Analiza protokołu TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) w systemie Microsoft® Windows® 2000 jest standardowym, rutowalnym 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, skalowaną 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.

Wprowadzenie do TCP/IP

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 role 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

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

Warstwa aplikacji

Warstwa aplikacji jest najwyższą warstwa 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 (Hyper text 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 dostarczania 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

Adres IP, Port TCP/UDP, Gniazdo

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 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 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

Stos protokołów 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)

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 komunikacje,, 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 nawiązuje 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 informacje sesyjną.
3. Komputer źródłowy zgadza się i wysyła potwierdzenie odebranych informacji.

UDP (User Datagram Protocol)

Protokół UDP (User Datagram Protocol) jest protokołem warstwy transportowej identyfikującym aplikację docelową w komunikacji sieciowej. Protokół UDP oferuje bezpołączeniową usługę transportową umożliwiającą szybką, 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 multimisją(multicast). Jest on również używany do przesyłania małych ilości danych lub danych, które nie są bardzo ważne. Multiemisyjny 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.

Protokół IP (Internet Protocol)

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 rutera.

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.

Protokół ICMP (Internet Control Message Protocol)

Protokół ICMP (Internet Control Message Protocol) oferuje możliwość rozwiązywania problemów oraz wysyłania komunikatów o błędach, w przypadku niedostarczenia pakietów. Dzięki protokołowi ICMP, komputery i rutery 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 ruterami 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 żądają 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.

Protokół IGMP (Internet Group Management Protocol)

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.

Protokół ARP (Address Resolution Protocol)

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

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

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 podłączenie 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.

US (Internet Information Services): US 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 konflgurację TCP/IP własnego komputera, należy użyć *pętli zwrotnej* (loopback). Pętla zwrotna ma adres IP 127.0.0.1. Aby sprawdzić konflgurację systemu za pomocą pętli zwrotnej, należy wpisać ping 127.0.0.1)

Rozwiązywanie nazw

Protokół TCP/IP identyfikuje komputery źródłowe i docelowe poprzez ich adresy IP. Jednakże, użytkownicy znacznie łatwiej zapamiętają 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

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 nazwa 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

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 adresy 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 i Lmhosts

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 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

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 zmienią, 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

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 nazwa 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, *7.* 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 powyższa metody NetBIOS nie rozwiążą nazwy, komputer A sprawdza plik Hosts.
7. Ostatecznie, komputer A zapytuje serwer DNS.

Badanie procesu przesyłania 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 wysyłać 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 przesyłać 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 warstwic 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

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 jest związany z transmisją za pomocą protokołu TCP. Zawiera nagłówek TCP, dodany do danych aplikacji.
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 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 jest związana z transmisją na warstwie interfejsu sieciowego i składa się z nagłówka dodanego na warstwie interfejsu sieciowego i danych z warstwy IP.

Elementy ramki

Ramka (określenie pakietu danych na warstwie interfejsu sieciowego) składa się z trzech elementów: nagłówka, danych oraz pola weryfikacji.
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 informacje kontroli poprawności ramki, zwaną sumą kontrolna *CRC (Cyclical Redundancy Check).* CRC jest liczbą obliczana 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

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.
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 sumą 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 aplikacje, są one dalej przetwarzane w specyficzny dla aplikacji sposób.

Ruting danych

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 rutera, który przekazuje pakiety do miejsca przeznaczenia.
W sekcji tej wyjaśniono znaczenie protokołu IP w procesie rutingu oraz opisano proces transmisji danych przez rutery.

Ruting 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 opakowuje pakiet IP do postaci ramki dla warstwy interfejsu sieciowego i adresuje pakiet na adres MAC rutera.

Tabela rutingu

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

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

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

Przesyłanie danych przez rutery

Protokół IP pełni ważną role w przesyłaniu danych w sieciach korporacyjnych. Pakiety IP są wymieniane i przetwarzane w każdym węźle: na warstwie internetowej komputera źródłowego, na ruterach 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 rutingu, w celu znalezienia drogi do zdalnego komputera. Jeśli znajdzie drogę, wysyła nią pakiety. W przeciwnym razie, przesyła pakiety do domyślnego rutera.

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 rutera, do którego pakiet zostanie przekazany.