógł przesłać innemu komputerowi dane, musi określić jego lokalizację.

- Adresy IP
- Klasy adresów IP

Aby dowolny komputer mógł komunikować się w sieci, musi mieć przypisany unikalny adres IP. W przypadku adresowania IP z podziałem na klasy, w trakcie przypisywania każdemu komputerowi adresu IP wykorzystywane są trzy klasy adresów. Wielkość oraz typ sieci determinują klasę adresu IP stosowaną do określania adresów IP dla komputerów i innych hostów w sieci.

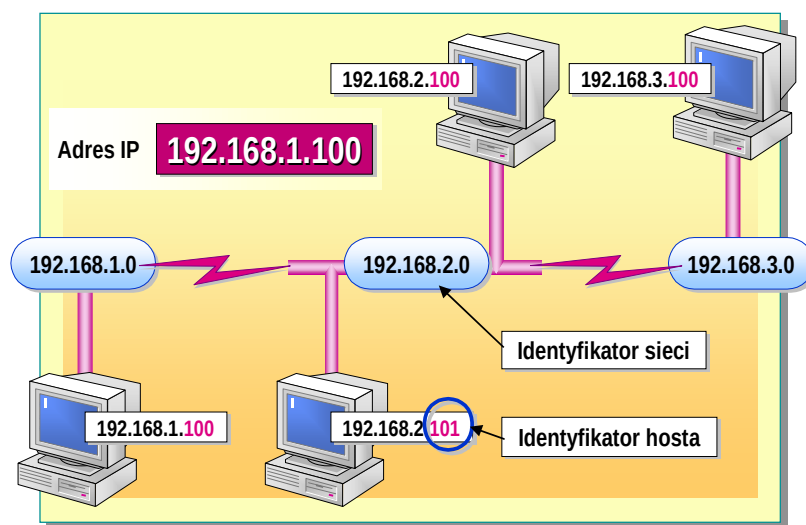
Adresy IP

Cel slajdu

Zilustrowanie, czym jest adres IP.

Wprowadzenie

Adresy IP tworzą szkielet procesu komunikacji TCP/IP.



Wskazówka

Na slajdzie pokazane zostały cztery komputery wraz z ich adresami IP, znajdujące się w trzech różnych sieciach. Slajd pokazuje, że adresy IP mogą mieć taki sam identyfikator sieci lub hosta, lecz aby możliwa była komunikacja między komputerami, poszczególne adresy IP muszą być unikalne.

Zagadnienie kluczowe

Adres IP stanowi nie tylko identyfikator, lecz także pozwala zlokalizować komputer w sieci. Dlatego właśnie na tej stronie wprowadzono pojęcie identyfikatora sieci i hosta. Na obecnym etapie słuchacze muszą tylko wiedzieć, że adresy IP są unikalne, przy czym ich pierwsza część stanowi identyfikator sieci, a druga identyfikator hosta. Dokładna budowa identyfikatora hosta i sieci została omówiona na następnej stronie.

Adres IP stanowi unikalny identyfikator, który pozwala rozróżniać komputery w sieci i ułatwia odnalezienie części sieci, w której dany komputer się znajduje. Każdy komputer, czy inny składnik sieci, taki jak ruter, który komunikuje się za pomocą pakietu protokołów TCP/IP, musi mieć przypisany adres IP.

Adres IP pozwala określić położenie danego komputera w sieci, w podobny sposób, jak adres pocztowy umożliwia odnalezienie dowolnego domu w danym mieście. Tak jak adres określonego domu musi być niepowtarzalny, lecz podporządkowany określonej sposobowi adresowania, tak adres IP powinien być unikalny, lecz zgodny z pewnym standardowym formatem. Adres IP składa się z czterech liczb, z których każda może przyjmować wartości od 0 do 255.

Składniki adresu IP

Tak jak każdy adres pocztowy składa się przynajmniej z dwóch części—adresu, czyli nazwy ulicy i numeru domu oraz kodu pocztowego—tak i adres IP składa się z dwóch elementów—identyfikatora hosta oraz identyfikatora sieci.

Identyfikator sieci

Pierwszą część adresu IP stanowi identyfikator sieci, który określa segment sieci, w którym znajduje się dany komputer. Komputery, znajdujące się w tym samym segmencie sieci, muszą mieć taki sam identyfikator sieci, tak jak domy, znajdujące się w jednym obszarze, muszą mieć taki sam kod pocztowy.

Identyfikator hosta

Drugą część adresu IP stanowi identyfikator hosta, pozwalający zidentyfikować komputer, ruter lub inne urządzenie w danym segmencie. Każdy host w obrębie segmentu musi posiadać unikalny identyfikator, tak jak każdy dom musi mieć odrębny adres w obszarze określanym jednym kodem pocztowym.

Należy zauważyć, że tak jak w obszarach o różnych kodach mogą stać domy o takim samym adresie, tak komputery o różnych identyfikatorach sieci mogą mieć taki sam identyfikator hosta. Jednak by umożliwić komunikację, dla każdego komputera kombinacja identyfikatora sieci i hosta musi być unikalna.

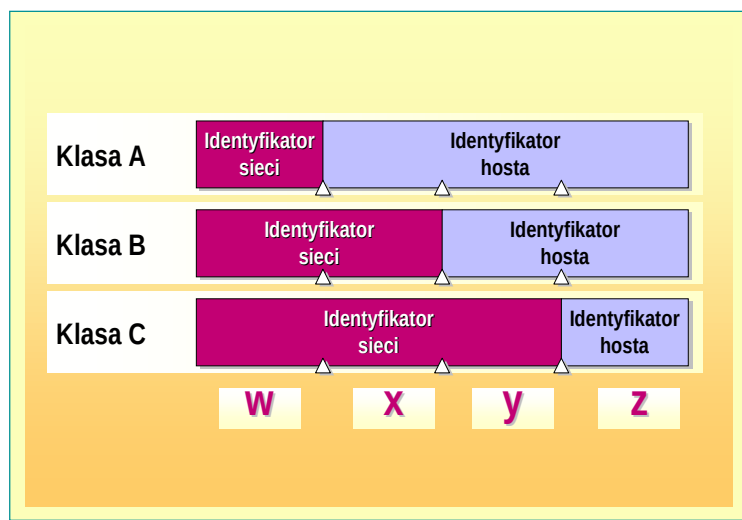
Klasy adresów IP

Cel slajdu

Zilustrowanie systemu klasyfikacji adresów IP.

Wprowadzenie

Aby ułatwić zarządzanie adresami IP, zostały one podzielone na pięć kategorii, z których trzy używane są do przypisywania adresów IP komputerom.



Zagadnienie kluczowe

Upewnij się, czy słuchacze rozumieją, że tylko adresy z klasy A, B, oraz C są przypisywane hostom. Wskaż także, że oprócz oddzielania identyfikatorów sieci od identyfikatorów hostów, klasy są także używane do przydzielania adresów IP, co umożliwia komunikację w Internecie.

Klasy adresów służą do przydzielania identyfikatorów sieci poszczególnym organizacjom tak, aby komputery w ich sieciach mogły komunikować się z Internetem. Klasy adresów pozwalają także oddzielać w adresie identyfikator sieci i identyfikator hosta. Danej organizacji przydzielany jest blok adresów IP, określanych poprzez wspólny adres identyfikatora sieci, którego typ jest uzależniony od wielkości organizacji. Na przykład organizacji, w której znajduje się 200 hostów, przydzielany jest identyfikator sieci klasy C, podczas kiedy organizacji z 20,000 hostów przydzielany jest identyfikator sieci klasy B.

Klasa A

Adresy klasy A przypisywane są sieciom z bardzo dużą liczbą hostów. W tej klasie może istnieć do 126 sieci, gdyż na identyfikator sieci przeznaczona jest pierwsza liczba adresu. Pozostałe trzy liczby przeznaczone są na identyfikator hosta, dzięki temu w każdej sieci może istnieć do 16,777,214 hostów.

Klasa B

Adresy klasy B przypisywane są sieciom o średnim lub dużym rozmiarze. W tej klasie może istnieć do 16,384 sieci, gdyż na identyfikator sieci przeznaczone są dwie pierwsze liczby adresu. Pozostałe dwie liczby przeznaczone są na identyfikator hosta, dzięki temu w każdej sieci może istnieć do 65,534 hostów.

Klasa C

Adresy klasy C przypisywane są niewielkim sieciom lokalnym (LAN). W tej klasie może istnieć maksymalnie 2,097,152 sieci, gdyż na identyfikator sieci przeznaczone są trzy pierwsze liczby adresu. Pozostała liczba przeznaczona jest na identyfikator hosta, dzięki temu w każdej sieci może istnieć do 254 hostów.

Klasy D oraz E

Klasy D oraz E nie są przydzielane hostom. Adresy klasy D są wykorzystywane podczas transmisji typu multicast, zaś adresy klasy E są zarezerwowane na rzecz przyszłych zastosowań.

Określanie klasy adresu

Adresowanie IP z podziałem na klasy jest oparte o strukturę adresu IP i pozwala w sposób systematyczny rozróżniać identyfikatory sieci i identyfikatory hosta. Adres IP składa się z czterech, zapisywanych liczbowo części. Adres IP może zostać przedstawiony schematycznie jako ciąg $w.x.y.z$, gdzie w , x , y oraz z są liczbami o wartościach z zakresu od 0 do 255. W oparciu o wartość pierwszej liczby, przedstawionej w schemacie jako w , adresy IP mogą zostać podzielone na pięć klas adresów, tak jak to zostało przedstawione w zamieszczonej poniżej tabeli.

Klasa adresu IP	Adres IP	Identyfikator sieci	Zakres wartości w
A	$w.x.y.z$	$w.0.0.0$	1 – 126*
B	$w.x.y.z$	$w.x.0.0$	128 – 191
C	$w.x.y.z$	$w.x.y.0$	192 – 223
D	$w.x.y.z$	niedostępne	224 – 239
E	$w.x.y.z$	niedostępne	240 – 255

*Identyfikator sieci 127.0.0.0 jest zarezerwowany na potrzeby testów połączeń.

Określanie identyfikatora sieci i hosta

W przypadku adresów IP klasy A, identyfikator sieci stanowi pierwszą liczbę adresu. W klasie B, na identyfikator sieci zarezerwowane są dwie pierwsze liczby, zaś w klasie C trzy pierwsze liczby adresu IP. Pozostałe liczby określają identyfikator hosta.

Identyfikator sieci składa się z czterech liczb, podobnie jak adres IP. Dlatego jeśli tylko pierwsza liczba adresu IP, czyli liczba w w schemacie, określa identyfikator sieci, to ten identyfikator przyjmuje postać $w.0.0.0$, gdzie trzy pozostałe liczby adresu mają wartość 0. Identyfikator hosta ma strukturę $x.y.z$. Należy zwrócić uwagę, że identyfikator hosta nie jest poprzedzany przez liczbę 0.

Na przykład, adres IP 172.16.53.46 należy do klasy B, gdyż wartość liczby w wynosi 172, czyli leży pomiędzy 128 oraz 191. Identyfikator sieci tego adresu ma postać 172.16.0.0 a identyfikator hosta 53.46 (bez kropki na końcu).

◆ Podział sieci na podsieci

Cel slajdu

Wprowadzenie pojęcia podziału na podsieci.

Wprowadzenie

Dzięki podsieciom duża liczba komputerów może się efektywnie komunikować w sieci. Aby było to możliwe, komputery muszą być w stanie odróżnić komputery znajdujące się w tej samej podsieci od tych, które są w innych podsieciach.

- **Podsieci**
- **Maski podsieci**
- **Rozróżnianie hostów lokalnych i zdalnych**

Sieć może zostać rozszerzona za pomocą fizycznych urządzeń, takich jak routery lub mosty, które umożliwiają dodawanie dodatkowych segmentów sieci. Za pomocą fizycznych urządzeń można także podzielić sieć na mniejsze segmenty w celu zwiększenia jej wydajności. Segmenty sieci, oddzielone od siebie routerami noszą nazwę *podsieci*.

W trakcie tworzenia podsieci, identyfikator sieci jest dzielony dla hostów w poszczególnych podsieciach. Dzielenie identyfikatora sieci, wykorzystywanego podczas komunikacji z siecią Internet, na mniejsze (w odniesieniu do liczby obsługiwanych adresów IP) identyfikatory sieci dla poszczególnych podsieci, nosi nazwę *dzielenia na podsieci*. Aby ustalić nowy identyfikator sieci dla każdej podsieci, należy użyć maski podsieci, określającej, jaka część adresu IP ma być wykorzystana jako nowy identyfikator sieci dla określonej podsieci.

Można określić położenie dowolnego hosta w sieci, analizując jego identyfikator sieci. Zestawiając ze sobą identyfikatory sieci można sprawdzić, które hosty znajdują się w tej samej podsieci. Jeśli identyfikatory podsieci nie są takie same, poszczególne hosty znajdują się w różnych podsieciach i konieczne jest zastosowanie routera, aby umożliwić pomiędzy nimi komunikację.

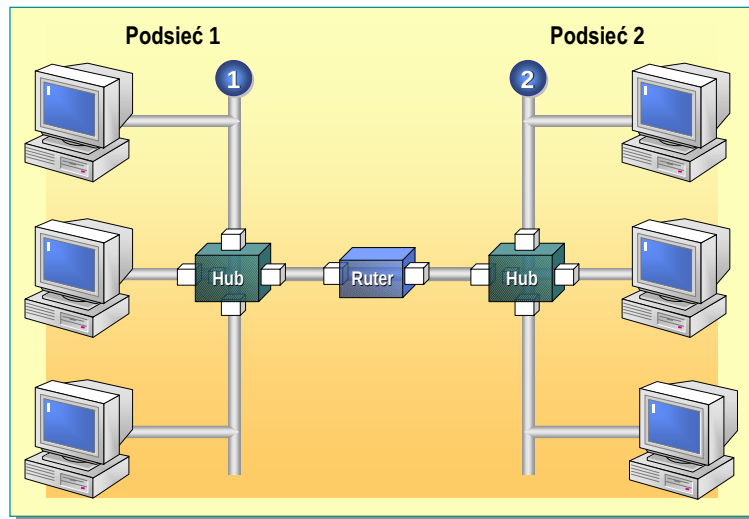
Podsieci

Cel slajdu

Zilustrowanie struktury podsieci.

Wprowadzenie

Ten temat przedstawia powody, dla których sieć dzieli się na mniejsze segmenty sieci.

**Zagadnienie kluczowe**

Zaznacz, że podczas tworzenia podsieci, każda podsieć otrzymuje własny identyfikator sieci. Połóż także nacisk na to, jak ważna jest funkcja rutera, który wyznacza granice pomiędzy podsieciami. Układ tworzony przez podsieci i routery prowadzi do pojęcia sieci wielosegmentowej, które oznacza sieć podzieloną na podsieci.

Większość sieci, w których wykorzystywany jest system Windows 2000, oparta jest o technologię Ethernet, w której komputery wysyłają informacje, korzystając z transmisji typu broadcast. Jeśli liczba komputerów oraz ilość ruchu w sieci Ethernet wzrasta, następuje także proporcjonalny wzrost kolizji danych oraz spadek wydajności sieci. Aby rozwiązać ten problem, komputery w sieci Ethernet są grupowane razem w pewne fizyczne sekcje, zwane segmentami, które są oddzielone od siebie fizycznymi urządzeniami, takimi jak ruter lub most.

W środowisku TCP/IP, segmenty, oddzielone od siebie za pomocą routerów, nazywane są podsieciami. Wszystkie komputery należące do jednej podsieci mają w swoim adresie IP taki sam identyfikator sieci. Aby możliwa była komunikacja pomiędzy podsieciami, każda z nich musi mieć inny identyfikator sieci. Podsieci, na podstawie identyfikatora sieci, wyznaczają logiczne sekcje sieci. Komputery znajdujące się w różnych podsieciach muszą podczas komunikacji przesyłać dane poprzez routery.

Maski podsieci

Cel slajdu

Zilustrowanie podziału adresu IP na identyfikator sieci i hosta za pomocą maski podsieci.

Wprowadzenie

Ten temat objaśnia proces, w jaki komputery odróżniają identyfikator sieci od identyfikatora hosta za pomocą maski podsieci.

Adres IP	10.50.100.	200
Maska podsieci	255.255.255.	0
Identyfikator sieci	10.50.100.	0

Wskazówka

Można zastosować inne maski, niż te, które zostały tu przedstawione, gdyż celem tego tematu jest takie przedstawienie zagadnienia masek podsieci, aby słuchacze nauczyli się konfigurować maskę podsieci bez stosowania ograniczeń podziału na klasy. Drugim celem jest przedstawienie sposobu, w jaki maska podsieci określa część adresu IP, która jest identyfikatorem sieci. Ponieważ nacisk został położony na identyfikator sieci, animowany slajd pokazuje, że adres IP 10.50.100.200 może mieć różne maski podsieci.

W przypadku zastosowania podziału na klasy, liczba dostępnych sieci i hostów dla poszczególnych klas adresów jest z góry ograniczona. W rezultacie, danej organizacji przydzielany jest jeden stały identyfikator sieci oraz pewna określona liczba hostów, zależna od klasy adresu IP.

Jeśli danej organizacji został przyznany tylko jeden identyfikator sieci, może w niej funkcjonować tylko jedna sieć, łącząca określoną liczbę hostów. Jeśli liczba hostów będzie zbyt duża, sieć nie będzie w stanie efektywnie działać. Aby rozwiązać ten problem, wprowadzona została możliwość dzielenia sieci.

Dzielenie sieci pozwala podzielić pojedynczy klasowy identyfikator sieci na mniejsze (w odniesieniu do liczby obsługiwanych adresów IP) identyfikatory sieci. Dzięki wykorzystaniu wielu mniejszych identyfikatorów sieci, pojedyncza sieć może zostać podzielona na segmenty, z których każdy będzie mieć inny identyfikator sieci, zwany także identyfikatorem podsieci.

Struktura masek podsieci

Podział identyfikatora sieci jest możliwy dzięki zastosowaniu maski podsieci. Maska podsieci stanowi rodzaj ekranu, który pozwala oddzielać w adresie IP identyfikator sieci od identyfikatora hosta, lecz nie podlega ograniczeniom wynikającym z podziału na klasy. Maska podsieci, podobnie jak adres IP, składa się z czterech liczb. Liczby te mogą przyjmować wartości od 0 do 255.

W przypadku zastosowania podziału na klasy, każda z tych liczb może przyjmować tylko dopuszczalną wartość maksymalną 255 lub minimalną 0. Cały ciąg, zawierający cztery liczby, składa się więc z kilku umieszczonych obok siebie liczb o wartość maksymalnej, po których umieszczonych jest kilka liczb o wartości minimalnej. Wartość maksymalna odpowiada identyfikatorowi sieci, zaś wartość minimalna identyfikatorowi hosta. Na przykład maska 255.255.0.0 jest poprawną maską podsieci, podczas kiedy maska 255.0.255.0 już nią nie jest. Maska podsieci 255.255.0.0 określa, że identyfikator sieci stanowią dwie pierwsze liczby adresu IP.

Domyślne maski podsieci

W przypadku zastosowania podziału na klasy, każda klasa adresów posiada domyślną maskę podsieci. Zamieszczona poniżej tabela zawiera listę domyślnych masek podsieci dla poszczególnych klas adresów.

Klasa adresu IP	Adres IP	Maska podsieci	Identyfikator sieci	Identyfikator hosta
A	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z
B	w.x.y.z	255.255.0.0	w.x.0.0	y.z
C	w.x.y.z	255.255.255.0	w.x.y.0	z

Niestandardowe maski podsieci

Dzieląc istniejący identyfikator sieci w celu utworzenia dodatkowych podsieci, można wykorzystać dowolną z podanych powyżej masek podsieci, niezależnie od adresu IP i identyfikatora sieci. Tak więc adres IP 172.16.2.200 może mieć maskę podsieci 255.255.255.0 i identyfikator sieci 172.16.2.0, zamiast domyślnej maski podsieci 255.255.0.0 i identyfikatora sieci 172.16.0.0. Pozwala to w danej organizacji podzielić istniejący identyfikator sieci klasy B 172.16.0.0 na mniejsze identyfikatory sieci w celu lepszego odzwierciedlenia bieżącej konfiguracji sieci.

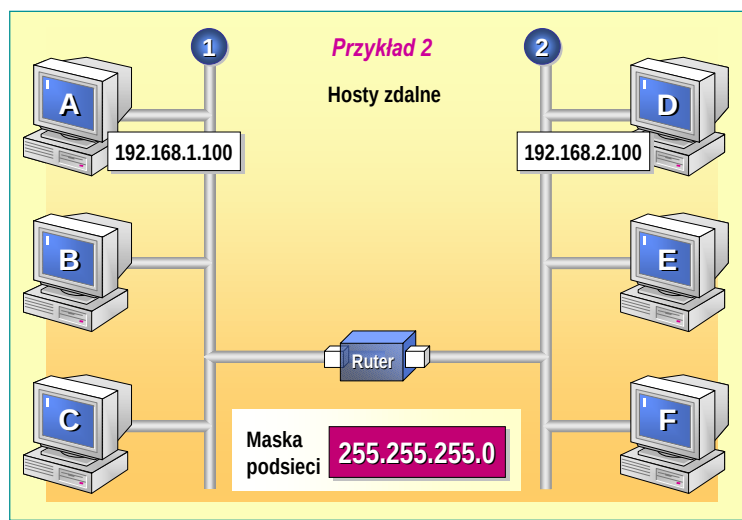
Rozróżnianie hostów lokalnych i zdalnych

Cel slajdu

Zilustrowanie różnicy między hostami lokalnymi i zdalnymi.

Wprowadzenie

Po określeniu identyfikatorów sieci adresów IP, można ustalić, czy dwa hosty są względem siebie hostami lokalnymi czy zdalnymi.



Wskazówka

Przypomnij słuchaczom, że jeśli sieć nie zostanie podzielona na podsieci, to cała komunikacja musi odbywać się lokalnie. Jeśli identyfikatory sieci nie są takie same, komunikacja nie jest możliwa. Po raz kolejny powinieneś przypomnieć, że za dostarczanie pakietów do miejsca przeznaczenia odpowiada protokół IP. Połóż nacisk na to, że protokół IP wyznacza ruter, który jest potrzebny do komunikacji. Zwróć uwagę, że adresy IP w przykładach są takie same, różnią się natomiast maski podsieci. Pokazuje to jak ważne jest odpowiednie skonfigurowanie maski podsieci.

Znając identyfikator sieci, można na jego podstawie w prosty sposób ustalić, czy dane hosty są względem siebie hostami lokalnymi czy też zdalnymi. Aby to zrobić, należy porównać identyfikatory sieci dwóch hostów. Jeśli identyfikatory sieci są takie same, oba hosty znajdują się w tej samej podsieci. Jeśli identyfikatory sieci różnią się, to hosty znajdują się w różnych podsieciach i do transmisji danych pomiędzy nimi potrzebny jest ruter.

Przykład 1

Rozważaniom poddane zostaną dwa komputery: A oraz B, którym przypisane zostały adresy IP, odpowiednio 192.168.1.100 oraz 192.168.2.100 oraz maska podsieci 255.255.0.0. Tak jak to zostało przedstawione w poniższej tabeli, identyfikatory sieci w ich adresach IP są takie same. Tak więc komputery A oraz B są względem siebie lokalne.

	Komputer A	Komputer B
Adres IP	192.168.1.100	192.168.2.100
Maska podsieci	255.255.0.0	255.255.0.0
Identyfikator sieci	192.168.0.0	192.168.0.0

Przykład 2

W kolejnym przykładzie przedstawione zostaną komputery A i D z adresami IP 192.168.1.100 oraz 192.168.2.100 oraz maską podsieci 255.255.255.0. Zgodnie z poniższą tabelą, identyfikatory sieci w adresach IP są różne. Tak więc komputer A jest uznawany za zdalny w stosunku do komputera D.

	Komputer A	Komputer D
Adres IP	192.168.1.100	192.168.2.100
Maska podsieci	255.255.255.0	255.255.255.0
Identyfikator sieci	192.168.1.0	192.168.2.0

Laboratorium A: Ustalanie klas adresów oraz masek podsieci

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na określaniu poprawnej klasy i maski podsieci danego adresu IP oraz wyznaczaniu identyfikatora hosta i sieci adresu IP.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Określić klasę adresu IP.
- Określić domyślną maskę podsieci dowolnego adresu IP.
- Określić identyfikator sieci adresu IP.
- Określić identyfikator hosta adresu IP.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Określanie identyfikatora sieci i hosta na podstawie klasy adresu IP

Scenariusz

Jesteś administratorem, który musi określić identyfikatory sieci i hosta adresów IP, aby ustalić, czy w celu zapewnienia komunikacji należy zastosować ruter.

Cel

W tym ćwiczeniu nauczysz się rozpoznawać klasy adresów IP oraz przypisane im domyślne maski podsieci. Następnie dowiesz się, jak wyodrębniać w adresie IP identyfikator sieci i hosta.

Zadania	Szczegółowe kroki
Określ klasę, maskę podsieci, identyfikator sieci oraz identyfikator hosta dla adresu IP 131.107.2.1	a. Na podstawie pierwszej liczby adresu IP określ domyślną klasę oraz związaną z nią maskę podsieci adresu. b. Określ identyfikator sieci w oparciu o wartości poszczególnych liczb adresu IP, na pozycji których w masce podsieci występuje wartość 255, uzupełniając pozostałe miejsca identyfikatora zerami (0). c. Określ identyfikator hosta w oparciu o wartości poszczególnych liczb adresu IP, na pozycji których w masce podsieci występuje wartość 0.
i Uwaga: Wykonaj podane powyżej kroki dla każdego adresu IP. Odpowiednie wartości dla pierwszego adresu zostały podane jako przykład.	

Adres IP	Klasa/Maska podsieci	Identyfikator sieci	Identyfikator hosta
129.102.197.23	B/255.255.0.0	129.102.0.0	197.23
131.107.2.1			
199.32.123.54			
32.12.54.23			
1.1.1.1			
221.22.64.7			
93.44.127.235			
23.46.92.184			
152.79.234.12			
192.168.2.200			
168.192.3.26			
224.224.224.224			
200.100.50.25			
172.71.243.2			
163.37.212.32			
76.35.61.23			

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Co możesz ustalić na podstawie obliczonego identyfikatora sieci? Identyfikator sieci obliczasz wtedy, kiedy chcesz go porównać z identyfikatorem sieci innego komputera. Jeśli oba identyfikatory sieci są takie same, oznacza to, że oba komputery znajdują się w tym samym segmencie. Jeśli identyfikatory sieci są różne, komunikacja między dwoma komputerami jest możliwa tylko za pośrednictwem rutera.	
? Chociaż identyfikator hosta wystarcza, aby zidentyfikować komputer w segmencie, jaki adres jest używany przez stos protokołów TCP/IP, aby określić czy komunikuje się on z odpowiednim komputerem? Chociaż identyfikator hosta jest przyjaznym dla użytkownika sposobem identyfikowania komputera, adres MAC zawsze stanowi podstawowy sposób identyfikacji, wykorzystywany w komunikacji pomiędzy komputerami. Identyfikator hosta jest jednak nadal ważny, gdyż nie może się on powtarzać w danym segmencie, dzięki czemu adres IP może zostać rozwiązany do adresu MAC.	
? Jaki typ transmisji jest wykorzystywany w celu identyfikowania adresów MAC oraz ograniczenia zasięgu procesu identyfikacji adresu MAC tylko do komputerów znajdujących się w jednym segmencie? Stos protokołów TCP/IP korzysta z protokołu ARP, który z kolei wykorzystuje transmisję typu broadcast do wysyłania wiadomości, co umożliwia rozwiązanie adresu IP do adresu MAC. Ponieważ protokół ARP wysyła zapytanie do wszystkich komputerów znajdujących się w tym samym segmencie, ważne jest, aby każdy komputer w danym segmencie miał unikalny adres IP.	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Dlaczego ważne jest, aby dzieląc fizycznie sieć, wykorzystywać routery? Fizyczny podział sieci umożliwia komunikowanie się większej liczbie komputerów, zapobiegając sytuacji, w której każdy komputer musi odbierać każdy wysłany pakiet. Dzięki temu tylko ograniczona liczba komputerów, znajdująca się w tym samym segmencie, będzie otrzymywać wszystkie wysłane pakiety. Tylko określone pakiety, skierowane jawnie do innych segmentów, są widoczne dla komputerów w więcej niż jednym segmencie.	

◆ Planowanie adresowania IP

Cel slajdu

Wprowadzenie wytycznych, dotyczących przypisywania identyfikatorów sieci i hosta.

Wprowadzenie

Po utworzeniu sieci, adresy IP muszą zostać przypisane wszystkim, znajdującym się w niej komputerom. W tej sekcji wyjaśnione zostało, w jaki sposób należy zaplanować przypisywanie adresów IP tak, aby nie powstawały konflikty.

- Zasady adresowania
- Przypisywanie identyfikatorów sieci
- Przypisywanie identyfikatorów hosta

Po utworzeniu sieci, każdemu znajdującemu się w niej komputerowi musi zostać przydzielony adres IP; mniej więcej na tej samej zasadzie, jak każdemu budynkowi w mieście musi zostać przyznany adres pocztowy. Bez adresu IP komputer nie jest w stanie odbierać skierowanych do niego danych. Tak jak w przypadku adresów pocztowych domów, format adresu IP musi spełniać kilka ogólnych reguł, aby zagwarantować, że dane będą przesyłane do właściwego komputera.

W tej sekcji podane są zasady dotyczące przypisywania identyfikatorów sieci i hosta.

Zasady adresowania

Cel slajdu

Przedstawienie najważniejszych zasad dotyczących adresowania.

Wprowadzenie

Nie wszystkie potencjalnie dostępne adresy IP mogą zostać przypisane hostom.



- Pierwszą liczbą identyfikatora sieci nie może być liczba 127
- Identyfikator hosta nie może składać się tylko z liczb 255
- Identyfikator hosta nie może składać się tylko z zer
- Identyfikator hosta nie może powtórzyć się w podsieci

Wskazówka

Chociaż zasady te zostały opisane w dalszej części, podczas omawiania adresów IP i masek podsieci w zapisie binarnym, sprawdzają się one także dla prostego i uwzględniającego podział na klasy przydzielania adresów IP (takich, dla których w masce podsieci występują tylko liczby 255). Istotne jest, aby nie podać tutaj żadnych informacji, które nie dotyczą zawartości tego rozdziału.

W trakcie przydzielania adresów IP z wykorzystaniem klas, należy uwzględnić kilka zasad dotyczących liczb składających się na identyfikator sieci oraz identyfikator hosta. Te zasady to:

- Pierwszą liczbą identyfikatora sieci nie może być liczba 127. Ta liczba identyfikatora zarezerwowana jest na potrzeby testowania połączeń, takie jak lokalna pętla zwrotna.
- Identyfikator hosta nie może składać się tylko z liczb 255, ponieważ jest to adres wykorzystywany przy transmisji typu broadcast.
- Identyfikator hosta nie może składać się tylko z zer (0), ponieważ ten adres wykorzystywany jest do oznaczenia identyfikatora sieci.
- Identyfikator hosta musi być unikalny w ramach jednego identyfikatora sieci.

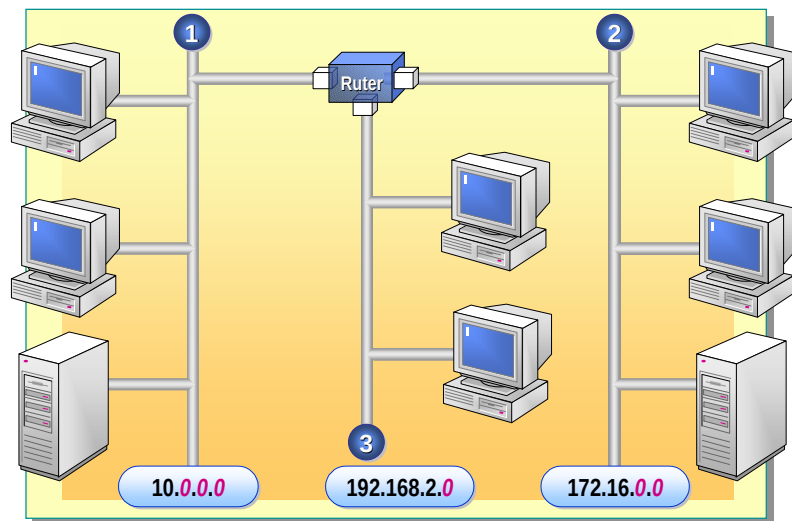
Przypisywanie identyfikatorów sieci

Cel slajdu

Przedstawienie dopuszczalnych zakresów dla identyfikatorów sieci.

Wprowadzenie

Każda podsieć musi posiadać własny identyfikator sieci.



Wskazówka

Przypomnij słuchaczom, że za pomocą klas można efektywnie przydzielać organizacjom adresy IP w Internecie. Dlatego właśnie, aby organizacja mogła komunikować się przez Internet, musi posiadać unikalny identyfikator sieci.

Identyfikator sieci pozwala zidentyfikować hosty TCP/IP znajdujące się w tej samej fizycznej podsieci. Aby zapewnić wszystkim hostom, znajdującym się w tej samej podsieci, możliwość komunikowania się ze sobą, musi zostać przypisany im ten sam identyfikator sieci.

Każda podsieć musi posiadać unikalny identyfikator sieci. Na przykład podsieć A może mieć identyfikator sieci 10.0.0.0, podsieć B może mieć identyfikator sieci 192.168.2.0, natomiast podsieć C może mieć identyfikator sieci 172.16.0.0.

Zamieszczona poniżej tabela zawiera zestaw dopuszczalnych wartości identyfikatorów sieci.

Klasa adresu	Początek zakresu	Koniec zakresu
Klasa A	1.0.0.0	126.0.0.0
Klasa B	128.0.0.0	191.255.0.0
Klasa C	192.0.0.0	223.255.255.0

Uwaga Jeżeli dana sieć ma zostać przyłączona do Internetu, należy się upewnić, czy część adresu IP, odpowiadająca identyfikatorowi sieci, nie powtarza się w żadnej sieci w obrębie całego Internetu. Odpowiedni numer IP sieci może zostać przydzielony przez dostawcę usług internetowych. Dana sieć może zostać jeszcze dalej podzielona, dzięki zastosowaniu odpowiednich masek podsieci.

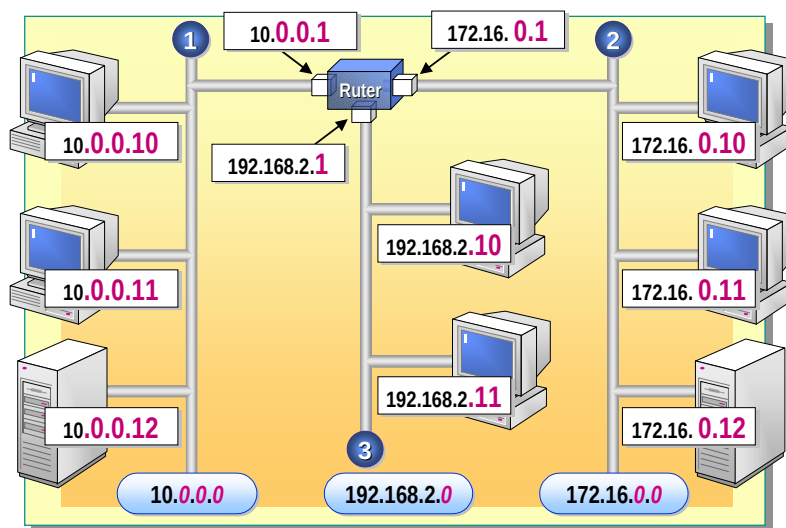
Przypisywanie identyfikatorów hosta

Cel slajdu

Przedstawienie dopuszczalnych zakresów dla identyfikatorów hosta.

Wprowadzenie

Przed przypisaniem identyfikatorów hosta należy rozważyć następujące kwestie.



Wskazówka

Chociaż obliczenie identyfikatora hosta ułatwia przypisywanie adresów IP w podsieci, identyfikator hosta jako taki nie jest użyteczny. Aby jednoznacznie określić host, należy znać pełen adres IP.

Identyfikator hosta określa dany host TCP/IP wewnątrz sieci i w związku z tym nie może powtarzać się w ramach jednego identyfikatora sieci. Wszystkie hosty TCP/IP, włączając w to routery, muszą posiadać unikalny identyfikator hosta. W zakresie przypisywania identyfikatorów hosta w podsieciach nie obowiązują żadne reguły. Na przykład, można numerować wszystkie hosty TCP/IP w kolejności lub numerować je w taki sposób, aby można było później łatwo je identyfikować, chociażby przypisując routerowi w każdej podsieci identyfikator hosta z liczbą 1 na ostatniej pozycji.

Poprawne identyfikatory hosta

Poniższa tabela zawiera zestaw dopuszczalnych wartości identyfikatorów hosta dla każdej klasy adresów.

Klasa adresu	Początek zakresu	Koniec zakresu
Klasa A	w.0.0.1	w.255.255.254
Klasa B	w.x.0.1	w.x.255.254
Klasa C	w.x.y.1	w.x.y.254

Domyślna brama

Adres IP routera, który znajduje się w tym samym segmencie co dany host, nazywany jest domyślną bramą hosta. Wszystkie informacje, które host wysyła do innych, niż własny, segmentów sieci, przesyłane są przez domyślną bramę.

Ponieważ host i jego domyślna brama znajdują się w tym samym segmencie, mają taki sam identyfikator sieci, lecz różne identyfikatory hosta. Na przykład, dla hosta o adresie IP 192.168.2.11 adres IP domyślnej bramy to 192.168.2.1.

Laboratorium B: Rozpoznawanie poprawnych adresów IP

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na przypisywaniu adresów IP oraz określeniu powodów, dla których w sieciach o różnych wielkościach stosuje się różne adresy IP.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Przydzielać adresy IP w środowisku złożonym z jednego segmentu.
- Przydzielać adresy IP w środowisku złożonym z wielu segmentów.
- Określać prawidłową konfigurację IP.

Przygotowanie laboratorium

To laboratorium jest symulacją. Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Microsoft Windows 2000, Microsoft Windows NT® 4.0, Microsoft Windows 98 lub Microsoft Windows 95.
- Przeglądarka Microsoft Internet Explorer 5 lub nowsza.
- Minimalna rozdzielczość ekranu 800 x 600 przy 256 kolorach. Zalecana rozdzielczość 800 x 600 w trybie high color (16-bit).

► Aby uruchomić laboratorium

1. Zaloguj się do systemu Windows 2000 jako Administrator, podając hasło **password**.
2. Kliknij dwukrotnie ikonę **Internet Explorer**, znajdującą się na pulpicie.
3. Na stronie Materiały dla słuchacza kliknij łącze **Symulacje laboratoriów**.
4. Kliknij łącze **Rozpoznawanie poprawnych adresów IP**.
5. Przeczytaj informacje wprowadzające, a następnie kliknij odpowiednie łącze, aby rozpocząć symulację.

Przewidywany czas ukończenia laboratorium: 30 minut

◆ Przypisywanie adresów TCP/IP

Cel slajdu

Przedstawienie procesu przypisywania adresów TCP/IP.

Wprowadzenie

Po ustaleniu identyfikatorów sieci i hosta, następnym krokiem jest skonfigurowanie komputerów zgodnie z nimi.

- Statyczne adresowanie IP
- Automatyczne adresowanie IP
- Przeglądanie konfiguracji TCP/IP
- Przeglądanie konfiguracji TCP/IP za pomocą programu Ipconfig

Adresy IP mogą być przypisywane na dwa sposoby—statycznie lub automatycznie. Jeśli wybrana zostanie metoda statycznego przypisywania adresu IP, adres każdego komputera w sieci będzie musiał zostać skonfigurowany ręcznie. Jeśli jednak wybrana zostanie metoda automatycznego przypisywania adresu IP, adresy IP dla całej sieci będą mogły zostać skonfigurowane w jednym miejscu, a następnie dynamicznie przydzielane poszczególnym komputerom.

Po ustaleniu adresu IP można sprawdzić konfigurację TCP/IP, korzystając z okna dialogowego **Internet Protocol (TCP/IP) Properties** lub narzędzia Ipconfig.

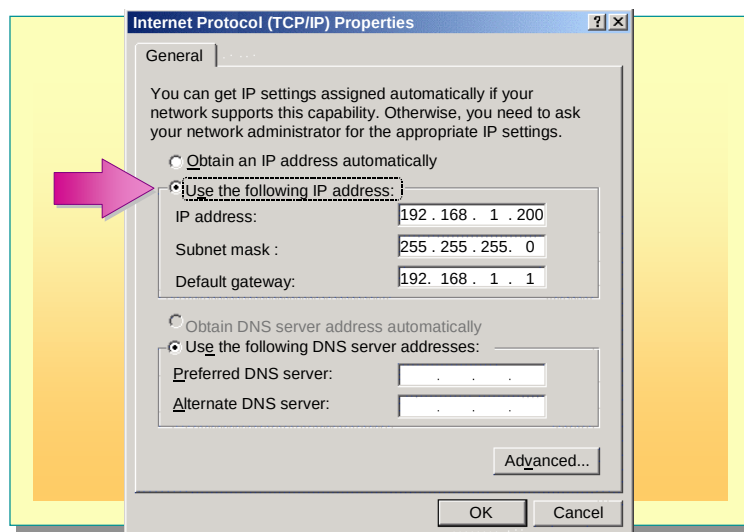
Statyczne adresowanie IP

Cel slajdu

Zilustrowanie statycznego adresowania IP.

Wprowadzenie

Adresy IP mogą zostać przypisane ręcznie w oknie dialogowym **Internet Protocol (TCP/IP) Properties**.



Wskazówka

Pokaż, w jaki sposób można korzystać z okna dialogowego **Internet Protocol (TCP/IP) Properties** oraz wytłumacz, jakie opcje należy wybrać, aby przypisać adresy statycznie. Możesz wykorzystać to jako wprowadzenie do zagadnień opisanych na następnej stronie, polecając słuchaczom wywołać okno dialogowe **Internet Protocol (TCP/IP) Properties** na swoich komputerach. Ponieważ słuchacze nie będą mogli sprawdzić adresów IP, możesz przejść do zagadnień opisanych dalej. Zwróć uwagę, że w przypadku standardowych ustawień komputerów w pracowni, adres IP komputera wykładowy jest przypisywany statycznie, podczas kiedy adresy słuchaczy są przydzielane automatycznie.

Statyczne adresowanie IP sprowadza się do ręcznej konfiguracji adresu IP. W przypadku tej metody adresowania, adres IP jest przypisywany za pomocą narzędzi dostępnych w systemie Windows 2000. W systemie Windows 2000 dostępne jest okno dialogowe **Internet Protocol (TCP/IP) Properties**, za pomocą którego można ręcznie przypisać adres IP hostowi lub urządzeniu TCP/IP.

Aby otworzyć okno dialogowe właściwości TCP/IP, należy:

1. W menu **Start** wskazać pozycję **Settings**, a następnie kliknąć ikonę **Network and Dial-up Connections**.
2. W oknie **Network and Dial-up Connections** kliknąć prawym przyciskiem myszy ikonę **Local Area Connection** i wybrać opcję **Properties**.
3. W oknie dialogowym **Local Area Connection Properties** wybrać kartę **Internet Protocol (TCP/IP)**, a następnie wybrać przycisk **Properties**, co spowoduje wyświetlenie okna dialogowego **Internet Protocol (TCP/IP) Properties**.

W tym oknie dialogowym należy zaznaczyć pole wyboru **Use the following IP address**, co umożliwi wpisanie adresu IP, maski podsieci oraz adresu domyślnej bramy.

Uwaga Generalnie, większość komputerów ma zainstalowaną tylko jedną kartę sieciową, a więc potrzebuje tylko jednego adresu IP. Jeśli w danym urządzeniu, takim jak ruter, zainstalowanych jest kilka kart sieciowych, każdej karcie musi zostać przypisany osobny adres IP.

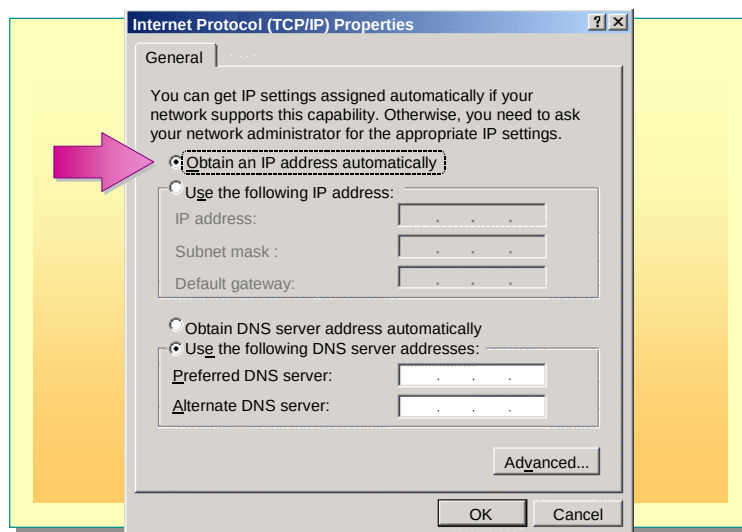
Automatyczne adresowanie IP

Cel slajdu

Przedstawienie automatycznego adresowania IP.

Wprowadzenie

System Windows 2000 obsługuje automatyczne przypisywanie adresów IP.



Wskazówka

Przedstaw okno dialogowe **Internet Protocol (TCP/IP) Properties** i pokaż, jak wybrać automatyczne opcje. Jeśli zastosowane zostały standardowe ustawienia komputerów w pracowni, komputery słuchaczy powinny mieć ustawioną automatyczną konfigurację.

Zgodnie z domyślnymi ustawieniami, system Windows 2000 jest w stanie automatycznie uzyskiwać adres IP, korzystając z protokołu DHCP (Dynamic Host Configuration Protocol).

Protokół DHCP

Protokół DHCP stanowi standard sieci TCP/IP, upraszczający zarządzanie konfiguracją IP i przypisywanie adresów w sieci korporacyjnej. Protokół DHCP zarządza dynamicznym przydzielaniem adresów IP za pomocą serwera DHCP, zawierającego bazę adresów IP, które mogą zostać nadane hostom w sieci.

Aby możliwe stało się wykorzystanie protokołu DHCP w sieci, znajdujące się w niej hosty muszą mieć włączoną jego obsługę. Aby włączyć obsługę protokołu DHCP, należy zaznaczyć pole wyboru **Obtain an IP address automatically**, co jest domyślnym ustawieniem systemu Windows 2000.

Protokół DHCP zmniejsza nakład pracy, którą musi wykonywać administrator, konfigurując komputery w sieciach wykorzystujących stos TCP/IP. Podczas przenoszenia komputera pomiędzy podsieciami zachodzi konieczność zmiany jego adresu IP ze względu na nowy identyfikator sieci. Protokół DHCP pozwala automatycznie przypisywać adresy IP hostom, zwanym także klientami DHCP, korzystając z bazy danych adresów przypisanych danej podsieci. Protokół ten jest także wykorzystywany do ponownego przypisywania adresu IP innemu klientowi, jeśli dany komputer jest odłączony od sieci przez określony czas.

APIPA (Automatic Private IP Addressing)

Jeśli w trakcie automatycznego przypisywania adresu IP serwer DHCP nie może zostać odnaleziony, system Windows 2000 określa adres, korzystając z zarezerwowanej przez Microsoft klasy adresowania IP, która obejmuje zakres od 169.254.0.1 do 169.254.255.254. Adres ten jest wykorzystywany do czasu znalezienia serwera DHCP. Ta metoda uzyskiwania adresu IP określana jest mianem automatycznego adresowania IP. W przypadku tej metody serwer DNS lub WINS, albo domyślna brama nie są przypisywane, gdyż metoda ta jest zarezerwowana dla niewielkich sieci, obejmujących tylko jeden segment.

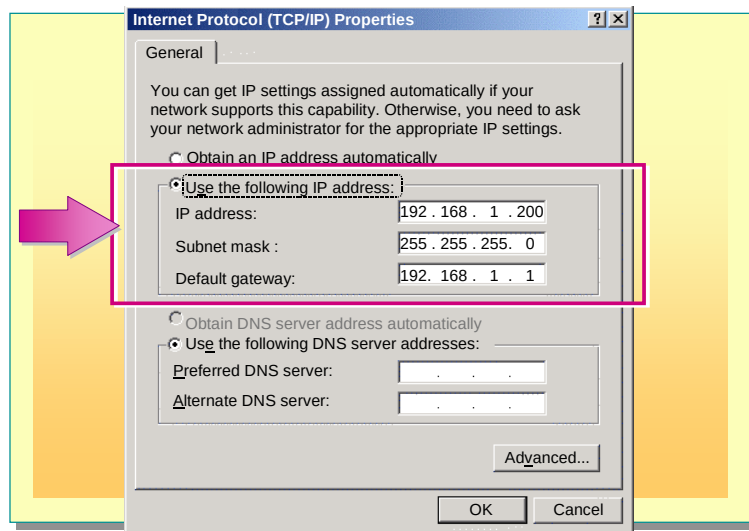
Przeglądanie konfiguracji TCP/IP

Cel slajdu

Przedstawienie sposobu przeglądania informacji TCP/IP za pomocą okna dialogowego **Internet Protocol TCP/IP Properties**.

Wprowadzenie

Po określeniu na komputerze konfiguracji TCP/IP, można ją w dowolnej chwili sprawdzić, pod warunkiem, że adres IP jest podawany statycznie.



Wskazówka

Jeśli słuchacze zapytają, w jaki sposób mogą sprawdzić adres IP swojego komputera, wykorzystaj to pytanie, jako wprowadzenie do następnego zagadnienia. Pamiętaj, że Ty możesz sprawdzić swój adres IP, lecz słuchacze nie mają takiej możliwości. Okno dialogowe **Internet Protocol (TCP/IP) Properties** jest jednak istotne, ponieważ za jego pomocą można wybrać, czy ustawienia TCP/IP mają być konfigurowane statycznie czy dynamicznie. Słuchacze będą korzystać z okna dialogowego, realizując laboratorium.

Zdarzają się sytuacje, w których konieczne jest sprawdzenie informacji dotyczących adresu IP określonego komputera. Na przykład komputer może nie być w stanie komunikować się z innymi komputerami w sieci lub też inne komputery mogą nie być w stanie komunikować się z danym komputerem. W takich przypadkach, aby odnaleźć źródło problemu, konieczne jest sprawdzenie adresów IP pozostałych komputerów.

Statyczne informacje dotyczące stosu protokołów TCP/IP mogą zostać sprawdzone za pomocą okna dialogowego **Internet Protocol (TCP/IP) Properties**.

Okno dialogowe Internet Protocol (TCP/IP) Properties

Korzystając z okna dialogowego **Internet Protocol (TCP/IP) Properties**, można określić, czy konfiguracja adresu IP jest realizowana dynamicznie, czy też statycznie. Jeśli jednak adres IP jest konfigurowany dynamicznie za pomocą protokołu DHCP lub konfigurowany automatycznie przez system Windows 2000, nie można sprawdzić wartości opcji konfiguracyjnych TCP/IP. Do opcji tych zalicza się: adres IP, maskę podsieci oraz domyślną bramę. Wartości tych opcji mogą zostać sprawdzone tylko pod warunkiem, że konfiguracja jest przeprowadzana w sposób statyczny.

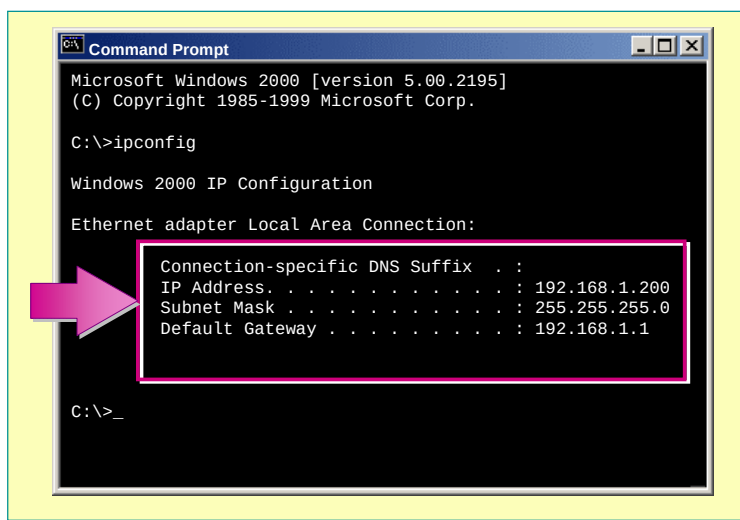
Przeglądanie konfiguracji TCP/IP za pomocą programu Ipconfig

Cel slajdu

Przedstawienie składni polecenia Ipconfig, pozwalającego przeglądać informacje TCP/IP.

Wprowadzenie

Po ustaleniu na komputerze konfiguracji TCP/IP, można ją w dowolnym momencie sprawdzić.



Wskazówka

Pokaż, w jaki sposób można uzyskać dostęp do narzędzia Ipconfig. Podkreśl, że za pomocą narzędzia Ipconfig nie można zmienić konfiguracji TCP/IP. Zapytaj słuchaczy o różnice pomiędzy informacjami wyświetlanymi przez narzędzie Ipconfig oraz dostępnymi w oknie dialogowym **Internet Protocol (TCP/IP) Properties**. Kwestia ta zostanie dokładnie poruszona w następnym laboratorium.

W skład systemu Windows 2000 wchodzi narzędzie Ipconfig, które pozwala przeglądać informacje dotyczące ustawień TCP/IP z poziomu wiersza poleceń.

Narzędzie Ipconfig

Narzędzie Ipconfig pozwala sprawdzić, lecz nie zmienić, opcje konfiguracji TCP/IP hosta, czyli takie ustawienia jak adres IP, maska podsieci oraz domyślna brama. Składnia polecenia uruchamiającego to narzędzie ma postać: *ipconfig*.

Aby uruchomić narzędzie Ipconfig, należy wpisać w wierszu poleceń **ipconfig**. Spowoduje to wyświetlenie trzech podstawowych parametrów konfiguracji. Nie można jednak w ten sposób ustalić, jaka metoda, statyczna czy dynamiczna, jest wykorzystywana w trakcie przypisywania adresu IP.

Ipconfig /all

Bardziej szczegółowe informacje można otrzymać, umieszczając po poleceniu Ipconfig przełącznik **all**. Aby uruchomić narzędzie Ipconfig z tym przełącznikiem, należy wpisać w wierszu poleceń **ipconfig /all**.

Na ekranie wyświetlone zostaną informacje dotyczące wszystkich opcji konfiguracji TCP/IP. Dzięki temu można określić, czy włączona jest obsługa protokołu DHCP. Jeśli obok etykiety DHCP Enabled wyświetlana jest wartość Yes oraz wyświetlany jest adres IP serwera DHCP, oznacza to, że adres IP hosta został przypisany przy wykorzystaniu protokołu DHCP.

Serwer DHCP przydziela klientowi adres IP na pewną określoną ilość czasu. Etykiety Lease Obtained oraz Lease Expires zawierają odpowiednio informacje o tym, kiedy został przypisany adres IP i kiedy zostanie on odebrany.

Jeśli w trakcie przypisywania adresu IP serwer DHCP nie był dostępny i adres IP został przypisany automatycznie, przed etykietą adresu IP komputera umieszczany jest termin Autoconfiguration. Obok etykiety Autoconfiguration Enabled wyświetlana jest wartość Yes, natomiast nie jest wyświetlany adres IP serwera DHCP.

Laboratorium C: Sprawdzanie konfiguracji TCP/IP

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na ocenieniu scenariusza, według którego były przydzielane adresy IP oraz określeniu błędów popełnionych podczas jego wykonania.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Przeglądać konfigurację TCP/IP za pomocą narzędzia Ipconfig.
- Przeglądać konfigurację TCP/IP za pomocą okna dialogowego **Internet Protocol (TCP/IP) Properties**.
- Znaleźć odpowiednie zastosowanie dla narzędzia Ipconfig oraz okna dialogowego **Internet Protocol (TCP/IP) Properties**.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Poznać działanie stosu protokołów TCP/IP systemu Microsoft Windows 2000.
- Zrozumieć, czym są adresy IP.
- Nauczyć się logować do systemu Windows 2000.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Sprawdzanie konfiguracji TCP/IP

Scenariusz

Jesteś administratorem niewielkiej sieci i chcesz sprawdzić konfigurację znajdujących się w niej komputerów.

Cel

W tym ćwiczeniu sprawdzisz aktualną konfigurację IP swojego komputera, porównując ze sobą ustawienia odczytane z okna dialogowego **Internet Protocol (TCP/IP) Properties** oraz uzyskane za pomocą narzędzia Ipconfig.

Zadania	Szczegółowe kroki
1. Zaloguj się jako Administrator, wpisując hasło password, a następnie otwórz okno dialogowe Internet Protocol (TCP/IP) Properties.	a. Zaloguj się do systemu Windows 2000 jako Administrator, wpisując hasło password. b. W menu Start wskaż pozycję Settings, a następnie kliknij Network and Dial-up Connections.  Wyświetlone zostanie okno <i>Network and Dial-up Connections</i>. c. Kliknij prawym przyciskiem myszy ikonę Local Area Connection. d. Wybierz opcję Properties. e. Wybierz kartę Internet Protocol (TCP/IP). f. Wybierz przycisk Properties.
Czy możesz stwierdzić, w jaki sposób przypisany został adres IP? Jeśli tak, napisz jak to nastąpiło? Komputer został tak skonfigurowany, aby automatycznie uzyskiwać adres IP.	
 Czy możesz sprawdzić adres IP swojego komputera? Jeśli tak, to jaki on jest? Nie.	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Czy możesz skonfigurować stos protokołów TCP/IP tak, aby korzystał on ze statycznego adresu IP? Jeśli tak, to w jaki sposób możesz to zrobić? Tak, aby to zrobić, należy zaznaczyć opcję Use the following IP address. _____ _____ _____ _____	
1. (ciąg dalszy)	g. Zamknij wszystkie otwarte okna (wybierając przycisk Cancel, jeśli jest to możliwe).
2. Sprawdź adres IP komputera, korzystając z narzędzia Ipconfig.	a. W menu Start wskaż pozycję Programs, a następnie kliknij pozycję Command Prompt. b. W oknie Command Prompt wpisz polecenie ipconfig.
? Czy możesz stwierdzić, w jaki sposób przypisany został adres IP? Jeśli tak, to w jaki sposób to nastąpiło? Nie. _____ _____ _____ _____	
? Czy możesz sprawdzić adres IP swojego komputera? Jeśli tak, to jaki on jest? Tak, 192.168.1.x (gdzie x ma wartość pomiędzy 100 i 199). _____ _____ _____ _____	
? Jakie dodatkowe informacje o konfiguracji są wyświetlane? Jakie wartości przyjmują dodatkowe parametry TCP/IP Twojego komputera? Maska podsieci oraz domyślna brama. 255.255.255.0 oraz w.x.y.z (adres IP instruktora). _____ _____ _____ _____	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Czy możesz ręcznie zmienić adres IP za pomocą narzędzia Ipconfig? Jeśli tak, to w jaki sposób? Nie.	
3. Sprawdź szczegółową konfigurację IP, uruchamiając ipconfig z przełącznikiem /all.	a. W oknie Command Prompt wpisz polecenie ipconfig /all.
? Czy możesz stwierdzić, w jaki sposób przypisany został adres IP? Jeśli tak, napisz jak to nastąpiło? Tak, adres IP został przypisany za pomocą protokołu DHCP.	
? Czy nadal możesz sprawdzić adres IP oraz opcje konfiguracji IP, tak jak to miało miejsce wcześniej? Tak.	
? Jaki jest adres IP serwera, który nadał Twojemu komputerowi adres IP? w.x.y.z (adres komputera instruktora).	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Kiedy wygasa adres IP Twojego komputera? Odpowiedź będzie różna, lecz data wygaśnięcia będzie przesunięta o osiem dni od czasu przyznania adresu.	
? Jeśli w oknie Command Prompt wpisałeś ipconfig /all, to jaki otrzymasz wynik w przypadku, gdy komputer został tak skonfigurowany, aby automatycznie otrzymywać adres IP, lecz serwer DHCP nie jest dostępny? Jakie informacje nie zostaną wyświetlone? Przed etykietą IP address wyświetlone zostanie słowo autoconfiguration, natomiast nie zostanie wyświetlony adres serwera DHCP.	
? Jakie korzyści wynikają z wykorzystania okna dialogowego Internet Protocol (TCP/IP) Properties zamiast narzędzia Ipconfig? Okno dialogowe Internet Protocol (TCP/IP) Properties pozwala administratorowi określić statyczny adres IP oraz wybrać statyczną lub automatyczną metodę uzyskiwania adresu IP.	
? Jakie korzyści wynikają z wykorzystania narzędzia Ipconfig zamiast okna dialogowego Internet Protocol (TCP/IP) Properties? Narzędzie Ipconfig pozwala administratorowi sprawdzić adres IP niezależnie od metody wykorzystanej do jego określenia. Możesz także użyć narzędzia Ipconfig, aby określić, czy wykorzystana została metoda automatycznej konfiguracji, czy protokół DHCP.	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Jaka jest klasa adresu IP Twojego komputera? Klasa C.	
? Czy maska podsieci, ustalona na Twoim komputerze, jest taka sama jak domyślna maska podsieci dla adresów IP klasy C? Tak, obie maski to 255.255.255.0.	
? Jaki jest identyfikator sieci Twojego komputera? 192.168.1.0.	
? Jaki jest adres IP domyślnej bramy? 192.168.1.200.	

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Czy domyślna brama ma taki sam identyfikator sieci, jak Twój komputer? Tak.	
? Czy domyślna brama znajduje się w tym samym segmencie sieci, jak Twój komputer ? Tak.	
? Jaką inną nazwą określa się domyślną bramę? Ruter.	
? Jak wiele adresów IP, z takim samym identyfikatorem sieci, może zostać przypisanych komputerom znajdującym się w tym samym segmencie, jak Twój komputer? 254	
4. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000.	a. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000.

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Pytania podsumowujące dotyczą głównych tematów omówionych w rozdziale.

- Adresowanie IP z podziałem na klasy
- Podział sieci na podsieci
- Planowanie adresowania IP
- Przypisywanie adresów TCP/IP

-
1. Do czego służy adres IP?

Adres IP pozwala rozróżniać komputery, jako niezależne elementy sieci i ułatwia lokalizowanie komputerów w sieci.

2. Które liczby (w , x , y , z) w adresach IP poszczególnych klas (A, B oraz C), odpowiadają identyfikatorowi sieci, a które identyfikatorowi hosta?

Klasa A: Identyfikatorem sieci jest pierwsza liczba adresu IP. Pozostałe trzy liczby określają identyfikator hosta.

Klasa B: Identyfikator sieci zawiera się w dwóch pierwszych liczbach adresu IP. Pozostałe dwie liczby określają identyfikator hosta.

Klasa C: Identyfikator sieci zawiera się w trzech pierwszych liczbach adresu IP. Pozostała liczba określa identyfikator hosta.

3. Jako administrator musisz upewnić się, że komputery w sieci mogą się ze sobą efektywnie komunikować. Co możesz zrobić, aby wraz ze wzrostem łącznej liczby komputerów w sieci, zredukować liczbę komputerów, znajdujących się w poszczególnych częściach sieci?

Podzielić sieć na podsieci.

4. Wyobraź sobie, że jesteś w trakcie przypisywania adresów IP komputerom znajdującym się w Twojej sieci. O czym musisz pamiętać, przypisując adresy IP?

Pierwszą liczbą identyfikatora sieci nie może być liczba 127, identyfikator hosta nie może składać się tylko z zer lub tylko z liczb 255 oraz identyfikator hosta nie może wystąpić dwa razy z tym samym identyfikatorem sieci. Należy także pamiętać, że przypisując identyfikator sieci, musi zostać przyznany jeden identyfikator sieci każdej podsieci.

5. Jako administrator dużej sieci będziesz z pewnością chciał uprościć proces przypisywania adresów IP. Jakie rozwiązanie możesz zastosować, aby automatycznie przypisywać adres IP każdemu komputerowi w sieci?

Protokół DHCP. Chociaż adresy IP są domyślnie przypisywane automatycznie także bez niego, metoda bez protokołu DHCP jest efektywna tylko w przypadku pojedynczej podsieci i nie pozwala na komunikację z Internetem.

6. Twój komputer nie jest w stanie komunikować się z innymi komputerami w trakcie pracy w sieci. Aby znaleźć źródło problemu, chcesz sprawdzić adres IP innych komputerów. Jakie dwa narzędzia, pozwalające przeglądać konfigurację adresu IP, są dostępne w systemie Windows 2000? Jakie są zalety każdej z tych metod?

Okno dialogowe Internet Protocol (TCP/IP) Properties oraz narzędzie Ipconfig, do którego dostęp uzyskuje się z wiersza poleceń. Okno dialogowe Internet Protocol (TCP/IP) Properties pozwala wybrać statyczny lub automatyczny sposób przypisywania adresu IP, jak również w sposób statyczny przypisać konkretny adres. Narzędzie Ipconfig pozwala przeglądać ustawienia opcji konfiguracji TCP/IP, wliczając w to automatycznie przyznawany adres IP oraz informacje o czasie przyznania adresu IP przez serwer DHCP.

