

Rozdział 6: Analiza protokołu TCP/IP

Spis treści

Przegląd zagadnień	1
Wprowadzenie do TCP/IP	2
Przegląd architektury stosu protokołów TCP/IP	7
Laboratorium A: Badanie programów narzędziowych TCP/IP	17
Rozwiązywanie nazw	20
Badanie procesu przesyłania danych	26
Ruting danych	32
Laboratorium B: Badanie procesów i protokołów stosu TCP/IP	37
Podsumowanie	38



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 Pierścioneek, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
105 minut

Laboratoria:
30 minut

W tym rozdziale znajdują się informacje na temat pojęć związanych z protokołem TCP/IP oraz na temat komunikacji za pomocą protokołu TCP/IP. Pierwsza sekcja rozdziału rozpoczyna się wprowadzeniem do procesu komunikacji i omówieniem czterech warstw w stosie protokołu. Sekcja kończy się omówieniem wykorzystania gniazd w identyfikacji aplikacji biorących udział w procesie komunikacji.

W następnej sekcji znajduje się opis stosu protokołów TCP/IP oraz ich funkcji w procesie komunikacji. Sekcja kończy się informacjami na temat niektórych programów narzędziowych—Hostname, Arp oraz Ping—zawartych w architekturze protokołu TCP/IP. W laboratorium kończącym tę sekcję, słuchacze użyją, jako przykładowych programów narzędziowych TCP/IP, programów Hostname, Arp oraz Ping do testowania połączeń.

Trzecia sekcja została poświęcona procesowi rozwiązywania nazw. Rozpoczyna się on omówieniem nazw hostów oraz nazw NetBIOS, a następnie wyjaśnione zostało statyczne i dynamiczne mapowanie oraz proces rozwiązywania nazw.

W następnej sekcji badany jest proces przesyłania danych za pomocą protokołu TCP/IP. W sekcji tej została wyjaśniona terminologia używana do opisu pakietu oraz omówiono składniki ramki i sposoby wyboru trasy obieranej przez dane podczas przesyłania od komputera źródłowego do komputera docelowego. Jest tutaj rozwinięcie tematu przedstawionego w pierwszej sekcji oraz opis współpracy protokołów TCP/IP umożliwiającej komunikację między komputerami.

W ostatniej sekcji został przedstawiony proces routingu. Wyjaśnione zostały metody dostarczania pakietów oraz szczegółowo omówiono proces wyboru trasy przesyłania danych przez sieć do punktu przeznaczenia. Temat przedstawiony w pierwszej sekcji kończy się tutaj wyjaśnieniem sposobu przesyłania pakietów od jednego ruteru do następnego, aż do osiągnięcia adresu docelowego. Na końcu rozdziału jest laboratorium, w którym słuchacze zapoznają się z procesami związanymi z rozwiązywaniem nazw oraz z protokołami zaangażowanymi podczas używania polecenia Ping poprzez ruter.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać proces komunikacji za pomocą protokołu TCP/IP.
- Nazwać protokoły ze stosu protokołów TCP/IP oraz opisać ich funkcje.
- Opisać proces rozwiązywania przyjaznej dla użytkownika nazwy komputera przez mapowanie nazwy do adresu IP.
- Opisać proces przesyłania pakietów danych między komputerami.
- Opisać, w jaki sposób proces routingu wpływa na przesyłanie informacji między segmentami, tak że komputery mogą komunikować się w dużych sieciach.

Materiały i sposób przygotowania

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

Wymagane materiały

Do przedstawienia tego rozdziału wykładowcy potrzebne będą następujące materiały:

- Plik 2243A_06.ppt, programu Microsoft® PowerPoint®
- Rozdział 6, „Analiza protokołu TCP/IP”

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału, należy:

- Przeczytać wszystkie materiały do tego rozdziału.
- Przeczytać temat TCP/IP w Pomocy systemu Windows 2000.
- Przeczytać publikacje, *Introduction to TCP/IP* oraz *TCP/IP Implementation Details for Windows*, znajdujące się na płycie kompaktowej Materiały trenerskie.
- Wykonać dwa laboratoria.
- Przeczytać wskazówki i uwagi znajdujące się na marginesie rozdziału.
- Przeczytać odpowiedzi do pytań i przygotować alternatywne odpowiedzi do dyskusji.
- Przewidzieć pytania słuchaczy i przygotować odpowiedzi na nie.

Strategia przedstawienia rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Wprowadzenie do TCP/IP
W tej sekcji należy przedstawić proces komunikacji danych. Następnie należy krótko opisać warstwy w stosie protokołów TCP/IP i wyjaśnić, w jaki sposób gniazda są wykorzystywane do rozróżniania połączeń.
- Przegląd architektury stosu protokołów TCP/IP
W tej sekcji należy opisać właściwości i funkcje każdego z protokołów w stosie TCP/IP oraz programy narzędziowe dostępne dla tego stosu protokołów. Następnie należy zademonstrować działanie poleceń Hostname, Arp oraz Ping.
- Rozwiązywanie nazw
W tej sekcji należy opisać dwa rodzaje nazw komputera, koncepcję statycznego i dynamicznego mapowania oraz proces rozwiązywania nazw hostów oraz nazw NetBIOS.
- Badanie procesu przesyłania danych
W tej sekcji należy wyjaśnić pojęcia związane z pakietami danych na różnych stopniach przygotowania ich do transmisji przez sieć. Następnie należy opisać składniki pakietu danych oraz proces przygotowania pakietu na komputerze źródłowym oraz dostęp do informacji w pakiecie na komputerze docelowym.
- Ruting danych
W tej sekcji należy opisać proces routingu IP oraz metody dostarczania pakietów. Następnie należy wyjaśnić proces wyboru trasy przesyłania danych między segmentami.

Informacje uzupełniające

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

Ważne Aby możliwe było wykonanie laboratorium, zawartego 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 tym rozdziale, została omówiona komunikacja za pomocą stosu protokołów TCP/IP w sieci opartej na systemie Windows 2000.

- Wprowadzenie do TCP/IP
- Przegląd architektury stosu protokołów TCP/IP
- Rozwiązywanie nazw
- Badanie procesu przesyłania danych
- Ruting danych

TCP/IP (Transmission Control Protocol/Internet Protocol) w systemie Microsoft® Windows® 2000 jest standardowym, rutownym protokołem sieciowym, który jest najbardziej kompletnym i akceptowalnym protokołem spośród dostępnych protokołów. Większość obecnie używanych sieciowych systemów operacyjnych, obsługuje protokół TCP/IP i duże sieci częściej działają na protokole TCP/IP, niż na innych protokołach.

TCP/IP udostępnia technologię umożliwiającą łączenie różnych systemów. Dostarcza również niezawodną, skalowalną platformę oprogramowania typu klient/serwer oraz podstawę dostępu do usług sieci Internet, takich jak World Wide Web oraz poczta elektroniczna.

Różne protokoły w stosie TCP/IP współpracują razem, aby komunikacja sieciowa sprawnie działała. Proces ten dotyczy wielu działań, włącznie z rozwiązywaniem przyjaznych dla użytkownika nazw na adresy IP (Internet Protocol), określaniem lokalizacji komputera przeznaczenia, pakowaniem, adresowaniem oraz wyznaczaniem trasy przesyłania danych, aż do miejsca przeznaczenia.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Opisać proces komunikacji za pomocą protokołu TCP/IP.
- Nazwać protokoły ze stosu protokołów TCP/IP oraz opisać ich funkcje.
- Opisać proces rozwiązania przyjaznej dla użytkownika nazwy komputera przez mapowanie nazwy do adresu IP.
- Opisać proces przesyłania pakietów danych między komputerami.
- Opisać, w jaki sposób proces routingu wpływa na przesyłanie informacji między segmentami, tak że komputery mogą komunikować się w dużych sieciach.

◆ Wprowadzenie do TCP/IP

Cel slajdu

Wprowadzenie do stosu protokołów TCP/IP.

Wprowadzenie

System Windows 2000 obsługuje TCP/IP zarówno jako protokół oraz jako sieciowe usługi służące do łączenia i zarządzania sieciami.

- Proces komunikacji
- Warstwy TCP/IP
- Identyfikacja aplikacji

TCP/IP (Transmission Control Protocol/Internet Protocol) jest przemysłowym standardem stosu protokołów używanych do komunikacji między komputerami działającymi w systemie Windows 2000. TCP/IP jest zaprojektowany do komunikacji w dużych sieciach.

Zadania związane z używaniem protokołu TCP/IP w procesie komunikacji są rozdzielone między cztery odrębne warstwy stosu TCP/IP. Każdy protokół w stosie TCP/IP pełni odrębną rolę w procesie komunikacji.

W procesie komunikacji, wiele aplikacji może komunikować się w tym samym czasie. TCP/IP posiada zdolność odróżniania aplikacji. TCP/IP identyfikuje aplikację na komputerze, a następnie przesyła dane z tej aplikacji do aplikacji na innym komputerze.

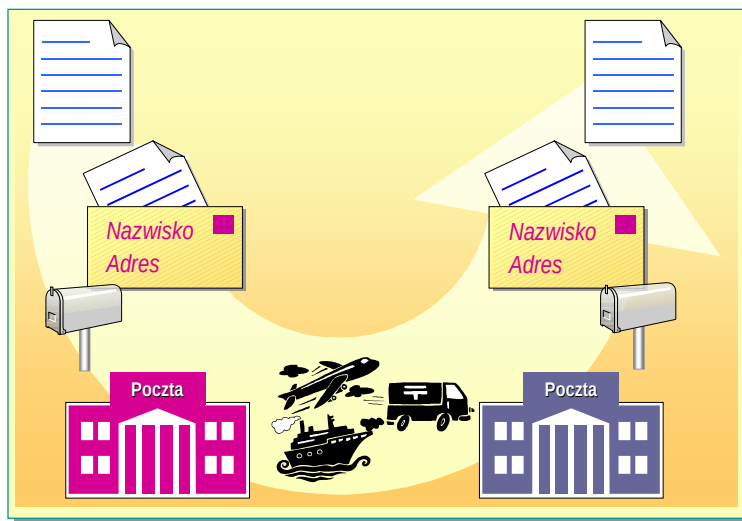
Proces komunikacji

Cel slajdu

Przedstawienie procesu komunikacji za pomocą protokołu TCP/IP.

Wprowadzenie

TCP/IP umożliwia komunikację między komputerami działającymi w systemie Windows 2000 poprzez definiowanie modelu komunikacji.

**Wskazówka**

Wyjaśnij, w jaki sposób komunikacja za pomocą protokołu TCP/IP nawiązuje do powszechnego schematu, jakim jest proces przesyłania listu. Użyj animowanych slajdów, aby pokazać słuchaczom, że proces ten jest podobny na każdym komputerze.

Proces przesyłania danych za pomocą protokołu TCP/IP między dwoma lokalizacjami jest podobny do procedury używanej do przesłania listu między miastami przez urzędy pocztowe.

Działanie TCP/IP

Proces komunikacji za pomocą TCP/IP jest inicjowany przez aplikację na komputerze źródłowym, która przygotowuje dane do przesłania w formacie odczytywalnym przez aplikację na komputerze docelowym. Można ten proces porównać do pisania listu w języku, który adresat może zrozumieć. Następnie dane są kojarzone z docelową aplikacją i komputerem, co można porównać do adresowania listu do odbiorcy. Adres komputera przeznaczenia jest dodawany do danych, podobnie jak wpisanie adresu odbiorcy na liście.

Po przeprowadzeniu tych czynności, dane oraz dodatkowe informacje, jak żądanie potwierdzenia odbioru są wysyłane przez sieć do miejsca przeznaczenia. Medium transmisyjne używane do przesłania danych zależy od powyższych czynności, podobnie jak transport listu między urzędami pocztowymi jest uzależniony od zawartości listu lub adresu.

Protokoły i warstwy TCP/IP

TCP/IP organizuje zarys procesu komunikacji poprzez przypisanie określonych czynności do różnych protokołów w stosie TCP/IP. Aby zwiększyć wydajność procesu komunikacyjnego, protokoły te są zorganizowane w warstwy. Informacja o adresie jest umieszczana jako ostatnia, tak że komputery w sieci mogą szybko sprawdzić, czy dane są adresowane do nich. Jedynie komputer przeznaczenia otwiera i przetwarza wszystkie dane.

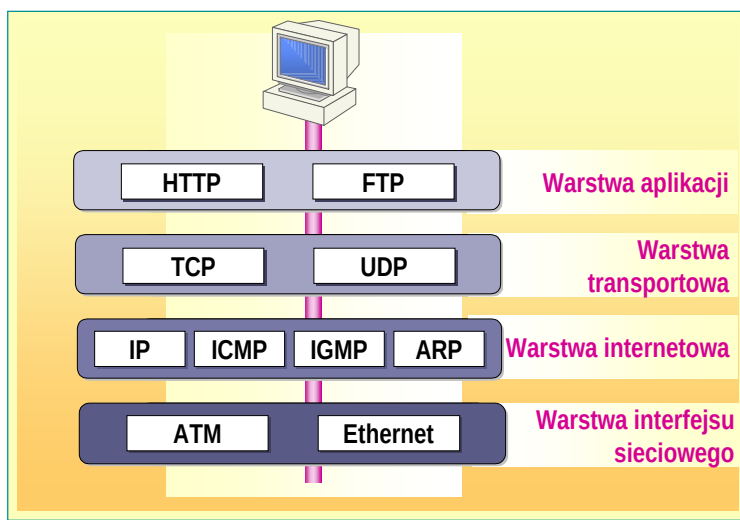
Warstwy TCP/IP

Cel slajdu

Przedstawienie warstw TCP/IP.

Wprowadzenie

TCP/IP używa czterowarstwowego modelu komunikacyjnego.

**Wskazówka**

Wyjaśnij, że cztery warstwy w stosie protokołów TCP/IP są specyficzną implementacją siedmiowarstwowego modelu OSI. Odniesz informacje zawarte w tym rozdziale do informacji o stosach protokołów zawartych w rozdziale 5, „Protokoły sieciowe”, w podręczniku do kursu 2243A, „Podstawy sieci i systemu operacyjnego Windows 2000”. Nie poświęcaj zbyt dużo czasu na omówienie określonych protokołów, gdyż będą one omawiane później. Zamiast tego, użyj tej strony do pokazania podziału zadań.

TCP/IP używa czterowarstwowego modelu komunikacyjnego do przesyłania danych między komputerami. Tymi czterema warstwami w tym modelu są, warstwa aplikacji, transportowa, internetowa oraz interfejsu sieciowego. Wszystkie protokoły ze stosu TCP/IP należą do tych warstw.

Warstwa aplikacji

Warstwa aplikacji jest najwyższą warstwą w stosie TCP/IP. Wszystkie aplikacje i programy użytkowe pracują na tej warstwie i przez tą warstwę uzyskują dostęp do sieci. Protokoły na tej warstwie są używane do formatowania i wymiany informacji użytkownika. Są to:

- HTTP (Hypertext Transfer Protocol)
Protokół HTTP jest używany do przesyłania plików charakteryzujących strony sieci Web.
- FTP (File Transfer Protocol)
Protokół FTP jest używany do interakcyjnego przesyłania plików.

Warstwa transportowa

Warstwa transportowa umożliwia uporządkowaną i gwarantowaną komunikację między komputerami oraz przekazuje dane wyżej, do warstwy aplikacji lub niżej, do warstwy internetowej. Warstwa transportowa określa również unikalny identyfikator aplikacji, do której dane są przeznaczone.

Warstwa transportowa ma dwa kluczowe protokoły określające metodę dostarczenia danych. Są to:

- TCP (Transmission Control Protocol)
Protokół TCP gwarantuje dostarczenie danych przez potwierdzenie odbioru.
- UDP (User Datagram Protocol)
Protokół UDP umożliwia szybki transfer danych, lecz bez gwarancji ich dostarczenia.

Warstwa internetowa

Warstwa internetowa jest odpowiedzialna za adresowanie, pakowanie oraz ruting transmitowanych danych. W warstwie tej znajdują się cztery kluczowe protokoły:

- IP (Internet Protocol)
Protokół IP jest odpowiedzialny za adresowanie oraz dostarczenie danych do miejsca przeznaczenia.
- ARP (Address Resolution Protocol)
Protokół ARP jest odpowiedzialny za znalezienie adresu MAC (Media Access Control) karty sieciowej komputera przeznaczenia.
- ICMP (Internet Control Message Protocol)
Protokół ICMP jest odpowiedzialny za funkcje diagnostyczne i informowanie o błędach z powodu niedostarczenia danych.
- IGMP (Internet Group Management Protocol)
Protokół IGMP jest odpowiedzialny za zarządzanie grupami multicastowymi w TCP/IP.

Warstwa interfejsu sieciowego

Warstwa interfejsu sieciowego jest odpowiedzialna za umieszczenie danych w medium transmisyjnym oraz za odbiór danych z medium transmisyjnego. Na tej warstwie znajdują się fizyczne urządzenia, takie jak karty sieciowe i okablowanie. Karta sieciowa posiada unikalny, 12-to znakowy heksadecymalny numer, np. B5-50-04-22-D4-65, znany jako adres MAC. Warstwa interfejsu sieciowego nie zawiera programowych protokołów, jak pozostałe trzy warstwy, lecz zawiera protokoły takie, jak Ethernet czy ATM (Asynchronous Transfer Mode), określające sposób transmisji danych przez sieć.

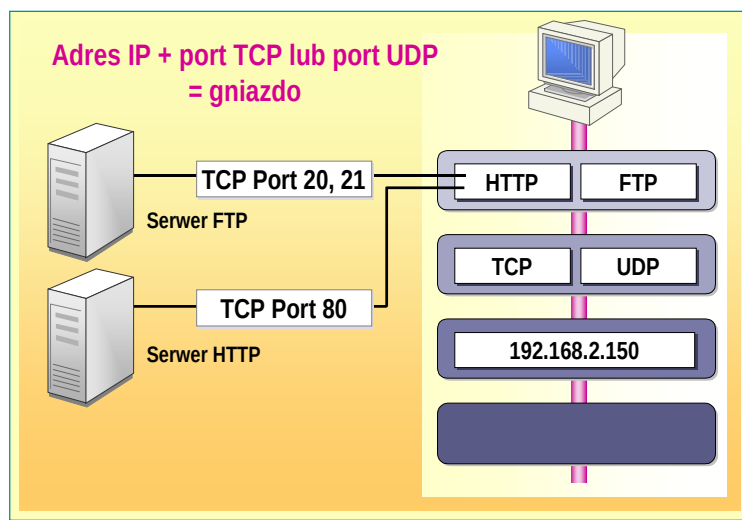
Identyfikacja aplikacji

Cel slajdu

Wyjaśnienie roli gniazd i portów w komunikacji sieciowej.

Wprowadzenie

W jaki sposób wiele aplikacji może równocześnie komunikować się w sieci?



Wskazówka

Użyj informacji na tej stronie, aby uświadomić słuchaczom, że należy określić zarówno komputer, do którego wysyłają dane, jak również aplikację na tym komputerze.

W sieci, wiele aplikacji komunikuje się w tym samym czasie. Kiedy wiele aplikacji jest uruchomionych na jednym komputerze, TCP/IP wymaga metody, za pomocą której można te aplikacje odróżnić. W tym celu, aby odróżnić aplikacje, TCP/IP używa gniazd, nazywanych również punktami końcowymi w komunikacji sieciowej.

Adres IP

Aby komunikacja sieciowa mogła się rozpocząć, lokalizacja komputera źródłowego oraz docelowego w sieci musi być znana. Lokalizacja jest określana przez unikalny numer, zwany adresem IP, który jest przypisywany do każdego komputera w sieci. Przykładem adresu może być adres 192.168.2.200.

Port TCP/UDP

Port jest identyfikatorem aplikacji działającej na komputerze. Port jest związany z protokołami TCP lub UDP warstwy transportowej i jest znany jako port TCP lub port UDP. Port może mieć dowolny numer z zakresu liczb od 0 do 65,535. Porty TCP/IP podstawowych aplikacji serwerowych są zarezerwowane z numerami poniżej 1,024, w celu zapobiegania konfliktom z innymi aplikacjami. Na przykład, serwer FTP używa portów TCP 20 i 21.

Gniazdo

Gniazdo jest złożeniem adresu IP i portu TCP lub portu UDP. Aplikacja tworzy gniazdo przez określenie adresu IP komputera, rodzaju usługi (TCP dla gwarancji dostarczenia danych, w przeciwnym razie UDP) oraz portu, który aplikacja monitoruje. Adres IP pomaga określić i zlokalizować komputer docelowy, a port określa aplikację, do której dane są wysyłane.

◆ Przegląd architektury stosu protokołów TCP/IP

Cel slajdu

Wprowadzenie do kluczowych protokołów w stosie protokołów TCP/IP firmy Microsoft.

Wprowadzenie

Stos protokołów TCP/IP składa się z sześciu kluczowych protokołów oraz zestawu programów narzędziowych.

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- ARP (Address Resolution Protocol)
- Programy narzędziowe TCP/IP

Stos protokołów TCP/IP firmy Microsoft umożliwia komunikację w sieci przedsiębiorstwa między komputerami z systemem Windows 2000.

Architektura stosu protokołów jest tworzona przez producenta lub organizację, w celu dostosowania stosu protokołów do swoich potrzeb. Dlatego stos protokołów jest zestawem protokołów zaprojektowanych i wdrożonych, jako wzajemnie uzupełniający się, dobrze działający zestaw.

Stos protokołów TCP/IP składa się z sześciu kluczowych protokołów oraz zestawu programów narzędziowych. Te sześć kluczowych protokołów—TCP, UDP, IP, ICMP, IGMP oraz ARP—oferuje zestaw standardów umożliwiających komunikację między komputerami oraz między sieciami. Wszystkie aplikacje oraz inne protokoły w stosie TCP/IP są uzależnione od podstawowych usług pełnionych przez te kluczowe protokoły.

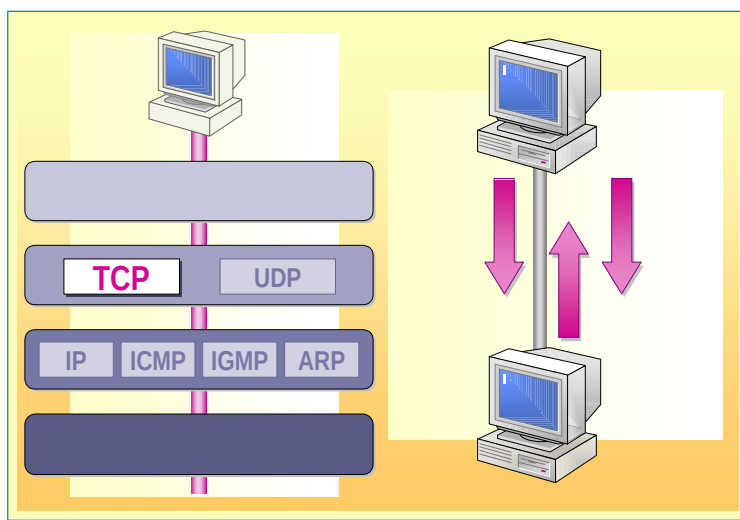
TCP (Transmission Control Protocol)

Cel slajdu

Opis właściwości protokołu TCP.

Wprowadzenie

Protokół TCP jest jednym z dwóch kluczowych protokołów działających na warstwie transportowej.

**Wskazówka**

Użyj slajdu do pokazania procesu potrójnego „podania ręki” inicjującego sesję TCP. Również podkreśl unicastową naturę protokołu TCP. Możesz wspomnieć, że przykładem użycia TCP jest transakcja za pomocą karty kredytowej.

Protokół TCP (Transmission Control Protocol) jest protokołem transportowym wchodzącym w skład stosu TCP/IP oferującym niezawodną, zorientowaną na połączenie usługę transportową między dwoma komputerami. Taka komunikacja nazywana jest emisją pojedynczą (unicast). W komunikacji zorientowanej na połączenie, zanim komputery rozpoczną wymianę danych, musi być nawiązana sesja.

Po nawiązaniu sesji, dane są przesyłane jedynie przez takie pojedyncze połączenie. Komunikacja zorientowana na połączenie oznacza również niezawodną komunikację, ponieważ gwarantuje dostarczenie danych do miejsca przeznaczenia.

Na komputerze źródłowym, TCP dzieli dane na wysyłane pakiety. Na komputerze docelowym, TCP składa pakiety, w celu odtworzenia danych.

Wymiana danych za pomocą protokołu TCP

Protokół TCP, w celu zwiększenia wydajności wysyła pakiety w grupach. Przypisuje numer do każdego pakietu i dzięki potwierdzeniu odbioru, sprawdza, czy komputer docelowy odebrał grupę pakietów. Jeśli komputer docelowy, w określonym przedziale czasu nie potwierdził odebrania każdej wysłanej grupy pakietów, komputer źródłowy ponownie wysyła dane.

Oprócz dodania numeru i żądania potwierdzenia odbioru pakietu, TCP dołącza do pakietu również numery portów aplikacji źródłowej i aplikacji przeznaczenia. Komputer źródłowy używa portu docelowego, w celu wysłania pakietu bezpośrednio do właściwej aplikacji na komputerze docelowym, a komputer docelowy używa portu źródłowego, w celu odpowiedzi do właściwej aplikacji źródłowej.

Potrójne „podanie ręki”

Ponieważ TCP jest niezawodnym protokołem, zanim dwa komputery rozpoczną wymianę danych za pomocą protokołu TCP, muszą nawiązać połączenie. Takie połączenie jest połączeniem *wirtualnym*, zwanym *sesją*. Dwa komputery używające TCP nawiązują połączenie lub sesję TCP w procesie zwanym potrójnym „podaniem ręki”. Proces ten synchronizuje numery kolejnych pakietów oraz dostarcza inne informacje niezbędne do nawiązania sesji.

Potrójne „podanie ręki” jest procesem trzyetapowym:

1. Komputer źródłowy inicjuje połączenie przez wysłanie informacji sesyjnej, zawierającej numer oraz rozmiar pakietu.
2. Komputer docelowy odpowiada, wysyłając swoją informację sesyjną.
3. Komputer źródłowy zgadza się i wysyła potwierdzenie odebranych informacji.

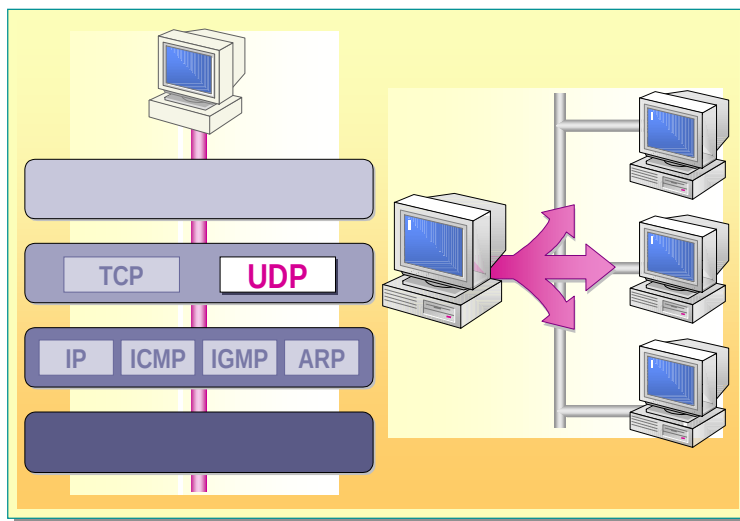
UDP (User Datagram Protocol)

Cel slajdu

Opis właściwości protokołu UDP.

Wprowadzenie

Razem z TCP, UDP jest następnym kluczowym protokołem działającym na warstwie transportowej.

**Wskazówka**

Chociaż protokół UDP ma możliwość obsługi transmisji unicastowej, użyj slajdu, aby podkreślić jego rozgłoszeniowy i multemisijny charakter. Zwróć uwagę na różnice z protokołem TCP. Dodatkowe przykłady mogą zawierać informacje na temat komunikacji większej liczby komputerów na raz lub na temat mniejszych porcji danych, których przesyłanie w protokole TCP byłoby nieefektywne.

Protokół UDP (User Datagram Protocol) jest protokołem warstwy transportowej identyfikującym aplikację docelową w komunikacji sieciowej. Protokół UDP oferuje bezpołączeniową usługę transportową umożliwiającą szybkość, lecz zawodną metodę dostarczania danych. UDP nie wymaga potwierdzenia odebrania danych i nie ponawia wysłania danych, w przypadku ich utraty lub uszkodzenia. Oznacza to, że mniej danych jest przesyłanych, lecz ani odebranie pakietów, ani prawidłowy porządek odebranych pakietów nie jest potwierdzany lub gwarantowany.

Protokół UDP jest używany przez aplikacje wysyłające dane do wielu komputerów przez rozgłaszanie lub multemisję (multicast). Jest on również używany do przesyłania małych ilości danych lub danych, które nie są bardzo ważne. Multemisijny strumień medialny, jak podczas wideo konferencji na żywo, rozgłaszanie listy nazw komputerów w lokalnej komunikacji, to przykładowe usługi używające protokołu UDP.

Aby używać protokołu UDP, aplikacja źródłowa musi dołączyć swój numer portu UDP, jak również port aplikacji docelowej. Warto zauważyć, że porty UDP są odrębne od portów TCP, nawet jeśli używają takich samych numerów.

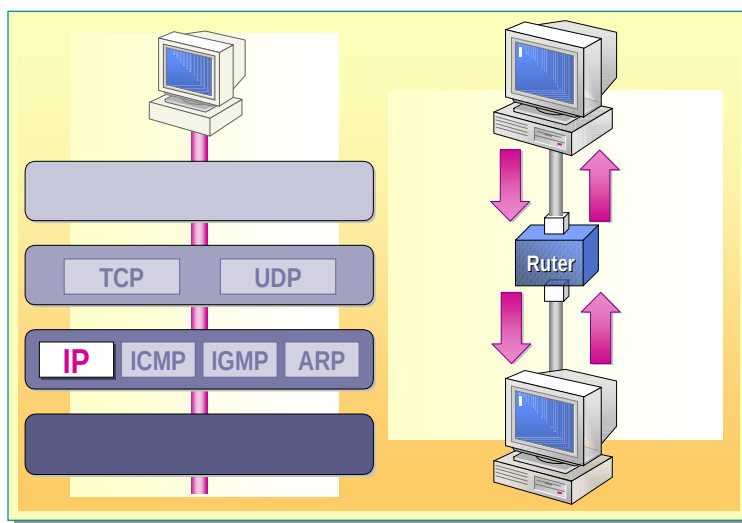
IP (Internet Protocol)

Cel slajdu

Przedstawienie właściwości protokołu IP.

Wprowadzenie

Protokół IP jest jednym z czterech kluczowych protokołów działających na warstwie internetowej.

**Wskazówka**

Użyj slajdu do przedstawienia znaczenia protokołu IP w przesyłaniu danych przez routery. Przypomnij słuchaczom, że chociaż karty sieciowe używają adresu MAC do identyfikacji komputera w lokalnym segmencie, to protokół IP przesyła dane do lokalnego segmentu.

Protokół IP (Internet Protocol) służy do określania lokalizacji komputera docelowego w komunikacji sieciowej. Protokół IP jest bezpołączeniowym, zawodnym protokołem odpowiedzialnym głównie za adresowanie pakietów oraz wybór trasy pakietów między komputerami w sieci. Chociaż protokół IP zawsze próbuje dostarczyć pakiet, pakiet może zostać utracony, uszkodzony, dostarczony w niewłaściwej kolejności, powielony lub opóźniony.

W przypadku wystąpienia tego typu błędów protokół IP nie próbuje odzyskać danych, przez żądanie ponownego ich wysłania. Za żądanie potwierdzenia odbioru pakietów oraz odzyskiwanie utraconych danych jest odpowiedzialny protokół wyższej warstwy, na przykład protokół TCP lub sama warstwa aplikacji.

Działanie protokołu IP

Protokół IP można sobie wyobrazić jako urząd pocztowy w stosie TCP/IP, gdzie ma miejsce sortowanie i dostarczanie pakietów. Pakiety są przekazywane w dół do protokołu IP, przez protokół UDP lub TCP z warstwy transportowej lub do góry z warstwy interfejsu sieciowego. Głównym zadaniem protokołu IP jest wybór trasy pakietów, aż do osiągnięcia ich celu.

Każdy pakiet zawiera adres IP hosta wysyłającego oraz adres IP hosta docelowego. Te adresy IP w pakiecie pozostają niezmienione przez całą drogę pakietu przez sieć.

Jeśli protokół IP rozpozna adres docelowy, jako adres w tym samym segmencie, przesyła pakiet bezpośrednio do komputera. Jeśli docelowy adres IP nie jest w tym samym segmencie, protokół IP musi wysłać informację za pośrednictwem routera.

Protokół IP jest również odpowiedzialny za to, że pakiet nie pozostanie w sieci na zawsze, dzięki określeniu ograniczonej liczby sieci przez które pakiet może przejść. Jest to zrealizowane przez przypisanie do każdego pakietu parametru TTL (Time to Live). Parametr TTL określa maksymalny przedział czasu, przez jaki pakiet może podróżować w sieci, zanim zostanie zniszczony.

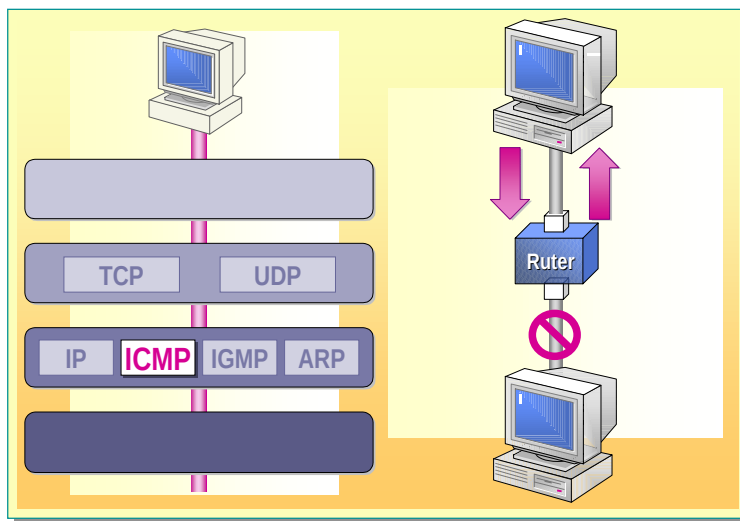
ICMP (Internet Control Message Protocol)

Cel slajdu

Opis właściwości protokołu ICMP.

Wprowadzenie

Protokół ICMP jest następnym kluczowym protokołem działającym na warstwie internetowej.



Zagadnienie kluczowe

Wspomnij słuchaczom, że zawodny (nie gwarantowany) sposób dostarczania pakietów, nie jest zły; niezawodna metoda jest w wielu przypadkach niepotrzebna. Także wysyłanie przez sieć prostych komunikatów o błędach nie zawsze jest konieczne. Jednakże, kiedy pakiet musi osiągnąć określony cel, używany jest protokół TCP. Na powyższym rysunku znajduje się przykład użycia komunikatu ICMP.

Protokół ICMP (Internet Control Message Protocol) oferuje możliwość rozwiązywania problemów oraz wysyłania komunikatów o błędach, w przypadku niedostarczenia pakietów. Dzięki protokołowi ICMP, komputery i routery mogą informować o błędach oraz wymieniać ograniczone informacje kontrolne i statusowe. Na przykład, jeśli protokół IP nie może dostarczyć pakietu do komputera docelowego, protokół ICMP wysyła komunikat Destination Unreachable (cel nieosiągalny) do komputera źródłowego.

Mimo, że do przesyłania danych między routerami jest używany protokół IP, protokół ICMP zwraca komunikaty o błędach oraz komunikaty kontrolne w imieniu IP. Protokół ICMP nie czyni protokołu IP niezawodnym, ponieważ same komunikaty ICMP nie wymagają potwierdzenia i dlatego są zawodne. Protokół ten tylko informuje o błędach oraz reaguje na określone warunki. Chociaż metoda ta może wydawać się mało wydajna, jest ona bardziej efektywna, niż zajmowanie łączy w celu potwierdzania każdego komunikatu ICMP.

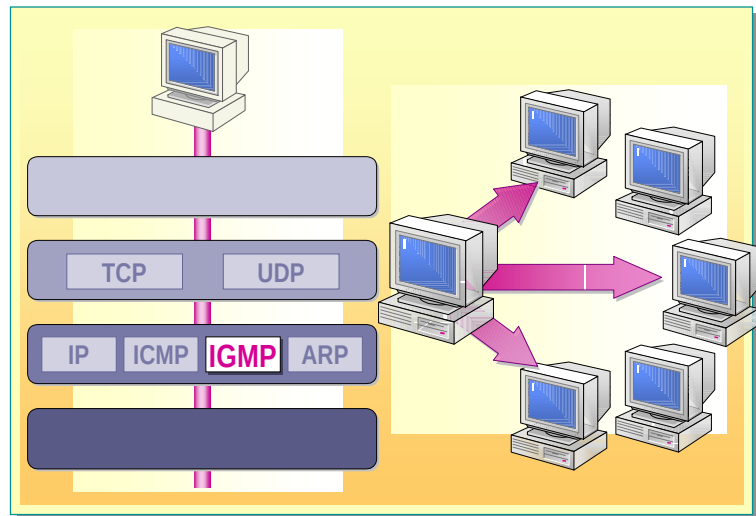
IGMP (Internet Group Management Protocol)

Cel slajdu

Opis właściwości protokołu IGMP.

Wprowadzenie

Protokół IGMP jest również jednym z kluczowych protokołów działających na warstwie internetowej.



Wskazówka

Upewnij się, że słuchacze będą rozróżniali protokoły IGMP oraz ICMP. Dobrą metodą jest zwrócenie uwagi, że G=grupa w protokole IGMP.

Protokół IGMP (Internet Group Management Protocol) jest protokołem zarządzającym członkostwem na listach multiemisji IP w sieci TCP/IP. Multiemisja IP jest procesem, w którym informacje są przesyłane do określonej grupy odbiorców, zwanej grupą multiemisji. Protokół IGMP zarządza listą komputerów należących do każdej grupy multiemisji.

Zarządzanie multiemisją IP

Wszyscy członkowie grupy multiemisji nasłuchują ruchu IP skierowanego do określonego adresu multiemisji IP i odbierają pakiety wysłane na ten adres IP. Jednakże, ponieważ multiemisja odnosi się do wielu komputerów, pakiety są wysyłane za pomocą zawodnego protokołu UDP, nie gwarantującego dostarczenia pakietów do grupy multiemisji.

Kiedy wiele komputerów potrzebuje dostępu do informacji, takich jak strumień mediów, używany jest adres IP zarezerwowany dla multiemisji. Rutery skonfigurowane do obsługi adresów multiemisji IP, odbierają takie informacje i przesyłają je do wszystkich członków grupy multiemisji, do których został przypisany adres multiemisji IP.

Aby informacja multiemisji dotarła do odbiorców, ważne jest, aby każdy ruter na trasie komunikacji obsługiwał multiemisję. Komputery działające pod kontrolą systemu Windows 2000 mogą zarówno wysyłać, jak i odbierać dane w komunikacji multiemisji IP.

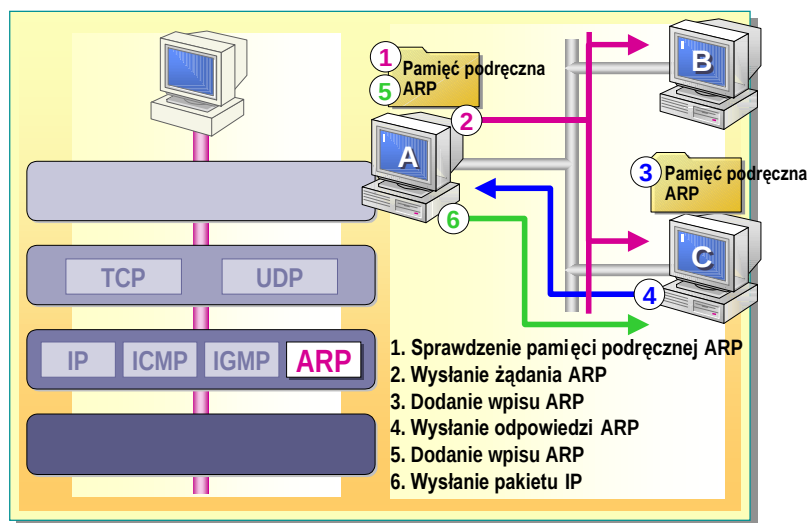
ARP (Address Resolution Protocol)

Cel slajdu

Opis właściwości protokołu ARP.

Wprowadzenie

Protokół ARP jest następnym z czterech kluczowych protokołów działających na warstwie internetowej.



Zagadnienie kluczowe

Zwróć uwagę, że protokół ARP jest używany tylko między komputerami w tym samym segmencie sieci, a do komunikacji między komputerami w różnych sieciach wymagany jest ruter.

Wskazówka

Sprawdź wiedzę słuchaczy, zadając pytania na temat komunikacji rozgłoszeniowej oraz rutowania pakietów.

Protokół ARP (Address Resolution Protocol) działający na warstwie internetowej stosu TCP/IP, jest odpowiedzialny za rozwiązanie adresów dla wychodzących pakietów. Rozwiązywanie adresu jest procesem, w którym adresy IP są mapowane do adresów MAC. Karta sieciowa używa adresu MAC do sprawdzenia, czy pakiet jest adresowany do tego komputera.

Bez adresu MAC, karta sieciowa nie jest w stanie określić, czy przekazać dane do wyższej warstwy, w celu dalszego przetworzenia. Kiedy wychodzący pakiet zostanie przygotowany do wysłania przez warstwę IP, musi zostać dodany źródłowy i docelowy adres MAC.

Pamięć podręczna ARP

Protokół ARP przechowuje tabelę zawierającą adresy IP i odpowiadające im adresy MAC. Obszar pamięci, w którym tabela jest przechowywana, nazywany jest pamięcią podręczną ARP. Pamięć podręczna ARP każdego komputera zawiera mapowania jedynie tych komputerów i ruterów, które są w tym samym segmencie.

Rozwiązywanie fizycznego adresu

Protokół ARP porównuje adres IP każdego wychodzącego pakietu, z pamięcią podręczną ARP, w celu określenia adresu MAC, do którego pakiet ma zostać wysłany. Jeśli odpowiedni wpis istnieje, adres MAC jest odczytywany z pamięci podręcznej. Jeśli nie, protokół ARP wysyła rozgłoszenie z żądaniem uzyskania adresu MAC od komputera z określonym adresem IP. Następnie, komputer z tym adresem IP dodaje do własnej pamięci podręcznej adres MAC komputera inicjującego żądanie i odpowiada, wysyłając swój adres MAC. Kiedy odpowiedź ARP zostanie odebrana, pamięć podręczna ARP jest aktualizowana nowymi informacjami, a pakiet zostaje wysłany.

Jeśli pakiet jest adresowany do innego segmentu, zamiast rozwiązywać adres komputera docelowego, protokół ARP określa adres MAC rutera dla swojego segmentu. Dalej ruter jest odpowiedzialny za znalezienie adresu MAC komputera docelowego lub za przekazanie pakietu do następnego rutera.

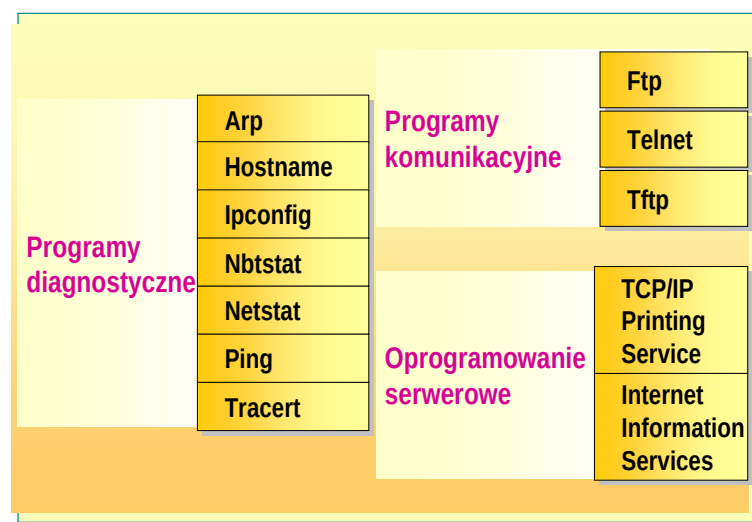
Programy narzędziowe TCP/IP

Cel slajdu

Wprowadzenie do programów narzędziowych TCP/IP.

Wprowadzenie

Stos protokołów TCP/IP zawiera kilka programów narzędziowych, za pomocą których użytkownik może uzyskać dostęp do informacji w sieci.



Wskazówka

Nie jest to pełna lista programów narzędziowych. Jest to tylko przedstawienie kilku rodzajów programów, dołączonych wraz ze stosem protokołów TCP/IP. Wspomnij słuchaczom, że wszystkie te programy pracują na warstwie aplikacji. Zademonstruj działanie poleceń Hostname, Arp oraz Ping. Zwróć uwagę, że Arp jest zarówno programem narzędziowym jak i protokołem (ARP). Również zwróć uwagę, że polecenie Ping używa innego protokołu, a mianowicie ICMP, do realizacji swoich zadań. Zauważ, że program Ipconfig jest omawiany w rozdziale 7, „Adresowanie IP,” w podręczniku do kursu 2243A, „Podstawy sieci i systemu operacyjnego Windows 2000” oraz, że korzystanie z powyższych poleceń jest przedmiotem następnego laboratorium.

Do stosu protokołów TCP/IP firmy Microsoft dołączone zostały podstawowe programy narzędziowe TCP/IP umożliwiające komputerowi z systemem Windows 2000 na dostęp do szerokiej gamy informacji w sieci. Za pomocą tych narzędzi można między innymi sprawdzić, czy dany komputer jest dostępny w sieci, jak również ściągać multimedialne dokumenty z sieci Internet.

W systemie Windows 2000 zawarte są trzy rodzaje programów narzędziowych TCP/IP: programy diagnostyczne, programy komunikacyjne oraz oprogramowanie serwerowe.

Programy diagnostyczne

Programy diagnostyczne umożliwiają użytkownikom wykrycie i rozwiązanie problemów z siecią. Do programów tych można zaliczyć:

- Arp: Wyświetla i modyfikuje pamięć podręczną protokołu ARP (Address Resolution Protocol).
- Hostname: Wyświetla nazwę hosta lokalnego komputera.
- Ipconfig: Wyświetla i aktualizuje bieżącą konfigurację TCP/IP, włącznie z adresem IP.
- Nbtstat: Wyświetla lokalną tablicę nazw NetBIOS, zawierającą mapowanie przyjaznych dla użytkownika nazw komputerów do ich adresów IP.
- Netstat: Wyświetla stan sesji TCP/IP.
- Ping: Sprawdza konfigurację IP oraz czy jest połączenie między dwoma komputerami. Polecenie Ping wysyła żądanie ICMP z komputera źródłowego, a komputer docelowy odpowiada komunikatem ICMP.
- Tracert: Sprawdza trasę przebytą przez pakiet do miejsca przeznaczenia.

Programy komunikacyjne

Programy komunikacyjne umożliwiają użytkownikowi połączenie oraz korzystanie z zasobów znajdujących się na różnych hostach, zarówno firmy Microsoft, jak i innych, np. w systemach UNIX. Najbardziej powszechne z nich, to:

- **Ftp:** Umożliwia transfer plików za pomocą protokołu TCP między komputerami z systemem Windows 2000 oraz komputerami z oprogramowaniem serwera plików FTP (File Transfer Protocol).
- **Telnet:** Umożliwia zdalny dostęp do zasobów sieciowych na komputerach z oprogramowaniem serwera Telnet.
- **Tftp:** Umożliwia transfer małych plików za pomocą protokołu UDP między komputerami z systemem Windows 2000 oraz komputerami z oprogramowaniem serwera plików TFTP (Trivial File Transfer Protocol).

Oprogramowanie serwerowe

Oprogramowanie to świadczy usługi drukowania i publikowania w systemie Windows 2000 dla klientów używających protokołu TCP/IP.

- **Usługa TCP/IP Printing:** Udostępnia standardowe usługi drukowania przez protokół TCP/IP. Umożliwiają one komputerom działającym pod kontrolą innych systemów operacyjnych, niż system Windows 2000 drukować na drukarce podłączonej do komputera z systemem Windows 2000.
- **IIS (Internet Information Services):** IIS udostępnia oprogramowanie serwera sieci Web, grup dyskusyjnych, poczty elektronicznej oraz serwera plików dla usług publikowania opartych na protokole TCP/IP.

Przykłady powszechnie używanych programów narzędziowych

Programy Hostname, Arp oraz Ping są trzema powszechnie używanymi programami narzędziowymi TCP/IP. Ponieważ są one często używane, warto nauczyć się z nich korzystać.

Hostname

Składnia tego polecenia wygląda następująco: *hostname*. Aby uruchomić ten program, w wierszu poleceń należy wpisać: **hostname**. System wyświetli nazwę hosta komputera.

Arp

Składnia polecenia umożliwiającego wyświetlenie zawartości pamięci podręcznej ARP wygląda następująco: *arp -a*. W wierszu poleceń należy wpisać: **arp -a**, aby wyświetlić informacje zawarte w pamięci podręcznej ARP.

Ping

Składnia polecenia umożliwiającego sprawdzenie połączenia wygląda następująco: *ping*. Aby sprawdzić połączenie używając adresu IP lub nazwy komputera, należy wpisać: **ping** [*adres_IP* lub *nazwa_komputera*].

Aby sprawdzić konfigurację TCP/IP własnego komputera, należy użyć *pętli zwrotnej* (loopback). Pętla zwrotna ma adres IP 127.0.0.1. Aby sprawdzić konfigurację systemu za pomocą pętli zwrotnej, należy wpisać **ping 127.0.0.1**

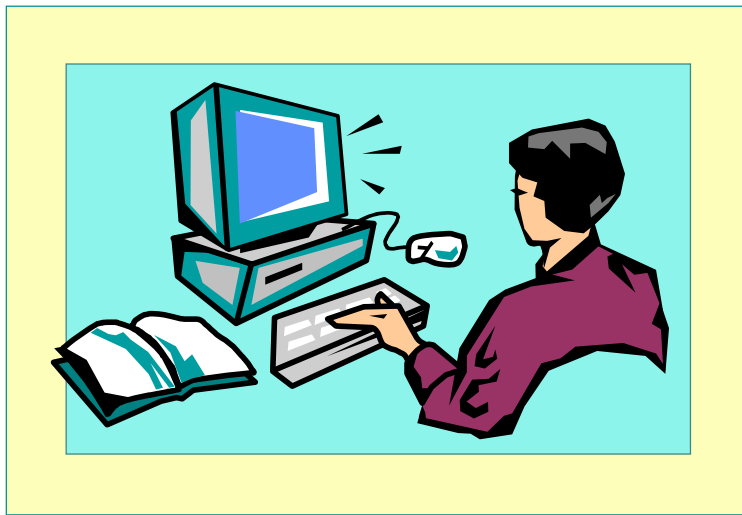
Laboratorium A: Badanie programów narzędziowych TCP/IP

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W laboratorium tym, za pomocą polecenia Ping zostanie sprawdzona poprawność konfiguracji TCP/IP. Za pomocą tego polecenia zostanie również sprawdzona łączność z innymi komputerami, za pomocą polecenia Hostname zostanie sprawdzona nazwa komputera, a za pomocą polecenia Arp adres MAC komputera.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Korzystać z polecenia Ping do testowania konfiguracji oraz możliwości połączenia.
- Korzystać z polecenia Hostname, w celu uzyskania nazwy swojego komputera.

Wymagania wstępne

Przed rozpoczęciem tego laboratorium należy:

- Nauczyć się logować do systemu Windows 2000.

Przewidywany czas ukończenia laboratorium: 15 minut

Ćwiczenie 1

Użycie programów narzędziowych TCP/IP

Scenariusz

Jesteś administratorem w małym przedsiębiorstwie i chcesz upewnić się, że serwer ma właściwą konfigurację TCP/IP oraz sprawdzić, czy może komunikować się z innymi komputerami w sieci.

Cel

W ćwiczeniu tym, za pomocą polecenia Ping, sprawdzisz, czy konfiguracja TCP/IP jest prawidłowa, a następnie za pomocą polecenia Hostname sprawdzisz nazwę swojego komputera. Następnie za pomocą polecenia Ping sprawdzisz połączenie z komputerem partnera, aby upewnić się, czy możesz komunikować się w sieci.

Zadania	Szczegółowe kroki
1. Zaloguj się na konto Administrator z hasłem password . Użyj polecenia Hostname do sprawdzenia nazwy hosta swojego komputera oraz polecenia Ping do sprawdzenia konfiguracji TCP/IP.	a. Zaloguj się w systemie Windows 2000 na konto Administrator z hasłem password . b. Wybierz menu Start, Programs, Accessories , a następnie kliknij polecenie Command Prompt . c. W oknie wiersza poleceń, wpisz PING 127.0.0.1
? Ile pakietów zostało wysłanych, odebranych oraz utraconych? Cztery pakiety zostały wysłane, cztery pakiety zostały odebrane i żaden pakiet nie został utracony, w przeciwnym razie jest problem z protokołem TCP/IP.	
? Czy protokół TCP/IP działa prawidłowo? Tak, jeśli wszystkie cztery pakiety zostały odebrane.	
2. Za pomocą polecenia Hostname sprawdź swoją nazwę hosta, a następnie użyj polecenie Ping ze swoją nazwą hosta, aby sprawdzić jaki masz adres IP.	a. W oknie wiersza poleceń, wpisz hostname b. W oknie wiersza poleceń, wpisz ping komputer (gdzie <i>komputer</i> jest nazwą hosta otrzymaną w punkcie a).

(cd)

Zadania	Szczegółowe kroki
? Jaka jest nazwa hosta Twojego komputera? Odpowiedzi będą różne; dla wykładowcy będzie to nazwa London.	
? Jaki jest adres IP Twojego komputera? 192.168.x.y (gdzie x jest numerem klasy, a y jest liczbą w zakresie od 1 do 199).	
3. Użyj polecenia Ping z nazwą komputera wykładowcy, aby sprawdzić, czy Twój komputer może komunikować się w sieci.	a. W oknie wiersza poleceń, wpisz ping London
? Jaki jest adres IP komputera London? 192.168.1.200.	
? Skąd wiesz, że możesz połączyć się z komputerem London? Ponieważ żaden pakiet nie został utracony.	
4. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000.	a. Zamknij wszystkie okna i wyloguj się z systemu Windows 2000.

◆ Rozwiązywanie nazw

Cel slajdu

Wprowadzenie do zagadnień związanych z rozwiązywaniem nazw.

Wprowadzenie

Wszystkie przyjazne dla użytkownika nazwy muszą być mapowane do ich adresów IP, w celu umożliwienia komunikacji.

- Rodzaje nazw
- Statyczne mapowanie IP
- Dynamiczne mapowanie IP
- Rozwiązywanie nazw w systemie Windows 2000

Protokół TCP/IP identyfikuje komputery źródłowe i docelowe poprzez ich adresy IP. Jednakże, użytkownicy znacznie łatwiej zapamiętują słowa (przyjazne dla użytkownika nazwy) niż numery (adresy IP). Istnieją różne rodzaje przyjaznych dla użytkownika nazw, za pomocą których komputer może być adresowany.

System operacyjny Windows 2000 posiada kilka różnych lokalizacji, w których przechowuje rekordy przyjaznych dla użytkownika nazw mapowanych do odpowiadających im adresów IP. Mapowanie adresu IP komputera może być przechowywane w statycznym lub dynamicznym pliku, w zależności od rodzaju używanej nazwy.

Niektóre aplikacje, jak program Microsoft Internet Explorer oraz program Ftp, do nawiązania komunikacji mogą używać adresu IP lub przyjaznej dla użytkownika nazwy. Kiedy jest używana przyjazna nazwa, komputery działające pod kontrolą systemu Windows 2000 używają procedury, zwanej rozwiązywaniem nazwy, w celu znalezienia odpowiedniego adresu IP, zanim komunikacja za pomocą protokołu TCP/IP będzie mogła się rozpocząć. Jednakże, jeśli użyty zostanie adres IP, komunikacja będzie mogła się rozpocząć od razu.

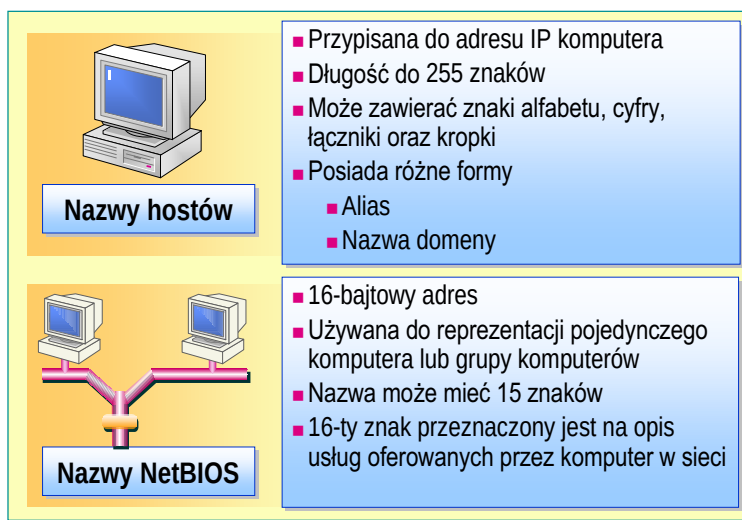
Rodzaje nazw

Cel slajdu

Charakterystyka dwóch rodzajów przyjaznych dla użytkownika nazw.

Wprowadzenie

Istnieją dwa popularne rodzaje przyjaznych dla użytkownika nazw.



Wskazówka

Zapytaj słuchaczy, co oznacza słowo NetBIOS. Do wyjaśnienia znaczenia NetBIOS użyj definicji. Powiedz słuchaczom, że niektóre aplikacje, wliczając w to zasoby NetBIOS, identyfikuje się wzajemnie za pomocą nazw NetBIOS, zamiast bardziej powszechnych nazw hostów. Nazwy hostów są używane przez takie produkty, jak przeglądarki internetowe i standardowo w systemie Windows 2000.

Istnieją dwa rodzaje przyjaznych dla użytkownika nazw: nazwy hostów oraz nazwy NetBIOS.

Nazwy hostów

Nazwa hosta jest to przyjazna dla użytkownika nazwa, przypisana do adresu IP komputera, w celu identyfikacji go jako hosta TCP/IP. Nazwa hosta może mieć do 255 znaków i może zawierać znaki alfabetu oraz cyfry, łączniki i kropki.

Nazwy hostów mogą mieć różną postać. Dwie najbardziej powszechne postaci to alias oraz nazwa domenowa. Alias jest to pojedyncza nazwa przypisana do adresu IP, jak np. London. Nazwa domenowa jest strukturą używaną w sieci Internet i zawiera kropki jako separatory. Przykładem nazwy domenowej jest nazwa london.nwtraders.msft.

Nazwy NetBIOS

Nazwa NetBIOS jest 16-to znakową nazwą używaną do identyfikacji zasobów NetBIOS w sieci. Nazwa NetBIOS może reprezentować pojedynczy komputer lub grupę komputerów, lecz jedynie pierwszych 15 znaków może być wykorzystanych na nazwę. Ostatni znak jest używany do identyfikacji zasobu lub usługi oferowanej przez komputer w sieci.

Przykładem usługi NetBIOS jest usługa File and Printer Sharing for Microsoft Networks na komputerze działającym pod kontrolą systemu Windows 2000. Kiedy komputer zostanie uruchomiony, ten składnik rejestruje unikalną nazwę NetBIOS, opartą na nazwie komputera, a jeden znak opisuje ten składnik.

Ważne W systemie Windows 2000, nazwa NetBIOS używa pierwszych 15 znaków nazwy hosta i nie może być konfigurowana oddzielnie. Chociaż system Windows 2000 nie wymaga nazw NetBIOS, wcześniejsze wersje systemu Windows wymagają nazw NetBIOS do obsługi sieci.

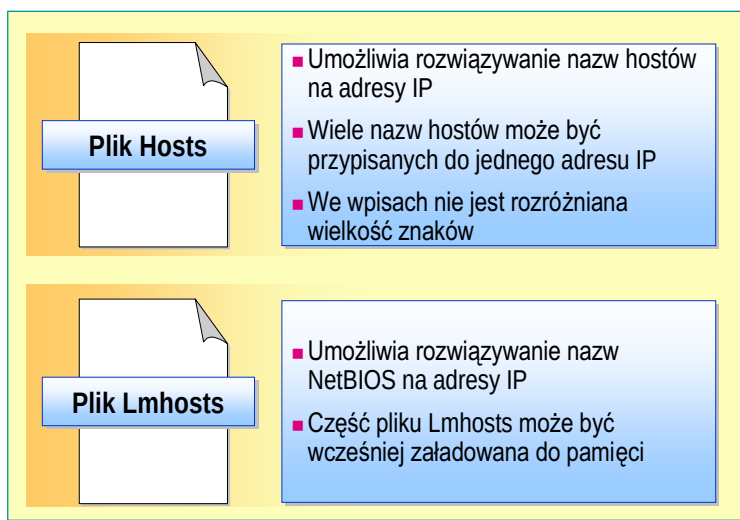
Statyczne mapowanie IP

Cel slajdu

Opis metody statycznego mapowania IP.

Wprowadzenie

Statyczne mapowanie IP jest metodą przechowywania informacji na temat przyjaznych dla użytkownika nazw i odpowiadających im adresów IP.



Kiedy do komunikacji z docelowym komputerem, użytkownicy używają przyjaznych nazw, aby transmisja mogła się rozpocząć, protokół TCP/IP nadal wymaga adresu IP. Nazwa komputera jest więc mapowana do adresu IP. Mapowanie jest przechowywane w statycznej lub dynamicznej tablicy. W przypadku statycznej tablicy, mapowanie jest przechowywane w dwóch plikach tekstowych: w pliku Hosts lub w pliku Lmhosts.

Zaletą używania statycznej tabeli jest to, że plik tekstowy jest umieszczany na każdym komputerze i może być odpowiednio dostosowany. Każdy użytkownik może utworzyć dowolną liczbę potrzebnych wpisów, wliczając w to łatwe do zapamiętania aliasy dla często używanych zasobów. Jednakże, trudno jest zarządzać i aktualizować statyczne tablice, jeśli zawierają dużą liczbę mapowanych adresów IP lub kiedy adresy IP często się zmieniają.

Plik Hosts

Plik Hosts jest plikiem tekstowym zawierającym mapowania adresów IP do nazw hostów. W pliku Hosts:

- Wiele nazw hostów może być przypisanych do tego samego adresu IP. Serwer o adresie 167.91.45.121 może być dostępny przez nazwę domenową (london.nwtraders.msft) lub przez alias (London). Pozwoli to użytkownikowi tego komputera na dostęp do serwera przez alias London, zamiast przez wpisywanie całej nazwy domenowej.
- Wielkość znaków we wpisach jest rozróżnialna, w zależności od platformy systemowej. Wielkość znaków we wpisach w pliku Hosts dla komputerów działających pod kontrolą systemów Windows 2000 oraz Microsoft Windows NT® 4.0 nie jest rozróżniana.

Plik Lmhosts

Plik Lmhosts jest plikiem tekstowym zawierającym mapowania adresów IP do nazw NetBIOS. Część pliku Lmhosts może zostać wcześniej załadowana do pamięci do obszaru zwanego pamięcią podręczną NetBIOS.

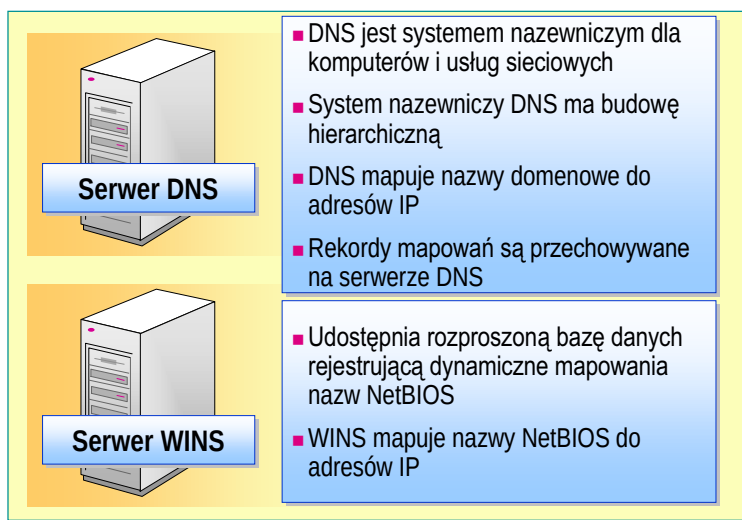
Dynamiczne mapowanie IP

Cel slajdu

Opis właściwości dynamicznego mapowania nazw do adresów IP.

Wprowadzenie

Ręczna aktualizacja mapowanych adresów jest nieefektywna.



Zaletą dynamicznych tablic, przechowujących mapowane adresy IP, jest ich automatyczna aktualizacja. Aby to osiągnąć, dynamiczne tablice używają dwóch usług: DNS (Domain Name System) oraz WINS (Windows Internet Name Service). DNS oraz WINS pełnią podobne funkcje jak pliki Hosts oraz Lmhosts, lecz nie wymagają ręcznej konfiguracji.

DNS (Domain Name System)

DNS jest metodą nazewniczą dla komputerów i usług sieciowych. Sieci TCP/IP używają konwencji nazewniczej DNS do znajdowania komputerów i usług, za pomocą przyjaznych dla użytkownika nazw domenowych. Kiedy użytkownik użyje nazwy domenowej w aplikacji, usługa DNS mapuje nazwę do adresu IP.

System nazewniczy DNS jest zorganizowany w hierarchiczny sposób, aby umożliwić skalowalność dużych systemów, jak sieć Internet. Dzięki użyciu hierarchicznego systemu do tworzenia nazw domenowych, komputery przechowujące mapowania adresów IP do nazw domenowych posiadają mapowania jedynie dla swojego obszaru. Komputery te, zwane serwerami DNS przetwarzają zapytania jedynie komputerów zlokalizowanych w ich obszarze. Jeśli mapowania w obszarze się zmieniają, serwery DNS działające pod kontrolą systemu Windows 2000 automatycznie zaktualizują informacje w swojej bazie.

WINS (Windows Internet Name Service)

WINS udostępnia rozproszoną bazę danych, w celu rejestracji dynamicznych mapowań nazw NetBIOS używanych w sieci. WINS mapuje nazwy NetBIOS do adresów IP i umożliwia używanie nazw NetBIOS w komunikacji przez rutery.

Uwaga Serwer WINS nie jest wymagany w sieci opartej wyłącznie na systemie Windows 2000, lecz jest zalecany, gdy środowisko sieciowe jest mieszane.

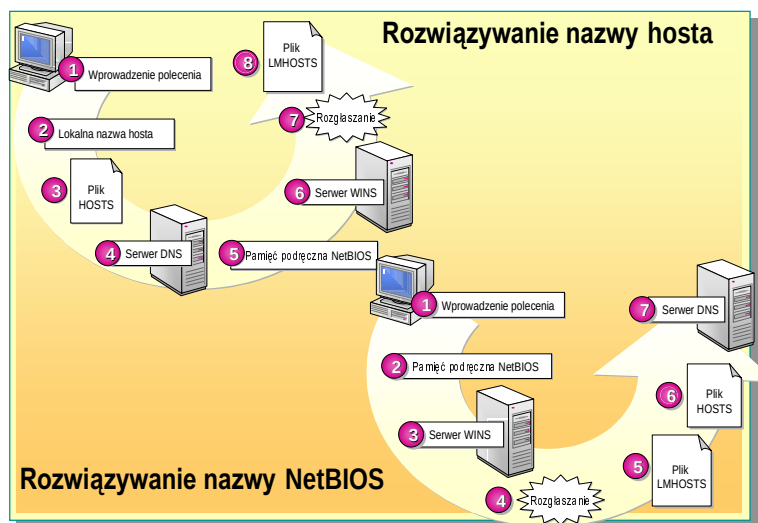
Rozwiązywanie nazw w systemie Windows 2000

Cel slajdu

Przedstawienie procesu rozwiązywania nazwy.

Wprowadzenie

System Windows 2000 rozwiązuje nazwy hostów oraz nazwy NetBIOS.



Zagadnienie kluczowe

Aplikacje systemu Windows 2000 są zaprojektowane do używania nazw hostów, lecz zarówno nazwy NetBIOS, jak i nazwy hostów mogą być rozwiązane w procesie rozwiązywania nazwy, jeśli komputer jest poprawnie skonfigurowany. Porządek rozwiązywania nazwy i czas mogą się różnić.

Rozwiązywanie nazwy jest procedurą rozwiązania lub mapowania nazwy do adresu IP. Kiedy w aplikacji zostanie wpisana nazwa przyjazna dla użytkownika, aplikacja określa czy jest to nazwa hosta, czy nazwa NetBIOS. Bieżące aplikacje systemu Windows 2000 używają procesu rozwiązywania nazwy hosta, lecz niektóre starsze aplikacje, jak te zaprojektowane dla systemów Microsoft Windows NT, Windows 95 oraz Windows 98 używają nazw NetBIOS. Jeśli proces rozwiązywania nazwy zawiedzie, aplikacja nie będzie mogła skomunikować się z miejscem przeznaczenia. Jeśli jest używany adres IP, rozwiązywanie nazwy nie jest potrzebna.

Proces rozwiązywania nazwy hosta

Nazwy hostów mogą zostać rozwiązane bezpośrednio przez plik Hosts lub przez serwer DNS. Domyślna procedura rozwiązywania nazwy jest następująca:

1. Na komputerze A wpisano polecenie, np. **FTP**, z nazwą hosta komputera B.
2. Komputer A, sprawdza, czy nie jest to własna lokalna nazwa hosta.
3. Jeśli nie, komputer A w pliku Hosts szuka nazwy hosta komputera B. Jeśli znajdzie nazwę hosta, rozwiązuje jej adres IP.
4. Jeśli komputer A nie znajdzie w pliku Hosts nazwy hosta komputera B, wysyła zapytanie do serwera DNS. Jeśli nazwa hosta zostanie znaleziona, jest rozwiązywany jej adres IP.

5. Jeśli serwer DNS nie znajdzie nazwy hosta, system Windows 2000 szuka nazwy w pamięci podręcznej NetBIOS. Dzieje się tak, ponieważ system Windows 2000 traktuje nazwę NetBIOS jak nazwę hosta.
6. Jeśli w pamięci podręcznej NetBIOS nie ma nazwy hosta (NetBIOS), zapytanie jest wysyłane do serwera WINS.
7. Jeżeli serwer WINS nie może rozwiązać nazwy, zostanie wysłany komunikat rozgłoszeniowy w sieci.
8. Jeśli żaden host nie odpowie na komunikat, nazwa hosta (NetBIOS) jest szukana w pliku Lmhosts.

Proces rozwiązywania nazwy NetBIOS

Domyślnie, nazwy NetBIOS nie działają w sieci TCP/IP. System Windows 2000 umożliwia klientom NetBIOS komunikować się za pomocą protokołu TCP/IP dzięki protokołowi NetBT. NetBT jest akronimem od NetBIOS over TCP/IP. Protokół ten umożliwia aplikacjom NetBIOS na komunikację za pomocą protokołu TCP/IP, dzięki translacji nazwy NetBIOS na adres IP. Jeśli skonfigurowano korzystanie z serwera WINS, wtedy procedura rozwiązywania nazwy NetBIOS jest następująca:

1. Na komputerze A wpisano polecenie, np. **net use**, z nazwą NetBIOS komputera B.
2. Komputer A szuka wpisanej nazwy w pamięci podręcznej NetBIOS.
3. Jeśli nie znajdzie, komputer A wysyła zapytanie do serwera WINS.
4. Jeśli serwer WINS nie może znaleźć nazwy, komputer A wysyła rozgłoszenie w sieci.
5. Jeśli rozgłoszenie nie rozwiąże nazwy, komputer A sprawdza plik Lmhosts.
6. Jeśli powyższe metody NetBIOS nie rozwiążą nazwy, komputer A sprawdza plik Hosts.
7. Ostatecznie, komputer A zapytuje serwer DNS.

Ważne Kolejność w jakiej system Windows 2000 używa tych metod, zależy od konfiguracji komputerów z systemem Windows 2000.

◆ Badanie procesu przesyłania danych

Cel slajdu

Wprowadzenie do znaczenia pakietów w przesyłaniu danych.

Wprowadzenie

Transfer danych jest złożonym procesem związanym z wieloma czynnikami.

- Terminologia pakietów
- Elementy ramki
- Przepływ danych

Protokół TCP/IP transmituje dane przez sieć, dzieląc je na mniejsze porcje, zwane pakietami. Pakiety są często określane różnymi terminami, w zależności od protokołu, z którym są powiązane. Podział danych na pakiety jest konieczny, ponieważ przesłanie dużej porcji danych przez sieć zajmuje dużo czasu i może zatkać sieć. Dopóki taka duża porcja danych jest przesyłana, żaden inny komputer nie może wysłać danych. Również, kiedy wystąpi błąd, cała porcja danych musi zostać ponownie wysłana.

Przeciwnie, jeśli małe pakiety są wysyłane przez sieć, są one szybciej przesyłane. Ponieważ małe pakiety nie zatykają sieci, inne komputery mogą również przysłać dane. Jeśli jakiś pakiet zostanie uszkodzony, tylko ten pakiet musi być ponownie wysłany, zamiast wszystkich danych.

Kiedy pakiet jest wysyłany przez warstwę interfejsu sieciowego, jest on nazywany ramką. Ramka składa się z różnych elementów, pełniących określone funkcje w przepływie danych na warstwie interfejsu sieciowego.

Proces przepływu danych składa się z kilku etapów, wliczając w to organizację danych w małe pakiety na komputerze źródłowym i ich odtworzenie w oryginalnej formie na komputerze docelowym. Każda warstwa stosu protokołów TCP/IP jest związana z podobnymi czynnościami na komputerze źródłowym i docelowym.

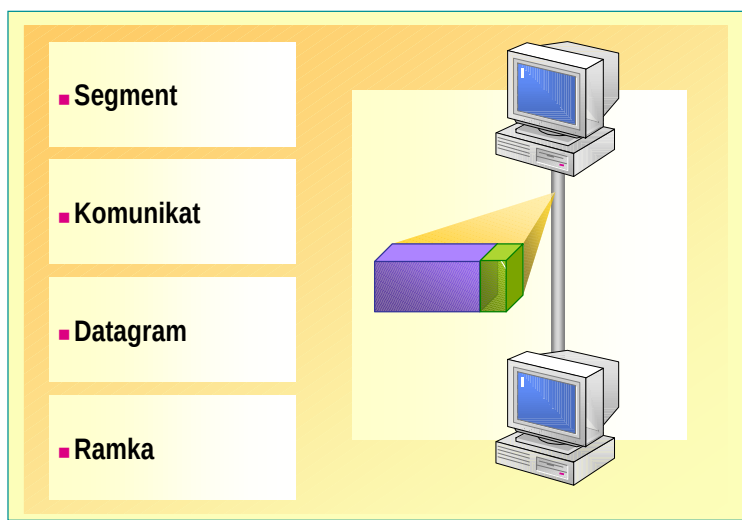
Terminologia pakietów

Cel slajdu

Wprowadzenie do terminologii związanej z pakietami.

Wprowadzenie

Na każdej warstwie stosu TCP/IP, pakiet jest określany inną nazwą.

**Wskazówka**

Informacje na tej stronie służą do wyjaśnienia faktu, że jest więcej niż jeden termin określający pakiet danych. Przypomnij słuchaczom znaczenie segmentu w sieci.

Kiedy pakiet danych jest przekazywany między warstwami w stosie TCP/IP, każdy protokół dodaje swój własny nagłówek. Pakiet, wraz z dodawanymi do niego informacjami, jest określany innymi technicznymi nazwami identyfikowanymi z różnymi protokołami. Te nazwy to segment, komunikat, datagram oraz ramka.

Segment

Segment jest związany z transmisją za pomocą protokołu TCP. Zawiera nagłówek TCP, dodany do danych aplikacji.

Komunikat

Komunikat jest związany z transmisją za pomocą zawodnych protokołów, jak ICMP, UDP, IGMP oraz ARP. Składa się z nagłówka protokołu, dodanego do danych aplikacji lub danych protokołu.

Datagram

Datagram jest związany z transmisją za pomocą protokołu IP. Składa się z nagłówka IP, dodanego do danych warstwy transportowej i jest również uważany za zawodny.

Ramka

Ramka jest związana z transmisją na warstwie interfejsu sieciowego i składa się z nagłówka dodanego na warstwie interfejsu sieciowego i danych z warstwy IP.

Uwaga Jak sugeruje nazwa UDP (User Datagram Protocol), pakiet taki też może być traktowany jako datagram. Jednakże, komunikat UDP jest ogólnie akceptowanym terminem. Termin segment jest również używany gdy sieć jest podzielona za pomocą fizycznego urządzenia. W znaczeniu pakietu, termin segment odnosi się do segmentu TCP.

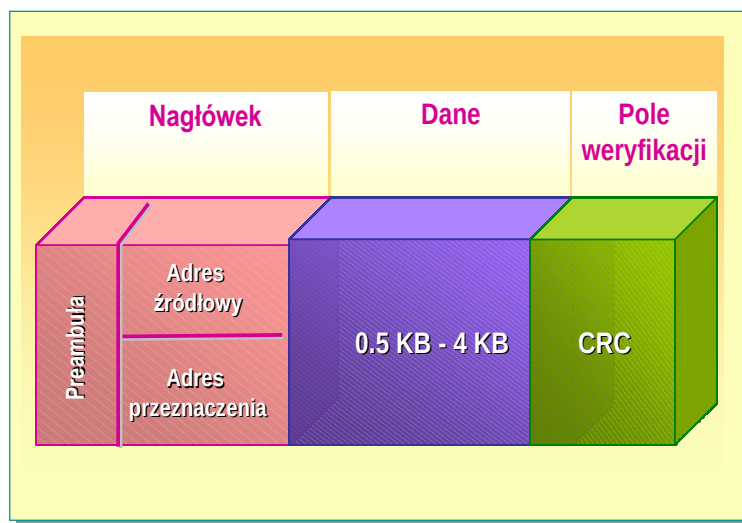
Elementy ramki

Cel slajdu

Przedstawienie trzech składników pakietu danych.

Wprowadzenie

Kiedy dane są dzielone na pakiety, dodawane są różne informacje, umożliwiające dostarczenie pakietu do celu.



Ramka (określenie pakietu danych na warstwie interfejsu sieciowego) składa się z trzech elementów: nagłówka, danych oraz pola weryfikacji.

Nagłówek

Nagłówek zawiera:

- Preambułę informującą o rozpoczęciu nadawania pakietu.
- Adres źródłowy.
- Adres przeznaczenia.

Dane

Informacje wysyłane przez aplikację. Ten element pakietu może się różnić rozmiarem, w zależności od ograniczeń sieci. Rozmiar sekcji danych w większości sieci wynosi od 0.5 kilobajta (KB) do 4 KB. W sieci Ethernet, rozmiar danych wynosi około 1.5 KB.

Ponieważ rozmiar większości oryginalnych danych jest większy od 4 KB, dane muszą być podzielone na odpowiednio mniejsze kawałki, aby można je było umieścić w pakiecie. Transmisja dużego pliku może wymagać podziału na wiele pakietów.

Pole weryfikacji

Zawartość pola weryfikacji zależy od *protokołu* warstwy interfejsu sieciowego. Jednakże, pole to zawiera zwykle informację kontroli poprawności ramki, zwaną sumą kontrolną *CRC* (*Cyclical Redundancy Check*). CRC jest liczbą obliczaną przez nadajnik na podstawie pakietu według wzoru matematycznego. Kiedy pakiet osiągnie cel, suma kontrolna jest obliczana ponownie. Jeśli wyniki będą takie same, oznacza to, że dane w pakiecie są nienaruszone. Jeśli wynik u odbiorcy będzie inny niż u nadawcy, oznacza to, że dane podczas transmisji zmieniły się. W takim przypadku, komputer źródłowy ponowi transmisję danych.

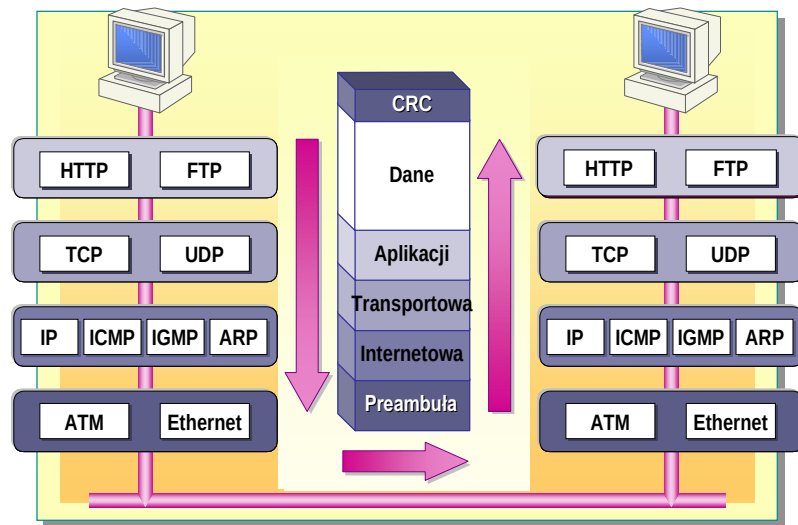
Przepływ danych

Cel slajdu

Przedstawienie procesu przesyłania danych.

Wprowadzenie

Przesyłanie pakietów między komputerami, angażuje warstwy TCP/IP zarówno komputera źródłowego, jak i komputera docelowego.



Wskazówka

Slajd na tej stronie rozszerza temat przedstawiony w pierwszej sekcji. Słuchacze powinni być już zaznajomieni z różnymi czynnościami związanymi z protokołem TCP/IP, a strona ta integruje te wiadomości, rozpatrując je na podstawie pojedynczego segmentu. Porównaj również CRC w ramce z sumami kontrolnymi dodawanymi przez protokoły na każdej warstwie. Wspomnij, że nie są to wszystkie informacje dodawane przez każdy protokół.

Pakiety danych przesyłane między komputerami, wędrują przez warstwy stosu protokołów TCP/IP. Kiedy pakiety przechodzą przez każdą warstwę, protokoły na tej warstwie dodają określone informacje do nagłówka. Informacje dodawane przez każdy protokół zawierają informacje kontroli poprawności, zwane *sumami kontrolnymi*. Suma kontrolna jest używana do sprawdzenia, czy informacje w nagłówku dodane przez protokół są takie same na komputerze docelowym, podobnie jak CRC, służy do sprawdzenia poprawności całego pakietu.

Informacje dodane przez protokół na danej warstwie są traktowane jak dane przez protokoły warstwy niższej. Kiedy pakiet jest odbierany, odpowiednia warstwa odrzuca nagłówek, a pozostały pakiet traktuje jako dane. Następnie pakiet jest przekazywany wyżej do odpowiedniego protokołu w stosie.

Warstwa aplikacji

Proces transmisji danych rozpoczyna się na warstwie aplikacji w stosie protokołów TCP/IP. Aplikacja, jak np. program Ftp, inicjuje proces na komputerze źródłowym, przygotowując dane w formacie zrozumiałym dla aplikacji na komputerze docelowym. Całym procesem steruje aplikacja na komputerze źródłowym.

Warstwa transportowa

Z warstwy aplikacji, dane wędrują do warstwy transportowej. Na warstwie tej znajdują się protokoły TCP oraz UDP. Aplikacja inicjująca transmisję prosi o wybranie protokołu—TCP lub UDP—a suma kontrolna jest dodawana dla obu protokołów TCP oraz UDP.

Jeśli wybrany został protokół TCP:

- Dodany jest numer porządkowy do każdego wysłanego segmentu.
- Dodane jest żądanie potwierdzenia odbioru dla transmisji zorientowanej na połączenie.
- Dodany jest numer portu TCP aplikacji źródłowej i docelowej.

Jeśli wybrany został protokół UDP:

- Dodany jest numer portu UDP aplikacji źródłowej i docelowej.

Warstwa internetowa

Po dodaniu informacji na warstwie transportowej, pakiet danych jest przekazywany do warstwy internetowej w stosie protokołów TCP/IP. Na tej warstwie protokół IP dodaje następujące informacje w nagłówku:

- Adres źródłowy IP
- Adres docelowy IP
- Protokół transportowy
- Wartość sumy kontrolnej
- Parametr Time to Live (TTL) określający czas życia pakietu

Oprócz dodania tych informacji, warstwa internetowa jest również odpowiedzialna za rozwiązanie adresu IP odbiorcy do jego adresu MAC. Protokół ARP dokonuje tego rozwiązania. Adres MAC jest dodany do nagłówka pakietu, a następnie pakiet jest przekazany niżej do warstwy interfejsu sieciowego.

Warstwa interfejsu sieciowego

Warstwa interfejsu sieciowego dodaje dwa rodzaje informacji—preambułę oraz sumę kontrolną CRC—do pakietu otrzymanego z warstwy IP. Preambuła jest to sekwencja bitów określająca rozpoczęcie ramki. Suma kontrolna CRC jest wynikiem matematycznego wzoru, dodawanego na końcu ramki, w celu sprawdzenia czy ramka nie została uszkodzona.

Po dodaniu informacji do ramek na warstwie interfejsu sieciowego są one wysyłane do sieci. Ramki są wysyłane do wszystkich komputerów w sieci.

Komputer docelowy

Kiedy ramki zostaną odebrane przez komputer docelowy, warstwa interfejsu sieciowego na tym komputerze usuwa preambułę i ponownie oblicza CRC. Jeśli jej wartość odpowiada wartości przed transmisją, sprawdzany jest adres MAC odbiorcy w ramce.

Jeżeli adres MAC jest adresem rozgłoszeniowym lub adres MAC odpowiada adresowi odbiorcy, ramka jest przekazywana do protokołu IP na wyższej warstwie internetowej, w przeciwnym razie ramka jest usuwana. Na warstwie IP, protokół IP ponownie oblicza sumę kontrolną i porównuje wynik z wartością obliczoną przed transmisją, w celu sprawdzenia czy pakiet nie został uszkodzony. Następnie warstwa IP przekazuje pakiet do protokołu transportowego, określonego w nagłówku IP.

Na warstwie transportowej, jeśli pakiet został odebrany przez protokół TCP, sprawdzana jest poprawność sumy kontrolnej, numer porządkowy i wysyłane jest potwierdzenie odbioru pakietu do TCP na komputerze źródłowym. Następnie, na podstawie numeru portu TCP, pakiet jest przekazywany dalej do odpowiedniej aplikacji na warstwie aplikacji.

Jeśli pakiet jest przekazany z warstwy internetowej do protokołu UDP, na podstawie numeru portu UDP, pakiet jest przekazywany do odpowiedniej aplikacji na warstwie aplikacji bez wysyłania potwierdzenia odebrania pakietu do komputera źródłowego. Po odebraniu danych przez aplikację, są one dalej przetwarzane w specyficzny dla aplikacji sposób.

◆ Ruting danych

Cel slajdu

Przedstawienie roli ruterów w przesyłaniu danych.

Wprowadzenie

W większości dużych sieci, dane muszą być rutowane między różnymi częściami sieci.

- Ruting IP
- Przesyłanie danych przez routery

Przepływ danych w sieci posiadającej jeden segment jest prosty. Każdy komputer przesyłający dane może za pomocą rozgłoszenia pytać o adres MAC komputera docelowego i wysłać do niego dane. Jednakże, w sieciach posiadających wiele segmentów, proces przesyłania danych jest bardziej złożony. W takich środowiskach sieciowych, protokół TCP/IP udostępnia wiele dróg między komputerami i zapobiega zbędnemu ruchowi między segmentami.

W środowisku jakim są połączone sieci, komputer źródłowy i docelowy mogą nie być w tym samym segmencie. Protokół IP określa, czy komputer docelowy jest lokalny, czy zdalny względem komputera źródłowego. Jeśli komputer docelowy jest w zdalnej sieci, dane nie mogą być wysłane bezpośrednio do niego. Zamiast tego, protokół IP wysyła je do routera, który przekazuje pakiety do miejsca przeznaczenia.

W sekcji tej wyjaśniono znaczenie protokołu IP w procesie routingu oraz opisano proces transmisji danych przez routery.

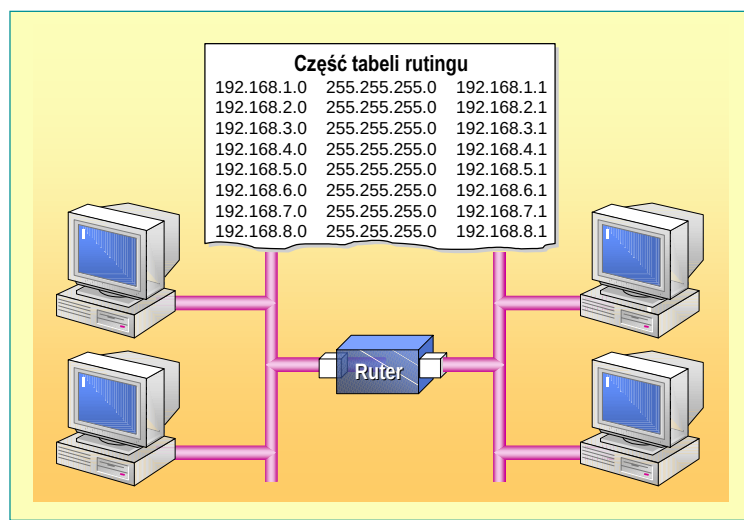
Ruting IP

Cel slajdu

Przedstawienie znaczenia protokołu IP w przesyłaniu danych.

Wprowadzenie

Protokół IP pełni bardzo ważną rolę w przesyłaniu danych między segmentami sieci.



Zagadnienie kluczowe

Wprowadź pojęcie sieci korporacyjnej, ponieważ podstawową funkcją stosu protokołów TCP/IP jest umożliwienie komunikacji na dużych obszarach. Zwróć uwagę, że routery są kluczem do zrozumienia, jak komunikacja w sieci korporacyjnej funkcjonuje. Upewnij się, że słuchacze rozumieją różnicę między bezpośrednim i pośrednim dostarczaniem pakietów, jako że jest to ważny aspekt działania protokołu IP.

Duże sieci TCP/IP, określane mianem sieci korporacyjnych, są dzielone na mniejsze segmenty, aby zmniejszyć ruch wewnątrz segmentów. *Sieć korporacyjna* składa się z wielu segmentów połączonych za pomocą ruterów. Najprostszymi ruterami są komputery z wieloma kartami sieciowymi, których podstawowym zadaniem jest łączenie dwóch lub więcej fizycznie odseparowanych segmentów.

Rutery przekazują pakiety IP między segmentami. Proces przekazywania pakietów IP znany jest jako ruting. Rutery podłączone są do dwóch lub więcej segmentów IP, umożliwiając przesyłanie pakietów między nimi.

Dostarczanie pakietów

IP używa przynajmniej jednej z dwóch metod dostarczania pakietów, w zależności od tego, czy pakiet IP jest dostarczany bezpośrednio do miejsca docelowego, czy do rutera. Te dwie metody dostarczania pakietów znane są jako bezpośrednie i pośrednie dostarczanie pakietów.

- Bezpośrednie dostarczenie pakietu ma miejsce, gdy komputer wysyła pakiet do miejsca docelowego w tym samym segmencie i adresuje pakiet na adres MAC odbiorcy.
- Pośrednie dostarczenie pakietu ma miejsce, gdy komputer wysyła pakiet do rutera, ponieważ adresat nie znajduje się w tym samym segmencie. Komputer opakuje pakiet IP do postaci ramki dla warstwy interfejsu sieciowego i adresuje pakiet na adres MAC rutera.

Tabela routingu

Aby określić, gdzie należy pakiet przesłać, routery używają tabeli routingu do przesyłania danych między segmentami sieci. Tabela routingu jest przechowywana w pamięci i dostarcza informacji o innych sieciach IP i hostach. Oprócz tego tabela routingu dostarcza informacji każdemu hostowi, jak komunikować się ze zdalnymi sieciami i hostami.

Na każdym komputerze w sieci IP można zarządzać tabelą routingu, zawierającą wpisy na temat wszystkich innych komputerów lub sieci, komunikujących się z lokalnym komputerem. Jednakże, w przypadku dużych sieci jest to niepraktyczne i tabela routingu jest utrzymywana na domyślnym routerze.

Tabela routingu może być zarówno statyczna jak i dynamiczna, w zależności od sposobu jej aktualizacji. Statyczna tabela routingu jest aktualizowana ręcznie. Ponieważ aktualizacja nie może być często przeprowadzana, informacje w tabeli routingu mogą nie być aktualne. Przeciwnie, dynamiczna tabela routingu jest aktualizowana automatycznie, jak tylko nowe informacje będą dostępne.

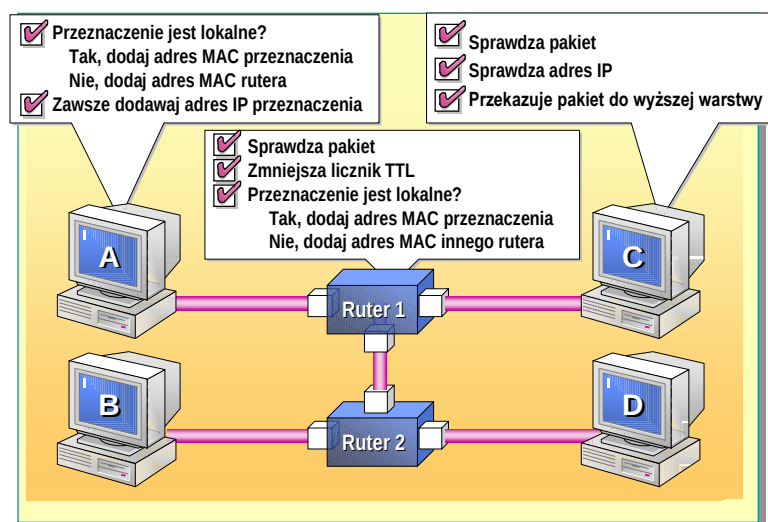
Przesyłanie danych przez routery

Cel slajdu

Przedstawienie procesu transmisji danych przez routery.

Wprowadzenie

Dane są przesyłane między sieciami za pośrednictwem routerów.



Wskazówka

Użyj slajdu jako nawiązanie do tematu przedstawionego w pierwszej sekcji. Najpierw użyj slajdu do wyjaśnienia procesu transmisji danych z komputera A przez ruter 1 do komputera C. Następnie zapytaj słuchaczy, jak będzie wyglądał proces transmisji danych z komputera A do komputera B lub D. Podkreśl użycie odpowiedniego adresu MAC w drugim przykładzie.

Protokół IP pełni ważną rolę w przesyłaniu danych w sieciach korporacyjnych. Pakiety IP są wymieniane i przetwarzane w każdym węźle: na warstwie internetowej komputera źródłowego, na routerach na trasie pakietu do miejsca przeznaczenia i na komputerze docelowym.

Aby przesłać dane między dwoma komputerami, znajdującymi się w różnych segmentach sieci, protokół IP sprawdza lokalną tabelę routingu, w celu znalezienia drogi do zdalnego komputera. Jeśli znajdzie drogę, wysyła nią pakiety. W przeciwnym razie, przesyła pakiety do domyślnego routera.

Protokół IP na komputerze źródłowym

Oprócz dodania takich informacji jak czas TTL, protokół IP zawsze dodaje do pakietu adres IP komputera przeznaczenia. W przypadku bezpośredniego dostarczenia pakietu, protokół ARP dodaje adres MAC komputera przeznaczenia. W przypadku pośredniego dostarczenia pakietu, protokół ARP dodaje adres routera, do którego pakiet zostanie przekazany.

Protokół IP na routerze

Kiedy pakiet zostanie przekazany do routera, protokół IP na routerze określa, gdzie dalej pakiet ma być przesłany. W tym celu, IP przeprowadza następujące czynności:

1. IP sprawdza sumę kontrolną i adres IP miejsca przeznaczenia.
Jeśli adres IP jest adresem routera, router przetwarza pakiet jako komputer docelowy (warstwa IP).
2. Następnie IP zmniejsza czas TTL i sprawdza swoją tabelę routingu w celu znalezienia najlepszej drogi do adresu IP odbiorcy.
3. W przypadku bezpośredniego dostarczenia pakietu, protokół ARP dodaje adres MAC komputera przeznaczenia. W przypadku pośredniego dostarczenia pakietu, protokół ARP dodaje adres routera, do którego pakiet zostanie przekazany.

Cały ten proces jest powtarzany na każdym routerze na trasie między komputerem źródłowym, a komputerem docelowym, dopóki pakiet nie zostanie dostarczony do routera w tym samym segmencie co komputer docelowy.

Fragmentacja i odtwarzanie

Kiedy pakiet jest za duży do przesłania przez sieć, podłączoną do routera, protokół IP dzieli pakiet na mniejsze pakiety, zanim prześle je dalej. Proces ten jest nazywany fragmentacją.

Następnie wszystkie fragmenty są przesyłane do zdalnej sieci. Nawet jeśli pakiety te będą przechodziły przez wiele routerów, fragmenty zostaną odtworzone dopiero, gdy wszystkie małe pakiety odpowiadające wszystkim danym, zostaną odebrane przez komputer docelowy. Jest to proces odtwarzania danych.

Protokół IP na komputerze docelowym

Kiedy pakiet zostanie odebrany przez komputer docelowy, jest on przekazywany do warstwy IP. Protokół IP na komputerze docelowym sprawdza sumę kontrolną i adres IP adresata. Następnie IP przekazuje pakiet do protokołu TCP lub UDP. Ostatecznie, na podstawie numeru portu pakiet jest przekazany do aplikacji docelowej w celu końcowej obróbki.

Uwaga Jeżeli czas TTL osiągnie zero lub jakiś etap procesu komunikacji nie powiedzie się, jak np. docelowa aplikacja nie zostanie znaleziona, pakiet jest porzucany i może zostać zwrócony komunikat ICMP. Chociaż dostarczenie pakietu ICMP nie jest gwarantowane, jeśli był używany protokół TCP, oryginalny pakiet zostanie ponownie wysłany.

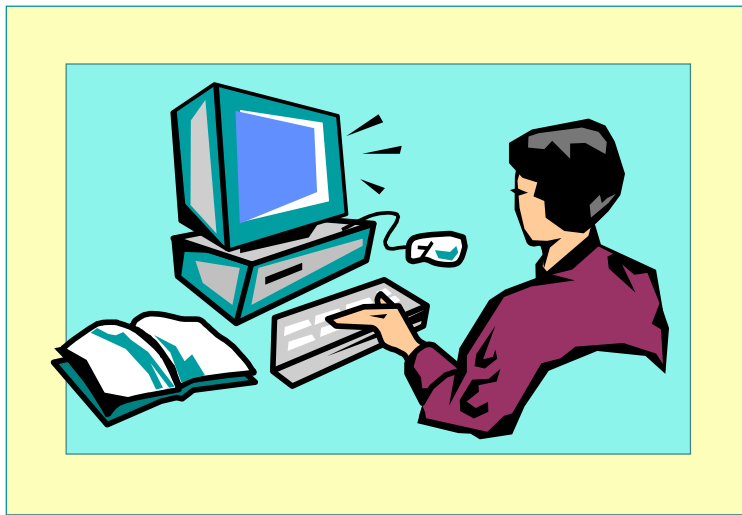
Laboratorium B: Badanie procesów i protokołów stosu TCP/IP

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W laboratorium tym, zostaną zbadane procesy związane z rozwiązywaniem nazw oraz protokoły zaangażowane podczas używania polecenia Ping poprzez ruter.



Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Rozpoznawać procesy związane z rozwiązywaniem nazw.
- Rozpoznawać protokoły zaangażowane podczas używania polecenia Ping poprzez ruter.

Przygotowanie laboratorium

Laboratorium to dostępne jest w formie symulacji. Do wykonania tego laboratorium niezbędne są:

- Komputer z systemem Microsoft Windows 2000, Microsoft Windows NT® 4.0, Microsoft Windows 98 lub Microsoft Windows 95.
- Minimalna rozdzielczość ekranu 800 x 600 i 256 kolorów. (Zalecane 16-bit).
- Program Microsoft Internet Explorer 5 lub nowszy.

► Aby rozpocząć laboratorium

1. Zaloguj się w systemie Windows 2000 na konto Administrator z hasłem **password**.
2. Na pulpicie, dwukrotnie kliknij ikonę programu **Internet Explorer**.
3. Na stronie Materiały studenckie wybierz polecenie **Symulacje**.
4. Wybierz polecenie **Badanie procesów i protokołów stosu TCP/IP**.
5. Przeczytaj informacje wstępne, a następnie kliknij odsyłacz, aby rozpocząć symulację.

Przewidywany czas ukończenia laboratorium: 15 minut

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Pytania podsumowujące dotyczą głównych tematów omówionych w rozdziale.

- **Wprowadzenie do TCP/IP**
- **Przegląd architektury stosu protokołów TCP/IP**
- **Rozwiązywanie nazw**
- **Badanie procesu przesyłania danych**
- **Ruting danych**

-
1. TCP/IP używa czterowarstwowego modelu transmisji danych. Jak nazywają się te warstwy?

Warstwa aplikacji, warstwa transportowa, warstwa internetowa oraz warstwa interfejsu sieciowego.

2. Jeśli dana aplikacja chce komunikować się z aplikacją na innym komputerze, w jaki sposób TCP/IP rozróżnia aplikacje od siebie, jak również komputery, na których one działają?

Używa gniazd.

3. Jakie trzy elementy charakteryzują gniazdo?

Adres IP, port oraz protokół warstwy transportowej.

4. Jak nazywa się sześć kluczowych protokołów w stosie protokołów TCP/IP firmy Microsoft?

TCP, UDP, ICMP, IGMP, IP oraz ARP.

5. Którego z sześciu kluczowych protokołów powinieneś użyć, jeśli chcesz stosować w aplikacji kartę kredytową i mieć pewność dostarczenia danych?

TCP.

-
6. Który z sześciu kluczowych protokołów jest odpowiedzialny za adresowanie i ruting danych do miejsca przeznaczenia?

IP.

7. Jako administrator sieci, chcesz sprawdzić, czy stos protokołów TCP/IP został poprawnie zainstalowany oraz czy jest możliwa komunikacja w sieci. Jakiego programu narzędziowego TCP/IP powinieneś użyć?

Ping.

8. Jeśli chcesz użyć nazwy komputera przyjaznej dla użytkownika, zamiast adresu IP, jakie są możliwe sposoby mapowania nazw komputerów do adresów IP?

Plik Hosts, plik Lmhosts, usługa DNS oraz usługa WINS.

9. Jeśli używana jest pośrednia metoda dostarczenia pakietu, z komputera źródłowego do komputera docelowego, komputer źródłowy musi najpierw określić adres MAC należący do _____.

Do rutera.

