

Rozdział 5: Protokoły sieciowe

Spis treści

Przegląd zagadnień	1
Wprowadzenie do tematu protokołów	2
Protokoły i przesyłanie danych	6
Podstawowe protokoły	10
Inne protokoły komunikacyjne	15
Protokoły zdalnego dostępu	18
Laboratorium A: Określanie właściwości protokołu	23
Podsumowanie	24



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 jakiegokolwiek 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 Pierścioneck, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
45 minut

Laboratoria:
15 minut

W rozdziale tym zawarte zostały informacje wprowadzające słuchaczy w zagadnienia związane z podstawowymi protokołami, obsługiwanymi przez system Microsoft® Windows® 2000. Rozdział ten rozpoczyna się od omówienia tematyki protokołów, typów protokołów, modelu OSI oraz stosu protokołów.

Dalej opisano protokoły rutowalne i nierutowalne, typy transmisji danych w sieci, oraz podstawowe protokoły, obsługiwane przez system Windows 2000, takie jak TCP/IP, IPX/SPX, NetBEUI i AppleTalk, wraz z ich właściwościami.

Kolejna część rozdziału poświęcona jest technologiom komunikacyjnym, obsługiwanym przez system Windows 2000, takim jak ATM czy IrDA. Pod koniec rozdziału opisane zostały protokoły zdalnego dostępu, obsługiwane przez system Windows 2000, takie jak protokół dial-up oraz protokoły VPN.

Po ostatniej sekcji tego rozdziału umieszczone zostało laboratorium, w którym słuchacze nauczą się określać właściwości protokołów.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Powiedzieć, czym jest protokół i opisać typy protokołów.
- Opisać właściwości protokołu i stwierdzić, czy dany komputer może się komunikować z innymi komputerami w sieci.
- Wymienić nazwy podstawowych protokołów sieciowych, obsługiwanych przez system Windows 2000 oraz opisać ich właściwości.
- Wymienić nazwy protokołów komunikacyjnych oraz technologii, kompatybilnych z systemem Windows 2000 oraz opisać ich właściwości.
- Opisać protokoły wykorzystywane do uzyskania zdalnego dostępu: protokół dial-up oraz protokoły wirtualnych sieci prywatnych VPN.

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_05.ppt
- Rozdział 5, „Protokoły sieciowe”

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału, należy:

- Przeczytać całość materiałów poświęconych temu rozdziałowi.
- Wykonać laboratorium.
- 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:

- Wprowadzenie to tematu protokołów
Przedstawiając tą sekcję, należy przybliżyć pojęcie protokołu i opisać jego dwa typy—protokoły otwarte oraz protokoły charakterystyczne dla producenta. Następnie należy krótko omówić model OSI oraz wyjaśnić, czym są stosy protokołów, nie porównując jednak typów protokołów w stosie z modelem OSI.
- Protokoły i przesyłanie danych
Prezentując tą sekcję, należy przedstawić różnicę między protokołami rutowalnymi i nierutowalnymi oraz opisać trzy sposoby przesyłania danych.
- Podstawowe protokoły
W tej sekcji należy omówić podstawowe protokoły, obsługiwane przez system Windows 2000 i porównać właściwości protokołów TCP/IP, IPX/SPX, NetBEUI oraz AppleTalk.
- Inne protokoły komunikacyjne
Omawiając tą sekcję należy, opisać właściwości innych technologii komunikacyjnych, obsługiwanych przez system Windows 2000, takich jak ATM oraz IrDA. Protokoły te powinny zostać omówione tylko ogólnie.
- Protokoły zdalnego dostępu
Podczas opisywania tej sekcji należy omówić dwa typy protokołów zdalnego dostępu, obsługiwane przez system Windows 2000. Opis i właściwości różnych protokołów dial-up oraz VPN powinny zostać podane tylko ogólnie.

Informacje uzupełniające

W sekcji tej opisane są wymagania dotyczące instalacji laboratorium dla tego rozdziału oraz 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).

Ten moduł obejmuje tylko interaktywne ćwiczenia laboratoryjne, wykonywane na komputerze, w związku z czym, nie ma żadnych dodatkowych wymagań instalacji laboratorium, ani zmian w konfiguracji, które mogłyby wpłynąć na powielenie lub dostosowywanie materiałów szkoleniowych.

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 powielenie lub dostosowywanie materiałów szkoleniowych.

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

W trakcie omawiania tego rozdziału przedstawione zostaną protokoły komunikacyjne i ich właściwości, podstawowe protokoły, używane w trakcie komunikacji w sieci oraz inne protokoły kompatybilne z sieciami opartymi na systemie Windows 2000.

- Wprowadzenie do tematu protokołów
- Protokoły i przesyłanie danych
- Podstawowe protokoły
- Inne protokoły komunikacyjne
- Protokoły zdalnego dostępu

Aby komputery połączone w sieć mogły się ze sobą komunikować, muszą korzystać ze wspólnego języka, czyli tak zwanego *protokołu*. Protokół stanowi zestaw zasad i standardów, które umożliwiają komunikację pomiędzy komputerami w sieci. Obecnie stosowanych jest wiele typów protokołów, różniących się między sobą właściwościami i możliwościami. Nie każdy protokół jest jednak kompatybilny z każdym typem komputera lub systemem operacyjnym. Aby móc stwierdzić, czy komputer, będący klientem sieci opartej na systemie Microsoft® Windows® 2000, może komunikować się z innymi podłączonymi do niej komputerami, należy poznać protokoły obsługiwane przez ten system.

System Windows 2000 obsługuje większość stosowanych obecnie protokołów sieciowych, jak również inne protokoły komunikacyjne, łącznie z protokołami zdalnego dostępu. To, że system Windows 2000 jest kompatybilny z różnymi typami protokołów sprawia, że istnieją duże możliwości wykorzystania go w różnych środowiskach sieciowych.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Powiedzieć, czym jest protokół i opisać typy protokołów.
- Opisać właściwości protokołu i stwierdzić, czy dany komputer może się komunikować z innymi komputerami w sieci.
- Wymienić nazwy podstawowych protokołów sieciowych, obsługiwanych przez system Windows 2000 oraz opisać ich właściwości.
- Wymienić nazwy protokołów komunikacyjnych oraz technologii, kompatybilnych z systemem Windows 2000 oraz opisać ich właściwości.
- Opisać protokoły wykorzystywane do uzyskiwania zdalnego dostępu: protokół dial-up oraz protokoły wirtualnych sieci prywatnych VPN.

◆ Wprowadzenie do tematu protokołów

Cel slajdu

Wprowadzenie do zagadnień związanych z typami protokołów, modelem OSI oraz pojęciem stosu protokołów.

Wprowadzenie

Protokoły wyznaczają zasady i procedury, które rządzą procesem komunikacji pomiędzy komputerami w sieci.

- Typy protokołów
- Model OSI (Open Systems Interconnection)
- Stosy protokołów

Protokoły w swojej istocie stanowią element oprogramowania i jako takie muszą zostać zainstalowane na składnikach sieci, które mają z nich korzystać. Komputery mogą komunikować się ze sobą tylko pod warunkiem, że korzystają z tego samego protokołu. Jeśli protokół, wykorzystywany w sieci przez jeden komputer, nie jest kompatybilny z protokołem, wykorzystywanym przez drugi komputer, to komputery te nie mogą wymieniać między sobą informacji. W danym środowisku sieciowym mogą być wykorzystywane bardzo różne protokoły. Chociaż każdy protokół jest w stanie zapewnić podstawową obsługę procesu komunikacji w sieci, każdy też ma pewne charakterystyczne funkcje, przeznaczone do realizacji specyficznych zadań.

Aby zrozumieć poszczególne funkcje różnych protokołów, konieczne jest poznanie standardowego modelu przeznaczonego dla sieci—modelu OSI (Open Systems Interconnection). Model ten składa się z zestawu siedmiu warstw protokołów, z których każda odpowiada za realizację pewnych funkcji, umożliwiających transmisję danych w obrębie sieci.

Zgodnie z modelem koncepcyjnym OSI, aby możliwa była prawidłowa transmisja danych w sieci, kilka protokołów musi pracować razem. W rzeczywistości jest to realizowane poprzez zastosowanie *stosu protokołów*. Stos protokołów stanowi zestaw protokołów, które funkcjonują razem, umożliwiając transmisję danych poprzez sieć komputerową.

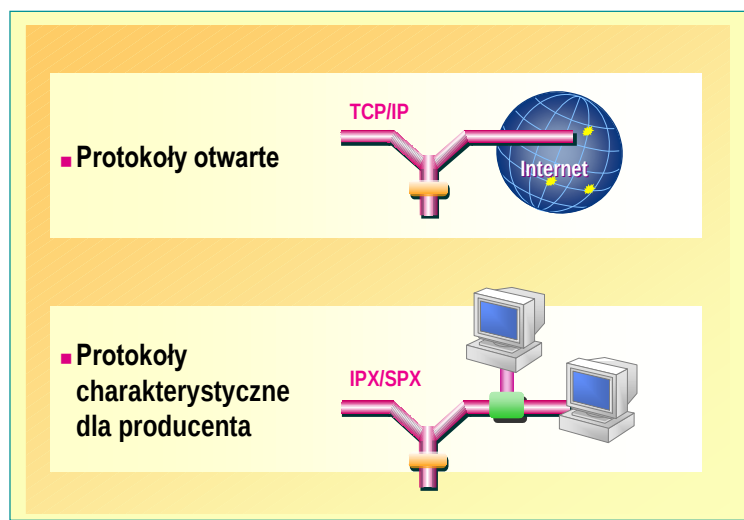
Typy protokołów

Cel slajdu

Przedstawienie dwóch typów protokołów sieciowych.

Wprowadzenie

Każdy protokół może należeć albo do kategorii protokołów otwartych, albo do kategorii protokołów charakterystycznych dla producenta.



Stosowane obecnie protokoły mogą należeć do jednej z dwóch grup protokołów: otwartych lub charakterystycznych dla producenta.

Protokoły otwarte

Protokoły otwarte stanowią grupę protokołów, napisanych w oparciu o powszechnie znane standardy przemysłowe. Protokół, który został stworzony zgodnie z tymi standardami, jest kompatybilny ze wszystkimi innymi protokołami, napisanymi w oparciu o te same standardy. Protokoły otwarte nie są protokołami własnościowymi (nie stanowią niczyjej prywatnej własności). Typowym przykładem protokołu należącego do tej grupy jest protokół TCP/IP (Transmission Control Protocol/Internet Protocol), który jest podstawowym protokołem transmisji w sieci Internet.

Protokoły charakterystyczne dla producenta

Grupa protokołów charakterystycznych dla producenta obejmuje protokoły własnościowe, opracowane przez różnych producentów i przeznaczone do pracy w specyficznych środowiskach. Na przykład firma Novell stworzyła zestaw protokołów, takich jak IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange), mając na uwadze specyfikę architektury NetWare.

Model OSI (Open Systems Interconnection)

Cel slajdu

Przedstawienie siedmiu warstw modelu OSI.

Wprowadzenie

Model OSI został zbudowany na bazie zestawu siedmiu warstw protokołów.



Zagadnienie kluczowe

W modelu OSI proces komunikowania się w sieci został podzielony na siedem warstw, przy czym każda warstwa pełni specyficzną funkcję podczas przesyłania danych w sieci.

Wskazówka

Wyjaśnij słuchaczom, że funkcje protokołów pracujących na każdej warstwie modelu OSI zależą od roli, jaką ta warstwa spełnia w procesie transmisji danych.

Zapotrzebowanie na międzynarodowe standardy technologiczne zaowocowało powstaniem organizacji ISO (International Organization for Standardization). Organizacja ISO miała doprowadzić do standaryzacji metod, za pomocą których komputery na całym świecie mogą się ze sobą komunikować. Aby to zrobić, organizacja ISO stworzyła model komunikacji sieciowej, zwany modelem OSI (Open Systems Interconnection).

Model OSI

W modelu OSI proces komunikowania się w sieci został podzielony na siedem warstw. Podczas przesyłania danych w sieci każda warstwa pełni inną funkcję.

Dane, przed przekazaniem przez poszczególne warstwy modelu OSI, są dzielone na *pakiety*. Pakiet stanowi jednostkę informacji, która jest przesyłana w całości przez sieć z jednego komputera na drugi. Pakiet przekazywany jest w sieci pomiędzy warstwami, przy czym na każdej warstwie dodawane są do niego pewne dodatkowe informacje.

To, na jakiej warstwie pracuje dany protokół, determinuje jego funkcje. Niektóre protokoły pracują tylko na poszczególnych warstwach modelu OSI.

Warstwa OSI	Funkcja
Warstwa aplikacji	Określa, w jaki sposób aplikacje współdziałają ze sobą
Warstwa prezentacji	Dodaje podstawowe formatowanie do prezentacji danych
Warstwa sesji	Tworzy kanały komunikacyjne i zarządza nimi
Warstwa transportu	Sprawdza poprawność przesyłanych danych
Warstwa sieci	Adresuje wiadomości wewnątrz i pomiędzy sieciami
Warstwa łącza danych	Określa sposób uzyskiwania dostępu do fizycznego medium, takiego jak przewód sieciowy
Warstwa fizyczna	Przesyła dane przez fizyczne medium

Stosy protokołów

Cel slajdu

Przedstawienie pojęcia stosu protokołów.

Wprowadzenie

Stos protokołów stanowi zestaw protokołów, które funkcjonują razem, umożliwiając transmisję danych pomiędzy komputerami.

**Zagadnienie kluczowe**

Stos protokołów stanowi podzielony na warstwy zestaw powiązanych ze sobą protokołów, umożliwiający poprawną transmisję danych poprzez sieć.

Wskazówka

Nie porównuj typów protokołów w stosie z warstwami modelu OSI. Zamiast tego, korzystając z ilustracji, wyjaśnij słuchaczom, że każdy stos protokołów jest podobny do podstawowego modelu OSI, ale może różnić się liczbą warstw.

Zgodnie z modelem OSI, do podziału na pakiety, wysyłania oraz odbierania transmisji danych w sieci służą oddzielne warstwy. Realizację tych zadań umożliwiają podzielone na warstwy zestawy protokołów. Taki podzielony na warstwy zestaw protokołów pracujących w sieci nazywany jest stosem protokołów. Protokoły składające się na stos wykonują razem wszystkie zadania, umożliwiając podział na pakiety, wysłanie i odbieranie transmisji.

Niektóre stosy protokołów zostały uznane za standardowe modele protokołów. Do podstawowych stosów protokołów zaliczyć można TCP/IP, IPX/SPX oraz AppleTalk. Każdej warstwie stosu protokołów przyporządkowany jest jeden protokół, odpowiedzialny za wykonanie zadania należącego do tej warstwy. Jednak ogólnie rzecz biorąc, odpowiedzialność za wykonanie poszczególnych zadań, zapewniających prawidłową komunikację, spoczywa na trzech typach protokołów: aplikacji, transportu oraz sieci.

Protokoły aplikacji

Protokoły aplikacji zapewniają wymianę danych pomiędzy aplikacjami pracującymi w sieci. Przykładem często stosowanego protokołu aplikacji jest protokół FTP (File Transfer Protocol) oraz SMTP (Simple Mail Transfer Protocol).

Protokoły transportu

Protokoły transportu odpowiadają za prowadzenie sesji komunikacyjnych pomiędzy komputerami oraz zapewniają, że dane są poprawnie przekazywane pomiędzy komputerami. Często stosowanym protokołem transportu jest protokół TCP (Transmission Control Protocol).

Protokoły sieci

Protokoły sieci zapewniają tzw. *usługi połączeniowe*. Protokoły te określają reguły komunikowania się w poszczególnych środowiskach sieciowych. Często stosowanym protokołem, odpowiedzialnym za usługi sieciowe, jest protokół IP (Internet Protocol).

◆ Protokoły i przesyłanie danych

Cel slajdu

Przedstawienie protokołów rutowalnych i nierutowalnych oraz typów transmisji danych.

Wprowadzenie

Protokoły mogą, lecz nie muszą, umożliwiać przesyłania danych pomiędzy segmentami sieci wzdłuż dowolnej ścieżki.

- Protokoły rutowalne i nierutowalne
- Typy transmisji danych

W dużych sieciach trudno jest efektywnie zarządzać procesem komunikacji z powodu zbyt dużego natężenia ruchu w sieci. Administratorzy sieci mogą rozwiązać ten problem, dzieląc dużą sieć na kilka *segmentów sieci*. Segmenty to mniejsze sieci, które po połączeniu tworzą dużą sieć.

Dane w sieci mogą być przesyłane z jednego segmentu sieci do drugiego wzdłuż dowolnej z istniejących ścieżek. Przesyłanie danych pomiędzy segmentami sieci nosi nazwę *rutingu*. Jednak nie każdy protokół obsługuje *ruting*. Protokoły można podzielić na dwie kategorie, w zależności od tego, czy są w stanie obsługiwać *ruting* czy też nie.

Dzięki temu, że część protokołów jest w stanie obsługiwać *ruting*, możliwa jest transmisja danych pomiędzy komputerami znajdującymi się w różnych segmentach sieci. Istnieją różne typy transmisji danych. Każdy typ transmisji określa, które komputery w sieci otrzymają wysyłane dane. Ponieważ nie wszystkie komputery w sieci muszą odbierać wszystkie wysyłane informacje, kontrolując typ transmisji można do pewnego stopnia określić, które komputery mogą otrzymywać i przetwarzać dane.

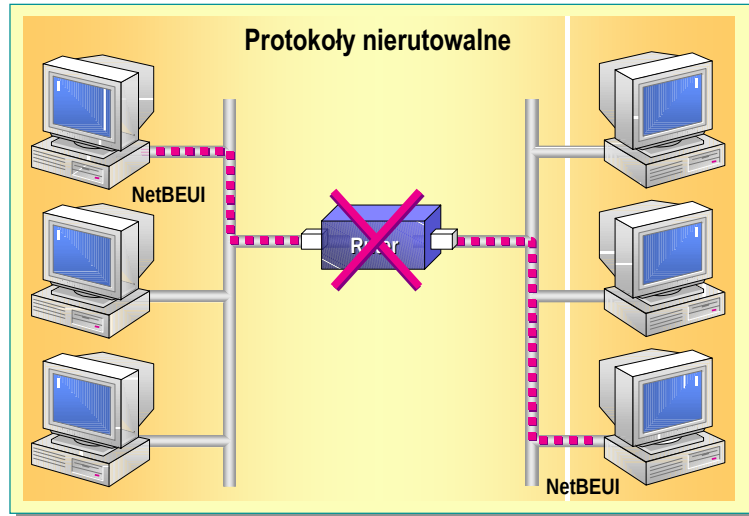
Protokoły rutowalne i nierutowalne

Cel slajdu

Zilustrowanie różnicy między protokołami rutowalnymi i nierutowalnymi.

Wprowadzenie

Protokoły mogą, lecz nie muszą, umożliwiać przesyłania danych pomiędzy różnymi segmentami sieci, w zależności od tego, czy są rutowalne czy też nierutowalne.



Zagadnienie kluczowe

Protokoły rutowalne umożliwiają komputerom, znajdującym się w jednym segmencie sieci, komunikowanie się z komputerami z innego segmentu.

Tylko komputery wykorzystujące protokoły rutowalne mogą wysłać dane do komputerów w innych segmentach sieci.

Wskazówka

Korzystając z animacji, wyjaśnij różnicę między protokołami rutowalnymi i nierutowalnymi.

W zależności od tego, czy określone protokoły są rutowalne czy też nierutowalne, mogą zostać podzielone na dwie kategorie.

Protokoły rutowalne

Protokoły rutowalne umożliwiają komunikację pomiędzy sieciami LAN lub segmentami sieci, które mogą być rozproszone w obrębie jednego budynku, niewielkiego obszaru geograficznego, takiego jak sieć uniwersytecka lub całego świata, tak jak to jest w przypadku sieci Internet. Protokoły rutowalne są w stanie zapewnić transmisję danych z jednego segmentu sieci do innego, wzdłuż dowolnej ścieżki, łączącej dwa segmenty sieci. Przykładowymi rutowalnymi protokołami są protokoły TCP/IP oraz IPX/SPX.

Protokoły nierutowalne

Protokoły nierutowalne, w przeciwieństwie do protokółów rutowalnych, nie zapewniają transmisji danych z jednego segmentu sieci do innego. Komputery korzystające z protokółów nierutowalnych mogą komunikować się tylko z komputerami znajdującymi się w tym samym segmencie sieci. Protokoły NetBEUI oraz DLC (Data Link Control) są przykładami protokółów nierutowalnych.

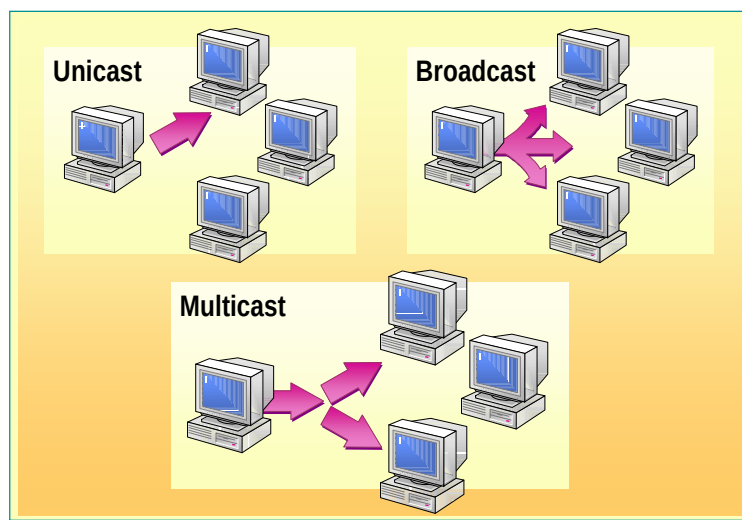
Typy transmisji danych

Cel slajdu

Przedstawienie trzech typów transmisji danych.

Wprowadzenie

Dane są przesyłane przez sieć zgodnie z trzema typami transmisji: unicast, broadcast oraz multicast.



Protokoły rutowalne umożliwiają transmisję danych pomiędzy komputerami, znajdującymi się w różnych segmentach sieci. Jednak z powodu dużego natężenia ruchu w sieci, wywołanego na przykład wprowadzeniem aplikacji multimedialnych, następuje obniżenie ogólnej efektywności pracy sieci, gdyż zmniejsza się prędkość transmisji danych. Natężenie ruchu w sieci różni się w zależności od przyjętego typu transmisji, takiego jak: unicast, broadcast oraz multicast. Aby zrozumieć, jak zastosowany typ transmisji danych wpływa na ruch w sieci, należy poznać charakterystykę poszczególnych typów transmisji.

Transmisja typu unicast

W przypadku transmisji typu unicast, oddzielna kopia danych przesyłana jest ze źródła do każdego komputera, będącego klientem, który ich zażąda. Żaden inny komputer w sieci nie musi zajmować się przetwarzaniem transmisji danych. Transmisja typu unicast nie jest jednak zbyt efektywna, jeśli wiele komputerów zażąda tych samych danych, ponieważ źródło musi wtedy nadać wiele jednakowych kopii informacji. Transmisja typu unicast funkcjonuje najbardziej wydajnie, kiedy tylko niewielka liczba komputerów, będących klientami, zażąda określonych danych. Transmisja typu unicast jest także nazywana transmisją skierowaną. Obecnie większość ruchu w sieci wywoływana jest przez transmisję typu unicast.

Transmisja typu broadcast

W trakcie transmisji danych typu broadcast, pojedyncza kopia danych jest przesyłana do wszystkich klientów, znajdujących się w tym samym segmencie sieci, co komputer wysyłający. Transmisja typu broadcast nie jest jednak zbyt efektywna, jeśli dane mają zostać wysłane tylko do części komputerów w segmencie, ponieważ przy tym typie transmisji dane są wysyłane do całego segmentu. Powoduje to niepotrzebne obniżenie wydajności sieci, ponieważ każdy klient musi przetwarzać przesyłane w ten sposób dane.

Transmisja typu multicast

W przypadku transmisji typu multicast, pojedyncza kopia danych jest wysyłana tylko do klientów, którzy ich zażądali. Przez sieć nie muszą więc być wysyłane liczne kopie tych samych danych. Ogranicza to ruch w sieci i umożliwia wprowadzenie aplikacji multimedialnych, bez niepotrzebnego przeciążenia sieci. Wiele usług internetowych wykorzystuje transmisję typu multicast do komunikacji z komputerami klienckimi.

◆ Podstawowe protokoły

Cel slajdu

Przedstawienie podstawowych protokołów sieciowych.

Wprowadzenie

System Windows 2000 obsługuje większość najczęściej używanych protokołów sieciowych.

- **Protokół TCP/IP (Transmission Control Protocol/Internet Protocol)**
- **Protokół IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)**
- **Protokół NetBEUI (NetBIOS Enhanced User Interface)**
- **Protokół AppleTalk**

System Windows 2000 obsługuje wiele różnych protokołów sieciowych. Poszczególne protokoły umożliwiają komunikację z systemami, urządzeniami oraz komputerami w różnych środowiskach sieciowych. Niektóre z protokołów są rutowalne, inne zaś nie. Na podstawie informacji o tym, jakie protokoły są wykorzystywane przez komputer, będący klientem, można określić, czy dany komputer może komunikować się z innymi komputerami w rutowalnej sieci, opartej na systemie Windows 2000. Podstawowymi protokołami, które mogą zostać wykorzystane w systemie Windows 2000, są:

- Stos protokołów TCP/IP
- Stos protokołów IPX/SPX
- Protokół NetBEUI
- Stos protokołów AppleTalk

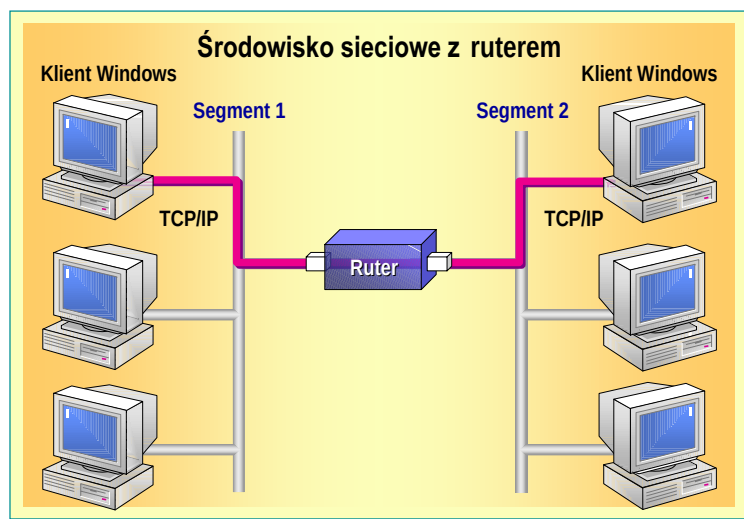
Protokół TCP/IP (Transmission Control Protocol/Internet Protocol)

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje stos protokołów TCP/IP w środowisku sieciowym zawierającym ruter.

Wprowadzenie

Stos protokołów TCP/IP jest zbudowany w oparciu o standardy przemysłowe i może być obsługiwany przez większość sieci, dzięki temu, że pracuje na różnych typach komputerów.



Zagadnienie kluczowe

Stos protokołów TCP/IP jest standardowym stosem protokołów, obsługiwanym przez większość sieci, dzięki temu, że może pracować na różnych typach komputerów.

Wskazówka

Skorzystaj z ilustracji umieszczonej na slajdzie, aby wyjaśnić słuchaczom, że stos protokołów TCP/IP pozwala komputerom komunikować się pomiędzy segmentami w środowisku sieciowym zawierającym ruter.

Stos protokołów (podzielony na warstwy zestaw protokołów) TCP/IP jest zbudowany w oparciu o standardy przemysłowe i umożliwia komunikację w różnych środowiskach sieciowych. Dzięki temu, że stos protokołów TCP/IP może pracować na różnych typach komputerów, obsługuje go większość typów sieci.

Stos protokołów TCP/IP obsługuje routingu i pozwala komunikować się komputerom leżącym w różnych segmentach sieci. Dzięki tej funkcji, jest protokołów TCP/IP jest standardowym protokołem komunikacji w sieci Internet. Duża niezawodność w zakresie przesyłania danych oraz szeroki zakres zastosowania spowodował, że stos protokołów TCP/IP stał się niezbędnym elementem, pozwalającym uzyskać dostęp do ogólnosięciowych sieci informacyjnych, takich jak Internet. Stos protokołów TCP/IP musi jednak zostać skonfigurowany na każdym komputerze, na którym ma być wykorzystywany jako protokół komunikacyjny.

Zalety stosu protokołów TCP/IP:

- Stos protokołów TCP/IP jest standardem przemysłowym. Jako standard przemysłowy należy on do grupy protokołów otwartych, w związku z czym nie jest kontrolowany przez żadną pojedynczą organizację.
- Stos protokołów TCP/IP zawiera zestaw narzędzi, pozwalający łączyć różne systemy operacyjne. Możliwość uzyskania połączenia pomiędzy dwoma komputerami nie zależy od sieciowego systemu operacyjnego, zainstalowanego na każdym z komputerów.
- Stos protokołów TCP/IP zbudowany jest w oparciu o skalowalną, niezależną od platformy, architekturę klient-serwer. Struktura stosu protokołów TCP/IP może zostać rozszerzona lub zawężona tak, aby sprostać przyszłym wymaganiom sieci.

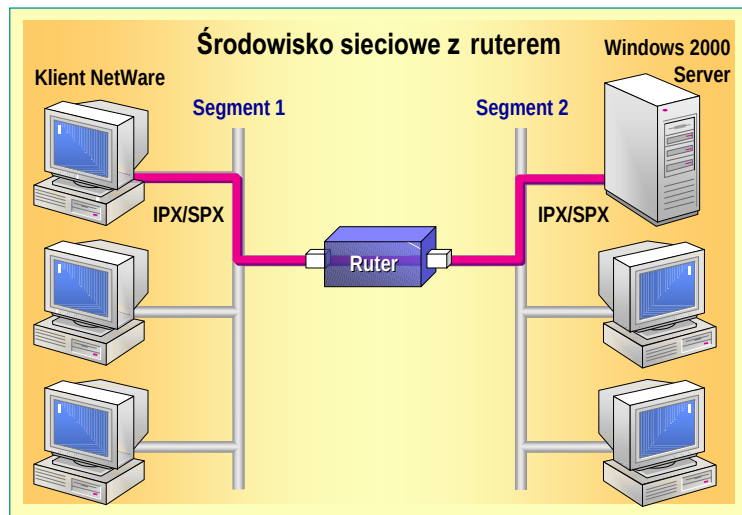
Protokół IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje stos protokołów IPX/SPX.

Wprowadzenie

System Windows 2000 obsługuje protokół IPX/SPX, który jest podstawowym protokołem, wykorzystywanym w sieciach NetWare.



Zagadnienie kluczowe

Stos protokołów IPX/SPX obsługuje ruting i jest przeznaczony do pracy w środowisku NetWare.

Wskazówka

Skorzystaj z ilustracji umieszczonej na slajdzie, aby wyjaśnić słuchaczom, że stos protokołów IPX/SPX umożliwia komputerom, które są klientami sieci NetWare, komunikowanie się z serwerem Windows 2000 w środowisku sieciowym zawierającym ruter.

Stos protokołów IPX/SPX został stworzony specjalnie dla architektury NetWare. Na stos protokołów IPX/SPX składa się protokół IPX oraz protokół SPX. Protokół IPX określa schemat adresowania, wykorzystany w sieci NetWare, natomiast protokół SPX zapewnia bezpieczeństwo i niezawodność pracy protokołu IPX. Protokół IPX jest protokołem obsługującym warstwę sieci i pełni tę samą funkcję, co protokół IP w stosie protokołów TCP/IP. Protokół SPX zapewnia niezawodność usług, realizowanych w warstwie transportu.

Właściwości stosu protokołów IPX/SPX:

- Protokół IPX/SPX jest zwykle wykorzystywany w sieciach, w których pracują serwery NetWare.
- Protokół IPX/SPX jest rutowalny. Pozwala on komputerom, pracującym w środowisku sieciowym zawierającym ruter, wymieniać informacje pomiędzy segmentami.

Uwaga Protokół NWLink IPX/SPX/NetBIOS Compatible Transport Protocol jest wersją stosu protokołów IPX/SPX opracowaną przez Microsoft, zawartą w systemie Windows 2000. Komputery klienckie pracujące w systemie Windows 2000 mogą korzystać z protokołu NWLink, aby uzyskiwać dostęp do aplikacji klienckich i serwerów aplikacji, pracujących na serwerach NetWare. Klienci serwerów NetWare mogą korzystać z protokołu NWLink, aby uzyskać dostęp do aplikacji klienckich i serwerów aplikacji, pracujących na serwerach opartych na systemie Windows 2000. Dzięki protokołowi NWLink, komputery pracujące w systemie Windows 2000 mogą komunikować się z innymi urządzeniami sieciowymi, takimi jak drukarki, które korzystają z protokołu IPX/SPX. Protokół NWLink może także zostać wykorzystany w niewielkich sieciach, które korzystają tylko z systemu Windows 2000 i innych systemów klienckich firmy Microsoft.

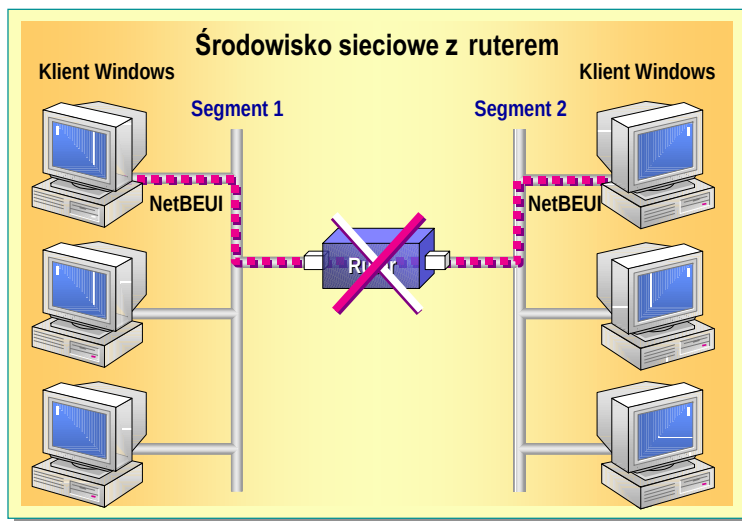
Protokół NetBEUI (NetBIOS Enhanced User Interface)

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje protokół NetBEUI.

Wprowadzenie

Protokół NetBEUI jest obsługiwany przez wszystkie produkty sieciowe firmy Microsoft, wliczając w to system Windows 2000.



Zagadnienie kluczowe

Protokół NetBEUI nie jest rutowalny, ale jest obsługiwany przez wszystkie produkty sieciowe firmy Microsoft, wliczając w to system Windows 2000.

Wskazówka

Skorzystaj z ilustracji umieszczonej na slajdzie, aby wyjaśnić słuchaczom, że protokół NetBEUI umożliwia komunikację pomiędzy dwoma komputerami klienckimi, które pracują w systemie Windows i znajdują się w tym samym segmencie w rutowalnym środowisku sieciowym.

Protokół NetBEUI był jednym z pierwszych protokołów przeznaczonych dla sieci składających się z komputerów osobistych. Protokół ten został zaprojektowany w oparciu o interfejs NetBIOS (Network Basic Input/Output System), dzięki czemu jest niewielkim, efektywnym protokołem, nadającym się do pracy w sieciach LAN, obejmujących od 20 do 200 komputerów, które nie muszą przysyłać danych do innych podsieci.

Obecnie protokół NetBEUI jest wykorzystywany wyłącznie w niewielkich, niewymagających routingu sieciach, zawierających komputery pracujące w różnych systemach operacyjnych.

Wersja protokołu NetBEUI, przeznaczona dla systemu Windows 2000, zwana protokołem NBF (NetBIOS Frame), jest implementacją protokołu NetBEUI, która może zostać zainstalowana na komputerach pracujących w systemie Windows 2000. Zapewnia to kompatybilność z istniejącymi sieciami LAN, w których wykorzystywany jest protokół NetBEUI.

Zalety protokołu NetBEUI:

- Niewielki rozmiar stosu.
- Brak konieczności przeprowadzania konfiguracji.
- Duża prędkość przesyłania danych w sieci.
- Kompatybilność ze wszystkimi systemami operacyjnymi firmy Microsoft, wliczając w to system Windows 2000.

Główną wadą protokołu NetBEUI jest brak obsługi routingu. W związku z tym, komputery wykorzystujące protokół NetBEUI mogą komunikować się tylko z innymi komputerami, znajdującymi się w tym samym segmencie sieci.

Uwaga Interfejs NetBIOS umożliwia aplikacjom uzyskiwanie dostępu do funkcji sieciowych systemu operacyjnego oraz pozwala zarządzać nazwami sieciowymi, wykorzystywanymi do komunikacji w sieci.

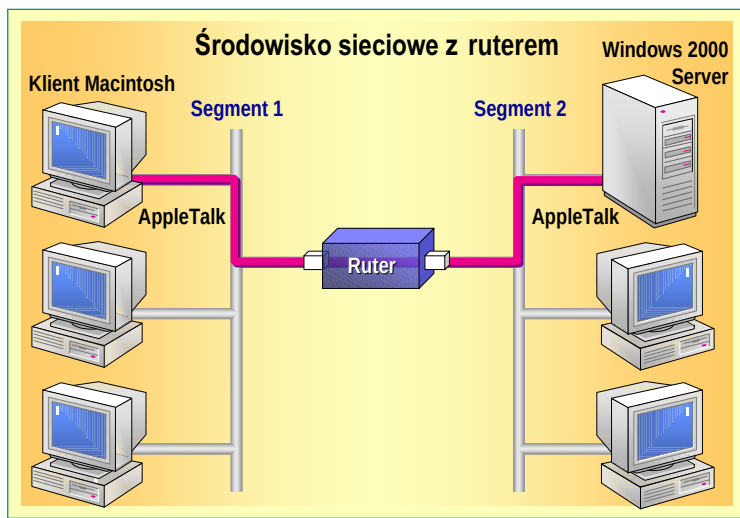
Protokół AppleTalk

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje protokół AppleTalk.

Wprowadzenie

System Windows 2000 obsługuje protokół AppleTalk, który umożliwia ruting i jest przeznaczony do pracy w sieciach Apple Macintosh.



Zagadnienie kluczowe

Protokół AppleTalk obsługuje ruting i jest wykorzystywany w środowisku Apple Macintosh.

Wskazówka

Skorzystaj z ilustracji umieszczonej na slajdzie, aby wyjaśnić słuchaczom, że stos protokołów AppleTalk pozwala komputerom klienckim firmy Macintosh komunikować się z serwerami opartymi na systemie Windows 2000 w rutowalnym środowisku sieciowym.

Stos protokołów AppleTalk jest własnością firmy Apple Computer i został zaprojektowany, aby zapewniać komputerom Apple Macintosh możliwość współdzielenia plików i drukarek w środowisku sieciowym.

Niektóre z właściwości stosu protokołów AppleTalk:

- Stos protokołów AppleTalk pozwala komputerom klienckim firmy Macintosh uzyskiwać dostęp do serwera pracującego w systemie Windows 2000.
- Stos protokołów AppleTalk obsługuje ruting. Korzystające z niego komputery mogą komunikować się pomiędzy segmentami w środowisku sieciowym zawierającym ruter.
- Stos protokołów AppleTalk umożliwia komputerom klienckim firmy Macintosh uzyskiwać dostęp do usług wydruku, na serwerze pracującym w systemie Windows 2000, jeśli zainstalowana została na serwerze usługa Print Server for Macintosh.

◆ Inne protokoły komunikacyjne

Cel slajdu

Przedstawienie innych technologii komunikacyjnych, obsługiwanych przez system Windows 2000.

Wprowadzenie

Oprócz obsługi często używanych protokołów sieciowych, system operacyjny Windows 2000 obsługuje także inne protokoły komunikacyjne i technologie, takie jak ATM oraz IrDA.

- **Protokół ATM (Asynchronous Transfer Mode)**
- **Protokół IrDA (Infrared Data Association)**

Oprócz obsługi większości często stosowanych protokołów sieciowych, system operacyjny Windows 2000 zapewnia także obsługę innych protokołów komunikacyjnych i technologii, takich jak:

- Protokół ATM (Asynchronous Transfer Mode).
- Protokół IrDA (Infrared Data Association).

Zarówno protokół ATM, jak i IrDA wyznaczają międzynarodowe standardy technologii komunikacyjnych. Protokół ATM został opracowany dla potrzeb transmisji z dużą szybkością treści multimedialnych, a protokół IrDA został opracowany dla połączeń bezprzewodowych.

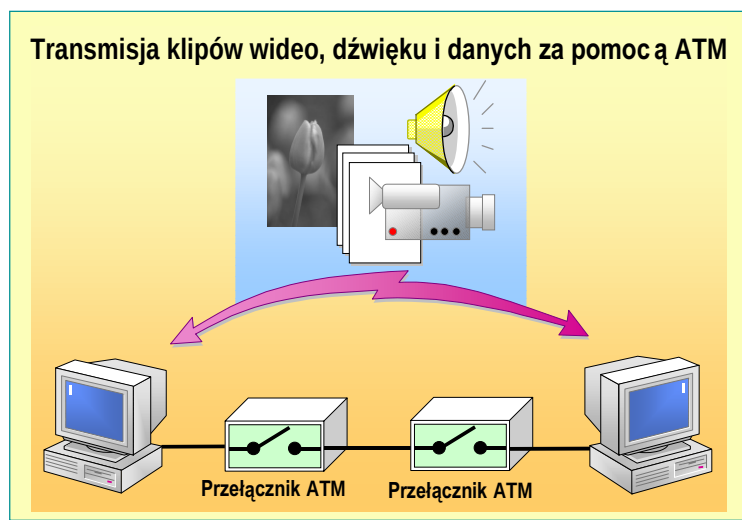
Protokół ATM (Asynchronous Transfer Mode)

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje protokół ATM.

Wprowadzenie

Protokół ATM jest zorientowanym na połączenie protokołem, zapewniającym dużą prędkość transmisji, który umożliwia transport różnych rodzajów informacji w sieci.



Zagadnienie kluczowe

Protokół ATM jest zorientowanym na połączenie protokołem, zapewniającym dużą prędkość transmisji, który umożliwia transport różnych rodzajów informacji w sieci.

Wskazówka

Skorzystaj z ilustracji umieszczonej na slajdzie, aby wyjaśnić słuchaczom, że protokół ATM zapewnia dużą prędkość transmisji aplikacji multimedialnych pomiędzy komputerami w sieci.

Protokół ATM pozwala na przesyłanie z dużą prędkością różnych rodzajów danych w sieci. Technologia ATM została opracowana na bazie międzynarodowych standardów równoległej transmisji danych, dźwięku oraz obrazu wideo z dużą prędkością. Komunikację w sieci z wykorzystaniem protokołu ATM umożliwiają urządzenia zwane przełącznikami ATM. Komputery klienckie komunikują się ze sobą za pomocą przełączników ATM.

Niektóre właściwości protokołu ATM:

- Protokół ATM pozwala jednocześnie przysyłać dźwięk, klipy wideo oraz dane przez pojedyncze połączenie sieciowe. Protokół ATM może równolegle przysyłać dane, pochodzące z różnych źródeł komunikacji elektronicznej, takich jak rozmowy telefoniczne, filmy, wiadomości poczty elektronicznej oraz pliki znajdujące się na serwerze sieci Web.
- Protokół ATM zapewnia dużą prędkość komunikacji.
- Zastosowanie protokołu ATM gwarantuje, że żaden z poszczególnych typów danych nie zajmie w całości linii. Protokół ATM efektywnie przydziela przepustowość pasma sieciowego, przez co zapewnia niezawodność połączenia.

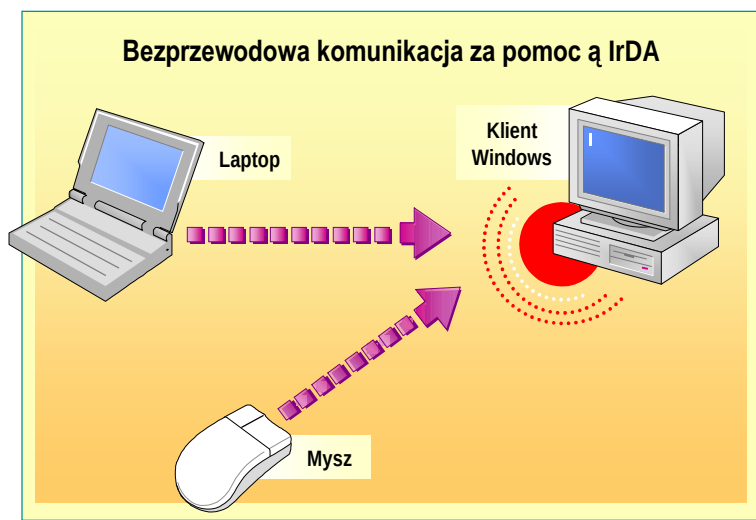
Protokół IrDA (Infrared Data Association)

Cel slajdu

Zilustrowanie sposobu, w jaki funkcjonuje protokół IrDA.

Wprowadzenie

Protokół IrDA umożliwia bezprzewodową komunikację pomiędzy urządzeniami różnego rodzaju, takimi jak kamery, komputery przenośne oraz drukarki.



Stos protokołów IrDA stanowi grupę protokołów, umożliwiających dwukierunkową, bezprzewodową transmisję o dużej prędkości w podczerwieni na niewielką odległość. Stos protokołów IrDA pozwala komputerom pracującym w systemie Windows 2000 łączyć się z urządzeniami peryferyjnymi lub innymi komputerami, bez używania przewodów. System Windows 2000 automatycznie wykrywa urządzenia mające gniazdo na podczerwień, takie jak inne komputery i kamery, które znajdują się w zasięgu. Protokół IrDA umożliwia użytkownikom przesyłanie informacji i współdzielenie zasobów, takich jak drukarki, kamery, komputery przenośne, komputery stacjonarne oraz urządzenia PDA (Personal Digital Assistant).

Protokół IrDA pozwala na bezprzewodową komunikację między dwoma urządzeniami mającymi gniazdo na podczerwień, znajdującymi się w swoim zasięgu. Na przykład, dwaj użytkownicy podróżujący z komputerami przenośnymi, zamiast korzystać z przewodu lub dyskietek, mogą przysyłać pliki, tworząc połączenia IrDA. Protokół IrDA automatycznie skonfiguruje połączenie, kiedy dwa komputery przenośne znajdą się obok siebie. Protokół IrDA pozwala także komputerom uzyskiwać dostęp do zasobów, które są przyłączone do innego komputera. Na przykład, jeśli użytkownik komputera przenośnego chce wydrukować dokument, może utworzyć połączenie IrDA z komputerem, który jest bezpośrednio lub przez sieć podłączony do drukarki. Po utworzeniu połączenia, użytkownik posiadający odpowiednie uprawnienia może wydrukować dokument, przesyłając go przez połączenie IrDA.

Właściwości bezprzewodowej komunikacji IrDA:

- Jest to międzynarodowy standard dla połączeń bezprzewodowych.
- Łatwa implementacja i wykorzystanie.
- Brak zagrożenia ze strony promieniowania podczerwonego.
- Nie wytwarza zakłóceń elektromagnetycznych.
- Brak regulacji rządowych.
- Mała podatność na zakłócenia sygnału ze strony komunikacji przewodowej.

◆ Protokoły zdalnego dostępu

Cel slajdu

Przedstawienie tematów związanych z protokołami zdalnego dostępu.

Wprowadzenie

Dostęp zdalny wymaga protokołów, które umożliwiają uzyskanie połączenia pomiędzy klientem i serwerem. Wybór odpowiedniego protokołu zależy od własnych wymagań.

- Protokoły dial-up

- Protokoły VPN

W systemie Windows 2000 można ustawić połączenie zdalne, poprzez zdalny dostęp typu dial-up lub poprzez wykorzystanie wirtualnych sieci prywatnych VPN (Virtual Private Network). Aby ustawić zdalne połączenie do sieci systemu Windows 2000, można skorzystać z następujących protokołów zdalnego dostępu:

- Protokoły dial-up
- Protokoły VPN

Protokoły zdalnego dostępu, obsługiwane przez system Windows 2000, mogą współpracować ze składnikami zdalnego dostępu firm trzecich. Zrozumienie funkcji poszczególnych protokołów pozwala zdecydować, który protokół jest odpowiedni dla danej sieci.

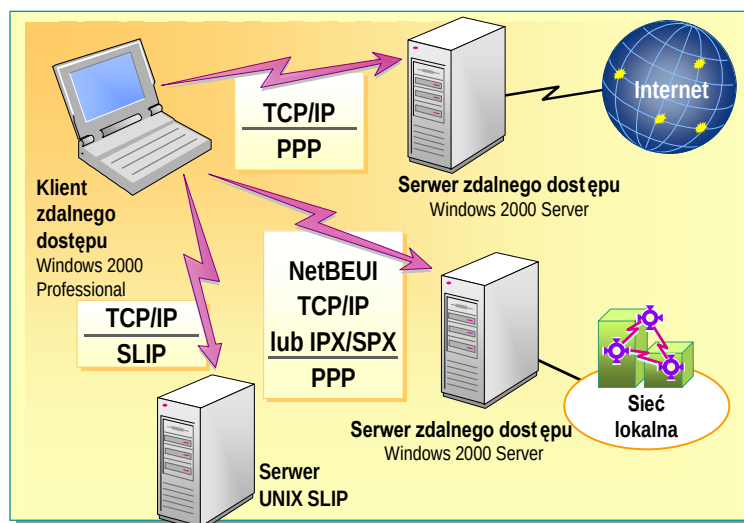
Protokoły dial-up

Cel slajdu

Zilustrowanie sposobu, w jaki protokoły zdalnego dostępu dial-up są wykorzystywane w celu uzyskania zdalnego połączenia klientów z serwerami.

Wprowadzenie

W przypadku połączenia dial-up, można zastosować zarówno protokół SLIP, jak i protokół PPP, aby umożliwić klientom połączenie z różnymi serwerami zdalnego dostępu.



Zagadnienie kluczowe

System Windows 2000 nie zawiera serwera SLIP, ponieważ serwery SLIP są gorzej zabezpieczone i mniej wydajne, niż serwery PPP.

System Windows 2000 obsługuje protokoły zdalnego dostępu dial-up, takie jak SLIP (Serial Line Internet Protocol) oraz PPP (Point-to-Point Protocol), pozwalając klientom łączyć się z różnymi serwerami zdalnego dostępu.

Protokół SLIP

Protokół SLIP umożliwia klientom zdalnego dostępu łączyć się z serwerami zdalnego dostępu poprzez modem. Pozwala to komputerom klienckim, pracującym w systemie Windows 2000, łączyć się z serwerami SLIP. Serwer SLIP jest składnikiem protokołu zdalnego dostępu, który obsługuje żądania połączeń, pochodzące od klientów SLIP. Chociaż komputery klienckie, pracujące w systemie Windows 2000, mogą łączyć się z serwerami SLIP, usługa Routing and Remote Access nie zawiera w sobie składnika serwera SLIP. Dlatego więc, komputer pracujący w systemie Windows 2000 nie może zostać użyty jako serwer SLIP. Zamiast tego, rolę serwera SLIP może pełnić serwer pracujący w systemie UNIX.

Protokół SLIP stanowi przemysłowy standard protokołu, który adresuje połączenia TCP/IP realizowane przez łącze szeregowe. Protokół SLIP jest obsługiwany przez usługę Routing and Remote Access i daje klientom, pracującym w systemie Windows 2000, dostęp do usług internetowych. Protokół SLIP ma następujące ograniczenia:

- Obsługuje tylko protokół TCP/IP. Protokół SLIP nie może bezpośrednio przysyłać innych protokołów sieciowych, takich jak IPX/SPX lub NetBEUI.
- Wymaga statycznego adresu IP. Protokół SLIP wymaga od klienta, aby skonfigurował wszystkie parametry konfiguracji TCP/IP, takie jak adres IP, niezbędne, aby ustanowić połączenie z serwerem.
- Wymaga typowo tekstowych sesji uwierzytelniania logowania oraz systemu obsługi skryptów, w celu zautomatyzowania procesu logowania.
- Wysyła hasła uwierzytelniania jawnym tekstem. Może to spowodować obniżenie poziomu bezpieczeństwa, ponieważ hasła nie są szyfrowane w procesie uwierzytelniania użytkownika.

Protokół PPP

Stos protokołów PPP to zgodny z przemysłowymi standardami zestaw protokołów, umożliwiający klientom i serwerom zdalnego dostępu pracę w sieci zawierającej składniki wyprodukowane przez różnych producentów. Protokół PPP, będący rozszerzeniem oryginalnej specyfikacji SLIP, obsługuje szyfrowany proces uwierzytelniania i jest standardową metodą wysyłania danych w sieci poprzez połączenie punkt-punkt.

Obsługa stosu protokołów PPP umożliwia komputerom pracującym w systemie Windows 2000 łączyć się ze zdalnymi sieciami poprzez dowolny serwer, który spełnia standard PPP. Zgodność ze standardem PPP pozwala również serwerom na odbieranie połączeń oraz zapewnia dostęp do oprogramowania zdalnego dostępu innych producentów.

Architektura stosu protokołów PPP pozwala klientom korzystać z dowolnej kombinacji protokołów transportowych, takich jak NetBEUI, TCP/IP oraz IPX/SPX. Można uruchamiać aplikacje napisane zgodnie z wymogami stosu protokołów IPX/SPX, NetBIOS lub interfejsu WinSock (Windows Sockets) na komputerach zdalnych pracujących w systemie Windows 2000. Architektura stosu protokołów PPP umożliwia serwerom pobierać i konfigurować parametry TCP/IP.

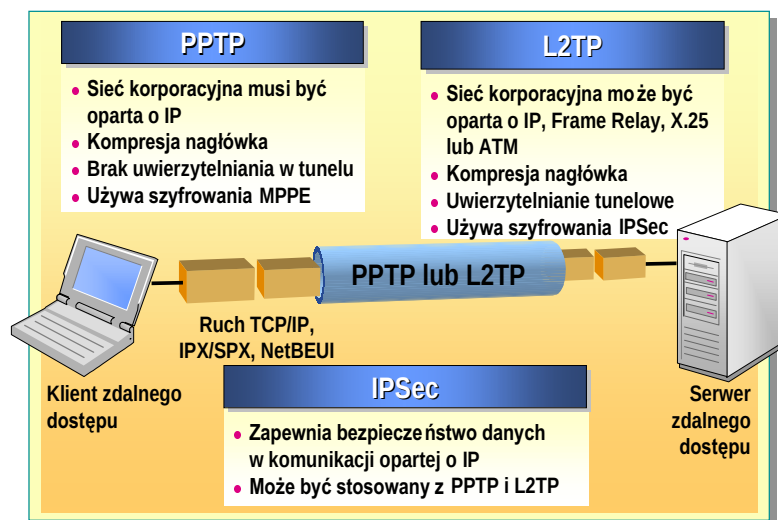
Protokoły VPN

Cel slajdu

Przedstawienie funkcji protokołów VPN, wykorzystywanych przez klientów i serwery zdalnego dostępu.

Wprowadzenie

Wirtualne sieci prywatne VPN pozwalają uzyskać zdalny dostęp, bez wykorzystania specjalnych urządzeń, poprzez użycie dodatkowych protokołów, które umożliwiają użytkownikom łączenie się z sieciami LAN przez ich dotychczasowe połączenia internetowe lub dial-up.



Wskazówka

Slajd dla tego tematu zawiera animację. Na początku wyświetli samą ilustrację, a następnie w trakcie omawiania wyświetlaj po kolei opis funkcji protokołów PPTP i L2TP oraz szyfrowania IPSec.

Zagadnienie kluczowe

W sieciach VPN pakiety danych są umieszczane wewnątrz zaszyfrowanych pakietów PPP.

Mechanizm wirtualnych sieci prywatnych VPN pozwala realizować połączenia z serwerami zdalnego dostępu, bez konieczności korzystania ze specjalnego sprzętu realizującego połączenia telefoniczne, takiego jak modemy. Sieci VPN korzystają z dodatkowych protokołów, które pozwalają użytkownikom połączyć się z sieciami LAN przez ich dotychczasowe połączenie z Internetem lub połączenie dial-up. Połączenia takie mogą być bezpieczne, nawet jeśli odbywają się za pośrednictwem sprzętu, stanowiącego element Internetu.

Protokoły VPN hermetyzują pakiety danych protokołów TCP/IP, IPX/SPX lub NetBEUI wewnątrz pakietów protokołu PPP. Serwer zdalnego dostępu, z pomocą klienta realizuje zadania zabezpieczania i uwierzytelniania oraz umożliwia szyfrowanie danych, czyniąc bezpiecznym przesyłanie danych przez niebezpieczne sieci, takie jak Internet. Zazwyczaj użytkownicy uzyskują połączenie z serwerem VPN, łącząc się najpierw z dostawcą usług internetowych, a później uzyskując dostęp do portów VPN przez połączenie z Internetem.

W sieciach VPN połączenie nawiązuje się za pomocą protokołu PPTP (Point-to-Point Tunneling Protocol) albo protokołu L2TP (Layer Two Tunneling Protocol).

Protokół PPTP (Point-to-Point Tunneling Protocol)

Protokół PPTP umożliwia bezpieczne przesyłanie hermetyzowanych danych od klienta PPTP do serwera PPTP przez sieć TCP/IP, taką jak Internet. Na czas transmisji przez sieć TCP/IP, protokół PPTP hermetyzuje ramki PPP w pakietach TCP/IP. Dzięki hermetyzacji możliwe staje się wykorzystanie wszystkich funkcji protokołu PPP, wliczając w to obsługę protokołów TCP/IP, IPX/SPX, NetBEUI oraz szyfrowanie MPPE (Microsoft Point-to-Point Encryption) w wirtualnych sieciach prywatnych opartych na protokole PPTP.

System Windows 2000 obsługuje protokół PPTP, który może zostać wykorzystany w prywatnej komunikacji między sieciami LAN.

Protokół L2TP (Layer Two Tunneling Protocol)

Protokół L2TP jest przemysłowym standardem protokołu tunelowego. Podobnie jak protokół PPTP, protokół L2TP wykorzystuje uwierzytelnianie i mechanizm kompresji protokołu PPP. W przeciwieństwie do protokołu PPTP, protokół L2TP nie korzysta z szyfrowania MPPE, aby zaszyfrowywać ramki PPP. Zamiast tego protokół L2TP wykorzystuje usługę szyfrowania IPSec (Internet Protocol Security). W rezultacie wirtualna sieć prywatna, oparta o połączenie L2TP, jest zazwyczaj kombinacją protokołu L2TP i usługi szyfrowania IPSec. Aby móc korzystać z zaszyfrowanych wirtualnych sieci prywatnych L2TP, zarówno klient, jak i serwer muszą obsługiwać protokół L2TP i usługę szyfrowania IPSec.

Protokół L2TP pozwala szyfrować i przesyłać pakiety protokołów TCP/IP, IPX/SPX oraz NetBEUI poprzez dowolne medium, obsługujące dostarczanie pakietów w trybie punkt-punkt, takie jak: Ethernet, X.25, Frame Relay czy ATM.

Szyfrowanie IPSec

Szyfrowanie IPSec gwarantuje bezpieczeństwo danych w komunikacji opartej o protokół TCP/IP, zapewniając dodatkową warstwę bezpieczeństwa sieciowego. Szyfrowanie IPSec integruje się z zabezpieczeniami wchodzącymi w skład systemu Windows 2000, chroniąc komunikację w sieci intranet i Internet. Protokoły sieci VPN, czyli protokoły PPTP oraz L2TP, mogą zostać połączone z zabezpieczeniami dostarczonymi przez szyfrowanie IPSec, aby zapewnić bezpieczeństwo danych.

Szyfrowanie IPSec zapewnia integralność i szyfrowanie danych. Jest to rozwiązanie lepsze, niż w przypadku protokołu PPTP, który stosuje szyfrowanie MPPE. Korzystanie z szyfrowania IPSec powoduje wzrost zapotrzebowania na zasoby procesora zarówno klienta, jak i serwera oraz zwiększa obciążenie sieci.

Laboratorium A: Określanie właściwości protokołu

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

Realizacja tego laboratorium polega na określaniu, które protokoły mogą zostać użyte do komunikacji z innymi komputerami, znajdującymi się w innym segmencie oraz rozróżnianiu typów transmisji, realizowanych przez komputery w sieci.



Objaśnij cele laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Określić, które protokoły są wykorzystywane, aby umożliwić komunikację z komputerami znajdującymi się w innym segmencie sieci.
- Określić różne typy transmisji, realizowane przez komputery w sieci.

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.
- Minimalna rozdzielczość ekranu 800 x 600 przy 256 kolorach. (zalecane 16-bit).
- Przeglądarka Microsoft Internet Explorer 5 lub nowsza.

► Aby rozpocząć 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 **Określanie właściwości protokołu**.
5. Przeczytaj informacje wprowadzające, a następnie kliknij odpowiednie łącze, 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 tematu protokołów
- Protokoły i przesyłanie danych
- Podstawowe protokoły
- Inne protokoły komunikacyjne
- Protokoły zdalnego dostępu

-
1. Chcesz zmienić używany obecnie protokół, aby lepiej dostosować się do potrzeb sieci. Zdajesz sobie sprawę, że możesz w tym celu użyć protokołu otwartego. Który z przedstawionych poniżej protokołów wybierzesz?
A. IPX/SPX.
B. AppleTalk.
C. NetBEUI.
D. TCP/IP.
D. TCP/IP.

 2. Użytkownikom w Twojej sieci potrzebna jest możliwość prowadzenia działalności przez Internet. Który z protokołów zainstalujesz w sieci, aby pozwolić użytkownikom komunikować się poprzez Internet?
A. IPX/SPX.
B. TCP/IP.
C. AppleTalk.
D. NetBEUI.
B. TCP/IP.

-
3. Masz niewielką grupę roboczą, w której używany jest system Windows 2000 oraz inne systemy operacyjne firmy Microsoft. Musisz zainstalować protokół, który wymaga minimalnej konfiguracji. Który protokół zainstalujesz?
- A. IPX/SPX.
 - B. TCP/IP.
 - C. AppleTalk.
 - D. NetBEUI.
 - D. NetBEUI.**
4. Musisz mieć możliwość przesyłania jednocześnie dużej ilości danych dźwiękowych, klipów wideo oraz plików danych przez sieć. Który z przedstawionych poniżej protokołów umożliwia transmisję tych danych z dużą prędkością?
- A. ATM.
 - B. TCP/IP.
 - C. IrDA.
 - D. NetBEUI.
 - A. ATM.**
5. Chcesz uruchomić serwer oparty na systemie Windows 2000, umożliwiający klientom uzyskiwanie zdalnego połączenia z nim przez protokół SLIP lub PPP. Czy możesz to zrobić? Jeśli tak, to czy wymaga to konfiguracji?
- A. Tak. Konfiguracja w procesie instalacji jest automatyczna.
 - B. Tak, możesz to zrobić bez dodatkowej konfiguracji.
 - C. Nie, ponieważ system Windows 2000 nie może być serwerem SLIP.
 - D. Nie, ponieważ system Windows 2000 nie może być serwerem PPP.
 - C. Nie, ponieważ system Windows 2000 nie może być serwerem SLIP.**

