Systemy IBM - iSeries

Sieci
Konfigurowanie TCP/IP

Wersja 5 Wydanie 4

Systemy IBM - iSeries

Sieci
Konfigurowanie TCP/IP

Wersja 5 Wydanie 4

Uwaga

Przed wykorzystaniem tych informacji i produktu, którego dotyczą, należy przeczytać informacje zawarte w dodatku “Uwagi”, na stronie 43.

Wydanie ósme (luty 2006)

Niniejsze wydanie dotyczy Wersji 5, Wydania 4, Modyfikacji 0 systemu operacyjnego i5/OS (numer produktu 5722–SS1) i wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie będzie wskazane inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Konfigurowanie TCP/IP

Serwer został dostarczony i można przystąpić do jego uruchomienia. Ten artykuł zawiera opis narzędzi i procedur potrzebnych do skonfigurowania TCP/IP w systemie i5/OS.

Informacje te mogą być potrzebne, na przykład podczas tworzenia opisu linii, interfejsu TCP/IP oraz trasy. Należy zapoznać się ze sposobem dostosowania konfiguracji TCP/IP przy użyciu programu iSeries Navigator oraz zaznajomić się z różnymi technikami TCP/IP, dzięki którym można kierować przepływem danych w sieci.

Przed wykorzystaniem tych informacji do skonfigurowania TCP/IP należy zapoznać się z sekcją Instalacja i używanie sprzętu, aby mieć pewność, że cały potrzebny sprzęt został zainstalowany. Po zakończeniu czynności początkowych związanych z konfigurowaniem TCP/IP można przystąpić do rozszerzania możliwości serwera przy użyciu aplikacji TCP/IP, protokołów i usług zgodnie z własnymi potrzebami.

Co nowego w wersji V5R4

Wymieniono tu zmiany wprowadzone w zestawie tematów dotyczących wersji V5R4.

Rozszerzenie obsługi IPv6

Nowe funkcje protokołu IPv6 (Internet Protocol version 6) są spójne na poziomie produktu ze swoimi odpowiednikami w protokole IPv4.

Protokół IPv6 jest obsługiwany przez następujące funkcje:

- Pętla zwrotna
- Wszystkie adaptery Ethernet (10/100 Mb/s, 1 Gb/s i 10 Gb/s)
- Wirtualna sieć Ethernet między partycjami

Wiele z adapterów Ethernet może być używanych równocześnie z protokołem IPv6.

Protokół IPv6 obsługuje następujące funkcje:

- Adres grupowy
- Fragmentacja i reasemblacja
- Rozszerzenia podstawowych pojęć gniazd (RFC 3494)

Konfigurowanie IPv6

- Działania Uruchomienie i Zakończenie pracy TCP/IP folderu **Konfigurowanie TCP/IP** zostały usunięte.
- Protokół IPv6 może być uruchamiany i zatrzymywany w ten sam sposób co protokół IPv4, czyli za pomocą komend Uruchomienie TCP/IP (Start TCP/IP - STRTCP) oraz Zakończenie pracy TCP/IP (End TCP/IP - ENDTCP). Protokół IPv6 nie może zostać uruchomiony lub zatrzymany niezależnie od protokołu IPv4.
- Interfejs pętli zwrotnej IPv6 ::1 jest tworzony domyślnie w sposób automatyczny podczas uruchamiania protokołu TCP/IP.
- Kreator konfigurowania protokołu IPv6 został usunięty.
- Użyj nowego interfejsu, aby skonfigurować bezstanowe autokonfigurowanie adresu.
- W podobny sposób możesz wykorzystywać nowy kreator w celu tworzenia interfejsów IPv6.
- Funkcje konfigurowania, uruchamiania, zatrzymywania i usuwania linii zostały dodane do menu kontekstowego ekranu Bezstanowe autokonfigurowanie adresu IPv6 (IPv6 Stateless Address Autoconfig).

Aliasy

Zarówno w protokole IPv4 , jak i IPv6 można teraz używać aliasów. Można określać nazwę identyfikującą interfejs IPv4 lub IPv6, zamiast używać notacji dziesiętnej z kropkami. Aliasy interfejsów mogą być konfigurowane za pomocą obydwu komend CL oraz programu iSeries Navigator.

Lista preferowanych interfejsów

Można utworzyć listę preferowanych interfejsów, aby kontrolować, które adaptery i adresy IP będą stanowiły preferowany interfejs agentów ARP proxy wirtualnego adresu IP. Jest to dostępne dla obu wirtualnych adresów IP oraz wirtualnej sieci Ethernet.

Co się zmieniło w wersji V5R4

Tunele nie są już obsługiwane przez IPv6:

- IPv6, IPv4 oraz protokół PPPoE (Point-to-Point Protocol over Ethernet) mogą być używane na tym samym adapterze.
- Routery sieciowe mogą być używane do wysyłania pakietów IPv6 w sieci IPv4.

Konfiguracja IPv6 z poprzednich wydań nie zostanie przeniesiona do wersji V5R4.

W jaki sposób wyróżnione są nowości i zmiany

W celu wyróżnienia wykonanych zmian technicznych w tej publikacji użyto:

- symbolu » który wskazuje początek nowej lub zmienionej informacji.
- symbolu «, który wskazuje koniec nowej lub zmienionej informacji.

Inne informacje na temat nowości i zmian w tym wydaniu znajdują się w dokumencie Informacje dla użytkowników.

Drukowanie plików PDF i podręczników

Informacje dotyczące przeglądania i drukowania tych informacji w formacie PDF.

Aby przejrzeć lub pobrać ten dokument w wersji PDF, wybierz Konfigurowanie TCP/IP (około 362 kB).

Można przeglądać lub pobierać następujące tematy pokrewne:

- Planowanie i konfigurowanie ochrony systemu na serwerzeiSeries (2.8 MB)
  - Planowanie podstawowej ochrony systemu w celu zabezpieczenia serwera iSeries i dołączonych operacji
  - Konfigurowanie ochrony systemu
- Rozwiązywanie problemów dotyczących protokołu TCP/IP (920 KB)
  - Rozwiązywanie problemów z połączeniami TCP/IP lub ruchem zarówno w sieci IPv4, jak i IPv6

Inne informacje

Można również przejrzeć lub pobrać następujące pliki PDF:

- Dokumentacja techniczna IBM Redbooks:
  - **TCP/IP Tutorial and Technical Overview** (7 MB) Ta dokumentacja techniczna IBM Redbook zawiera podstawowe informacje na temat protokołu TCP/IP.
  - **TCP/IP for AS/400: More Cool Things Than Ever** (9 MB) Ta dokumentacja techniczna IBM Redbook zawiera szczegółową listę typowych aplikacji i usług TCP/IP.

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego dalszego wykorzystania:

1. W przeglądarce kliknij prawym przyciskiem myszy plik PDF (kliknij prawym przyciskiem myszy powyższy odsyłacz).
2. Kliknij opcję lokalnego zapisywania pliku PDF.
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Kopię programu można pobrać z serwisu WWW Adobe (www.adobe.com/products/acrobat/readstep.html) .

Protokół IPv6

Protokół IPv6 odegra ważną rolę w przyszłości sieci Internet. Obecnie można jej już używać na serwerze iSeries. Temat ten przedstawia ogólne informacje o protokole IPv6 i jego implementacji na serwerze.

Protokół IPv6 jest aktualizacją wersji IPv4 protokołu i jako standard internetowy stopniowo zastępuje wersję poprzednią.

Poniższe tematy zawierają podstawowe informacje o protokole IPv6 i o tym, jak z niego korzystać na serwerze iSeries.

Co to jest protokół IPv6

Powody wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyści użytkowania nowego protokołu.

Protokół IPv6 jest nowszą, udoskonaloną wersją protokołu IP. W przeważającej części Internetu od ponad 20 lat używany jest protokół IPv4, który jest niezawodny i elastyczny. Ma on jednakże pewne ograniczenia, które w związku z rozwojem Internetu powodują wiele problemów.

Przede wszystkim jest to kurcząca się przestrzeń adresów IPv4, potrzebnych wszystkim nowym urządzeniom podłączanym do Internetu. Kluczem do sukcesu IPv6 jest rozszerzenie przestrzeni adresowej adresu IP z 32 do 128 bitów, co umożliwia tworzenie wirtualnie niemal nieograniczonej liczby unikalnych adresów IP. Format tekstowy nowego adresu IPv6 to:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

gdzie każdy znak x oznacza 4-bitową cyfrę w zapisie szesnastkowym.

Możliwość rozszerzenia zakresu adresów w protokole IPv6 rozwiązuje problem braku przestrzeni adresowej w dotychczasowym rozwiązaniu. Jest to szczególnie ważne, gdyż coraz więcej osób korzysta z komputerów przenośnych, takich jak telefony przenośne czy komputery kieszonkowe. Do kurczenia się zasobów adresów IPv4 przyczynia się także rosnące zapotrzebowanie na te adresy ze strony użytkowników sieci bezprzewodowych. Rozszerzenie zakresu adresów IP w protokole IPv6 dostarcza wystarczającej liczby adresów IP dla rosnącej liczby urządzeń bezprzewodowych.

Oprócz możliwości związanych z adresowaniem, protokół IPv6 udostępnia nowe funkcje, upraszczające konfigurowanie i zarządzanie adresami w sieci. Konfiguracja i pielęgnacja sieci to trudna praca. Protokół IPv6 pozwala zmniejszyć obciążenie poprzez zautomatyzowanie niektórych zadań administratora sieci.

Używając IPv6, podczas zmiany dostawcy usług internetowych, nie trzeba zmieniać adresów urządzeń. Zmiana adresów urządzeń jest to ważny wbudowany element protokołu IPv6, który wykonywany jest głównie w sposób automatyczny. Druga część adresu IPv6 pozostanie niezmieniona, ponieważ tradycyjnie jest to część MAC adresu

adaptera Ethernet. Nowy przedrostek IPv6 zostanie przypisany przez dostawcę usług internetowych, a następnie rozprowadzony wśród wszystkich końcowych hostów poprzez aktualizację routerów IPv6 w sieci oraz zezwolenie na ponowne ″nauczenie się″ nowego prefiksu za pomocą bezstanowego autokonfigurowania protokołu IPv6.

Trasy domyślne oraz adresy interfejsów zostaną skonfigurowane automatycznie za pomocą opcji bezstanowego autokonfigurowania IPv6. W autokonfigurowaniu bezstanowym protokół IPv6 składa część adresu MAC maszyny oraz przedrostek sieciowy dostarczany przez lokalny router i na ich podstawie tworzy nowy unikalny adres IPv6. Dzięki tej opcji nie ma potrzeby stosowania protokołu DHCP serwera.

Pojęcia pokrewne

"Dostępne funkcje protokołu IPv6"
Opis implementacji protokołu IPv6 na serwerze iSeries.

Odsyłacze pokrewne

"Informacje związane z protokołem IPv6" na stronie 17
Odsyłacze do zasobów pomocnych w zrozumieniu protokołu IPv6.

Dostępne funkcje protokołu IPv6

Opis implementacji protokołu IPv6 na serwerze iSeries.

Firma IBM zaimplementowała protokół IPv6 w kilku wersjach oprogramowania serwera iSeries. Funkcje IPv6 są przezroczyste dla istniejących aplikacji TCP/IP i współistnieją z funkcjami IPv4.

Najważniejsze opcje serwera iSeries, na które ma wpływ protokół IPv6:

- **Konfigurowanie**

  Podając wartość parametru Uruchomienie IPv6 (Start IPv6 - STRIP6) komendy Uruchomienie TCP/IP (Start TCP/IP - STRTCP), można opcjonalnie uruchamiać protokół IPv6 podczas uruchamiania protokołu TCP/IP. Domyślną wartością parametru Uruchomienie IPv6 (Start IPv6 - STRIP6) komendy Uruchomienie TCP/IP (Start TCP/IP - STRTCP) jest *YES.

  Po skonfigurowaniu protokołu IPv6, pakiety IPv6 są wysyłane w sieci IPv6. Scenariusz opisujący konfigurowanie protokołu IPv6 w sieci znajduje się w sekcji "Tworzenie sieci lokalnej IPv6" na stronie 5.

  Elementy menu Uruchom i Zatrzymaj zostały usunięte z folderu **Konfigurowanie TCP/IP**. Protokół IPv6 może być uruchamiany i zatrzymywany w ten sam sposób co protokół IPv4 czyli za pomocą komend STRTCP i ENDTCP. Protokół IPv6 nie może zostać uruchomiony lub zatrzymany niezależnie od protokołu IPv4.

  Kreator konfigurowania protokołu IPv6 został usunięty z programu iSeries Navigator. Opcje konfiguracji linii kreatora zostały zastąpione przez działania na indywidualnych liniach w folderze **Linie**. W podobny sposób można wykorzystywać nowy kreator w celu tworzenia interfejsów IPv6. Więcej informacji na temat konfigurowania sieci dla protokołu IPv6 znajduje się w sekcji "Konfigurowanie IPv6" na stronie 22.

- **Gniazda**

  Projektowanie i testowanie aplikacji używających gniazd z wykorzystaniem narzędzi i funkcji API IPv6. Protokół IPv6 rozszerza pojęcie gniazd, więc aplikacje mogą używać IPv6 korzystając z nowej rodziny adresów AF_INET6. Rozszerzenia te nie mają wpływu na istniejące aplikacje IPv4. Można tworzyć aplikacje wykorzystujące współbieżnie ruch IPv4 i IPv6 lub jedynie ruch IPv6.

- **System DNS**

  System nazw domen (Domain Name System - DNS) obsługuje adresy AAAA i nową domenę przeznaczoną do wyszukiwania wstecz: IP6.ARPA. System DNS otrzymuje informacje IPv6, jednak serwer musi do komunikacji z DNS używać IPv4.

- **Rozwiązywanie problemów dotyczących protokołu TCP/IP**

  Do rozwiązywania problemów z sieciami IPv6 należy używać standardowych narzędzi, takich jak PING, netstat, śledzenie trasy czy śledzenie komunikacji. Obecnie wszystkie te narzędzia obsługują format adresów IPv6. Aby znaleźć rozwiązanie problemów z siecią IPv4 i IPv6, warto zapoznać się z sekcją Rozwiązywanie problemów dotyczących protokołu TCP/IP.

Pojęcia pokrewne

“Co to jest protokół IPv6” na stronie 3
Powody wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyści użytkowania nowego protokołu.

Odsyłacze pokrewne

“Informacje związane z protokołem IPv6” na stronie 17
Odsyłacze do zasobów pomocnych w zrozumieniu protokołu IPv6.

Scenariusz: używanie protokołu IPv6

Przykłady, które pomogą zrozumieć, kiedy można zastosować protokół IPv6 w celach biznesowych oraz w jaki sposób konfigurować sieć.

Uwaga: W scenariuszu adresy IP x:x:x:x:x:x:x:x reprezentują adresy segmentowe IP. Wszystkie użyte w scenariuszu adresy są tylko przykładami.

Pojęcia pokrewne

“Konfigurowanie IPv6” na stronie 22
Instrukcje zawarte w tym temacie dotyczą konfigurowania serwera dla funkcji IPv6. Korzyści płynące z możliwości rozszerzonego adresowania i opcje związane ze stabilnością tego protokołu IP.

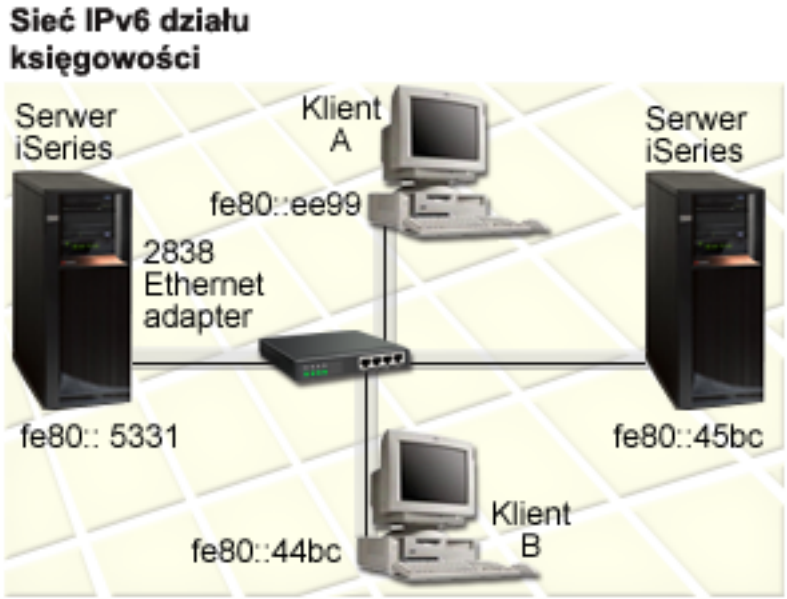
“Pojęcia: IPv6” na stronie 6
Podstawowe pojęcia związane z protokołem IPv6. Jeśli nie ma pewności co do tego, jakie są różnice pomiędzy protokołami IPv4 i IPv6, należy przejrzeć szczegółowe porównania, na przykład dotyczące sposobu adresowania czy nagłówków pakietów.

Tworzenie sieci lokalnej IPv6

Scenariusz opisuje sposób tworzenia lokalnej sieci IPv6.

Opis sytuacji

Protokół IPv6 zastąpi w przyszłości w Internecie protokół IPv4. Dlatego też przedsiębiorstwo podjęło decyzję o zaimplementowaniu protokołu IPv6 w operacjach finansowych i zakupiło nowy system księgowy, używający do łączności protokołu IPv6. Aplikacja musi być połączona z inną instancją aplikacji, znajdującą się na innym serwerze połączonym z lokalną siecią Ethernet. Twoim zadaniem jest taka konfiguracja serwera dla protokołu IPv6, aby firma mogła korzystać z programu księgowego. Rysunek przedstawia konfigurację sieci stworzonej na potrzeby scenariusza.



Rozwiązanie

Aby utworzyć sieć LAN IPv6 należy skonfigurować opis linii Ethernet. Pakiety IPv6 poruszają się pomiędzy serwerami iSeries i klientami w sieci, kiedy pracownicy korzystają z programu księgowego.

Wymagania konfiguracji obejmują:

- i5/OS Wersja 5 Wydanie 4
- Program iSeries Access for Windows and iSeries Navigator (komponent sieciowy programu iSeries Navigator)
- Serwer powinien mieć skonfigurowany protokół TCP/IP oraz adres IPv4, ponieważ protokół IPv6 musi zostać skonfigurowany za pomocą programu iSeries Navigator. Obecnie program iSeries Navigator łączy się z internetem tylko za pomocą protokołu IPv4. Jeśli serwer nie został jeszcze skonfigurowany dla protokołu IPv4, przed skonfigurowaniem protokołu IPv6 na serwerze należy zapoznać się z sekcją Pierwsze konfigurowanie protokołu TCP/IP.

Konfigurowanie

Aby skonfigurować IPv6, należy użyć programu iSeries Navigator. Protokół IPv6 można konfigurować tylko z programu iSeries Navigator, nie można tego zrobić za pomocą interfejsu znakowego.

Należy uruchomić stos IPv6 za pomocą parametru STRIP6 (*YES) komendy STRTCP. Następnie należy wykorzystać działania na indywidualnych liniach w folderze **Linie**, aby określić opcje konfiguracji linii. Informacje na temat automatycznego konfigurowania adresów IPv6 za pomocą programu iSeries Navigator znajdują się w sekcji “Konfigurowanie bezstanowego autokonfigurowania adresu IPv6” na stronie 23.

Pojęcia: IPv6

Podstawowe pojęcia związane z protokołem IPv6. Jeśli nie ma pewności co do tego, jakie są różnice pomiędzy protokołami IPv4 i IPv6, należy przejrzeć szczegółowe porównania, na przykład dotyczące sposobu adresowania czy nagłówków pakietów.

Pojęcia pokrewne

“Scenariusz: używanie protokołu IPv6” na stronie 5
Przykłady, które pomogą zrozumieć, kiedy można zastosować protokół IPv6 w celach biznesowych oraz w jaki sposób konfigurować sieć.

Formaty adresów protokołu IPv6

Wielkość i format adresu protokołu IPv6 rozwijają możliwości adresowania.

Wielkość adresu IPv6 wynosi 128 bitów. Preferowana reprezentacja adresu IPv6 to: x:x:x:x:x:x:x:x, gdzie x jest wartością szesnastkową ośmiu 16-bitowych fragmentów adresu. Adresy IPv6 są z zakresu od 0000:0000:0000:0000:0000:0000:0000:0000 do ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Oprócz preferowanego formatu, adresy IPv6 można podawać w dwóch innych, skróconych formatach:

Z pominięciem zer wiodących
Adresy IPv6 podawane z pominięciem zer wiodących. Na przykład adres 1050:0000:0000:0000:0005:0600:300c:326b można zapisać jako 1050:0:0:0:5:600:300c:326b.

Z podwójnym dwukropkiem
Adresy IPv6 podawane z użyciem podwójnego dwukropka (::) w miejsce serii zer. Na przykład adres ff06:0:0:0:0:0:0:c3 można zapisać jako ff06::c3. Podwójnych dwukropków można w danym adresie IP użyć tylko raz.

Alternatywny format adresów IPv6 stanowi połączenie notacji z kropkami i z dwukropkami, co umożliwia wbudowanie adresu IPv4 w adres IPv6. Wartości szesnastkowe są podawane dla położonych najbardziej na lewo 96 bitów, a wartości dziesiętne dla położonych najbardziej na prawo 32 bitów wskazując wbudowany adres IPv4. Format taki zapewnia zgodność pomiędzy węzłami IPv6 i IPv4 w trakcie pracy w mieszanym środowisku sieciowym.

Adres IPv6 odwzorowany na protokole IPv4 wykorzystuje format alternatywny. Ten typ adresu jest używany do reprezentowania węzłów IPv4 jako adresów IPv6. Umożliwia bezpośrednią komunikację aplikacji IPv6 z aplikacjami. Na przykład 0:0:0:0:0:ffff:192.1.56.10 i ::ffff:192.1.56.10/96 (format skrócony).

Wszystkie wymienione formaty są poprawnymi adresami IPv6. Formaty adresu IPv6, poza adresem odwzorowanym na protokole IPv4, można podać w programie iSeries Navigator.

Typy adresów IPv6

Używanie nowych typów adresów dla protokołu IPv6.

Adresy IPv6 można podzielić na trzy podstawowe typy:

Adres pojedynczy (unicast)
Adres pojedynczy określa pojedynczy interfejs. Pakiet wysłany na docelowy adres pojedynczy przechodzi od jednego hosta, do hosta docelowego.

Istnieją dwa typy regularne adresów pojedynczych:

Adres segmentowy (link-local)
Adresy przeznaczone do stosowania w pojedynczych połączeniach lokalnych (w sieci lokalnej) i są automatycznie konfigurowane dla wszystkich interfejsów. Ten typ adresu korzysta z przedrostka fe80::/10. Routery nie przekazują pakietów, które zawierają adres segmentowy jako adres docelowy lub źródłowy.

Adres globalny (global)
Adresy przeznaczone do stosowania w dowolnej sieci. Ich przedrostek zaczyna się od 001 w postaci binarnej.

Istnieją dwa zdefiniowane specjalne adresy pojedyncze:

Adres nieokreślony (unspecified)
Adres nieokreślony to 0:0:0:0:0:0:0:0. Można go skrócić do postaci dwóch dwukropków (::). Adres nieokreślony oznacza brak adresu i może nie być przypisany do hosta. Może być używany przez hosta IPv6, który jeszcze nie ma przypisanego adresu. Na przykład gdy host wysyła pakiet, aby wykryć czy adres jest wykorzystywany przez inny węzeł, korzysta z adresu nieokreślonego jako swojego adresu źródłowego.

Adres pętli zwrotnej
Adres pętli zwrotnej to 0:0:0:0:0:0:0:1. Adres ten może zostać skrócony do ::1. Jest to adres używany przez węzeł do wysyłania pakietów do siebie.

Adres dowolny (anycast)
Adres ten określa zbiór interfejsów, które mogą być w różnych miejscach, ale które współużytkują jeden adres. Pakiet wysłany na taki adres dochodzi tylko do najbliższego członka grupy. Obecnie serwer iSeries nie obsługuje tego typu adresowania.

Adres grupowy (multicast)
Adres ten określa zbiór interfejsów, które mogą być w wielu miejscach. Przedrostek tego adresu to ff. Kopia pakietu wysłanego na adres grupowy jest dostarczana do każdego członka w grupie. Obecnie serwer iSeries obsługuje tylko podstawowe elementy tego typu adresowania.

Protokół Neighbor discovery

Protokół Neighbor discovery umożliwia komunikację hostów i routerów.

Funkcje Neighbor discovery są wykorzystywane przez węzły IPv6 (hosty i routery) do wykrywania obecności innych węzłów IPv6, wykrywania adresów warstwy łącza tych węzłów, znajdowania routerów przekazujących pakiety IPv6 i do obsługi pamięci podręcznej zawierającej dane o aktywnych sąsiadach IPv6. Węzły IPv6 korzystają do komunikacji z innymi węzłami z następujących pięciu komunikatów protokołu ICMPv6:

Żądanie routera
Komunikaty wysyłane przez hosty z żądaniem, aby router wygenerował swój anons. Host wysyła początkowe żądanie routera, gdy po raz pierwszy podłącza się do sieci.

Komunikat routera
Komunikaty wysyłane przez routery systematycznie lub w odpowiedzi na komunikat żądania routera. Dzięki informacjom dostarczonym przez komunikaty routerów hosty tworzą automatycznie interfejsy globalne i powiązane trasy. Ponadto komunikaty routerów zawierają inne wykorzystywane przez hosta informacje związane z konfigurowaniem, takie jak maksymalna jednostka transmisji czy limit przeskoku.

Żądanie sąsiada
Komunikaty wysyłane przez węzły w celu określenia adresu warstwy łącza sąsiada lub służące do sprawdzenia, czy sąsiad jest nadal osiągalny.

Komunikat sąsiada
Komunikaty wysyłane przez węzły w odpowiedzi na żądanie sąsiada lub bez takiego żądania, jako komunikaty zgłaszające zmianę adresu.

Przekierowanie
Komunikaty używane przez routery do informowania hostów o najlepszym pierwszym przeskoku dla danego miejsca docelowego.

Więcej informacji o wykrywaniu sąsiada i routera zawiera dokument RFC 2461. Dokument ten można przejrzeć w serwisie WWW RFC Editor (www.rfc-editor.org/rfcsearch.html) .

Bezstanowe autokonfigurowanie adresu
Bezstanowe autokonfigurowanie adresu automatyzuje niektóre zadania administratora.

Bezstanowe autokonfigurowanie adresu to proces używany przez węzły IPv6 (hosty i routery) do automatycznego konfigurowania adresów IPv6 dla interfejsów. Węzeł buduje adresy IPv6, łącząc przedrostek adresu z identyfikatorem wyprowadzonym z adresu MAC węzła lub identyfikatorem interfejsu określonym przez użytkownika. Przedrostek składa się z przedrostka segmentowego (fe80::/10) i 64-bitowych przedrostków anonsowanych przez lokalne routery IPv6 (jeśli takie istnieją).

Węzeł dokonuje podwójnego wykrywania adresu, aby przed przypisaniem go do interfejsu zapewnić jego niepowtarzalność. Na nowy adres węzeł wysyła zapytanie typu żądanie sąsiada i czeka na odpowiedź. Jeśli odpowiedź nie nadejdzie, wtedy zakłada, że adres jest niepowtarzalny. Jeśli nadejdzie odpowiedź w postaci anonsu sąsiada, oznacza to, że adres jest już używany. Jeśli węzeł stwierdzi, że proponowany adres IPv6 nie jest niepowtarzalny, zakończy autokonfigurowanie i niezbędna będzie ręczna konfiguracja interfejsu.

Porównanie IPv4 z IPv6
Porównanie atrybutów protokołów IPv4 i IPv6.

Firma IBM zaimplementowała protokół IPv6 w kilku wersjach oprogramowania serwera iSeries. Obecnie protokół IPv6 jest gotowym produktem.

Można się zastanawiać, w jaki sposób protokół IPv6 różni się od protokołu IPv4. Poniższa tabela umożliwia szybki wgląd w specyficzne funkcje i porównanie ich zastosowania w każdym z tych protokołów. Należy wybrać odpowiedni atrybut z listy i porównać go z atrybutem przedstawionym w tabeli.
- Adres
- Przydzielanie adresu
- Czas życia adresu
- Maska adresu
- Przedrostek adresu
- Protokół ARP
- Zasięg adresu
- Typy adresu
- Śledzenie komunikacji

- Konfigurowanie
- System DNS
- Protokół DHCP
- Protokół FTP
- Fragmenty
- Tabela hostów
- Interfejs
- Protokół ICMP
- Protokół IGMP
- Nagłówek IP
- Opcje nagłówka IP
- Bajt protokołu nagłówka IP
- Bajt typu usługi TOS nagłówka IP
- Obsługa programu iSeries Navigator
- Połączenie LAN
- Protokół L2TP
- Adres pętli zwrotnej
- Jednostka MTU
- Netstat
- Translacja adresu sieciowego (NAT)
- Tabela sieci
- Zapytanie o węzeł
- Filtrowanie pakietu
- Przekazywanie pakietu
- Komenda PING
- Protokół PPP
- Ograniczenia portu
- Porty
- Adresy prywatne i publiczne
- Tabela protokołu
- Usługa QoS
- Zmiana numerów
- Trasa
- Protokół routingu RIP
- Tabela usług
- Protokół SNMP
- Funkcje API gniazd
- Wybór adresu źródłowego
- Uruchamianie i zatrzymywanie
- Telnet
- Śledzenie trasy
- Warstwy transportowe
- Adres nieokreślony
- Sieć VPN

Opis	IPv4	IPv6
Adres	Długość 32 bity (4 bajty). Składa się z części sieciowej i części hosta, która zależy od klasy adresu. W zależności od paru początkowych bitów, zdefiniowane są różne klasy adresów: A, B, C, D i E. Łączna liczba adresów IPv4 wynosi 4 294 967 296. W postaci tekstowej adres IPv4 jest następujący: nnn.nnn.nnn.nnn, gdzie 0<=*nnn*<=255, a każdy znak *n* jest cyfrą dziesiętną. Zera wiodące można pominąć. Maksymalna liczba drukowanych znaków wynosi 15, nie licząc maski.	Długość 128 bitów (16 bajtów). Podstawowa architektura zakłada 64 bity na numer sieci i 64 bity na numer hosta. Część hosta adresu IPv6 (lub jej fragment) będzie często wyprowadzana z adresu MAC lub innego identyfikatora interfejsu. W zależności od przedrostka podsieci protokół IPv6 ma bardziej skomplikowaną architekturę niż IPv4. Liczba adresów IPv6 jest 10^{28} (79 228 162 514 264 337 593 543 950 336) razy większa niż liczba adresów IPv4. Adres IPv6 w postaci tekstowej wygląda następująco: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, gdzie każdy znak x to cyfra szesnastkowa reprezentująca 4 bity. Zera wiodące można pominąć. W postaci tekstowej adresu można jednokrotnie użyć podwójnego dwukropka (::), wskazującego dowolną liczbę bitów zerowych. Na przykład adres ::ffff:10.120.78.40 to odwzorowany na adresie IPv4 adres IPv6. (Więcej szczegółowych danych zawiera dokument RFC 3513. Dokument ten można przejrzeć w serwisie WWW RFC Editor (www.rfc-editor.org/rfcsearch.html).
Przydzielanie adresu	Pierwotnie adresy były wyznaczane przez klasę sieci. Przestrzeń adresowa została uszczuplona, zrobiono mniejsze przydziały za pomocą metody CIDR. Liczba adresów przydzielonych państwom i instytucjom nie jest zrównoważona.	Przydzielanie znajduje się dopiero w fazie początkowej. Zarówno grupa wykonawcza IETF, jak i komisja IAB zaleciły, aby w pierwszym rzędzie dla każdej organizacji, domu lub jednostki została przydzielona długość przedrostka podsieci /48. Zostawia to organizacji 16 bitów na realizację podsieci. Przestrzeń adresowa jest wystarczająco duża, aby każda osoba na świecie miała swoją własną długość przedrostka podsieci /48.
Czas życia adresu	Koncepcja rzadko stosowana, z wyjątkiem adresów przydzielanych przez DHCP.	Adresy IPv6 mają dwa czasy życia: preferowany i poprawny, przy czym preferowany czas życia jest zawsze mniejszy lub równy poprawnemu. Po wygaśnięciu preferowanego czasu życia adres nie będzie używany jako źródłowy adres IP, jeśli dostępny będzie równie dobry preferowany adres. Po wygaśnięciu poprawnego czasu życia adres nie będzie używany (rozpoznawany) jako poprawny docelowy adres IP dla pakietów przychodzących lub jako źródłowy adres IP. Niektóre adresy IPv6 mają z założenia nieskończony preferowany i poprawny czas życia, czego przykładem jest adres segmentowy (patrz Zasięg adresu).
Maska adresu	Używana do oddzielenia części sieciowej od części hosta.	Nieużywana (patrz Przedrostek adresu).

Opis	IPv4	IPv6
Przedrostek adresu	Czasami używany do oddzielenia części sieciowej od części hosta. Zapisywany w prezentowanej postaci adresu jako przyrostek /nn.	Używany do oddzielenia przedrostka podsieci adresu. Zapisywany po drukowanej postaci adresu jako przyrostek /nnn (do 3 cyfr dziesiętnych, gdzie 0 <= nnn <= 128). Przykładem jest adres fe80::982:2a5c/10, gdzie pierwszych 10 bitów obejmuje przedrostek podsieci.
Protokół ARP	Protokół ARP jest wykorzystywany w IPv4 do odnajdywania fizycznego adresu, na przykład adresu MAC lub adresu łącza powiązanego z adresem IPv4.	Protokół IPv6 osadza te funkcje w samym protokole IP jako część algorytmu bezklasowego autokonfigurowania i wykrywania sąsiada za pomocą protokołu ICMPv6. Dlatego też nie istnieje nic takiego, jak ARP6.
Zasięg adresu	Koncepcja ta nie ma zastosowania w przypadku adresów pojedynczych. Istnieją zakresy adresów prywatnych i pętla zwrotna, poza tym wszystkie adresy są globalne.	W protokole IPv6 zasięg adresu stanowi część architektury. Adresy pojedyncze mają zdefiniowane dwa zasięgi, w tym segmentowy i globalny; adresy grupowe mają 14 zasięgów. Wybór adresu domyślnego, dla miejsca źródłowego i docelowego, obejmuje zasięg w ramach konta. Strefa zasięgu jest instancją zasięgu w danej sieci. W konsekwencji adresy IPv6 czasami trzeba wpisywać lub łączyć z identyfikatorem strefy. Składnia jest następująca: %zid, gdzie zid to numer (zazwyczaj mały) lub nazwa. Identyfikator strefy zapisywany jest po adresie i przed przedrostkiem. Na przykład: 2ba::1:2:14e:9a9b:c%3/48.
Typy adresu	Pojedyncze, grupowe i rozgłaszania.	Pojedyncze, grupowe i dowolne. Opis znajduje się w sekcji Typy adresów IPv6.
Śledzenie komunikacji	Narzędzie do gromadzenia szczegółowych danych śledzenia pakietów TCP/IP (i innych), które trafiają do serwera iSeries i opuszczają go.	Ten sam dla IPv6 i IPv6 jest obsługiwany.
Konfigurowanie	W celu komunikowania się z innymi systemami nowo zainstalowane systemy wymagają skonfigurowania, czyli przypisania adresów IP i tras.	Konfigurowanie jest opcjonalne, w zależności od oczekiwanej funkcjonalności. Protokół IPv6 może być używany z dowolnym adapterem Ethernet i może być uruchamiany za pomocą interfejsu pętli zwrotnej. Interfejsy IPv6 dokonują samokonfiguracji za pomocą bezstanowego autokonfigurowania IPv6. Interfejs IPv6 można również konfigurować ręcznie. Dlatego system będzie mógł komunikować się z innymi systemami IPv6, zdalnymi lub lokalnymi, w zależności od typu sieci i od tego, czy istnieje router IPv6.

Opis	IPv4	IPv6
System DNS	Aplikacje akceptują nazwy hostów, a następnie korzystają z systemu DNS, aby uzyskać adres IP za pomocą funkcji API gniazd gethostbyname(). Aplikacje akceptują także adresy IP i korzystają z systemu DNS do uzyskania nazw hostów, za pomocą funkcji gethostbyaddr(). W protokole IPv4 nazwa domeny dla wyszukiwania wstecz to in-addr.arpa.	Tak samo jest w przypadku protokołu IPv6. Obsługa IPv6 korzysta z typu rekordu AAAA (poczwórne A) i wyszukiwania wstecz (IP-na-nazwę). Aplikacja może wybierać, czy akceptować adresy IP z systemu DNS (czy nie) i następnie skorzystać (lub nie) z IPv6 do komunikacji. Funkcja API gniazda gethostbyname() obsługuje tylko protokół IPv4. W protokole IPv6 używana jest nowa funkcja API getaddrinfo(), za pomocą której można uzyskiwać (wybór na poziomie aplikacji) wyłącznie adresy IPv6 lub IPv4 i IPv6. W protokole IPv6 domeną używaną do wyszukiwania wstecznego jest ip6.arpa lub, jeśli nie zostanie ona odnaleziona, ip6.int (patrz Funkcja API getnameinfo()).
Protokół DHCP	Używany do dynamicznego uzyskiwania adresu IP i innych danych o konfiguracji.Serwer iSeries obsługuje serwer DHCP dla protokołu IPv4.	Obecnie implementacja protokołu DHCP w systemie i5/OS nie obsługuje IPv6.
Protokół FTP	Protokół FTP umożliwia wysyłanie i odbieranie plików przez sieć.	Obecnie implementacja protokołu FTP w systemie i5/OS nie obsługuje IPv6.
Fragmenty	Gdy pakiet jest za duży dla następnego odcinka połączenia, przez które podróżuje, może być podzielony przez wysyłający host lub router na mniejsze fragmenty.	W przypadku protokołu fragmentacja może nastąpić tylko w węźle źródłowym, a ponowne połączenie tylko w węźle docelowym. Używany jest nagłówek rozszerzenia fragmentacji.
Tabela hostów	W programie iSeries Navigator jest to konfigurowalna tabela kojarząca adres internetowy z nazwą hosta, na przykład 127.0.0.1 i pętla zwrotna. Z tabeli korzysta program tłumaczący nazwy gniazd, przed wyszukaniem DNS lub po, jeśli wyszukiwanie DNS się nie powiedzie (jest to określone przez priorytet wyszukiwania nazwy hosta).	Obecnie tabela ta nie obsługuje protokołu IPv6. Aby rozstrzygać domeny IPv6, użytkownicy muszą skonfigurować rekord AAAA w systemie DNS. Serwer DNS może działać na tym samym systemie, co program tłumaczący, może też być uruchomiony na innym systemie.
Interfejs	Pojęcie koncepcyjne lub logiczne, używane przez protokół TCP/IP do wysyłania i otrzymywania pakietów, zawsze ściśle związane z adresem IPv4 lub nazwane adresem IPv4. Czasami nazywany interfejsem logicznym. Może być uruchamiany i zatrzymywany niezależnie od innych interfejsów i niezależnie od protokołu TCP/IP, za pomocą komend STRTCPIFC i ENDTCPIFC oraz programu iSeries Navigator.	Koncepcja taka sama, jak w protokole IPv4. Może być uruchamiany i zatrzymywany niezależnie od innych interfejsów i niezależnie od protokołu TCP/IP, tylko za pomocą programu iSeries Navigator.

Opis	IPv4	IPv6
Protokół ICMP	Protokół ICMP jest używany przez IPv4 do wymiany informacji o sieci.	Podobnie jest używany przez IPv6, jednak ICMPv6 dostarcza kilku nowych atrybutów. Pozostały najprostsze typy błędów, takie jak miejsce docelowe nieosiągalne, echo żądania i odpowiedzi. Dodane zostały nowe typy i kody obsługujące wykrywanie sąsiada i funkcje pokrewne.
Protokół IGMP	Protokół IGMP jest używany przez routery IPv4 do odnajdywania hostów, które chcą przyjmować ruch sieciowy rozgłaszany dla określonej grupy, i przez hosty IPv4 do informowania routerów IPv4 o istniejących programach nasłuchujących rozgłaszanie.	Zastąpione przez protokół MLD (wykrywanie programów nasłuchujących rozgłaszanie) dla IPv6. Działa tak samo, jak IGMP dla IPv4, ale korzysta z protokołu ICMPv6, dodając kilka charakterystycznych dla MLD typów wartości ICMPv6.
Nagłówek IP	Zmienna długość z zakresu od 20 do 60 bajtów, w zależności od obecności opcji IP.	Zmienna długość do 40 bajtów. Nie ma żadnych opcji nagłówka IP. Ogólnie nagłówek IPv6 jest prostszy niż nagłówek IPv4.
Opcje nagłówka IP	Do nagłówka IP można dodawać różne opcje (przed nagłówkiem warstwy transportowej).	Nagłówek IPv6 nie ma żadnych opcji. W zamian protokół IPv6 dodaje opcjonalne nagłówki rozszerzeń. Nagłówki rozszerzeń to: AH i ESP (niezmienione od IPv4), hop-by-hop, routing, fragment i destination. Obecnie protokół IPv6 obsługuje niektóre nagłówki rozszerzeń.
Bajt protokołu nagłówka IP	Kod protokołu warstwy transportowej lub ładunku pakietu, na przykład ICMP.	Typ nagłówka następuje bezpośrednio po nagłówku IPv6 i korzysta z tych samych wartości, co pole protokołu IPv4. Takie rozwiązanie umożliwiło pozostawienie już zdefiniowanego zakresu następnych nagłówków i łatwe dalsze rozszerzanie. Następnym nagłówkiem będzie nagłówek transportowy, nagłówek rozszerzenia lub ICMPv6.
Bajt typu usługi TOS nagłówka IP	Wykorzystywany przez usługi QoS i DiffServ do wyznaczenia klasy ruchu.	Wyznacza klasę ruchu IPv6, podobnie jak dla protokołu IPv4. Korzysta z innych kodów. Obecnie protokół IPv6 nie obsługuje TOS.
Obsługa programu iSeries Navigator	Program iSeries Navigator zawiera wszystkie rozwiązania konfiguracyjne TCP/IP.	Tak samo jest w przypadku protokołu IPv6. Nie ma żadnych komend CL do konfigurowania protokołu IPv6.
Połączenie LAN	Używane przez interfejs IP w celu uzyskania dostępu do sieci fizycznej. Istnieje wiele typów, na przykład Token Ring i Ethernet. Czasami nazywane interfejsem fizycznym, łączem lub linią.	Protokół IPv6 może być używany z dowolnym adapterem Ethernet i jest obsługiwany za pomocą wirtualnej sieci Ethernet pomiędzy partycjami logicznymi.
Protokół L2TP	O protokole L2TP można myśleć, jak o wirtualnym połączeniu PPP, pracuje on poprzez dowolny obsługiwany typ linii.	Obecnie implementacja protokołu L2TP w systemie i5/OS nie obsługuje IPv6.
Adres pętli zwrotnej	Interfejs z adresem 127.*.*.* (zazwyczaj 127.0.0.1), wykorzystywany przez węzeł do wysyłania pakietów do siebie samego. Interfejs fizyczny (opis linii) został nazwany *LOOPBACK.	Koncepcja taka sama, jak w protokole IPv4. Pojedynczy adres pętli zwrotnej wynosi 0000:0000:0000:0000:0000:0000:0000:0001 lub ::1 (w wersji skróconej). Wirtualny interfejs fizyczny został nazwany *LOOPBACK.

Opis	IPv4	IPv6
Jednostka MTU	Maksymalna jednostka przesyłania łącza to maksymalna liczba bajtów, które obsługuje dany typ łącza, na przykład Ethernet lub modem. Dla protokołu IPv4 typową wartością minimalną jest 576.	Protokół IPv6 ma zaprojektowaną najniższą granicę MTU wynoszącą 1280 bajtów. Oznacza to, że poniżej tego limitu protokół IPv6 nie będzie dzielił pakietów. Aby wysłać pakiet IPv6 łączem o jednostce MTU mniejszej niż 1280, warstwa łącza musi podzielić i ponownie połączyć pakiety IPv6 w sposób przezroczysty dla protokołu.
Netstat	Narzędzie do sprawdzania statusu połączeń TCP/IP, interfejsów lub tras. Dostępne za pomocą programu iSeries Navigator i terminalu 5250.	Tak samo jest w przypadku protokołu IPv6, który jest obsługiwany zarówno dla terminalu 5250, jak i programu iSeries Navigator.
Translacja adresu sieciowego (NAT)	Podstawowe funkcje firewalla są zintegrowane z protokołem TCP/IP i konfigurowane za pomocą programu iSeries Navigator.	Obecnie NAT nie obsługuje protokołu IPv6. Ogólnie rzecz biorąc, protokół IPv6 nie potrzebuje NAT. Rozszerzona przestrzeń adresowa protokołu IPv6 eliminuje problem braku adresów i ułatwia zmianę numeracji.
Tabela sieci	W programie iSeries Navigator jest to konfigurowalna tabela kojarząca nazwę sieci z adresem IP bez maski. Na przykład host Siec14 i adres IP 1.2.3.4.	Obecnie dla protokołu IPv6 nie wprowadzono żadnych zmian do tej tabeli.
Zapytanie o węzeł	Nie istnieje.	Proste i wygodne narzędzie sieciowe, które powinno działać podobnie jak komenda ping, z taką różnicą, że węzeł IPv6 może zapytać inny węzeł IPv6 o nazwę DNS hosta docelowego, adres pojedynczy IPv6 lub adres IPv4. Obecnie nieobsługiwane.
Filtrowanie pakietu	Podstawowe funkcje firewalla są zintegrowane z protokołem TCP/IP i konfigurowane za pomocą programu iSeries Navigator.	Nie można zastosować filtrowania pakietu dla protokołu IPv6.
Przekazywanie pakietu	Serwer iSeries można skonfigurować w taki sposób, aby przekazywał otrzymane pakiety IP do nielokalnych adresów IP. Zazwyczaj interfejs dla połączeń przychodzących i interfejs dla połączeń wychodzących są połączone z innymi sieciami lokalnymi.	Pakiety IPv6 nie są przekazywane.
Komenda PING	Podstawowe narzędzie TCP/IP do sprawdzania, czy miejsce docelowe jest osiągalne. Dostępne za pomocą programu iSeries Navigator i terminalu 5250.	Tak samo jest w przypadku protokołu IPv6, który jest obsługiwany zarówno dla terminalu 5250, jak i dla programu iSeries Navigator.
Protokół PPP	Protokół PPP obsługuje interfejsy połączeń modemowych dla różnych modemów i typów linii.	Obecnie implementacja protokołu PPP w systemie i5/OS nie obsługuje IPv6.
Ograniczenia portu	Panele serwera iSeries umożliwiają klientom konfigurowanie wybranych numerów portów lub zakresu numerów portów dla protokołu TCP lub UDP, tak aby były one dostępne tylko dla określonego profilu.	Tak samo jest w przypadku protokołu IPv6. Ograniczenia portu dla IPv6 są takie same jak te, które są dostępne w protokole IPv4.

Opis	IPv4	IPv6
Porty	Protokoły TCP i UDP mają oddzielne przestrzenie portów, każdy port jest definiowany przez numer portu z zakresu 1-65535.	W protokole IPv6 porty działają tak samo jak w protokole IPv4. Ponieważ istnieje nowa rodzina adresów, pojawiły się 4 nowe, oddzielne przestrzenie portów. Istnieją na przykład dwie przestrzenie 80 portu TCP, do których aplikacja może się konsolidować, jedna w AF_INET i druga w AF_INET6.
Adresy prywatne i publiczne	Wszystkie adresy IPv4 są publiczne, poza adresami z zakresów wyznaczonych jako prywatne w dokumencie RFC 1918 grupy IETF: 10.*.*.* (10/8), 172.16.0.0 do 172.31.255.255 (172.16/12) i 192.168.*.* (192.168/16). Domeny adresów prywatnych są zwykle używane wewnątrz organizacji. Adresy prywatne nie mogą być kierowane przez Internet.	Protokół IPv6 ma podobną koncepcję, ale z ważnymi różnicami. Adresy są publiczne lub tymczasowe, poprzednio były nazywane anonimowymi. Patrz dokument RFC 3041. W przeciwieństwie do adresów prywatnych IPv4, adresy tymczasowe mogą być kierowane globalnie. Inna jest także motywacja, adresy krótkotrwałe IPv6 mają osłonić tożsamość klienta, gdy nawiązuje on komunikację (związane są z ochroną prywatności). Adresy tymczasowe mają ograniczony czas życia i nie zawierają identyfikatora interfejsu, czyli dołączonego adresu MAC. Ogólnie są nie do rozróżnienia od adresów publicznych. W protokole IPv6 istnieje pojęcie ograniczonego zasięgu adresu, korzystające z wbudowanych określeń zasięgu (patrz Zasięg adresu).
Tabela protokołu	W programie iSeries Navigator jest to konfigurowalna tabela kojarząca nazwę protokołu z przypisanym mu numerem protokołu, na przykład UDP, 17. System jest dostarczany z niewielką ilością wpisów: IP, TCP, UDP, ICMP.	Tabela bez żadnych zmian może być używana z protokołem IPv6.
Usługa QoS	Jakość usługi umożliwia zgłoszenie priorytetu pakietu i pasma dla aplikacji TCP/IP.	Obecnie implementacja usługi QoS w systemie i5/OS nie obsługuje IPv6.
Zmiana numerów	Zmiana konfiguracji wykonywana ręcznie, z możliwym wyjątkiem dla protokołu DHCP. Ogólnie dla ośrodka lub organizacji jest to proces trudny, związany z problemami i w miarę możliwości unikany.	Jest to ważny wbudowany element protokołu IPv6, wykonywany głównie automatycznie, szczególnie w ramach przedrostka /48.
Trasa	Logiczne odwzorowanie zbioru adresów IP (może to być zbiór jednoelementowy) na interfejsie fizycznym i pojedynczym adresie IP następnego przeskoku. Pakiety IP, których adres docelowy znajduje się w tym zbiorze, są przekazywane określoną linią do następnego przeskoku. Trasy IPv4 są powiązane z interfejsem IPv4, a co za tym idzie z adresem IPv4. Trasą domyślną jest *DFTROUTE.	Pod względem pojęciowym zbliżony do IPv4. Jedna istotna różnica: trasy IPv6 są powiązane z interfejsem fizycznym (łącze, ETH03), a nie z interfejsem. Jedną z przyczyn kojarzenia trasy z interfejsem fizycznym jest to, że funkcje wyboru adresu źródłowego są inne w IPv6 niż w IPv4. Patrz Wybór adresu źródłowego.
Protokół routingu RIP	Protokół routingu RIP jest obsługiwany przez demona routed.	Obecnie protokół routingu RIP nie obsługuje protokołu IPv6. Routing w protokole IPv6 korzysta z tras statycznych.

Opis	IPv4	IPv6
Tabela usług	Na serwerze iSeries jest to konfigurowalna tabela, kojarząca nazwę usługi z portem i protokołem, na przykład: nazwa usługi FTP-control, port 21, TCP i UDP. W tabeli usług znajduje się dużo ogólnie znanych usług. Aplikacje korzystają z tej tabeli do określenia, którego portu użyć.	Dla protokołu IPv6 nie wprowadzono żadnych zmian do tej tabeli.
Protokół SNMP	Protokół SNMP służy do zarządzania systemem.	Obecnie implementacja protokołu SNMP w systemie i5/OS nie obsługuje IPv6.
Funkcje API gniazd	Funkcje API gniazd to metody korzystania z protokołu TCP/IP przez aplikacje. Aplikacje, które nie potrzebują protokołu IPv6, są niewrażliwe na zmiany dotyczące obsługi gniazd w IPv6.	Protokół IPv6 rozszerza pojęcie gniazd, a aplikacje mogą teraz używać IPv6 korzystając z nowej rodziny adresów: AF_INET6. Rozszerzenia te zostały tak zaprojektowane, że istniejące aplikacje IPv4 są całkiem niewrażliwe na zmiany związane z protokołem IPv6 i funkcjami API. Aplikacje, które mają obsługiwać współbieżnie ruch IPv4 i IPv6 albo tylko ruch IPv6, można łatwo przystosować korzystając z adresów IPv4 odwzorowanych na IPv6 w postaci::ffff:a.b.c.d, gdzie a.b.c.d to adres IPv4 klienta. Nowe funkcje API zawierają także obsługę konwersji adresów IPv6 z postaci tekstowej na binarną i odwrotnie. Więcej informacji o rozszerzeniach gniazd dla protokołu IPv6 zawiera sekcja Używanie rodziny adresów AF_INET6.
Wybór adresu źródłowego	Aplikacja może wyznaczyć źródłowy IP (zazwyczaj korzystając z funkcji gniazd bind()). Jeśli źródłowy IP zostanie powiązany z INADDR_ANY, jest wybierany na podstawie trasy.	Tak jak w protokole IPv4, aplikacja może wyznaczyć źródłowy adres IPv6 korzystając z funkcji bind(). Podobnie do protokołu IPv4, może pozwolić, aby system wybrał adres źródłowy IPv6, korzystając z in6addr_any. Ale ponieważ linie IPv6 mają wiele adresów IPv6, inna jest wewnętrzna metoda wyboru źródłowego IP.
Uruchamianie i zatrzymywanie	Do uruchomienia lub zatrzymania TCP/IP służą komendy STRTCP i ENDTCP.	Tak samo jak w protokole IPv4. Protokoły IPv4 i IPv6 nie są uruchamiane lub zatrzymywane niezależnie od siebie lub od protokołu TCP/IP. Oznacza to, że można uruchomić lub zatrzymać protokół TCP/IP, a nie tylko protokół IPv4 lub IPv6. Interfejsy IPv6 są uruchamiane automatycznie, jeśli parametr AUTOSTART = *YES (wartość domyślna). Protokół IPv6 nie może być używany lub konfigurowany bez protokołu IPv4. Interfejs pętli zwrotnej IPv6 ::1 zostanie zdefiniowany i aktywowany automatycznie podczas uruchamiania protokołu IPv6.
Telnet	Usługa Telnet umożliwia zalogowanie się i korzystanie ze zdalnego komputera, tak jak przy połączeniu bezpośrednim.	Obecnie implementacja protokołu Telnet w systemie i5/OS nie obsługuje IPv6.

Opis	IPv4	IPv6
Śledzenie trasy	Podstawowe narzędzie TCP/IP do określania trasy. Dostępne za pomocą programu iSeries Navigator i terminalu 5250.	Tak samo jest w przypadku protokołu IPv6, który jest obsługiwany zarówno dla terminalu 5250, jak i programu iSeries Navigator.
Warstwy transportowe	TCP, UDP, RAW.	Takie same warstwy transportowe znajdują się w protokole IPv6.
Adres nieokreślony	Niezdefiniowany. Programowanie z użyciem gniazd korzysta z 0.0.0.0 jako INADDR_ANY.	Zdefiniowany jako ::/128 (128 bitów o wartości 0). Używany jako źródłowy adres IP w niektórych pakietach wykrywania sąsiada i w innych kontekstach, na przykład w gniazdach. Programowanie z użyciem gniazd korzysta z ::/128 jako in6addr_any.
Sieć VPN	Sieć VPN (korzystająca z protokołu IPsec) umożliwia rozszerzenie chronionych sieci prywatnych poprzez istniejące sieci publiczne.	Obecnie implementacja VPN w systemie i5/OS nie obsługuje IPv6.

Rozwiązywanie problemów dotyczących protokołu IPv6

Problemy dotyczące protokołów IPv4 i IPv6 można rozwiązywać za pomocą wielu narzędzi rozwiązywania problemów.

Jeśli protokół IPv6 został już skonfigurowany na serwerze, użytkownik może posłużyć się kilkoma narzędziami przeznaczonymi do rozwiązywania problemów dotyczących protokołu IPv4. Narzędzia takie jak śledzenie trasy czy komenda PING przyjmują obydwa formaty adresów, można więc ich użyć do sprawdzenia połączeń i tras dla obu typów sieci. Ponadto można użyć funkcji śledzenia komunikacji do śledzenia danych na obu liniach komunikacyjnych, IPv4 i IPv6.

Artykuł Rozwiązywanie problemów związanych z TCP/IP zawiera wiele informacji i opisów metod postępowania pomocnych podczas rozwiązywania problemów dotyczących protokołów IPv4 i IPv6.

Informacje związane z protokołem IPv6

Odsyłacze do zasobów pomocnych w zrozumieniu protokołu IPv6.

- The Internet Engineering Task Force (IETF) (www.ietf.cnri.reston.va.us/) Informacje na temat wykonawców protokołu internetowego, w tym IPv6.
- IP Version 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html) Bieżące specyfikacje IPv6 i odniesienia do źródeł informacji o IPv6.
- IPv6 Forum (www.ipv6forum.com/) Artykuły oraz wydarzenia związane z projektowaniem protokołu IPv6.

Planowanie konfiguracji protokołu TCP/IP

Temat ten zawiera informacje pomocne podczas instalowania i konfigurowania protokołu TCP/IP na serwerze iSeries. Podano tu podstawowe wymagania niezbędne podczas instalowania i konfigurowania oraz wszystkie podstawowe informacje potrzebne do rozpoczęcia konfigurowania protokołu TCP/IP.

Przed rozpoczęciem instalowania i konfigurowania serwera iSeries należy poświęcić parę chwil na zaplanowanie działań. Odpowiednie wskazówki znajdują się w sekcjach prezentowanych poniżej. Wskazówki dotyczą podstawowego konfigurowania TCP/IP z wykorzystaniem protokołu IPv4. Jeśli IPv6 trzeba konfigurować, to wymagania i instrukcje z tym związane zawiera sekcja Konfigurowanie protokołu IPv6.

Zbieranie informacji konfiguracyjnych TCP/IP

Należy zebrać podstawowe informacje konfiguracyjne wymagane podczas konfigurowania protokołu TCP/IP.

Wydrukuj tę stronę, a także zapisz informacje dotyczące konfiguracji swojego serwera oraz protokołu TCP/IP sieci, z którą jesteś połączony. Informacje te będą potrzebne później, podczas konfigurowania protokołu TCP/IP. Pod tabelą znajdziesz instrukcje, które pomogą w określeniu wartości pierwszych dwóch wierszy. Więcej informacji na temat instalacji podstawowej oraz procedur konfiguracyjnych znajduje się w dokumentacji technicznej IBM Redbook TCP/IP for AS/400: More Cool Things Than Ever  .

Wymagane informacje	Dla systemu użytkownika	Przykład
Rodzaj adaptera komunikacyjnego zainstalowanego w systemie (patrz instrukcje poniżej)		Ethernet
Nazwa zasobu		CMN01
Adres IP serwera iSeries		199.5.83.158
Maska podsieci serwera iSeries		255.255.255.0
Adres bramy		199.5.83.129
Nazwa hosta i nazwa domeny w systemie		sys400.xyz.company.com
Adres IP dla serwera nazw domen		199.4.191.76

Aby znaleźć informacje dotyczące adaptera komunikacyjnego:

1. W wierszu komend serwera wpisz go hardware i naciśnij klawisz Enter.
2. Aby wybrać opcję 1 (Praca z zasobami komunikacji), wpisz 1 i naciśnij klawisz Enter.

   Wyświetlone zasoby komunikacji będą uporządkowane według nazw. Aby pracować z zasobami lub zobaczyć więcej szczegółów, należy postępować zgodnie z wyświetlonymi instrukcjami.

Kolejne czynności Instalowanie TCP/IP

Metody ochrony protokołu TCP/IP

Przed zainstalowaniem protokołu TCP/IP należy uwzględnić wymogi ochrony.

Podczas planowania konfiguracji protokołu TCP/IP należy uwzględnić wymogi ochrony. Strategie przedstawione poniżej mogą pomóc ograniczyć wpływ czynników zewnętrznych na protokół TCP/IP:

- **Uruchamianie tylko niezbędnych aplikacji TCP/IP.** Każda aplikacja TCP/IP posiada swoją własną unikalną ochronę przed wpływem czynników zewnętrznych. Odrzucanie żądań dla poszczególnych aplikacji nie zależy od routera. Drugim sposobem zabezpieczenia jest ustawienie takich wartości autostartu aplikacji, które nie wymagają wartości NO.
- **Uruchamianie aplikacji TCP/IP tylko wtedy, gdy jest to niezbędne.** Można ograniczyć wpływ czynników zewnętrznych przez redukcję godzin, podczas których serwery są uruchomione. Jeśli jest to możliwe, należy zatrzymać serwery protokołów TCP/IP, takich jak FTP czy Telnet poza godzinami pracy.
- **Kontrolowanie, kto może uruchamiać i zmieniać aplikacje TCP/IP.** Domyślnie, aby zmienić ustawienia konfiguracyjne protokołu TCP/IP jest wymagane uprawnienie *IOSYSCFG. Użytkownik nie posiadający go potrzebuje uprawnienia *ALLOBJ lub jawnego uprawnienia do uruchamiania protokołu TCP/IP. Nadawanie specjalnych uprawnień użytkownikom jest elementem ochrony przed czynnikami zewnętrznymi. Należy ocenić zapotrzebowanie na uprawnienia specjalne dla każdego użytkownika i utrzymywać je na minimalnym poziomie. Należy regularnie sprawdzać listę użytkowników posiadających uprawnienia specjalne i od czasu do czasu sprawdzać, czy mają właściwe uprawnienia. To również ogranicza dostęp do serwera poza godzinami pracy.
- **Sterowanie routingiem TCP/IP:**
  - Brak zgody na przesyłanie IP uniemożliwi hakerom użycie serwera WWW do ataku na inne systemy zaufane.

– Należy zdefiniować tylko jedną trasę w publicznym serwerze WWW: domyślną trasę do dostawcy usług internetowych.
– Nie należy konfigurować nazw hostów i adresów IP zewnętrznych systemów ochrony w tabeli hostów protokołu TCP/IP na serwerze WWW użytkownika. Należy w niej umieszczać tylko nazwy innych serwerów publicznych, do których dostęp jest niezbędny.

- **Kontrolowanie serwerów TCP/IP przeznaczonych do zdalnego, interaktywnego wpisywania się.** Aplikacje, takie jak FTP czy Telnet, są bardziej podatne na atak zewnętrzny. Szczegóły dotyczące sposobów kontrolowania wpływu czynników zewnętrznych znajdują się w temacie poświęconym kontrolowaniu interaktywnego wpisywania się w dokumencie Wartości systemowe wpisania się.

Więcej informacji na temat ochrony i dostępnych użytkownikowi opcji zawiera publikacja iSeries a ochrona internetowa.

Instalowanie protokołu TCP/IP

Temat ten zawiera informacje potrzebne podczas instalowania produktów przygotowujących serwer iSeries do pracy.

Podstawowa obsługa protokołu TCP/IP jest elementem systemu i5/OS i umożliwia połączenie serwera iSeries z siecią. Jednak aby korzystać z aplikacji TCP/IP, takich jak FTP i SMTP, trzeba zainstalować również TCP/IP Connectivity Utilities. Jest to instalowany oddzielnie program licencjonowany dostarczany z systemem operacyjnym.

Aby zainstalować na serwerze iSeries narzędzie TCP/IP Connectivity Utilities, należy wykonać następujące czynności:

1. Włóż nośnik instalacyjny TCP/IP do odpowiedniego urządzenia w serwerze. Jeśli jest to dysk CD-ROM, włóż go do urządzenia optycznego. Jeśli jest to taśma, włóż ją do napędu taśm.
2. W wierszu komend wpisz GO LICPGM i naciśnij klawisz Enter, aby uzyskać dostęp do ekranu Praca z programami licencjonowanymi (Work with Licensed Programs).
3. Wybierz opcję 11 (Instalowanie programów licencjonowanych) na ekranie Praca z programami licencjonowanymi (Work with Licensed Programs), aby zobaczyć listę programów licencjonowanych i listę ich opcjonalnych części.
4. Wpisz 1 (Instalowanie) w kolumnie Opcja obok 57*xx*TC1 (TCP/IP Connectivity Utilities for iSeries). Naciśnij klawisz Enter. Ekran Potwierdzenie instalacji programów licencjonowanych (Confirm Licensed Programs to Install) pokazuje, które programy licencjonowane mają zostać zainstalowane. Naciśnij klawisz Enter, aby potwierdzić.
5. Wypełnij ekran Opcje instalacji (Install Options):

Urządzenie instalacyjne	Jeśli instalowanie odbywa się z dysku CD-ROM, wpisz QOPT. Jeśli instalowanie odbywa się z napędu taśm, wpisz TAP01.
Instalowane obiekty	Opcja ta pozwala wybrać programy i obiekty języka, albo tylko programy lub tylko obiekty języka.
Automatyczny restart	Opcja ta określa, czy system automatycznie wykona IPL po pomyślnym zakończeniu procesu instalacji.

   Po pomyślnym zainstalowaniu TCP/IP Connectivity Utilities pojawi się menu Praca z programami licencjonowanymi (Work with Licensed Programs) lub ekran Wpisanie się do systemu (Sign On).
6. Wybierz opcję 50 (Wyświetlenie protokołu komunikatów), aby sprawdzić, czy program licencjonowany został zainstalowany pomyślnie.

   Jeśli wystąpił błąd, na górze ekranu Praca z programami licencjonowanymi (Work with Licensed Programs) będzie widoczny komunikat Funkcja Praca z programami licencjonowanymi nie zakończyła się pomyślnie (Work with licensed program function not complete). Prawdopodobnie wystąpił problem, spróbuj ponownie zainstalować TCP/IP Connectivity Utilities. Jeśli problem nie został rozwiązany, należy skontaktować się ze wsparciem technicznym.

Uwaga: Inne programy licencjonowane, które można zainstalować to:

- IBM eServer iSeries Access for Windows (5722–XE1) zawierający program iSeries Navigator używany podczas konfigurowania niektórych komponentów TCP/IP.
- IBM HTTP Server for iSeries (57*xx*–DG1) zawierający obsługę serwera WWW.
- Niektóre aplikacje TCP/IP wymagają instalacji dodatkowych programów licencjonowanych. Należy sprawdzić, które programy są potrzebne oraz przejrzeć instrukcje konfigurowania aplikacji, które mają być zainstalowane.

Konfigurowanie TCP/IP

Temat ten zawiera informacje o tym, jak używać serwera i konfigurować protokół TCP/IP. Ponadto zawiera informacje o konfigurowaniu protokołu IPv6.

Do skorzystania z funkcji IPv6 niezbędne może okazać się zmienienie istniejącej konfiguracji lub, gdy serwer jest nowy, skonfigurowanie go po raz pierwszy. Aby skonfigurować protokół TCP/IP na serwerze, należy zapoznać się z poniższymi sekcjami:

Pierwsze konfigurowanie protokołu TCP/IP

Instrukcje przydatne podczas konfigurowania nowego serwera. Pierwsze konfigurowanie protokołu TCP/IP i nawiązywanie połączenia.

Aby skonfigurować protokół TCP/IP na nowym serwerze, należy wybrać jedną z poniższych metod.

Konfigurowanie protokołu TCP/IP za pomocą kreatora EZ-Setup

Zalecaną metodą w przypadku, gdy komputer PC jest wyposażony w ten program, jest użycie kreatora EZ-Setup. Kreator EZ-Setup jest dostarczany z serwerem iSeries.

Program iSeries Navigator to graficzny interfejs użytkownika, który udostępnia zwięzłe okna dialogowe i kreatory do konfigurowania protokołu TCP/IP. Podczas konfigurowania początkowego, do pierwszego konfigurowania protokołu TCP/IP i nawiązania połączenia należy użyć kreatora EZ-Setup programu iSeries Navigator. Jest to zalecana metoda pracy z serwerem, gdyż interfejs jest łatwy w użyciu. Dysk CD-ROM zawierający kreator EZ-Setup jest dostarczany z serwerem iSeries.

Aby skonfigurować serwer, wykonaj następujące czynności:

1. Użyj kreatora EZ-Setup. Znajduje się on na dysku CD-ROM dostarczanym z serwerem. Aby skonfigurować protokół TCP/IP, wykonuj kolejne instrukcje kreatora.
2. Uruchom TCP/IP.
   a. W programie iSeries Navigator, rozwiń *serwer* → **Sieć**.
   b. Kliknij prawym przyciskiem myszy **Konfiguracja TCP/IP** i wybierz **Uruchom**. Wszystkie interfejsy i serwery, które mają być uruchomione automatycznie podczas uruchomienia protokołu TCP/IP, zostaną w tym momencie uruchomione.

Na tym kończy się proces konfigurowania na serwerze protokołu TCP/IP. Jeśli konfiguracja sieci wymaga zmian, należy użyć programu iSeries Navigator.

Aby dodać trasy i interfejsy, należy zapoznać się z sekcją Dostosowanie protokołu TCP/IP za pomocą iSeries Navigator, natomiast aby korzystać w sieci z protokołu IPv6, należy przejść do sekcji Konfigurowanie protokołu IPv6.

Konfigurowanie protokołu TCP/IP za pomocą interfejsu znakowego

Należy skorzystać z tej metody, jeśli nie można użyć kreatora EZ-Setup.

Jeśli nie można użyć kreatora EZ-Setup programu iSeries Navigator, należy użyć w zamian interfejsu znakowego. Aby na przykład skorzystać z programu iSeries Navigator na komputerze PC, który uruchomieniem programu iSeries Navigator wymaga podstawowego skonfigurowania protokołu TCP/IP, trzeba posłużyć się interfejsem znakowym.

Aby wykonać opisane tu czynności konfiguracyjne, trzeba posiadać uprawnienia specjalne *IOSYSCFG. Więcej informacji na temat tego typu uprawnień zawiera rozdział o profilach użytkowników w publikacji iSeries Ochrona

W celu skonfigurowania protokołu TCP/IP za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz GO TCPADM, aby wyświetlić menu Administrowanie TCP/IP (TCP/IP Administration) i naciśnij klawisz Enter.
2. Wybierz opcję 1 (Konfigurowanie TCP/IP), aby wyświetlić menu Konfigurowanie TCP/IP (CFGTCP) (Configure TCP/IP) i naciśnij klawisz Enter. Z menu wybierz zadania konfiguracyjne. Przed przystąpieniem do konfigurowania serwera zapoznaj się z menu.

Aby skonfigurować protokół TCP/IP na serwerze, wykonaj następujące czynności.

Konfigurowanie opisu linii (Ethernet):

| Instrukcje te odnoszą się do konfigurowania TCP/IP za pomocą adaptera komunikacyjnego Ethernet.

W celu skonfigurowania opisu linii, wykonaj następujące czynności:

1. W wierszu komend wpisz CRTLINETH, aby wyświetlić panel Utworzenie opisu linii (Ethernet) CRTLINETH (Create Line Desc) i naciśnij klawisz Enter.
2. Podaj nazwę linii. (możesz użyć dowolnej nazwy).
3. Podaj nazwę zasobu.
4. Kilkakrotnie naciśnij klawisz Enter, aby uruchomić komendę.

Włączanie przesyłania datagramów IP:

Włączanie przesłania datagramów IP, aby pakiety mogły być przesyłane między różnymi podsieciami.

Aby włączyć przesyłanie datagramów IP, wykonaj następujące czynności:

1. W wierszu komend wpisz CHGTCPA i naciśnij klawisz F4.
2. W polu *Przesyłanie datagramów IP* wpisz *YES.

Konfigurowanie interfejsu:

W celu skonfigurowania interfejsu, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP, aby uzyskać dostęp do menu Konfigurowanie TCP/IP (Configure TCP/IP) i naciśnij klawisz Enter.
2. Wybierz opcję 1 (Praca z interfejsami TCP/IP) menu Konfigurowanie TCP/IP (Configure TCP/IP) i naciśnij klawisz Enter.
3. Wybierz opcję 1 (Dodanie), aby wyświetlić ekran Dodawanie interfejsu TCP/IP (Add TCP/IP Interface) i naciśnij klawisz Enter.
4. Podaj adres, który chcesz przydzielić serwerowi iSeries, maskę podsieci i uprzednio zdefiniowaną nazwę opisu linii, a następnie naciśnij klawisz Enter.

Aby uruchomić interfejs, podaj opcję 9 (Uruchomienie) dla skonfigurowanego interfejsu i naciśnij klawisz Enter.

Konfigurowanie trasy:

Dla każdej sieci zdalnej wymagana jest przynajmniej jedna pozycja routingu. Jeśli ręcznie nie zostaną dodane żadne pozycje routingu, serwer nie będzie mógł połączyć się z systemami znajdującymi się w sieci innej niż ta, do której jest przyłączony. Pozycje routingu należy dodać także po to, aby zapewnić prawidłową pracę klientów TCP/IP łączących się z serwerem z sieci zdalnej.

Należy zaplanować definicję tabeli routingu, gdyż zawsze powinna być w niej uwzględniona trasa domyślna (*DFTROUTE). Jeśli nie można dopasować żadnego innego wpisu w tabeli routingu, dane są wysyłane do routera IP, określonego przez pierwszą dostępną pozycję routingu domyślnego.

Aby skonfigurować trasę domyślną, wykonaj następujące czynności:

1. Wybierz opcję 2 (Praca z trasami TCP/IP) menu Konfigurowanie TCP/IP (Configure TCP/IP) i naciśnij klawisz Enter.
2. Wybierz opcję 1 (Dodanie), aby wyświetlić ekran Dodawanie trasy TCP/IP (ADDTCPRTE) (Add TCP/IP Route) i naciśnij klawisz Enter.
3. Jako cel trasy podaj *DFTROUTE, jako maskę podsieci podaj *NONE, określ adres IP następnego przeskoku i naciśnij klawisz Enter.

Definiowanie domeny lokalnej i nazw hostów:

Aby zdefiniować domenę lokalną i nazwy hostów, wykonaj następujące czynności:

1. Wybierz opcję 12 (Zmiana domeny TCP/IP) z menu Konfigurowanie TCP/IP (Configure TCP/IP) i naciśnij klawisz Enter.
2. Wprowadź nazwy wybrane jako nazwy lokalnych hostów i nazwę domeny lokalnej, pozostałe parametry pozostaw domyślne i naciśnij klawisz Enter.

Definiowanie tabeli hostów:

Aby zdefiniować tabelę hostów, wykonaj następujące czynności:

1. Wybierz opcję 10 (Praca z pozycjami tabeli hostów TCP/IP) menu Konfigurowanie TCP/IP (Configure TCP/IP) i naciśnij klawisz Enter.
2. Wybierz opcję 1 (Dodanie), aby wyświetlić ekran Dodawanie pozycji tabeli hostów TCP/IP (Add TCP/IP Host Table Entry) i naciśnij klawisz Enter.
3. Wprowadź adres IP, powiązaną nazwę lokalną hosta i pełną nazwę hosta, a następnie naciśnij klawisz Enter.
4. Jeśli istnieje taka potrzeba, wprowadź znak plus (+), aby utworzyć miejsce na więcej niż jedną nazwę hosta.
5. Powtarzaj czynności od 1 do 4 dla wszystkich pozostałych hostów w sieci, z którymi chcesz się komunikować z użyciem nazwy, i dodaj wpis dla każdego z nich.

Uruchom TCP/IP.:

Usługi TCP/IP nie będą dostępne, dopóki nie zostanie uruchomiony protokół TCP/IP.

Aby uruchomić TCP/IP, w wierszu komend wpisz STRTCP.

| Komenda Uruchomienie TCP/IP (Start TCP/IP - STRTCP) rozpoczyna i aktywuje przetwarzanie TCP/IP, uruchamia
| interfejsy TCP/IP i zadania serwera. Komenda STRTCP uruchamia jedynie te interfejsy i serwery, które mają
| ustawioną wartość AUTOSTART *YES. Interfejsy i serwery TCP/IP, które mają ustawioną wartość AUTOSTART
| *YES, profile PPP oraz protokół IPv6 mogą być uruchamiane opcjonalnie.

Na tym kończy się proces konfigurowania na serwerze protokołu TCP/IP. Jeśli konfiguracja sieci wymaga zmian, należy użyć programu iSeries Navigator. Aby dodać trasy i interfejsy, należy zapoznać się z sekcją Dostosowanie protokołu TCP/IP za pomocą iSeries Navigator, natomiast aby korzystać w sieci z protokołu IPv6, należy przejść do sekcji Konfigurowanie protokołu IPv6.

Konfigurowanie IPv6

Instrukcje zawarte w tym temacie dotyczą konfigurowania serwera dla funkcji IPv6. Korzyści płynące z możliwości rozszerzonego adresowania i opcje związane ze stabilnością tego protokołu IP.

W sekcji Protokół IPv6 znajduje się krótki przegląd informacji na temat tego protokołu. Przed konfigurowaniem IPv6 na serwerze należy skonfigurować protokół TCP/IP.

Protokół IPv6 pozwala korzystać z zalet następnej generacji sieci Internet. Aby używać protokołu IPv6, należy go skonfigurować na istniejącej linii za pomocą ręcznego konfigurowania interfejsów lub używając opcji IPv6 Bezstanowe autokonfigurowanie adresu, można również wykorzystać obie możliwości.

Pojęcia pokrewne

"Scenariusz: używanie protokołu IPv6" na stronie 5
Przykłady, które pomogą zrozumieć, kiedy można zastosować protokół IPv6 w celach biznesowych oraz w jaki sposób konfigurować sieć.

Wymagania sprzętowe i programowe

Wymagania sprzętowe i programowe niezbędne do skonfigurowania serwera dla protokołu IPv6.

Konfigurowanie linii sieci Ethernet dla protokołu IPv6

Aby możliwe było skonfigurowanie linii sieci Ethernet, tak aby protokół IPv6 działał na serwerze, system powinien spełniać następujące warunki:

- i5/OS Wersja 5 Wydanie 4.
- Program iSeries Access for Windows i iSeries Navigator:
  - Komponent sieciowy programu iSeries Navigator.
- Router z możliwością obsługi IPv6, aby wysyłać ruch IPv6 poza bezpośrednią sieć LAN.
- Skonfigurowany protokół TCP/IP (korzystający z IPv4), ponieważ na serwerze musi być uruchomiony protokół TCP/IP. Jeśli jeszcze nie skonfigurowano serwera dla IPv4, to przed konfiguracją linii dla IPv4 należy zapoznać się z sekcją Pierwsze konfigurowanie protokołu TCP/IP.

Konfigurowanie bezstanowego autokonfigurowania adresu IPv6

Aby wykorzystać protokół IPv6, można użyć opcji IPv6 bezstanowego autokonfigurowania adresu. Istnieją na to dwa sposoby.

Aby skonfigurować bezstanowe autokonfigurowanie adresu IPv6, należy wykonać następujące czynności:

1. W programie iSeries Navigator rozwiń **Sieć → Konfiguracja TCP/IP → Linie**.
2. Kliknij prawym przyciskiem myszy jedną z linii w prawym panelu i wybierz **Bezstanowe autokonfigurowanie adresu IPv6 → Konfiguruj**.
3. Prawym przyciskiem myszy kliknij skonfigurowaną linię, wybierz **Bezstanowe autokonfigurowanie adresu IPv6 → Uruchom**.

Aby skonfigurować bezstanowe autokonfigurowanie adresu IPv6, należy wykonać następujące czynności:

1. W programie iSeries Navigator rozwiń **Sieć → Konfiguracja TCP/IP → Linie**.
2. Kliknij prawym przyciskiem myszy **Linie** i wybierz **Bezstanowe autokonfigurowanie adresu IPv6**.

Uwaga: Aby sprawdzić, czy proces ten odbędzie się automatycznie podczas uruchamiania protokołu TCP/IP, należy wybrać **Uruchom podczas uruchamiania TCP/IP** na ekranie **Konfigurowanie linii IPv6 (Configure Line for IPv6)**.

Tworzenie nowego interfejsu IPv6

Protokół IPv6 można również wykorzystywać, aby za pomocą nowego kreatora, ręcznie utworzyć nowy interfejs IPv6.

Aby utworzyć nowy interfejs IPv6, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **Sieć → Konfiguracja TCP/IP → IPv6**.
2. Kliknij prawym przyciskiem myszy **Interfejs**, a następnie wybierz **Nowy Interfejs**.

3. Aby utworzyć nowy interfejs IPv6, postępuj zgodnie z instrukcjami zawartymi w kreatorze nowego interfejsu IPv6. Nowy interfejs zostanie wyświetlony w prawym panelu po zakończeniu konfigurowania.
4. Kliknij prawym przyciskiem myszy nowy interfejs IPv6, a następnie wybierz **Uruchom**.

   Można również sprawdzić pole wyboru **Uruchom podczas uruchamiania TCP/IP** w kreatorze nowego interfejsu IPv6, aby się upewnić, że protokół zostanie wystartowany automatycznie podczas kolejnego uruchamiania TCP/IP.
5. W programie iSeries Navigator wybierz **Sieć → Konfiguracja TCP/IP → Narzędzia → Komenda ping**, aby przetestować nowy interfejs IPv6 i sprawdzić połączenie z siecią.

   Uwaga: Aby aktywować pozycję menu nowego interfejsu, należy posiadać uprawnienie *IOSYSCFG.

Konfigurowanie TCP/IP, gdy system operacyjny jest w stanie zastrzeżonym

Tej metody należy użyć, jeśli istnieje potrzeba uruchomienia TCP/IP w momencie, gdy system operacyjny jest w stanie zastrzeżonym.

Opis sytuacji

Jako administrator sieci powinieneś uzyskać raporty o statusie kopii zapasowej dla serwera. Podczas uruchamiania procedur tworzenia kopii zapasowych system operacyjny musi znajdować się w stanie zastrzeżonym, aby uniemożliwić użytkownikom zmianę konfiguracji. Ponieważ jesteś użytkownikiem zdalnym, możesz uzyskać dostęp do raportów o statusie używając komputera PDA (lub dowolnego urządzenia sieciowego TCP/IP). PDA używa aplikacji obsługującej gniazda, która wymaga dostępu do aktywnego interfejsu TCP/IP w celu komunikacji z serwerem. Aby umożliwić tę komunikację, w pierwszej kolejności należy uruchomić TCP/IP, używając specjalnych parametrów. Następnie należy uruchomić konkretny interfejs TCP/IP, aby uzyskać dostęp do systemu. Szczegółowe informacje na ten temat znajdują się poniżej.

Ograniczenia

Poniższe ograniczenia dotyczą sytuacji, w której system operacyjny znajduje się w stanie zastrzeżonym.

- Nie można uruchomić serwerów TCP/IP (komenda CL STRTCPSRV), ponieważ wymagają one aktywnych podsystemów.
- Można uruchomić tylko jeden interfejs dla wybranego typu linii (Ethernet, Token Ring lub DDI), która nie jest dołączona do opisu serwera sieciowego (NWSD) lub do opisu interfejsu sieciowego (NWID).

Czynności konfiguracyjne

1. Uruchom TCP/IP, używając specjalnych parametrów.

   Jeśli system iSeries znajduje się w stanie zastrzeżonym, uruchom następującą komendę w wierszu komend: STRTCP STRSVR(*NO) STRIFC(*NO) STRPTPPRF(*NO) STRIP6(*NO). Są to jedyne parametry akceptowane przez system operacyjny znajdujący się w stanie zastrzeżonym. Powyższa komenda spowoduje uruchomienie TCP/IP, jednak nie będzie mogła uruchomić serwerów aplikacji TCP/IP ani interfejsów IP.
2. Uruchom wybrany interfejs TCP/IP. Po uruchomieniu TCP/IP w stanie zastrzeżonym można uruchomić wybrany interfejs do wykorzystania w aplikacji obsługującej gniazda.
   a. Sprawdź, czy wybrany interfejs używa opisu linii *ELAN, *TRLAN, lub *DDI.

      Aby wyświetlić typ linii dla wybranego interfejsu, w wierszu komend wprowadź CFGTCP i wybierz opcję 1 (Praca z interfejsami TCP/IP).
   b. Upewnij się, że interfejs nie jest podłączony do NWID lub NWSD. Próba wywołania innej opcji spowoduje błąd.

      Aby sprawdzić, czy interfejs nie jest podłączony do NWID lub NWSD, w wierszu komend wprowadź DSPLIND *abc* (gdzie *abc* jest nazwą opisu linii). Upewnij się, że nazwą zasobu nie jest *NWID lub *NWSD.

      Uwaga: Jeśli interfejs jest podłączony do NWID lub NWSD, zalecane jest wybranie innego interfejsu.

c. Uruchom interfejs. W wierszu komend wprowadź:STRTCPIFC INTNETADR('*a.b.c.d*'). W miejsce *a.b.c.d* wpisz adres interfejsu IP.

   Uwaga: Upewnij się, że nie podano STRTCPIFC INTNETADR(*AUTOSTART).

3. Sprawdź, czy interfejs jest aktywny.

   Wykonaj komendę ping do wybranego interfejsu dla aplikacji. Niewiele narzędzi pokrewnych TCP/IP działa w stanie zastrzeżonym. Należą do nich ping i netstat. Więcej informacji na temat używania komend ping i netstat znajduje się w temacie Narzędzia do sprawdzania sieci w artykule Rozwiązywanie problemów związanych z TCP/IP.

Dostosowanie konfiguracji TCP/IP za pomocą programu iSeries Navigator

Temat ten zawiera informacje dotyczące opcji konfiguracyjnych dostępnych w programie iSeries Navigator.

Bezpośrednio po zakończeniu konfigurowania TCP/IP można dostosować konfigurację. Ponieważ sieć się rozrasta, trzeba zmienić jej właściwości, dodać interfejsy lub trasy. Aby korzystać z aplikacji IPv6, można skonfigurować serwer dla protokołu IPv6. Korzystanie z kreatorów w programie iSeries Navigator pozwoli szybko wykonać wiele z tych zadań.

Aby dostosować konfigurację za pomocą programu iSeries Navigator, należy wybrać temat z poniższej listy. Tematy te stanowią punkt wyjścia do zarządzania konfiguracją TCP/IP za pomocą programu iSeries Navigator.

Zmiana ustawień TCP/IP

Zawarte w temacie instrukcje pomagają konfigurować odpowiednie ustawienia TCP/IP.

Za pomocą programu iSeries Navigator można przeglądać i zmieniać ustawienia protokołu TCP/IP. Pozwala on też zmienić właściwości hosta, nazwę hosta, nazwę domeny, serwer nazw, pozycje tabeli hostów, atrybuty systemu, ograniczenia dotyczące portów, a także połączenia serwerów i klientów. Poza tym umożliwia zarówno zmianę właściwości ogólnych, jak i właściwości charakterystycznych dla IPv4 albo IPv6, takich jak na przykład warstwa transportowa.

Aby otworzyć stronę właściwości ogólnych protokołu TCP/IP, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć**.
2. Kliknij prawym przyciskiem myszy **Konfiguracja TCP/IP** i wybierz **Właściwości**, aby otworzyć okno dialogowe **Właściwości TCP/IP**.
3. Wybierz zakładki znajdujące się na górze okna dialogowego, aby wyświetlić i edytować informacje o protokole TCP/IP.

Aby dodać lub zmienić pozycje tabeli hostów, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć**.
2. Kliknij prawym przyciskiem myszy **Konfiguracja TCP/IP** i wybierz **Tabela hostów**, aby otworzyć okno dialogowe **Tabela hostów**.
3. Aby dodać, zmienić lub usunąć pozycje tabeli hostów, użyj okna dialogowego **Tabela hostów**.

Aby otworzyć strony właściwości charakterystyczne dla protokołu IPv4, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz **Serwer → Sieć**.
2. Kliknij prawym przyciskiem myszy **IPv4** i wybierz **Właściwości**, aby otworzyć okno dialogowe **Właściwości IPv4**.
3. Aby przeglądać lub zmieniać ustawienia właściwości IPv4, na górze okna dialogowego wybierz odpowiednie zakładki.

Aby otworzyć strony właściwości charakterystyczne dla protokołu IPv6, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć**.
2. Kliknij prawym przyciskiem myszy **IPv6** i wybierz **Właściwości**, aby otworzyć okno dialogowe **Właściwości IPv6**.
3. Aby przeglądać lub zmieniać ustawienia właściwości IPv6, na górze okna dialogowego wybierz odpowiednią zakładkę.

Konfigurowanie IPv6

Zawarte w temacie informacje pomagają w konfigurowaniu protokołu IPv6.

W sekcji “Protokół IPv6” na stronie 3 znajduje się przegląd informacji na temat tego protokołu.

Aby skonfigurować IPv6, należy zmienić konfigurację serwera za pomocą programu iSeries Navigator. Przed rozpoczęciem konfiguracji należy zapoznać się z instrukcjami i szczególnymi wymaganiami zawartymi w sekcji “Konfigurowanie IPv6” na stronie 22.

Dodawanie interfejsów IPv4

Zawarte w temacie instrukcje pomagają utworzyć nowe interfejsy IPv4.

Aby utworzyć nowy interfejs IPv4, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć** → **Konfiguracja TCP/IP** → **IPv4**.
2. Kliknij prawym przyciskiem myszy **Interfejsy**, wybierz **Nowy interfejs** i **Sieć lokalna (LAN)**, **Sieć rozległa (WAN)** lub **Wirtualny adres IP**, aby utworzyć odpowiedni typ interfejsu.
3. Aby skonfigurować nowy interfejs IPv4, wykonaj instrukcje kreatora.

Dodawanie interfejsów IPv6

Zawarte w temacie instrukcje pomagają utworzyć nowe interfejsy IPv6.

Aby utworzyć nowy interfejs IPv6, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć** → **Konfiguracja TCP/IP** → **IPv6**.
2. Kliknij prawym przyciskiem myszy **Interfejsy** i wybierz **Nowy interfejs**.
3. Aby skonfigurować nowy interfejs IPv6, wykonaj instrukcje kreatora.

Dodawanie tras IPv4

Zawarte w temacie instrukcje pomagają konfigurować nowe trasy IPv4.

Wszystkie zmiany wprowadzone do informacji o routingu działają od momentu ich wprowadzenia.

Aby skonfigurować nową trasę IPv4, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz *serwer* → **Sieć** → **Konfiguracja TCP/IP** → **IPv4**.
2. Kliknij prawym przyciskiem myszy **Trasy** i wybierz **Nowa trasa**.
3. Aby skonfigurować nową trasę IPv4, wykonaj instrukcje kreatora.

Dodawanie tras IPv6

Zawarte w temacie instrukcje pomagają konfigurować nowe trasy IPv6.

Wszystkie zmiany wprowadzone do informacji o routingu działają od momentu ich wprowadzenia.

Aby skonfigurować nową trasę IPv6, wykonaj następujące czynności:

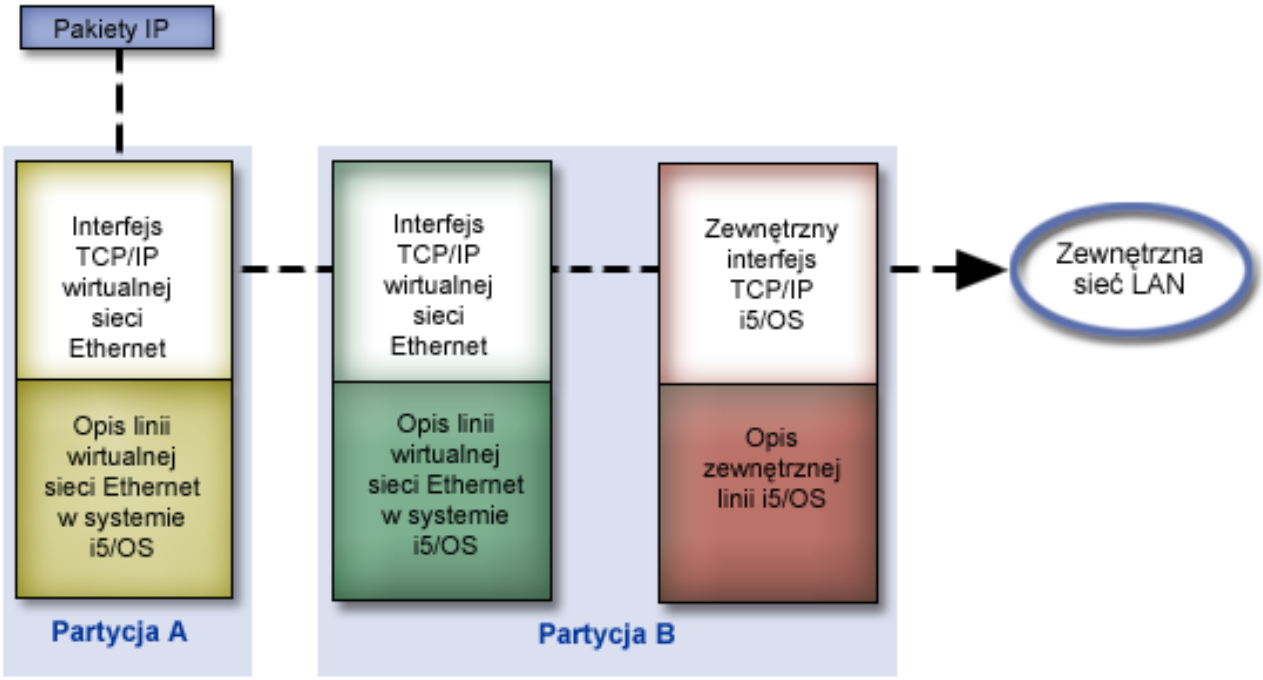
1. W programie iSeries Navigator wybierz *serwer* → **Sieć** → **Konfiguracja TCP/IP** → **IPv6**.

2. Kliknij prawym przyciskiem myszy **Trasy** i wybierz **Nowa trasa**.
3. Aby skonfigurować nową trasę IPv6, wykonaj instrukcje kreatora.

Techniki TCP/IP umożliwiające połączenie wirtualnej sieci Ethernet z zewnętrznymi sieciami LAN

Zalety wirtualnej sieci Ethernet w systemiei5/OS.

Jeżeli do interpretacji zmian używana jest wirtualna sieć Ethernet, należy włączyć te partycje w celu umożliwienia komunikacji z zewnętrzną fizyczną siecią LAN. Istnieje kilka sposobów połączenia wirtualnej sieci Ethernet z zewnętrzną siecią LAN przy użyciu różnych technik TCP/IP. Należy umożliwić ruch TCP/IP między wirtualną siecią Ethernet a zewnętrzną siecią LAN. Ten rysunek przedstawia przepływ logiczny pakietów IP.



Ruch IP zainicjowany w partycji A idzie wewnątrz wirtualnej sieci Ethernet od interfejsu na partycji A do interfejsu na partycji B. Po zaimplementowaniu jednej z trzech opisanych poniżej technik TCP/IP można umożliwić ruch pakietów do interfejsu zewnętrznego - i dalej do miejsca przeznaczenia.

Istnieją trzy metody łączenia wirtualnej sieci Ethernet z zewnętrzną siecią LAN. Różnią się szczegółami, które każdą z nich czynią łatwiejszą do zastosowania w zależności od posiadanej wiedzy o TCP/IP i od środowiska. Należy wybrać jedną spośród następujących metod:

- Metoda ARP proxy
- Metoda translacji adresu sieciowego (NAT)
- Metoda routingu TCP/IP

Metoda Address Resolution Protocol proxy

Metoda ARP proxy używa przezroczystej podsieci w celu powiązania wirtualnego interfejsu partycji z interfejsem zewnętrznym. Funkcja ARP proxy jest wbudowana w stos TCP/IP. To rozwiązanie jest zalecane w przypadku, gdy znane są wszystkie adresy IP.

Więcej informacji o przezroczystych podsieciach znajduje się w dokumentacji technicznej

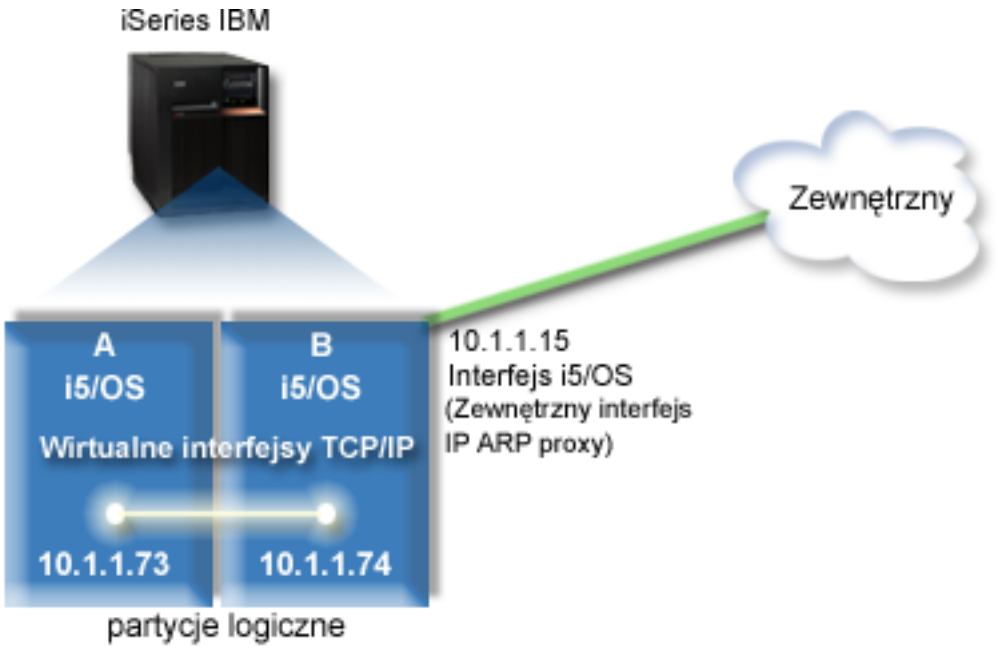
- V4 TCP/IP for AS/400: More Cool Things Than Ever

W tej dokumentacji technicznej IBM (Redbook) udostępniono przykłady scenariuszy opisujących powszechnie stosowane rozwiązania oraz przykładowe konfiguracje. Informacje zawarte w tej dokumentacji pomagają instalować, dostosowywać i konfigurować TCP/IP na serwerze iSeries, a także rozwiązywać ewentualne problemy.

- Routing TCP/IP i równoważenie obciążenia

  Ten dokument opisuje techniki i instrukcje dotyczące routingu i równoważenia obciążeń.

Jeśli wybraną metodą będzie ARP proxy, należy mieć wystarczającą wiedzę na temat podsieci i TCP/IP. Poza tym trzeba uzyskać zakres adresów IP, które są obecne w tabelach routingu. Zakres ten należy podzielić na podsieci. W tym przykładzie zostanie użyty zakres złożony z czterech adresów IP (od 10.1.1.72 do 10.1.1.75). Ponieważ zakres ten zawiera cztery adresy, maska podsieci dla nich wynosi 255.255.255.252. Jak pokazuje ten rysunek, każdy z adresów zostanie przypisany do jednego interfejsu wirtualnego TCP/IP na każdej partycji.



W tym przykładzie ruch TCP/IP z partycji A przechodzi przez wirtualną sieć Ethernet do interfejsu 10.1.1.74 na partycji B. Ponieważ interfejs 10.1.1.74 jest powiązany z zewnętrznym interfejsem ARP proxy 10.1.1.15, pakiety IP wychodzą z wirtualnej sieci Ethernet przy użyciu interfejsu ARP proxy.

Aby skonfigurować wirtualną sieć Ethernet w celu używania metody ARP proxy, należy wykonać poniższe zadania konfiguracyjne.

Krok 1: Aktywowanie partycji logicznych, aby mogły być uwzględniane w wirtualnej sieci Ethernet

Uwaga: Podczas konfigurowania wirtualnej sieci Ethernet na serwerze model 5*xx* należy zapoznać się z instrukcjami zawartymi w temacie Wirtualny Ethernet dla partycji logicznych systemu i5/OS Centrum informacyjnego - sprzęt IBM.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycja A) wpisz STRSST i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.
3. W panelu Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi).
4. W panelu Praca z partycjami systemu (Work with System Partitions) wybierz opcję 3 (Praca z konfiguracją partycji).

5. Naciśnij klawisz F10 (Praca z wirtualną siecią Ethernet).
6. Wpisz 1 w odpowiedniej kolumnie dla partycji A i dla partycji B, aby umożliwić obu partycjom wzajemną komunikację w wirtualnej sieci Ethernet.
7. Wyjdź z ekranu Narzędzia SST (System Service Tools - SST), aby powrócić do wiersza komend.

Informacje pokrewne

Konsolidowanie partycji i5/OS, AIX® i Linux® w systemie IBM eServer™ i5

Krok 2: Tworzenie opisu linii sieci Ethernet

W zależności od modelu używanego serwera możliwe są dwa sposoby wykonania tej czynności.

Tworzenie opisu linii sieci Ethernet na serwerach model 270 i 8*xx*:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów model 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu obsługi wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

   Port sieci Ethernet o numerze 268C jest zasobem wirtualnej sieci Ethernet. Dla każdej wirtualnej sieci Ethernet połączonej z partycją logiczną istnieje jeden port.
3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć adres portu. Adres portu odpowiada wirtualnej sieci Ethernet, która została wybrana podczas konfigurowania partycji logicznej.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego portu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).
   a. W polu *Opis linii* wpisz VETH0. Nazwa VETH0, choć przypadkowa, odpowiada numerowanej kolumnie na stronie wirtualnej sieci Ethernet, w której została aktywowana partycja logiczna w celu komunikacji. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
   b. W polu *Szybkość linii* wpisz 1G.
   c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
   d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

      Zostanie wyświetlony komunikat o utworzeniu opisu linii.
6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Tworzenie opisów linii na serwerach modeli innych niż 270 i 8xx:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów modeli innych niż 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu obsługi wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

   Porty sieci Ethernet o numerach 268C są zasobami wirtualnej sieci Ethernet. Dla każdego adaptera wirtualnej sieci Ethernet istnieje jeden port. Każdy port o numerze 268C ma powiązany kod położenia wprowadzony podczas tworzenia adaptera wirtualnej sieci Ethernet przy użyciu konsoli HMC (krok 1).
3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć zasób o numerze 268C, który jest powiązany z konkretnym kodem położenia utworzonym dla tej wirtualnej sieci Ethernet.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego zasobu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).
   a. W polu *Opis linii* wpisz VETH0. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa VETHO, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
   b. W polu *Szybkość linii* wpisz 1G.
   c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
   d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

      Zostanie wyświetlony komunikat o utworzeniu opisu linii.
6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Krok 3: Włączanie przesyłania datagramów IP

Włączanie przesłania datagramów IP, aby pakiety mogły być przesyłane między różnymi podsieciami.

Aby włączyć przesyłanie datagramów IP, wykonaj następujące czynności:

1. W wierszu komend partycji B wpisz CHGTCPA i naciśnij klawisz F4.
2. W polu *Przesyłanie datagramów IP* wpisz *YES.

Krok 4: Tworzenie interfejsu w celu aktywowania ARP proxy

Aby utworzyć interfejs TCP/IP w celu aktywowania ARP proxy, wykonaj następujące czynności:

1. Uzyskaj zakres adresów IP, które są obecne w tabelach routingu.

   Ponieważ w wirtualnej sieci Ethernet istnieją dwie partycje, potrzebny jest zakres czterech adresów. Czwarty segment pierwszego adresu IP w tym zakresie musi być podzielny przez cztery. Pierwszy i ostatni adres IP tego zakresu są adresami IP podsieci oraz rozgłaszania i nie można ich wykorzystać. Drugi i trzeci adres IP mogą być używane dla interfejsów TCP/IP w wirtualnej sieci Ethernet na partycji A i na partycji B. W opisywanej procedurze zakres adresów IP wynosi od 10.1.1.72 do 10.1.1.75 z maską podsieci 255.255.255.252.

   Potrzebny jest również jeden adres IP używany jako jako zewnętrzny adres TCP/IP. Ten adres IP nie musi należeć do powyższego zakresu adresów IP, ale powinien znajdować się wewnątrz tej samej pierwotnej maski podsieci 255.255.255.0. W opisywanej procedurze zewnętrznym adresem IP jest 10.1.1.15.

2. Utwórz interfejs TCP/IP i5/OS dla partycji B. Ten interfejs jest znany jako zewnętrzny interfejs ARP proxy. Aby utworzyć ten interfejs, wykonaj następujące czynności:
   a. W wierszu komend partycji B wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
   c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* wpisz '10.1.1.15'.
   e. W polu *Opis linii* wpisz nazwę opisu linii, na przykład ETHLINE.
   f. W polu *Maska podsieci* wpisz '255.255.255.0'.
3. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

Krok 5: Tworzenie wirtualnego interfejsu TCP/IP na partycji A

Aby utworzyć interfejs wirtualny, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
3. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
4. W polu *Adres internetowy* wpisz '10.1.1.73'.
5. W polu *Opis linii* wpisz nazwę opisu linii, na przykład ETHLINE.
6. W polu *Maska podsieci* wpisz '255.255.255.252'.
7. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

Krok 6: Tworzenie wirtualnego interfejsu TCP/IP na partycji B

Aby utworzyć interfejs wirtualny, wykonaj następujące czynności:

1. W wierszu komend partycji B wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
3. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
4. W polu *Adres internetowy* wpisz '10.1.1.74'.
5. W polu *Opis linii* wpisz nazwę opisu linii, na przykład ETHLINE.
6. W polu *Maska podsieci* wpisz '255.255.255.252'.
7. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

Krok 7: Tworzenie listy preferowanych interfejsów

Można utworzyć listę preferowanych interfejsów, aby kontrolować, które adaptery i adresy IP będą stanowiły preferowany interfejs agentów ARP proxy wirtualnej sieci Ethernet.

Aby utworzyć listę preferowanych interfejsów, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **Sieć → Konfiguracja TCP/IP → IPv4**.
2. Wybierz pozycję **Interfejsy**.
3. Z wyświetlonej listy interfejsów wybierz interfejs wirtualnej sieci Ethernet, dla której ma zostać utworzona lista preferowanych interfejsów.

4. Kliknij prawym przyciskiem myszy interfejs, a następnie wybierz opcję **Właściwości**.
5. Kliknij zakładkę **Zaawansowane**.
6. Wybierz adresy interfejsów z listy dostępnych interfejsów w panelu i kliknij **Dodaj**.

   Można również usunąć interfejs z listy preferowanych interfejsów w prawym panelu, klikając **Usuń** lub też przesunąć interfejs w górę lub w dół listy w celu dokonania zmiany kolejności, klikając **Przesuń w górę** i **Przesuń w dół**.
7. Zaznacz pole wyboru **Włącz ARP proxy**, aby aktywować listę.
8. Kliknij przycisk **OK**, aby zapisać utworzoną listę preferowanych interfejsów.

Uwagi:

a. Lista preferowanych interfejsów może zawierać tylko 10 interfejsów. Jeśli zostanie skonfigurowanych więcej niż 10, lista będzie skrócona do pierwszych 10 interfejsów.
b. Interfejs dla którego będzie tworzona lista preferowanych interfejsów, musi być nieaktywny, aby lista mogła zostać skonfigurowana. Interfejsy znajdujące się na liście preferowanych interfejsów nie muszą być nieaktywne podczas konfigurowania listy.

Krok 8: Tworzenie trasy

Aby utworzyć domyślną trasę w celu umożliwienia pakietom wyjścia z wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz CFGTCP i naciśnij klawisz Enter.
2. Wybierz opcję 2 (Praca z trasami TCP/IP) i naciśnij klawisz Enter.
3. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter.
4. W polu *Cel trasy* wpisz *DFTROUTE.
5. W polu *Maska podsieci* wpisz *NONE.
6. W polu *Następny przeskok* wpisz '10.1.1.74'.

   Pakiety z partycji A przesyłane są przez wirtualną sieć Ethernet do interfejsu 10.1.1.74 przy użyciu domyślnej trasy. Ponieważ interfejs 10.1.1.74 jest powiązany z zewnętrznym interfejsem ARP proxy 10.1.1.15, pakiety IP wychodzą z wirtualnej sieci Ethernet przy użyciu interfejsu ARP proxy.

Krok 9: Sprawdzanie komunikacji sieciowej

Sprawdź komunikację sieciową za pomocą następującej komendy ping:

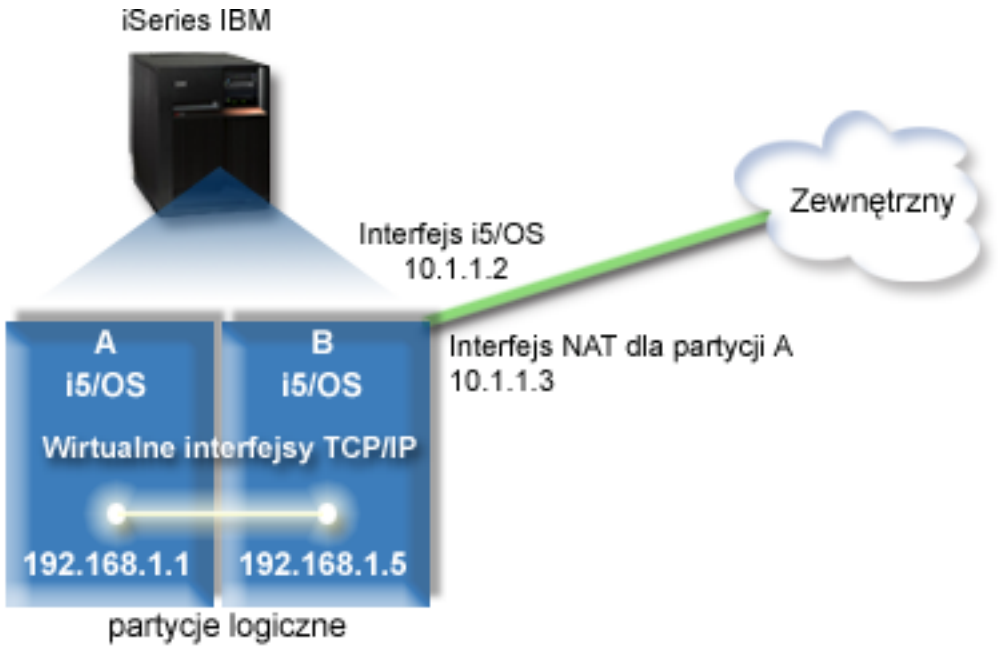
- Z partycji A wykonaj komendę ping do interfejsu wirtualnej sieci Ethernet 10.1.1.74 i zewnętrznego hosta.
- Z zewnętrznego hosta i5/OS wykonaj komendę ping do interfejsów wirtualnej sieci Ethernet 10.1.1.73 i 10.1.1.74.

Metoda translacji adresu sieciowego (NAT)

Filtrowanie pakietów w systemie i5/OS może być używane w celu kierowania ruchem między partycją a siecią zewnętrzną.

Translacja adresu sieciowego (Network address translation - NAT) umożliwia przekierowywanie ruchu między wirtualną siecią Ethernet a siecią zewnętrzną. Ta szczególna forma translacji NAT nazywa się statyczną translacją NAT i umożliwia ruch przychodzący do wirtualnej sieci Ethernet i wychodzący z tej sieci. Inne formy translacji NAT, na przykład maskowana translacja NAT, działają również, jeśli do wirtualnej sieci Ethernet nie przychodzi ruch zainicjowany przez klientów zewnętrznych. Podobnie jak w metodach routingu TCP/IP i ARP proxy można skorzystać z zalet istniejącego połączenia i5/OS. Ponieważ wymagane jest stosowanie reguł pakietów IP, należy skorzystać z programu iSeries Navigator w celu utworzenia reguł i ich zastosowania.

Poniższy rysunek przedstawia przykład użycia translacji NAT w celu połączenia wirtualnej sieci Ethernet z siecią zewnętrzną. Sieć 10.1.1.*x* reprezentuje sieć zewnętrzną, a sieć 192.168.1.*x* wirtualną sieć Ethernet.



W tym przykładzie cały ruch TCP/IP dla serwera przechodzi przez interfejs 10.1.1.2. Został utworzony nowy interfejs 10.1.1.3 w celu komunikacji między siecią 10.1.1.x i siecią 192.168.1.x. Ponieważ jest to scenariusz odwzorowania statycznego, ruch przychodzący jest przekształcany z interfejsu 10.1.1.3 do interfejsu 192.168.1.5. Ruch wychodzący jest przekształcany z interfejsu 192.168.1.5 do interfejsu zewnętrznego 10.1.1.3. Partycje A i B używają swoich interfejsów wizualnych 192.168.1.1 i 192.168.1.5 w celu wzajemnej komunikacji.

Aby statyczna translacja NAT mogła działać należy w pierwszej kolejności skonfigurować komunikację i5/OS i TCP/IP. Następnie należy utworzyć i zastosować reguły pakietów IP. Aby skonfigurować wirtualną sieć Ethernet w celu używania metody NAT, należy wykonać następujące zadania konfiguracyjne:

Krok 1: Aktywowanie partycji logicznych, aby mogły być uwzględniane w wirtualnej sieci Ethernet

Uwaga: Podczas konfigurowania wirtualnej sieci Ethernet na serwerze model 5*xx* należy zapoznać się z instrukcjami zawartymi w temacie Wirtualny Ethernet dla partycji logicznych systemu i5/OS Centrum informacyjnego - sprzęt IBM.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycja A) wpisz STRSST i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.
3. W panelu Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi).
4. W panelu Praca z partycjami systemu (Work with System Partitions) wybierz opcję 3 (Praca z konfiguracją partycji).
5. Naciśnij klawisz F10 (Praca z wirtualną siecią Ethernet).
6. Wpisz 1 w odpowiedniej kolumnie dla partycji A i dla partycji B, aby umożliwić obu partycjom wzajemną komunikację w wirtualnej sieci Ethernet.
7. Wyjdź z ekranu Narzędzia SST (System Service Tools - SST), aby powrócić do wiersza komend.

Informacje pokrewne

Konsolidowanie partycji i5/OS, AIX® i Linux® w systemie IBM eServer™ i5

Krok 2: Tworzenie opisu linii sieci Ethernet

W zależności od modelu używanego serwera możliwe są dwa sposoby wykonania tego kroku. Biorąc pod uwagę model używanego serwera, należy wybrać jeden z tych sposobów w celu utworzenia opisu linii.

Tworzenie opisu linii sieci Ethernet na serwerach model 270 i 8*xx*:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów model 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu używania wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

   Port sieci Ethernet o numerze 268C jest zasobem wirtualnej sieci Ethernet. Dla każdej wirtualnej sieci Ethernet połączonej z partycją logiczną istnieje jeden port.
3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć adres portu. Adres portu odpowiada wirtualnej sieci Ethernet, która została wybrana podczas konfigurowania partycji logicznej.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego portu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).
   a. W polu *Opis linii* wpisz VETH0. Nazwa VETH0, choć przypadkowa, odpowiada numerowanej kolumnie na stronie wirtualnej sieci Ethernet, w której została aktywowana partycja logiczna w celu komunikacji. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
   b. W polu *Szybkość linii* wpisz 1G.
   c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
   d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

      Zostanie wyświetlony komunikat o utworzeniu opisu linii.
6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Tworzenie opisów linii na serwerach modeli innych niż 270 i 8xx:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów modeli innych niż 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu obsługi wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

Porty sieci Ethernet o numerach 268C są zasobami wirtualnej sieci Ethernet. Dla każdego adaptera wirtualnej sieci Ethernet istnieje jeden port. Każdy port o numerze 268C ma powiązany kod położenia wprowadzony podczas tworzenia adaptera wirtualnej sieci Ethernet przy użyciu konsoli HMC (krok 1).

3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć zasób o numerze 268C, który jest powiązany z konkretnym kodem położenia utworzonym dla tej wirtualnej sieci Ethernet.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego zasobu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).
   a. W polu *Opis linii* wpisz VETH0. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa VETHO, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
   b. W polu *Szybkość linii* wpisz 1G.
   c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
   d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

      Zostanie wyświetlony komunikat o utworzeniu opisu linii.
6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Krok 3: Włączanie przesyłania datagramów IP

Włączanie przesłania datagramów IP, aby pakiety mogły być przesyłane między różnymi podsieciami.

Aby włączyć przesyłanie datagramów IP, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz CHGTCPA i naciśnij klawisz F4.
2. W polu *Przesyłanie datagramów IP* wpisz *YES.

Krok 4: Tworzenie interfejsów

Aby utworzyć interfejsy TCP/IP, wykonaj następujące czynności:

1. Utwórz i uruchom interfejs TCP/IP i5/OS na partycji B w celu ogólnej komunikacji z serwerem w obie strony. Aby utworzyć ten interfejs, wykonaj następujące czynności:
   a. W wierszu komend partycji B wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
   c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* wpisz '10.1.1.2'.
   e. W polu *Opis linii* wpisz ETHLINE.
   f. W polu *Maska podsieci* wpisz '255.255.255.0'.
   g. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.
2. Utwórz i uruchom inny interfejs TCP/IP połączony z zewnętrzną siecią. Powinien on używać tego samego opisu linii, którego używa istniejący zewnętrzny interfejs TCP/IP. Ten interfejs wykona ostatecznie translację adresu dla partycji. Aby utworzyć ten interfejs, wykonaj następujące czynności:

a. W wierszu komend partycji B wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
d. W polu *Adres internetowy* wpisz '10.1.1.3'.
e. W polu *Opis linii* wpisz ETHLINE.
f. W polu *Maska podsieci* wpisz '255.255.255.0'.
g. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

3. Utwórz i uruchom interfejs TCP/IP i5/OS na partycji A dla wirtualnej sieci Ethernet. Aby utworzyć ten interfejs, wykonaj następujące czynności:
   a. W wierszu komend partycji A wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
   c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* wpisz '192.168.1.1'.
   e. W polu *Opis linii* wpisz VETH0.
   f. W polu *Maska podsieci* wpisz '255.255.255.0'.
   g. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.
4. Utwórz i uruchom interfejs TCP/IP i5/OS na partycji B dla wirtualnej sieci Ethernet. Aby utworzyć ten interfejs, wykonaj następujące czynności:
   a. W wierszu komend partycji B wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
   c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* wpisz '192.168.1.5'.
   e. W polu *Opis linii* wpisz VETH0.
   f. W polu *Maska podsieci* wpisz '255.255.255.0'.
   g. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

Krok 5: Sprawdzanie komunikacji sieciowej

Sprawdź komunikację sieciową za pomocą następującej komendy ping:

- Z partycji A wykonaj komendę ping do interfejsu wirtualnej sieci Ethernet 192.168.1.5 i zewnętrznego hosta.
- Z zewnętrznego hosta i5/OS wykonaj komendę ping do każdego z interfejsów wirtualnej sieci Ethernet 192.168.1.1 i 192.168.1.5.

Krok 6: Tworzenie reguł pakietów

W programie iSeries Navigator należy użyć kreatora translacji adresów w celu utworzenia reguł pakietów odwzorowujących adres prywatny na partycji A na adres publiczny na partycji B.

Aby utworzyć reguły pakietów, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń *serwer* → **Sieć** → **Strategia IP**.
2. Prawym klawiszem myszy kliknij **Reguły pakietów** i wybierz **Edytor reguł**.

3. Wybierz **Translacja adresu** w menu **Kreator**.
4. Wykonuj instrukcje kreatora, aby utworzyć reguły pakietów. W tej procedurze użyj następujących wyborów:
   - Wybierz **Odwzoruj translację adresu**.
   - Wpisz adres prywatny IP 192.168.1.1.
   - Wpisz adres publiczny IP 10.1.1.3.
   - Wybierz linię, w której skonfigurowane są interfejsy, na przykład ETHLINE.
5. Wybierz **Aktywuj reguły** w menu **Plik**.

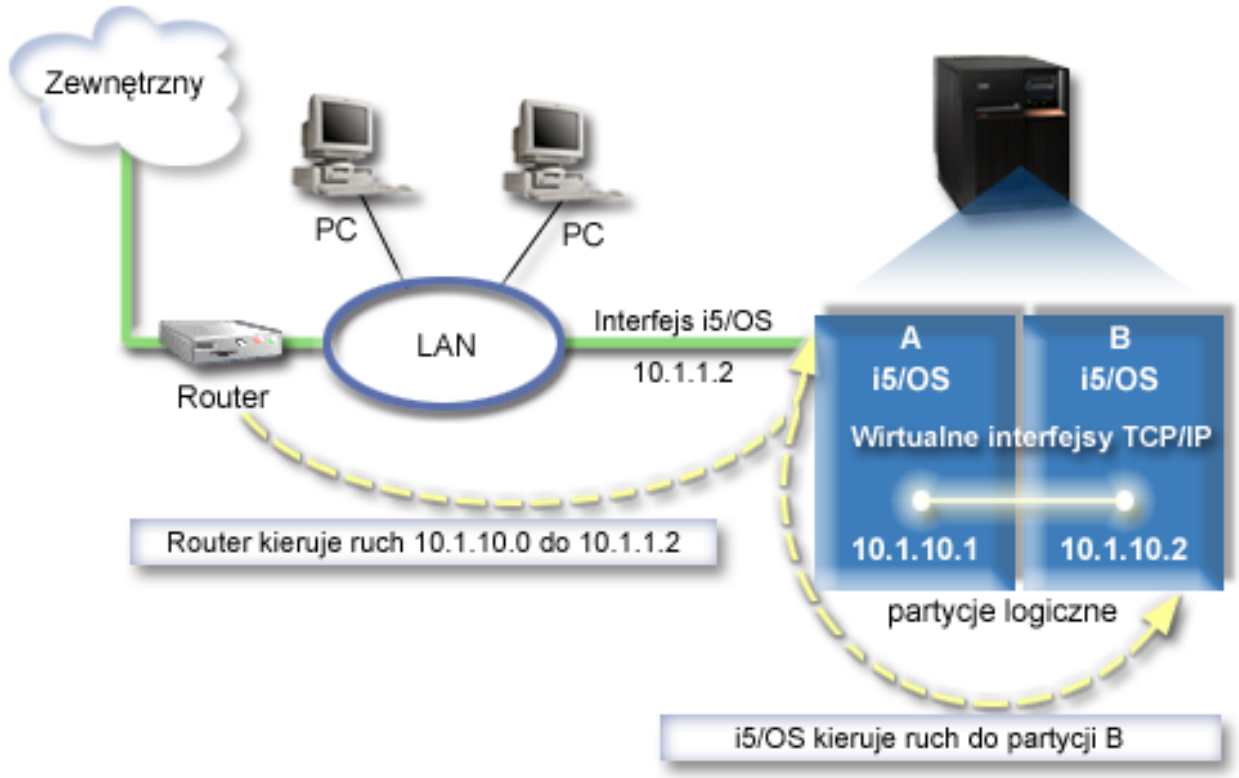
Krok 7: Sprawdzanie komunikacji sieciowej

Po utworzeniu reguł pakietów należy sprawdzić komunikację sieciową. Aby przetestować komunikację wychodzącą, należy wykonać komendę ping z partycji A do hosta zewnętrznego. Następnie z hosta zewnętrznego należy wykonać komendę ping do partycji A w celu przetestowania komunikacji przychodzącej.

Metoda routingu TCP/IP

Standardowy routing TCP/IP używany jest do kierowania ruchu do wirtualnej sieci Ethernet w ten sam sposób, w jaki odbywa się kierowanie ruchu do każdej innej sieci LAN. W tym celu konieczna jest aktualizacja tabel routingu w sieci.

W celu przekierowania ruchu do swoich partycji przez serwer iSeries można ponadto użyć różnych technik routingu. Ta metoda nie jest trudna do skonfigurowania na serwerze, ale w zależności od topologii sieci, jej zaimplementowanie może być niewygodne. Należy rozważyć poniższy rysunek.



Istniejący interfejs (10.1.1.2) połączony jest z siecią LAN. Sieć LAN jest połączona ze zdalnymi sieciami za pomocą routera. Wirtualny interfejs TCP/IP na partycji B ma adres 10.1.10.2, a wirtualny interfejs na partycji A - 10.1.10.1. W systemie i5/OS po włączeniu przekazywania datagramów IP, system i5/OS przekieruje pakiety IP do partycji B i z partycji B. Podczas definiowania połączenia TCP/IP dla partycji B adres routera musi być równy 10.1.10.1.

Ten rodzaj routingu może być trudny w związku z pobieraniem pakietów IP do serwera iSeries. W tym scenariuszu można zdefiniować trasę na routerze w taki sposób, aby pakiety kierowane do sieci 10.1.10.0 wędrowały do interfejsu

10.1.1.2. To działa dla zdalnych klientów sieci. Może to również działać w przypadku klientów lokalnej sieci LAN (klientów połączonych z tą samą siecią LAN, z którą połączony jest serwer iSeries), jeśli ten sam router jest rozpoznawany jako następny przeskok. W przeciwnym razie każdy klient musi mieć trasę, która przekierowuje ruch 10.1.10.0 do interfejsu i5/OS 10.1.1.2. Na tym polega niepraktyczność tej metody. Dla dużej liczby klientów LAN należy zdefiniować dużą liczbę tras.

Aby skonfigurować wirtualną sieć Ethernet w celu używania metody routingu TCP/IP, należy wykonać następujące instrukcje:

Krok 1: Aktywowanie partycji logicznych, aby mogły być uwzględniane w wirtualnej sieci Ethernet

Uwaga: Podczas konfigurowania wirtualnej sieci Ethernet na serwerze model 5*xx* należy zapoznać się z instrukcjami zawartymi w temacie Wirtualny Ethernet dla partycji logicznych systemu i5/OS Centrum informacyjnego - sprzęt IBM.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycja A) wpisz STRSST i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.
3. W panelu Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi).
4. W panelu Praca z partycjami systemu (Work with System Partitions) wybierz opcję 3 (Praca z konfiguracją partycji).
5. Naciśnij klawisz F10 (Praca z wirtualną siecią Ethernet).
6. Wpisz 1 w odpowiedniej kolumnie dla partycji A i dla partycji B, aby umożliwić obu partycjom wzajemną komunikację w wirtualnej sieci Ethernet.
7. Wyjdź z ekranu Narzędzia SST (System Service Tools - SST), aby powrócić do wiersza komend.

Informacje pokrewne

Konsolidowanie partycji i5/OS, AIX® i Linux® w systemie IBM eServer™ i5

Krok 2: Tworzenie opisu linii sieci Ethernet

W zależności od modelu używanego serwera możliwe są dwa sposoby wykonania tego kroku. Biorąc pod uwagę model używanego serwera, należy wybrać jeden z tych sposobów w celu utworzenia opisu linii.

Tworzenie opisu linii sieci Ethernet na serwerach model 270 i 8*xx*:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów model 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu obsługi wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

   Port sieci Ethernet o numerze 268C jest zasobem wirtualnej sieci Ethernet. Dla każdej wirtualnej sieci Ethernet połączonej z partycją logiczną istnieje jeden port.
3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć adres portu. Adres portu odpowiada wirtualnej sieci Ethernet, która została wybrana podczas konfigurowania partycji logicznej.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego portu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).

a. W polu *Opis linii* wpisz VETH0. Nazwa VETH0, choć przypadkowa, odpowiada numerowanej kolumnie na stronie wirtualnej sieci Ethernet, w której została aktywowana partycja logiczna w celu komunikacji. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
b. W polu *Szybkość linii* wpisz 1G.
c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

   Zostanie wyświetlony komunikat o utworzeniu opisu linii.

6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Tworzenie opisów linii na serwerach modeli innych niż 270 i 8xx:

Tworzenie opisu linii sieci Ethernet jest pierwszym krokiem konfigurowania serwera w celu użycia wirtualnej sieci Ethernet. Poniższe czynności można wykorzystać do konfigurowania serwerów modeli innych niż 270 i 8*xx*.

Aby skonfigurować nowe opisy linii sieci Ethernet w celu obsługi wirtualnej sieci Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz WRKHDWRSC *CMN i naciśnij klawisz Enter.
2. W panelu Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetl szczegóły zasobów) obok odpowiedniego portu wirtualnej sieci Ethernet.

   Porty sieci Ethernet o numerach 268C są zasobami wirtualnej sieci Ethernet. Dla każdego adaptera wirtualnej sieci Ethernet istnieje jeden port. Każdy port o numerze 268C ma powiązany kod położenia wprowadzony podczas tworzenia adaptera wirtualnej sieci Ethernet przy użyciu konsoli HMC (krok 1).
3. W panelu Wyświetlanie szczegółów zasobów (Display Resource Details) przewiń w dół, aby znaleźć zasób o numerze 268C, który jest powiązany z konkretnym kodem położenia utworzonym dla tej wirtualnej sieci Ethernet.
4. W panelu Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji) obok odpowiedniego zasobu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W panelu Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić ekran Tworzenie opisu linii Ethernet (Create Line Description Ethernet - CRTLINETH).
   a. W polu *Opis linii* wpisz VETH0. Jeśli dla opisu linii i dla powiązanej z nią wirtualnej sieci Ethernet zostanie użyta taka sama nazwa VETHO, łatwiej będzie można śledzić konfigurację wirtualnej sieci Ethernet.
   b. W polu *Szybkość linii* wpisz 1G.
   c. W polu *Dupleks* wpisz *FULL i naciśnij klawisz Enter.
   d. W polu *Maksymalna wielkość ramki* wpisz 8996 i naciśnij klawisz Enter. Zmiana wielkości ramki na 8996 powoduje poprawę przesyłania danych w wirtualnej sieci Ethernet.

      Zostanie wyświetlony komunikat o utworzeniu opisu linii.
6. Udostępnij opis linii. Wpisz WRKCFGSTS *LIN i wybierz opcję 1 (Udostępnij) dla VETH0.
7. Powtórz czynności od 1 do 6, ale wykonaj je z wiersza komend partycji B, aby utworzyć opis linii sieci Ethernet dla partycji B.

   Chociaż nazwy opisów linii są przypadkowe, dobrze jest używać takich samych nazw dla wszystkich opisów linii powiązanych z wirtualną siecią Ethernet. W tym scenariuszu wszystkie opisy linii mają nazwę VETH0.

Kolejne czynności: Włączanie przesyłania datagramów IP

Krok 3: Włączanie przesyłania datagramów IP

Włączanie przesłania datagramów IP, aby pakiety mogły być przesyłane między różnymi podsieciami.

Aby włączyć przesyłanie datagramów IP, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz CHGTCPA i naciśnij klawisz F4.
2. W polu *Przesyłanie datagramów IP* wpisz *YES.

Krok 4: Tworzenie interfejsów

Aby utworzyć interfejsy TCP/IP, wykonaj następujące czynności:

1. Utwórz interfejs TCP/IP i5/OS na partycji A. Aby utworzyć ten interfejs, wykonaj następujące czynności:
   a. W wierszu komend partycji A wpisz CFGTCP i naciśnij klawisz Enter w celu wyświetlenia panelu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 1 (Praca z interfejsami TCP/IP) i naciśnij klawisz Enter.
   c. Wybierz opcję 1 (Dodaj) i naciśnij klawisz Enter w celu wyświetlenia panelu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* wpisz '10.1.1.2'.
   e. W polu *Opis linii* wpisz nazwę opisu linii, na przykład ETHLINE.
   f. W polu *Maska podsieci* wpisz '255.255.255.0'.
2. Uruchom interfejs. W panelu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.
3. Powtórz czynności 2 i 3 w celu utworzenia i uruchomienia interfejsów TCP/IP na partycjach A i B.

   Te interfejsy są używane w wirtualnej sieci Ethernet. Dla tych interfejsów należy zastosować adresy 10.1.10.1 i 10.1.10.2 oraz maskę podsieci 255.255.255.0.

Uwagi na temat wirtualnej sieci Ethernet

Wirtualna sieć Ethernet może być używana jako rozwiązanie alternatywne dla karty sieciowej w komunikacji między partycjami.

Umożliwia ona nawiązywanie szybkich połączeń między partycjami logicznymi bez potrzeby kupowania dodatkowego sprzętu. Dla każdego z 16 włączonych portów system tworzy port komunikacyjny wirtualnej sieci Ethernet, taki jak CMN*xx*, którego typem zasobu jest 268C. Dzięki temu partycje logiczne przypisane do tej samej sieci lokalnej (LAN) stają się dostępne do komunikacji przez to łącze. System fizyczny umożliwia skonfigurowanie maksimum 16 różnych wirtualnych sieci lokalnych. Wirtualna sieć Ethernet pełni taką samą funkcję jak adapter Ethernet 1 Gb. Sieć Token Ring lub sieci lokalne Ethernet 10 Mbps i 100 Mbps nie są obsługiwane przez wirtualną sieć Ethernet.

Wirtualna sieć Ethernet jest oszczędnym rozwiązaniem sieciowym przynoszącym znaczne korzyści:

- Oszczędność: Potencjalnie nie jest wymagany żaden dodatkowy sprzęt sieciowy. Można dodać partycje do serwera i komunikować się z zewnętrzną siecią LAN bez potrzeby instalowania dodatkowych fizycznych kart LAN. Jeśli serwer bieżący ma ograniczoną liczbę dostępnych gniazd na karty, w których można zainstalować dodatkowe karty LAN, używanie wirtualnej sieci Ethernet stwarza możliwość działania na partycjach przyłączonych do sieci LAN bez konieczności aktualizowania serwera.
- Elastyczność: Możliwe jest skonfigurowanie maksymalnie 16 różnych połączeń umożliwiających konfigurowanie selektywnych ścieżek komunikacyjnych między partycjami. Dodatkowo ten model konfiguracji umożliwia partycjom logicznym implementowanie zarówno wirtualnej sieci Ethernet, jak i fizycznego połączenia sieci LAN. Ta cecha jest przydatna podczas używania partycji Linux w celu udostępnienia aplikacji firewall.
- Szybkość: Wirtualna sieć Ethernet emuluje połączenie Ethernet 1 Gb oraz zapewnia szybką i dogodną komunikację między partycjami. To stwarza możliwość zintegrowania oddzielnych aplikacji uruchomionych na różnych partycjach logicznych.
- Wszechstronność: Bez względu na to, czy partycje uruchomione są w systemie i5/OS czy w systemie Linux, mogą być połączone z tą samą wirtualną siecią Ethernet.

- Zredukowane obciążenie: Używanie wirtualnej sieci Ethernet do komunikacji między partycjami powoduje zmniejszenie ruchu w zewnętrznej sieci LAN. W przypadku sieci Ethernet, w której kolizje występują standardowo, zapobiega to pogorszeniu jakości usług dla innych użytkowników sieci LAN.

Informacje pokrewne dotyczące konfigurowania protokołu TCP/IP

Wymieniono tu podręczniki dotyczące produktów oraz dokumentację techniczną IBM (Redbooks) w formacie PDF, serwisy WWW oraz tematy Centrum informacyjnego związane z konfigurowaniem TCP/IP. Wszystkie pliki PDF można przeglądać lub drukować.

Dokumentacja techniczna IBM (Redbooks)

- TCP/IP Tutorial and Technical Overview (7 MB) Ta dokumentacja techniczna IBM (Redbook) zawiera podstawowe informacje na temat protokołu TCP/IP.
- TCP/IP for AS/400: More Cool Things Than Ever (9 MB) Ta dokumentacja techniczna IBM (Redbook) zawiera szczegółową listę typowych aplikacji i usług TCP/IP.

Serwisy WWW

- The Internet Engineering Task Force (IETF) (www.ietf.cnri.reston.va.us)
  Informacje o grupie, która tworzy protokół IP, w tym IPv6.
- IP Version 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  Aktualne specyfikacje protokołu IPv6 i odnośniki do kilku źródeł na temat IPv6.
- IPv6 Forum (www.ipv6forum.com)
  Najnowsze artykuły oraz wydarzenia związane z projektowaniem protokołu IPv6.

Inne informacje

- TCP/IP: Ten temat zawiera informacje o aplikacjach i usługach TCP/IP innych niż konfiguracyjne.
- Rozwiązywanie problemów dotyczących protokołu TCP/IP: Ten temat zawiera informacje, które pomogą w rozwiązaniu problemów z połączeniami TCP/IP lub ruchem w sieci IPv4 i IPv6.
- Planowanie i instalowanie ochrony systemu: Ten temat zawiera informacje na temat planowania oraz instalowania ochrony systemu na serwerze iSeries.

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego dalszego wykorzystania:

1. W przeglądarce kliknij prawym przyciskiem myszy plik PDF (kliknij prawym przyciskiem myszy powyższy odsyłacz).
2. Kliknij opcję lokalnego zapisywania pliku PDF.
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Kopię programu można pobrać z serwisu WWW Adobe (www.adobe.com/products/acrobat/readstep.html) .

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of
Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ ZNAJDUJE (“ AS IS”) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy są fikcyjne i jakiekolwiek ich podobieństwo do nazwisk, nazw i adresów używanych w rzeczywistych przedsiębiorstwach jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje na temat interfejsu programistycznego

Niniejsza publikacja opisuje planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu operacyjnego IBM i5/OS.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

| AIX
| AS/400
| eServer
| i5/OS
| IBM
| IBM (logo)
| iSeries
| Redbooks

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

| Linux jest znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i/lub w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY

DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.