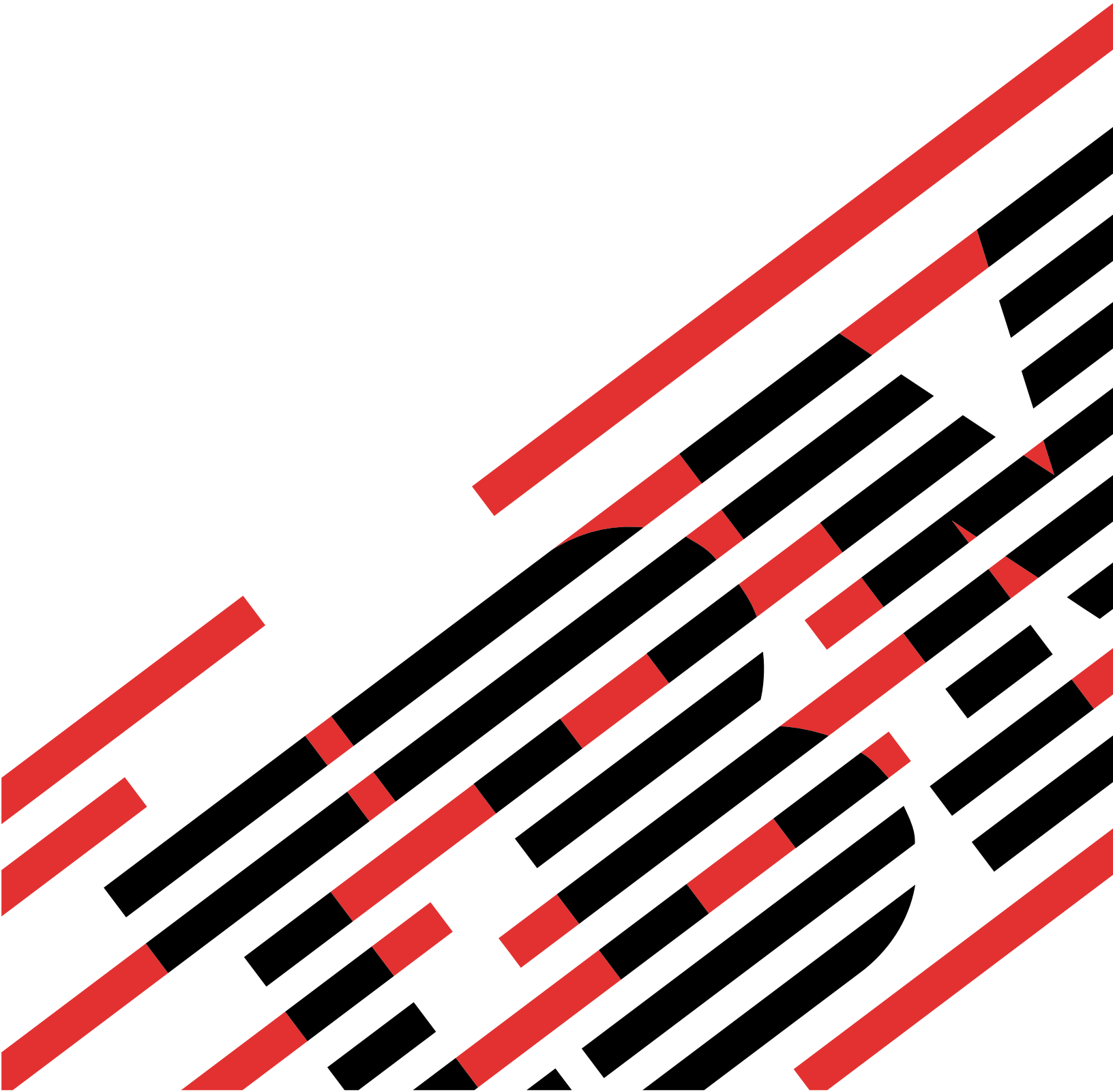
IBM

eserver

iSeries

Sieci
Konfigurowanie TCP/IP



IBM

@server

iSeries

Sieci
Konfigurowanie TCP/IP

Spis treści

Część 1. Konfigurowanie TCP/IP

Otrzymałeś wreszcie swój serwer iSeries i chcesz go uruchomić. W tej sekcji opisano narzędzia i procedury przeznaczone do konfigurowania połączenia i protokołu TCP/IP na serwerze iSeries. Po wykonaniu czynności wstępnych będziesz mógł rozszerzyć TCP/IP o aplikacje spełniające Twoje specyficzne wymagania.

Co nowego w wersji V5R2
Zapoznanie się z nowymi i zmienionymi funkcjami TCP/IP.

Drukowanie tego dokumentu
W temacie tym opisano drukowanie lub przeglądanie wersji PDF dokumentacji o konfigurowaniu TCP/IP.

Protokół IPv6
Nowa wersja protokołu IP odgrywa ważną rolę w tworzeniu przyszłości sieci Internet. Obecniemożna jej już używać na serwerze iSeries. Temat ten przedstawia ogólne informacje o protokole IPv6 i jego implementacji na serwerze iSeries.

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. Podano również odsyłacze do terminów i koncepcji pokrewnych.

Instalowanie TCP/IP
Temat ten zawiera informacje potrzebne podczas instalowania produktów przygotowujących serwer iSeries do normalnej pracy.

Konfigurowanie TCP/IP
Temat ten zawiera informacje o tym, jak wykorzystać serwer iSeries i skonfigurować protokół TCP/IP. Ponadto zawiera też informacje o konfigurowaniu protokołu IPv6.

Dostosowanie konfiguracji TCP/IP za pomocą programu iSeries Navigator
Temat ten zawiera informacje dotyczące opcji konfiguracyjnych dostępnych w programie iSeries Navigator.

Rozwiązywanie problemów z TCP/IP
Jeśli wystąpią jakieś problemy z połączeniami lub ruchem TCP/IP, znalezienie rozwiązania ułatwi temat Rozwiązywanie problemów z TCP/IP. Informacje w nim zawarte powinny pomóc rozwiązać zarówno problemy związane z protokołem IPv4, jak i IPv6.

Informacje związane z konfigurowaniem protokołu TCP/IP
Ten temat zawiera odpowiedź na pytanie ″Co jeszcze mogę zrobić?″ Zawiera odsyłacze do serwisów i aplikacji umożliwiających poprawę wydajności serwera.

Rozdział 1. Co nowego w wersji V5R2

Nowe punkty o konfigurowaniu TCP/IP w wersji 5 wydanie 2:

- **Konfigurowanie TCP/IP za pomocą interfejsu znakowego**
  Instrukcje konfigurowania TCP/IP dla użytkowników konfigurujących serwer za pomocą interfejsu znakowego. Zalecaną metodą konfigurowania TCP/IP jest korzystanie z kreatora EZ-Setup; aby jednak użyć programu iSeries Navigator z komputera PC, co wymaga wstępnego skonfigurowania TCP/IP, należy najpierw skonfigurować TCP/IP za pomocą interfejsu znakowego.
- **Protokół IPv6**
  Podstawowe informacje o protokole IPv6 i o jego implementacji na serwerze iSeries.
- **Konfigurowanie protokołu IPv6**
  Wymagania wstępne i instrukcja konfigurowania serwera dla protokołu IPv6.
- **Dostosowanie konfiguracji TCP/IP za pomocą programu iSeries Navigator**
  Ten temat został rozwinięty i zawiera nowe metody dostosowywania konfiguracji TCP/IP. Program iSeries Navigator zawiera nowe kreatory do konfigurowania protokołu IPv6 i tworzenia nowych interfejsów i tras.

Więcej informacji o nowościach i zmianach w tym wydaniu zawiera dokument Informacje dla użytkowników  .

Rozdział 2. Drukowanie tego dokumentu

Aby przejrzeć lub pobrać wersję PDF tego dokumentu, należy wybrać Konfigurowanie TCP/IP (około 326 kB lub 41 stron).

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

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

Pobieranie programu Adobe Acrobat Reader

Program Adobe Acrobat Reader, potrzebny do przeglądania i drukowania plików PDF, można pobrać z serwisu WWW firmy Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Rozdział 3. Protokół IPv6

Protokół IPv6 jest aktualizacją wersji 4 protokołu IP i jako standard internetowy stopniowo zastępuje wersję poprzednią.

Zarówno gdy protokół IPv6 służy firmie do poszerzenia działalności w zakresie e-biznesu, jak i do tworzenia aplikacji korzystających z tego protokołu, w obu tych wypadkach konieczne są dokładniejsze informacje na temat jego możliwości. Podstawowe informacje o IPv6 i o tym, jak z niego korzystać na serwerze iSeries, znajdują się w następujących sekcjach:

Co to jest protokół IPv6
Powody wymiany standardu IPv4 na IPv6 i korzyści płynące z nowego protokołu.

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

Scenariusze wykorzystania protokołu IPv6
Przykłady, które pomogą zrozumieć, kiedy można zastosować protokół IPv6.

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

Konfigurowanie protokołu IPv6
Programowe i sprzętowe wymagania i instrukcje dotyczące konfigurowania protokołu IPv6 na serwerze.

Rozwiązywanie problemów dotyczących protokołu IPv6
Rozwiązania problemów dotyczących protokołu IPv6.

Informacje związane z protokołem IPv6
Odsyłacze do zasobów pomocnych w zrozumieniu protokołu IPv6.

Co to jest protokół IPv6

Protokół IPv6 jest nowszą, udoskonaloną wersją protokołu IP. W przeważającej części Internetu używany jest protokół IPv4, który był niezawodny i elastyczny przez ponad 20 lat. 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 szesnastkową.

Możliwość rozszerzenia adresów stanowi rozwiązanie problemu uszczuplania ich zasobów. 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 rozwiązuje te problemy dostarczając 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.

Jeśli używasz IPv6, nie musisz zmieniać adresów swoich urządzeń przy zmianie dostawcy usług internetowych. Możesz zatrzymać te same adresy, gdyż są one unikalne w skali globalnej.

Opcja autokonfiguracji IPv6 dokona automatycznej konfiguracji interfejsu i adresu routera. W autokonfiguracji bezstanowej protokół IPv6 połączy adres MAC urządzenia i przedrostek sieci dostarczony przez węzeł lokalny, tworząc w ten sposób nowy, unikalny adres IPv6. Opcja ta eliminuje konieczność korzystania z serwera DHCP, a co za tym idzie oszczędza czas administratora i pieniądze przedsiębiorstwa.

Więcej informacji o IPv6 zawiera temat Informacje związane z IPv6.

Temat Dostępne funkcje protokołu IPv6 zawiera informacje o IPv6 dotyczące przede wszystkim serwera iSeries.

Dostępne funkcje protokołu IPv6

Firma IBM zaimplementowała protokół IPv6 już w kilku wersjach oprogramowania serwera iSeries. Obecnie protokół IPv6 został zaimplementowany w platformie tworzenia aplikacji, umożliwiając projektowanie i testowanie aplikacji korzystających z protokołu IPv6. Funkcje IPv6 są przezroczyste dla istniejących aplikacji TCP/IP i współistnieją z funkcjami IPv4.

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

- **Konfigurowanie**
  Proces konfigurowania w przypadku protokołu IPv6 jest inny, niż analogiczny proces dla IPv4. Aby korzystać z funkcji IPv6, należy zmienić konfigurację TCP/IP serwera, konfigurując linię dla IPv6. Dla protokołu IPv6 można skonfigurować linię Ethernet lub tunel.

  Po skonfigurowaniu linii Ethernet dla ruchu IPv6 wysyła się pakiety IPv6 w sieci IPv6. Scenariusz opisujący, kiedy konfigurować linię Ethernet dla IPv6, zawiera sekcja Tworzenie sieci lokalnej IPv6.

  Po skonfigurowaniu tunelu, pakiety IPv6 będą wysyłane przez istniejącą sieć IPv4. Scenariusze opisujące dwie przykładowe sytuacje, w których warto skonfigurować tunel dla IPv6, znajdują się w sekcjach Wysyłanie pakietów IPv6 przez sieć lokalną IPv4 i Wysyłanie pakietów IPv6 przez sieć rozległą IPv4.

  Aby skonfigurować sieć dla protokołu IPv6, zapoznaj się z sekcją Konfigurowanie protokołu IPv6.
- **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 obsługujące współbieżnie ruch IPv4 i IPv6 lub jedynie ruch IPv6. Więcej informacji o gniazdach w IPv6 zawiera sekcja Używanie rodziny adresów AF_INET6.
- **DNS**
  System nazw domen (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 i tunelami 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 zarówno związanych z siecią IPv4, jak i z siecią IPv6, warto zapoznać się z sekcją Rozwiązywanie problemów dotyczących protokołu TCP/IP.

Źródła danych dotyczących IPv6 są przedstawione w sekcji Informacje związane z IPv6.

Scenariusze: używanie protokołu IPv6

Przeglądnij następujące scenariusze, aby zrozumieć, dlaczego zaimplementować IPv6 i jak skonfigurować sieć w każdej z przedstawionych sytuacji:

- Tworzenie sieci lokalnej IPv6
- Wysyłanie pakietów IPv6 przez sieć lokalną IPv4
- Wysyłanie pakietów IPv6 przez sieć rozległą IPv4

Uwaga: W scenariuszu adres IP 10.x.x.x reprezentuje publiczny adres IP. Wszystkie użyte w scenariuszu adresy są tylko przykładami.

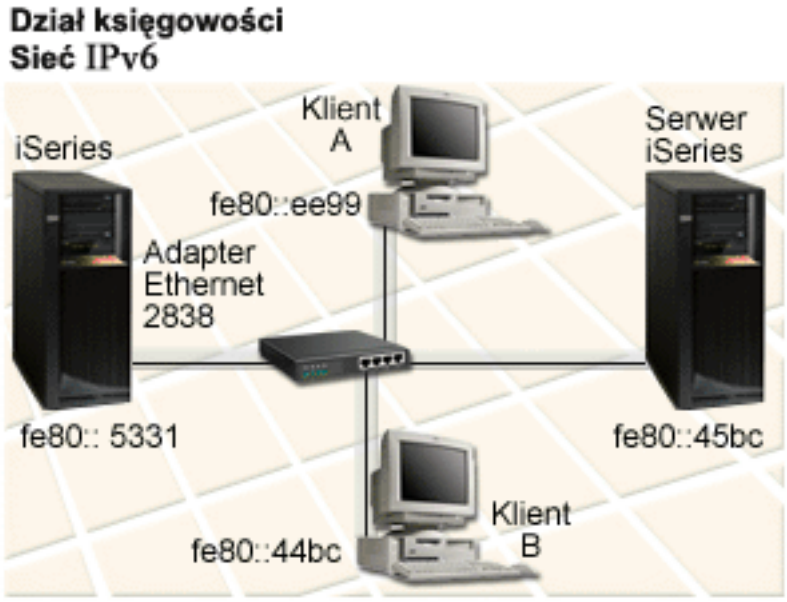
Aby skonfigurować serwer dla protokołu IPv6, zapoznaj się z sekcją Konfigurowanie protokołu IPv6.

Definicje podstawowych pojęć związanych z IPv6 znajdziesz w sekcji Pojęcia związane z IPv6.

Tworzenie sieci lokalnej 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 musisz skonfigurować opis linii Ethernet dla IPv6. Pakiety IPv6 poruszają się pomiędzy serwerami i klientami iSeries, a pracownicy mogą korzystać z programu księgowego.

Wymagania konfiguracji obejmują:

- System operacyjny OS/400 wersja 5 wydanie 2 lub nowsze.
- Adaptery Ethernet 2838 lub 2849, jedyne adaptery, które obsługują protokół IPv6.
- Program iSeries Access for Windows i iSeries Navigator (komponent sieciowy programu iSeries Navigator).
- Przed rozpoczęciem konfigurowania linii Ethernet należy na serwerze skonfigurować oddzielny interfejs fizyczny dla IPv6, ponieważ musi na nim działać protokół TCP/IP. Jeśli serwer nie jest skonfigurowany do korzystania z IPv4, to przed rozpoczęciem konfigurowania dla IPv6 należy przeczytać sekcję Konfigurowanie po raz pierwszy protokołu TCP/IP.

Konfigurowanie

Aby skonfigurować opis linii Ethernet dla IPv6, należy użyć kreatora **Konfiguracja IPv6** z programu iSeries Navigator. Protokół IPv6 można konfigurować tylko z programu iSeries Navigator, nie można tego zrobić z interfejsu znakowego.

Kreator wymaga podania nazwy sprzętowego zasobu komunikacyjnego na serwerze, na którym będzie konfigurowany protokół IPv6; na przykład CMN01. Musi to być adapter Ethernet 2838 lub 2849, jeszcze nie skonfigurowany dla IPv4.

Aby skorzystać z kreatora **Konfiguracja IPv6**, wykonaj następujące czynności:

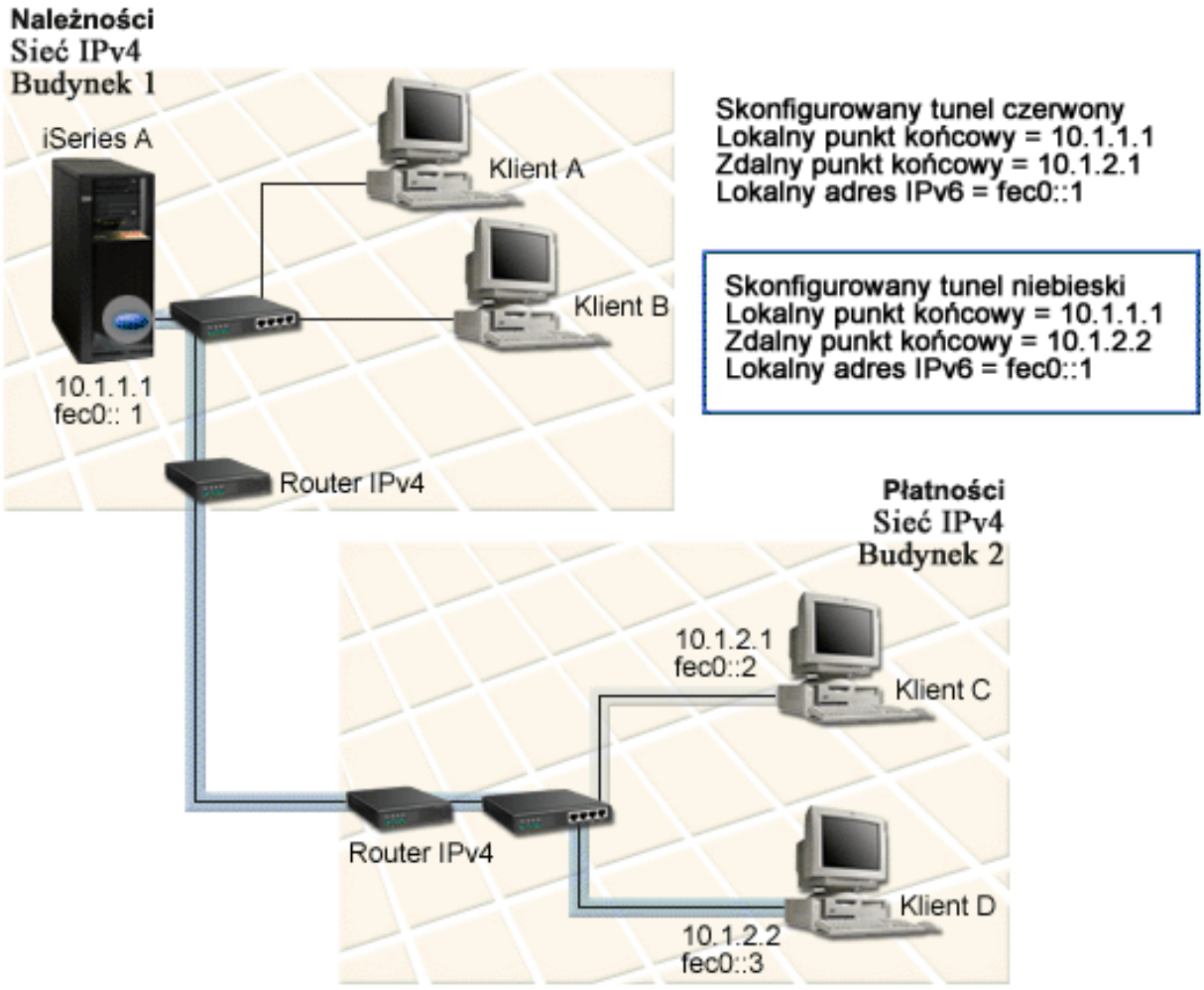
1. W programie iSeries Navigator wybierz **serwer —> Sieć —> Konfiguracja TCP/IP**.
2. Kliknij prawym przyciskiem myszy **IPv6** i wybierz **Konfiguracja IPv6**, a następnie skonfiguruj linię Ethernet dla IPv6 wykonując kolejne instrukcje kreatora.

Wysyłanie pakietów IPv6 przez sieć lokalną IPv4

Opis sytuacji

W firmie powstał nowy program do obsługi księgowości, korzystający z protokołu IPv6. Jest to program typu klient/serwer, który będzie używany lokalnie. Program komunikuje się z innymi swoimi instancjami w ramach przedsiębiorstwa, znajdującymi się w innych budynkach i sieciach LAN. Wprawdzie firma chce na potrzeby tej aplikacji korzystać z protokołu IPv6, ale nie jest jeszcze gotowa do zmiany całej istniejącej infrastruktury opartej na protokole IPv4 na nowy protokół. Twoim zadaniem więc jest takie skonfigurowanie tuneli, aby pakiety IPv6 przechodziły przez lokalne sieci IPv4. Rysunek przedstawia konfigurację sieci używanej dla

potrzeb scenariusza.



Rozwiązanie

Aby korzystać z protokołu IPv6 przez istniejące sieci IPv4, należy utworzyć dwa skonfigurowane tunele i kilka powiązanych z nimi tras. Dla przykładu pierwszy tunel został zaznaczony kolorem czerwonym, drugi niebieskim.

Najpierw należy zwrócić uwagę na tunel czerwony:

- Tunel czerwony zaczyna się na serwerze iSeries A (lokalny punkt końcowy 10.1.1.1) w Budynku 1, a kończy na Kliencie C (zdalny punkt końcowy 10.1.2.1) w Budynku 2.
- Serwer iSeries A hermetyzuje pakiet IPv6 w pakiecie IPv4 i wysyła pakiet IPv4 przez tunel do Klienta C, który go dehermetyzuje i przekazuje do innej instancji aplikacji IPv6.

Następnie należy zapoznać się z tunelem niebieskim:

- Tunel niebieski zaczyna się na serwerze iSeries A (lokalny punkt końcowy 10.1.1.1) w Budynku 1, podobnie jak tunel czerwony, jednak kończy się na Kliencie D (zdalny punkt końcowy 10.1.2.2) w Budynku 2.
- Serwer iSeries A hermetyzuje pakiet IPv6 w pakiecie IPv4 i wysyła pakiet IPv4 przez tunel do Klienta D, który go dehermetyzuje i przekazuje do innej instancji aplikacji IPv6.

Każde połączenie tunelowe jest połączeniem typu punkt z punktem, dlatego dla każdego tunelu trzeba zdefiniować zdalny punkt końcowy. Definiowanie to polega na utworzeniu dwóch tras. Każda trasa jest przypisana do tego samego tunelu, ale jako następny przeskok definiuje inny zdalny punkt końcowy. Innymi słowy, definiowanie zdalnych punktów końcowych każdego tunelu odbywa się podczas tworzenia tras.

Oprócz utworzenia tras początkowych, definiujących punkty końcowe tunelu i pozwalających pakietom dotrzeć do klientów w Budynku 2, należy utworzyć dwie dodatkowe trasy, aby pakiety mogły wrócić do serwera w Budynku 1.

Wymagania konfiguracji obejmują:

- System operacyjny OS/400 wersja 5 wydanie 2 lub nowsze.
- Program iSeries Access for Windows i iSeries Navigator (komponent sieciowy programu iSeries Navigator).
- Przed rozpoczęciem konfigurowania tunelu należy na serwerze skonfigurować protokół TCP/IP (korzystający z protokołu IPv4). Jeśli serwer nie jest skonfigurowany do korzystania z IPv4, to przed rozpoczęciem konfigurowania tunelu dla IPv6 należy przeczytać sekcję Konfigurowanie po raz pierwszy protokołu TCP/IP.

Konfigurowanie

Aby utworzyć skonfigurowany tunel, należy użyć kreatora **Konfiguracja IPv6** i kreatora **Nowa trasa IPv6** z programu iSeries Navigator. Protokół IPv6 można konfigurować tylko z programu iSeries Navigator, nie można tego zrobić z interfejsu znakowego.

Aby skorzystać z kreatora **Konfiguracja IPv6** do utworzenia czerwonego tunelu, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz **serwer —> Sieć —> Konfiguracja TCP/IP**.
2. Kliknij prawym przyciskiem myszy **IPv6** i wybierz kreator **Konfiguracja IPv6**, a następnie skonfiguruj tunel dla IPv6 wykonując kolejne instrukcje kreatora. Po zakończeniu tych czynności kreator **Konfiguracja IPv6** zapyta o utworzenie nowej trasy dla skonfigurowanego tunelu i pojawi się okno dialogowe kreatora **Nowa trasa IPv6**. Aby zezwolić na ruch pakietów IPv6 przez czerwony tunel, musisz utworzyć nową trasę.
3. W kreatorze **Nowa trasa IPv6** utwórz trasę dla tunelu czerwonego. Jako następny przeskok podaj zdalny punkt końcowy 10.1.2.1, a jako adres docelowy podaj fec0::2.

Ponownie uruchom kreator **Nowa trasa IPv6**, aby utworzyć trasę dla tunelu niebieskiego. Zauważ, że do utworzenia tunelu niebieskiego nie trzeba korzystać z kreatora **Konfiguracja IPv6**. Jest on tworzony w momencie definiowania jego zdalnego punktu końcowego za pomocą kreatora **Nowa trasa IPv6**. Aby użyć kreatora **Nowa trasa IPv6**, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz swój **serwer —> Sieć —> Konfiguracja TCP/IP —> IPv6**.
2. Kliknij prawym przyciskiem myszy **Trasy**, wybierz **Nowa trasa**, a następnie wykonuj kolejne instrukcje kreatora, konfigurując trasę IPv6 dla tunelu niebieskiego. Jako następny przeskok podaj zdalny punkt końcowy 10.1.2.2, a jako adres docelowy podaj fec0::3.

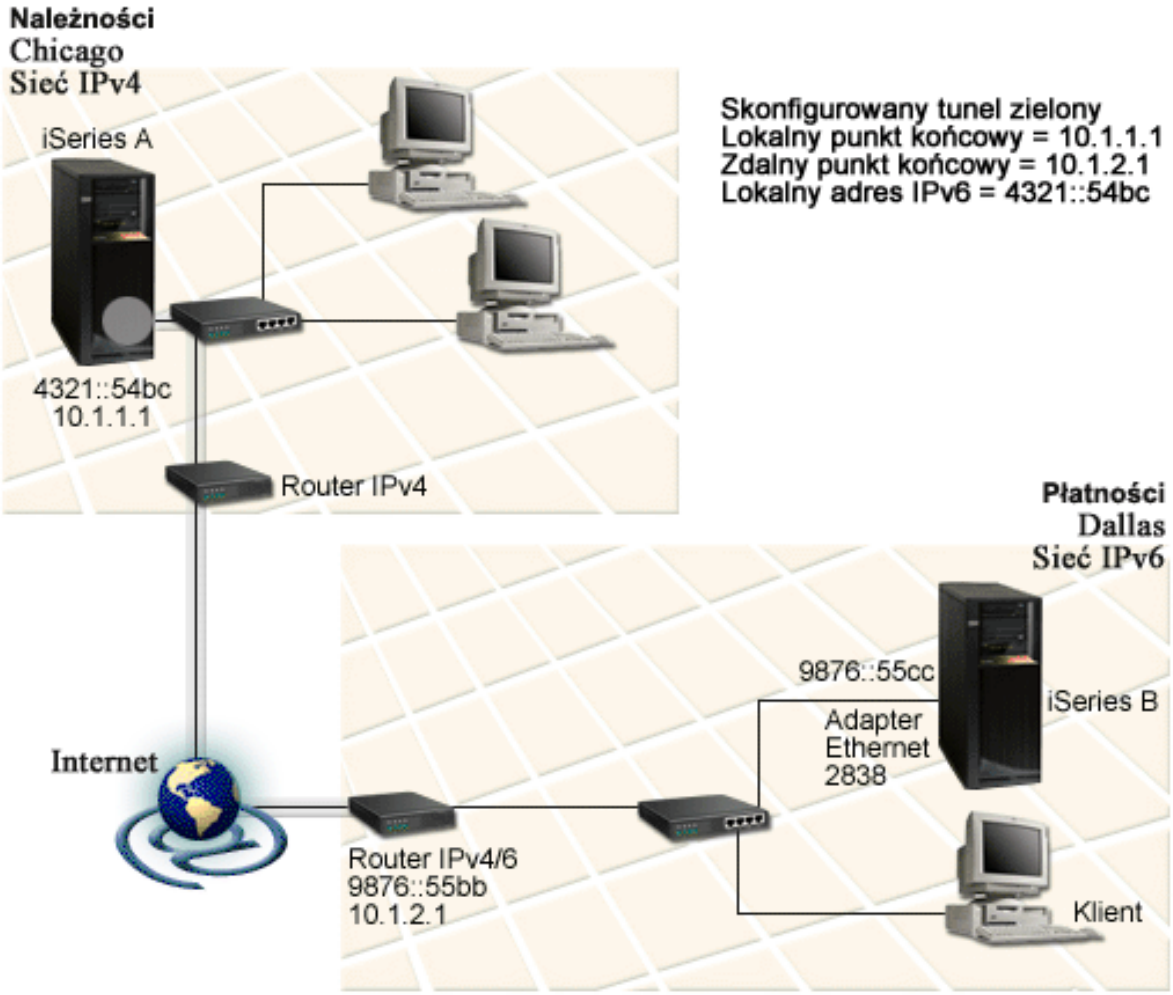
Po utworzeniu skonfigurowanego tunelu i tras definiujących punkty końcowe tunelu, należy utworzyć trasy na serwerach Klient C i Klient D, pozwalające na powrót pakietów do serwera w Budynku 1. Dla każdej z tych tras należy podać 10.1.1.1 jako następny przeskok, a jako adres docelowy fec0::1.

Wysyłanie pakietów IPv6 przez sieć rozległą IPv4

Opis sytuacji

Twoja firma korzysta z programu do obsługi księgowości do rozliczania należności na serwerze znajdującym się w biurze w Chicago. Masz połączyć tę aplikację z serwerem w biurze w Dallas. Na obydwu serwerach, w obydwu miastach używa ona adresowania IPv6. Ponieważ jednak dostawca ISP nie udostępnia routerów IPv6 pomiędzy tymi miejscami, musisz skonfigurować tunel pomiędzy dwoma serwerami. Pakiety aplikacji przechodzą pomiędzy serwerami przez tunel poprzez sieć rozległą IPv4. Rysunek przedstawia konfigurację sieci stworzonej na potrzeby tego scenariusza.

Uwaga: W scenariuszu adres IP 10.x.x.x reprezentuje publiczny adres IP, który może być używany globalnie. Wszystkie użyte w scenariuszu adresy są tylko przykładami.



Rozwiązanie

Aby korzystać z protokołu IPv6 poprzez sieć rozległą opartą na infrastrukturze IPv4, należy skonfigurować tunel i kilka powiązanych z nim tras. Połączenie działa w następujący sposób:

- Tunel zaczyna się na serwerze iSeries A (lokalny punkt końcowy 10.1.1.1) w Chicago i kończy na routerze IPv4/6 (zdalny punkt końcowy 10.1.2.1) w Dallas.
- Aplikacja znajdująca się na serwerze iSeries A chce połączyć się z aplikacją znajdującą się na serwerze iSeries B. Serwer iSeries A hermetyzuje pakiet IPv6 w pakiecie IPv4, następnie wysyła go tunelem do routera IPv4/6, który dehermetyzuje pakiet IPv6 i przekazuje go do serwera iSeries B.
- Pakiet wraca do Chicago odwrotną ścieżką.

Połączenie tunelowe jest połączeniem typu punkt z punktem, dlatego trzeba zdefiniować zdalny punkt końcowy tunelu. Definiowanie to polega na utworzeniu trasy powiązanej z tunelem. Trasa ta definiuje zdalny punkt końcowy (10.1.2.1) jako następny przeskok. Innymi słowy, definiowanie zdalnych punktów końcowych odbywa się podczas tworzenia tras. Ponadto trasa definiuje adres docelowy jako 9876::55cc (adres IPv6 powiązany z serwerem iSeries B).

Oprócz utworzenia trasy początkowej, definiującej punkt końcowy tunelu i pozwalającej pakietowi dostać się do serwera iSeries B w Dallas, należy utworzyć dwie dodatkowe trasy, aby pakiet mógł wrócić do serwera iSeries A w Chicago.

Wymagania konfiguracji obejmują:

- System operacyjny OS/400 wersja 5 wydanie 2 lub nowsze.
- Program iSeries Access for Windows i iSeries Navigator (komponent sieciowy programu iSeries Navigator).
- Przed rozpoczęciem konfigurowania tunelu należy na serwerze skonfigurować protokół TCP/IP (korzystający z protokołu IPv4). Jeśli serwer nie jest skonfigurowany do korzystania z IPv4, to przed rozpoczęciem konfigurowania tunelu dla IPv6 należy przeczytać sekcję Konfigurowanie po raz pierwszy protokołu TCP/IP.

Konfigurowanie

Aby utworzyć skonfigurowany tunel, należy użyć kreatora **Konfiguracja IPv6** i kreatora **Nowa trasa IPv6** z programu iSeries Navigator. Skonfigurowane tunele można konfigurować tylko z programu iSeries Navigator, nie można tego zrobić z interfejsu znakowego.

Aby skorzystać z kreatora **Konfiguracja IPv6** do utworzenia tunelu, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz **serwer —> Sieć —> Konfiguracja TCP/IP**.
2. Kliknij prawym przyciskiem myszy **IPv6** i wybierz **Konfiguracja IPv6**, a następnie skonfiguruj tunel dla IPv6 wykonując kolejne instrukcje kreatora. Po zakończeniu tych czynności kreator **Konfiguracja IPv6** zapyta o utworzenie nowej trasy dla skonfigurowanego tunelu i pojawi się okno dialogowe kreatora **Nowa trasa IPv6**. Aby zezwolić na ruch pakietów IPv6 przez tunel, musisz utworzyć nową trasę.
3. W kreatorze **Nowa trasa IPv6** utwórz trasę hosta dla tunelu. Jako następny przeskok podaj zdalny punkt końcowy 10.1.2.1, a jako adres docelowy podaj 9876::55cc.

Po utworzeniu skonfigurowanego tunelu i trasy definiującej punkt końcowy tunelu, należy utworzyć trasy na serwerze iSeries B i routerze IPv4/6, aby pakiety mogły wrócić do Chicago. Przy tworzeniu trasy na serwerze iSeries B jako następny przeskok należy podać 9876::55bb, a jako adres docelowy 4321::54bc. Przy tworzeniu trasy na routerze IPv4/6 jako następny przeskok podaj 10.1.1.1, a jako adres docelowy 4321::54bc.

Uwaga: Router IPv4/6 będący w Dallas powinien mieć bezpośrednią trasę do 9876::55cc, odkąd jednak jest ona tworzona automatycznie, ręczne konfigurowanie stało się zbędne.

Pojęcia: IPv6

Aby dokładniej zapoznać się z protokołem IPv6, przeczytaj opisy pojęć z nim związanych:

Porównanie IPv4 z IPv6
Porównanie atrybutów protokołów IPv4 i IPv6. Tabela umożliwia szybki wgląd w specyficzne funkcje i porównanie ich zastosowania w każdym z tych protokołów.

Formaty adresów protokołu IPv6
Wielkość i format adresu protokołu IPv6.

Typy adresów IPv6
Nowe typy adresów w protokole IPv6.

Tunelowanie pakietów IPv6
Jak tunelowanie pakietów IPv6 umożliwia ich przesyłanie przez sieć IPv4.

Wykrywanie sąsiada
Jak wykrywanie sąsiada umożliwia komunikację hostów i routerów.

Bezstanowe autokonfigurowanie adresu
Jak bezstanowe autokonfigurowanie adresu automatyzuje niektóre zadania administratora.

Formaty adresów protokołu IPv6

Wielkość adresu IPv6 wynosi 128 bitów. Preferowana reprezentacja adresu IPv6 to: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, gdzie każdy znak x to szesnastkowa cyfra reprezentująca 4 bity. 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.

Opisany format alternatywny został użyty w następujących dwóch typach adresów IPv6:

- **Adres IPv6 będący odwzorowanym adresem IPv4**
  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).
- **Adres IPv6 zgodny z adresem IPv4**
  Typ adresu używany do tunelowania, umożliwia komunikację węzłów IPv6 przez infrastrukturę IPv4. Na przykład 0:0:0:0:0:0:192.1.56.10 i ::192.1.56.10/96 (format skrócony).

Wszystkie wymienione formaty są poprawnymi adresami IPv6. Jeden z nich należy podać w programie iSeries Navigator.

Typy adresów 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 trzy typy 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 ośrodka (site-local)
Adresy przeznaczone do stosowania w określonym ośrodku. Ich przedrostek to fec0::/10. Routery nie przekazują poza określony ośrodek pakietów, które zawierają adres ośrodka jako adres źródłowy.

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

Istnieją dwa typy specjalne adresów pojedynczych:

Adres nieokreślony (unspecified)
Adres nieokreślony to 0:0:0:0:0:0:0:0, może on być skrócony do dwóch dwukropków (::). Oznacza on 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, żeby wykryć adres od innego węzła, korzysta z adresu nieokreślonego jako swojego adresu źródłowego.

Adres pętli zwrotnej (loopback)
Adres pętli zwrotnej to 0:0:0:0:0:0:0:1, może on być 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. Nie dysponuje jeszcze obsługą tworzenia interfejsu grupowego ani obsługą aplikacji.

Tunelowanie IPv6

Tunelowanie IPv6 umożliwia łączenie się serwera iSeries z węzłami IPv6 (hostami i routerami) przez domeny IPv4. Tunelowanie umożliwia wyodrębnionym węzłom lub sieciom IPv6 komunikowanie się bez zmieniania bazowej infrastruktury IPv4. Ponadto umożliwia współpracę protokołów IPv4 i IPv6, dostarczając w ten sposób przejściowej metody implementacji IPv6 przy zachowaniu połączeń IPv4.

Tunel składa się z dwóch węzłów z podwójnymi stosami (IPv4 i IPv6) będących w sieci IPv4. Mają one możliwość przetwarzania zarówno komunikacji IPv4, jak i IPv6. Jeden z tych węzłów znajdujący się na krawędzi infrastruktury IPv6 dokleja nagłówek IPv4 przed każdym przychodzącym pakietem IPv6 (hermetyzuje pakiet) i wysyła go jak normalny pakiet IPv4 przez istniejące łącza. Routery IPv4 przekazują te pakiety dalej. Po drugiej stronie tunelu inny węzeł z podwójnym stosem usuwa dodatkowy nagłówek IP z pakietu IPv6 (dehermetyzuje pakiet) i przekazuje go do ostatecznego miejsca docelowego, korzystając już ze standardu IPv6.

Tunelowanie IPv6 dla serwera iSeries przebiega przez skonfigurowane tunele, będące liniami wirtualnymi. Skonfigurowane tunele zapewniają możliwość komunikacji IPv6 z dowolnym węzłem o kierowalnym adresie IPv4, który obsługuje tunele IPv6. Węzły takie mogą znajdować się gdziekolwiek, wewnątrz lokalnej domeny IPv4 lub w domenie zdalnej.

Połączenia skonfigurowanym tunelem to połączenia typu punkt z punktem. Aby skonfigurować ten typ linii, należy podać lokalny punkt końcowy tunelu (adres IPv4), na przykład 124.10.10.150 i lokalny adres IPv6, na przykład 1080:0:0:0:8:800:200c:417a. Ponadto należy utworzyć trasę IPv6, aby tunelem mógł przebiegać ruch w sieci. Podczas tworzenia trasy definiuje się jeden ze zdalnych punktów końcowych tunelu (adres IPv4) i następny przeskok trasy. Można skonfigurować dowolną liczbę punktów końcowych dla dowolnej liczby tuneli.

Scenariusz i rysunki przedstawiające tunelowanie IPv6 znajdują się w sekcjach: Wysyłanie pakietów IPv6 przez sieć lokalną IPv4 i Wysyłanie pakietów IPv6 przez sieć rozległą IPv4.

Wykrywanie sąsiada

Funkcje wykrywania sąsiada 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.

Anons routera
Komunikaty wysyłane przez routery systematycznie lub w odpowiedzi na komunikat żądania routera. Dzięki informacjom dostarczonym przez anonsy routerów hosty tworzą automatycznie interfejsy ośrodka, interfejsy globalne i powiązane trasy. Ponadto anonsy 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.

Anons 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 pobrać z adresu RFC Editor (http://www.rfc-editor.org/rfcsearch.html) .

Bezstanowe autokonfigurowanie adresu

Bezstanowe autokonfigurowanie adresu to proces używany przez węzły IPv6 (hosty i routery) do automatycznego konfigurowania adresów IPv6 dla interfejsów. Węzeł buduje różne adresy IPv6 łącząc przedrostek adresu z adresem MAC węzła lub identyfikatorem interfejsu podanym przez użytkownika. Przedrostek składa się z przedrostka segmentowego (fe80::/10) i 64-bitowych przedrostków anonsowanych przez lokalne routery IPv6 (jeśli takie istnieją). Jeśli typ łącza zezwala na rozgłaszanie, to bezstanowe autokonfigurowanie adresu tworzy także odpowiednie interfejsy grupowe.

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

Firma IBM zaimplementowała protokół IPv6 już w kilku wersjach oprogramowania serwera iSeries. Obecnie protokół IPv6 został zaimplementowany w platformie tworzenia aplikacji, umożliwiając projektowanie i testowanie aplikacji IPv6.

Protokoły IPv6 i IPv4 różnią się od siebie pewną ilością szczegółów. W tabeli zebrane zostały atrybuty powiązane z IPv4 i ich porównanie z odpowiednimi atrybutami IPv6. Z poniższej listy należy wybrać odpowiedni atrybut i porównać go z atrybutem przedstawionym w tabeli.

	IPv4	**IPv6**
adres (address)	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 wygląda następująco: nnn.nnn.nnn.nnn, gdzie 0<=nnn<=255, a każdy znak n to cyfra dziesiętna. 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. Często część hosta adresu IPv6 (lub jej fragment) będzie adresem MAC lub innym identyfikatorem interfejsu. W zależności od przedrostka podsieci 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 od liczby 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 adres IPv6 adres IPv4 (więcej szczegółowych danych zawiera dokument RFC 2373, znajdujący się pod adresem RFC Editor (http://www.rfc-editor.org/rfcsearch.html).
przydzielenie adresu (address allocation)	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.

	IPv4	IPv6
czas życia adresu (address lifetime)	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. Po wygaśnięciu poprawnego czasu życia adres nie będzie używany (rozpoznawany) jako poprawny docelowy adres IP dla pakietów przychodzących. Niektóre adresy IPv6 mają z założenia nieskończony preferowany i poprawny czas życia, przykładem jest adres segmentowy (patrz w “zasięg adresu (address scope)”).
maska adresu (address mask)	Używana do oddzielenia części sieciowej od części hosta.	Nieużywana (patrz “przedrostek adresu (address prefix)”).
przedrostek adresu (address prefix)	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 (Address Resolution Protocol)	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 (address scope)	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 3 zasięgi, w tym segmentowy, ośrodka 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 adresów (address types)	Pojedyncze, grupowe i rozgłaszania.	Pojedyncze, grupowe i dowolne. Opis znajduje się w sekcji Typy adresów IPv6.
śledzenie komunikacji (communications trace)	Narzędzie do gromadzenia szczegółowych danych śledzenia pakietów TCP/IP (i innych), które trafiają do serwera iSeries i opuszczają go.	Tak samo dla IPv6, protokół IPv6 jest obsługiwany włącznie z pakietami IPv6 tunelowanymi w protokole IPv4.

	IPv4	IPv6
konfigurowanie (configuration)	Nowo zainstalowane systemy wymagają skonfigurowania przed połączeniem, należy przypisać adresy IP i trasy.	Konfigurowanie jest opcjonalne, w zależności od oczekiwanej funkcjonalności. Odpowiedni interfejs Ethernet lub tunel muszą zostać określone jako interfejs IPv6 za pomocą programu iSeries Navigator. Po wykonaniu tego, interfejsy IPv6 konfigurują się same. 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.
system DNS (Domain Name System)	Aplikacje akceptują nazwy hostów i następnie korzystają z systemu DNS do uzyskania adresu 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 gniazd gethostbyname() jest niezmieniona dla IPv6, a funkcji API getaddrinfo() można użyć do uzyskania (wybór należy do aplikacji) wyłącznie adresu IPv6 lub obu adresów, IPv4 i IPv6. W protokole IPv6 domena używana do wyszukiwania wstecznego półbajtu to ip6.arpa, a jeśli nie zostanie znaleziona, to ip6.int (patrz funkcja API getnameinfo()).
protokół DHCP (Dynamic Host Configuration Protocol)	Używany do dynamicznego uzyskiwania adresu IP i innych danych o konfiguracji.	Obecnie protokół DHCP nie obsługuje IPv6.
protokół FTP ((File Transfer Protocol)	Protokół FTP umożliwia wysyłanie i odbieranie plików przez sieć.	Obecnie protokół FTP nie obsługuje IPv6.
fragmenty (fragments)	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. Obecnie nagłówek rozszerzenia fragmentacji nie jest obsługiwany.
tabela hostów (host table)	W programie iSeries Navigator jest to konfigurowalna tabela kojarząca adres internetowy z nazwą hosta, na przykład: 127.0.0.1 i loopback. 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.

	IPv4	IPv6
interfejs (interface)	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 i 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.
protokół ICMP (Internet Control Message Protocol)	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 (Internet Group Management Protocol)	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 (IP header)	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 (IP header options)	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 nie obsługuje żadnych nagłówków rozszerzeń.
bajt protokołu nagłówka IP (IP header protocol byte)	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 (IP header Type of Service (TOS) byte)	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 (iSeries Navigator support)	Program iSeries Navigator ma wszystkie funkcje do konfiguracji TCP/IP.	Program iSeries Navigator dostarcza pełnej konfiguracji opcjonalnej dla IPv6, włącznie z kreatorem **Konfiguracja IPv6**.

	IPv4	IPv6
połączenie LAN (LAN connection)	Używane przez interfejs IP w celu uzyskania dostępu do sieci fizycznej. Istnieje wiele typów, na przykład Token Ring, Ethernet czy PPP. Czasami nazywane interfejsem fizycznym, łączem lub linią.	W protokole IPv6 istnieje ta sama koncepcja. Obecnie obsługiwane są tylko karty Ethernet 2838 i 2849 oraz tunel.
protokół L2TP (Layer 2 Tunnel Protocol)	O protokole L2TP można myśleć, jak o wirtualnym połączeniu PPP, pracuje on poprzez dowolny obsługiwany typ linii.	Obecnie protokół L2TP nie obsługuje IPv6.
adres pętli zwrotnej (loopback address)	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 nazwany został *LOOPBACK6.
jednostka MTU (Maximum Transmission Unit)	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.
narzędzie netstat (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 przez terminal 5250, jak i przez program iSeries Navigator.
translacja adresu sieciowego ((Network Address Translation)	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 (network table)	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 (node info query)	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 pakietów (packet filtering)	Podstawowe funkcje firewalla są zintegrowane z protokołem TCP/IP i konfigurowane za pomocą programu iSeries Navigator.	Obecnie filtrowanie pakietów nie obsługuje protokołu IPv6. Można jednak zastosować filtrowanie protokołu IPv4 do tunelowanego ruchu IPv6.
przekazywanie pakietów (packet forwarding)	Serwer iSeries można skonfigurować, 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.	Obecnie pakiety IPv6 nie są przekazywane.

	IPv4	IPv6
tunelowanie pakietów (packet tunneling)	W protokole IPv4 tunelowanie istnieje w sieciach VPN dla połączeń VPN trybu tunelowego (IPv4 tunelowane w IPv4) i w protokole L2TP.	W przypadku protokołu IPv6 tunelowanie w pakietach IPv4 jest ważną częścią rozwoju protokołu IPv6. Obecnie grupa IETF zdefiniowała przynajmniej 5 różnych typów tunelowania 6-w-4, każdy typ ma inne atrybuty i zalety. Podstawowym i elastycznym typem tunelowania IPv6-w-IPv4 jest obsługa komunikacji między węzłami IPv6 poprzez istniejącą strukturę IPv4 (Internet). Tak zwane **tunelowanie skonfigurowane** dostarcza wirtualnego łącza typu punkt z punktem pomiędzy węzłami IPv6 i korzysta z nowego typu tunelu nazywanego *TNLCFG64.
narzędzie PING (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 (Point-to-Point Protocol)	Protokół PPP obsługuje interfejsy połączeń modemowych dla różnych modemów i typów linii.	Obecnie PPP nie obsługuje protokołu IPv6.
ograniczenia portów (port restrictions)	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.	Nieobsługiwane dla IPv6. Konfigurowanie ograniczeń dotyczy tylko protokołu IPv4.
porty (ports)	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.

	IPv4	IPv6
adresy prywatne i publiczne (private and public addresses)	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 (address scope)” na stronie 20).
tabela protokołów (protocol table)	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 obsługuje protokół IPv6.
jakość usługi (Quality of Service)	Jakość usługi umożliwia zgłoszenie priorytetu pakietu i pasma dla aplikacji TCP/IP.	Obecnie QoS nie obsługuje protokołu IPv6. Jeśli jednak pakiety IPv6 są tunelowane w IPv4, można wykorzystać istniejące możliwości QoS serwera iSeries do ruchu IPv4, który następnie obsłuży obciążenie IPv6 w sposób przezroczysty.
zmiana numerów (renumbering)	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 (route)	Logiczne odwzorowanie zbioru adresów IP (może to być zbiór jednoelementowy) na interfejs fizyczny i pojedynczy adres 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.	Koncepcja taka sama, jak w protokole IPv4. Jedna istotna różnica: trasy IPv6 są powiązane z interfejsem fizycznym (łącze, takie jak *TNLCFG64 czy ETH03), a nie z interfejsem. Powody tego są różne. Jedną z przyczyn jest to, że funkcje wyboru adresu źródłowego są inne w IPv6 niż IPv4. Patrz “wybór adresu źródłowego (source address selection)” na stronie 26. Dozwolone są podwójne trasy, w celu zwiększenia odporności na błędy, są jednak one ignorowane w trakcie wyszukiwania tras.
protokół routingu RIP (Routing Information Protocol)	Protokół routingu RIP jest obsługiwany przez demona routed.	Obecnie protokół routingu RIP nie obsługuje protokołu IPv6. Routing w protokole IPv6 korzysta z tras statycznych.

	IPv4	IPv6
tabela usług (services table)	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 (Simple Network Management Protocol)	Protokół SNMP służy do zarządzania systemem.	Obecnie protokół SNMP nie obsługuje protokołu IPv6. Routing w protokole IPv6 korzysta z tras statycznych.
funkcje API gniazd (sockets API)	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 (source address selection)	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 (starting and stopping)	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). Protokołu IPv6 nie można użyć lub konfigurować bez protokołu IPv4 i musi on mieć skonfigurowaną pętlę zwrotną IPv6 (::1).

	IPv4	IPv6
usługa Telnet (Telnet)	Usługa Telnet umożliwia zalogowanie się i korzystanie ze zdalnego komputera, tak jak przy połączeniu bezpośrednim.	Obecnie usługa Telnet nie obsługuje IPv6.
śledzenie trasy (trace route)	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 przez terminal 5250, jak i przez program iSeries Navigator.
warstwy transportowe (transport layers)	TCP, UDP, RAW. Nowa warstwa transportowa, protokół SCTP (Stream Control Transmission Protocol) ma połączyć najlepsze cechy protokołów TCP i UDP, czyli gwarantowaną komunikację bezpołączeniową. Protokół SCTP znajduje się w początkowej fazie wykorzystania i nie jest obsługiwany na serwerze iSeries.	Te trzy warstwy transportowe istnieją i są funkcjonalnie niezmienione dla protokołu IPv6.
adres nieokreślony (unspecified address)	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 (virtual private networking)	Sieć VPN (korzystająca z protokołu IPsec) umożliwia rozszerzenie chronionych sieci prywatnych poprzez istniejące sieci publiczne.	Obecnie sieć VPN nie obsługuje protokołu IPv6. Jeśli jednak protokół IPv6 jest tunelowany w IPv4, można wykorzystać możliwości VPN serwera iSeries do ruchu IPv4, który następnie obsłuży obciążenie IPv6 w sposób przezroczysty.

Informacje związane z protokołem IPv6

Więcej informacji o protokole IPv6 można znaleźć w następujących źródłach:

The Internet Engineering Task Force (IETF) (http://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 (http://www.ipv6forum.com/)
Nowe artykuły i zdarzenia związane z rozwojem protokołu IPv6.

Rozdział 4. Planowanie konfiguracji 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.

Wymagania podczas konfigurowania protokołu TCP/IP
Podstawowe informacje konfiguracyjne wymagane podczas konfigurowania protokołu TCP/IP należy zebrać i zapisać.

Metody ochrony protokołu TCP/IP
Nowy użytkownik sieci powinien sprecyzować swoje wymagania dotyczące ochrony.

Wymagania 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. Jeśli nie znasz tych terminów, zapoznaj się z dokumentacją techniczną IBM redbook TCP/IP for AS/400: More Cool Things Than Ever  i z rozdziałem drugim, ″TCP/IP: Basic Installation and Configuration″.

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 **Enter**.
2. Aby wybrać opcję Praca z zasobami komunikacji (Opcja 1), 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.

Co dalej:
Instalowanie protokołu TCP/IP

Metody ochrony protokołu TCP/IP

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. Aby poznać szczegóły dotyczące sposobów kontrolowania wpływu czynników zewnętrznych, przeczytaj sekcje zawierające rady, jak kontrolować interaktywne wpisywanie się, w dokumencie Wskazówki i narzędzia dotyczące ochrony iSeries  .

Więcej informacji na temat ochrony i dostępnych użytkownikowi opcji zawiera publikacja IBM Secureway: iSeries a Internet.

Rozdział 5. Instalowanie protokołu TCP/IP

Podstawowa obsługa protokołu TCP/IP jest elementem systemu OS/400 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, wykonaj 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 mieć 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 **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, może zaistnieć potrzeba kontaktu z obsługą.

Uwaga:

Można zainstalować między innymi następujące programy licencjonowane:

- iSeries Access for Windows 95/NT (5769–XD1 wersja V3R1M3 lub nowsza) zawiera program iSeries Navigator używany podczas konfigurowania niektórych komponentów TCP/IP.
- IBM HTTP Server for iSeries (57*xx*–DG1) zawiera 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.

Rozdział 6. Konfigurowanie protokołu TCP/IP

Do skorzystania z funkcji IPv6 niezbędne może okazać się zmienienie istniejącej konfiguracji lub, gdy serwer jest nowy, skonfigurowanie go po raz pierwszy. Niniejsza sekcja zawiera instrukcje dotyczące konfigurowania TCP/IP w każdej z tych sytuacji. 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.

Konfigurowanie protokołu IPv6
Instrukcje dotyczące konfigurowania serwera dla funkcji IPv6. Korzyści płynące z możliwości rozszerzonego adresowania i opcje związane ze stabilnością tego protokołu IP. Jeśli nie wiesz zbyt dużo o protokole IPv6, to krótki przegląd znajdziesz w sekcji Protokół IPv6. Przed konfigurowaniem IPv6 na serwerze należy skonfigurować protokół TCP/IP.

Pierwsze konfigurowanie protokołu TCP/IP

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

Konfigurowanie protokołu TCP/IP za pomocą interfejsu znakowego
Skorzystaj z tej metody, jeśli nie możesz użyć kreatora EZ-Setup. Metoda ta jest przydatna na przykład wtedy, gdy chcesz użyć programu iSeries Navigator na komputerze PC, który przed uruchomieniem programu iSeries Navigator wymaga podstawowego skonfigurowania protokołu TCP/IP.

Konfigurowanie protokołu TCP/IP za pomocą kreatora EZ-Setup

Program iSeries Navigator to graficzny interfejs użytkownika, który udostępnia zwięzłe okna dialogowe i kreatory do konfigurowania protokołu TCP/IP. Podczas konfigurowania początkowego należy użyć kreatora EZ-Setup programu iSeries Navigator do pierwszego konfigurowania protokołu TCP/IP i nawiązania połączenia. 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 pozycje **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 ustawienia sieci wymagają zmian w konfiguracji, użyj programu iSeries Navigator. Aby dodać trasy i interfejsy, przeczytaj sekcję Dostosowanie protokołu TCP/IP za pomocą programu iSeries Navigator, a jeśli chcesz w sieci korzystać z protokołu IPv6, przejdź do sekcji Konfigurowanie protokołu IPv6.

Konfigurowanie protokołu TCP/IP za pomocą interfejsu znakowego

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 przed uruchomieniem programu iSeries Navigator wymaga podstawowego skonfigurowania protokołu TCP/IP, trzeba posłużyć się interfejsem znakowym.

Aby wykonać opisane tu czynności konfiguracyjne, musisz mieć uprawnienie specjalne *IOSYSCFG. Więcej informacji o tym typie uprawnienia zawiera rozdział o profilach użytkowników w publikacji iSeries Security Reference .

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. W menu wybierz zadania konfiguracyjne. Przed przystąpieniem do konfigurowania serwera zapoznaj się z menu.

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

1. Skonfiguruj opis linii.
2. Skonfiguruj interfejs.
3. Skonfiguruj trasę.
4. Zdefiniuj domenę lokalną i nazwy hostów.
5. Zdefiniuj tabelę hostów.
6. Uruchom TCP/IP.

Konfigurowanie opisu linii (Ethernet)

Instrukcje te odnoszą się do konfigurowania protokołu TCP/IP dla adaptera komunikacyjnego typu Ethernet. Jednak jeśli korzystasz z innego typu adaptera, na przykład z Token Ring, to komendy dla tego adaptera znajdziesz w artykule TCP/IP Configuration and Reference, w *Dodatku A*.

W celu skonfigurowania opisu linii, wykonaj następujące czynności:

1. W wierszu komend wpisz CRTLINETH, aby wyświetlić menu Tworzenie opisu linii (Create Line Desc), i naciśnij klawisz Enter.
2. Wprowadź nazwę linii i naciśnij klawisz Enter (możesz użyć dowolnej nazwy).
3. Wprowadź nazwę zasobu i naciśnij klawisz Enter.

Co dalej:
Konfigurowanie interfejsu

Konfigurowanie interfejsu

W celu skonfigurowania interfejsu, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP, aby wyświetlić 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.

Co dalej:
Konfigurowanie trasy

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), przejdź do ekranu 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.

Co dalej:
Definiowanie domeny lokalnej i nazw hostów

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.

Co dalej:
Definiowanie tabeli hostów

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 przejść do ekranu 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 to potrzebne, wprowadź znak plus (+), aby zrobić miejsce na więcej niż jedną nazwę hosta.
5. Powtarzaj te kroki dla wszystkich pozostałych hostów w sieci, z którymi chcesz się komunikować z użyciem nazwy, i dodaj wpis dla każdego z nich.

Co dalej:
Uruchamianie protokołu TCP/IP

Uruchamianie protokołu 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. Uruchamia ona jedynie te interfejsy i serwery, które mają ustawioną wartość AUTOSTART *YES.

Na tym kończy się proces konfigurowania na serwerze protokołu TCP/IP. Jeśli ustawienia sieci wymagają zmian w konfiguracji, użyj programu iSeries Navigator. Aby dodać trasy i interfejsy, przeczytaj sekcję Dostosowanie protokołu TCP/IP za pomocą programu iSeries Navigator, a jeśli chcesz w sieci korzystać z protokołu IPv6, przejdź do sekcji Konfigurowanie protokołu IPv6.

Konfigurowanie protokołu IPv6

Protokół IPv6 pozwala korzystać z zalet następnej generacji sieci Internet. Aby korzystać z funkcji IPv6, należy zmienić konfigurację TCP/IP, konfigurując linię dedykowaną dla IPv6. Linię należy skonfigurować na adapterze Ethernet 2838 lub 2849 albo na skonfigurowanym tunelu (linia wirtualna). Instrukcje dotyczące konfigurowania IPv6 zawierają następujące sekcje:

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

Konfigurowanie protokołu IPv6 za pomocą kreatora Konfiguracja IPv6
Instrukcja korzystania z kreatora **Konfiguracja IPv6**.

Wymagania związane z konfiguracją

Określ, który z dwóch typów konfiguracji IPv6 jest dla Ciebie odpowiedni. Jeśli nie masz pewności, który typ wybrać, zapoznaj się z przykładami w sekcji Scenariusze IPv6.

Aby protokół IPv6 działał na serwerze, należy spełnić następujące warunki:

Aby skonfigurować linię Ethernet dla IPv6:
- System operacyjny OS/400 wersja 5 wydanie 2 lub nowsze.
- Program iSeries Access for Windows i iSeries Navigator
  - komponent sieciowy programu iSeries Navigator.
- Adapter Ethernet 2838 lub 2849 Ethernet, który będzie dedykowany dla IPv6.
- Jeśli chcesz wysyłać ruch IPv6 poza bezpośrednią sieć lokalną, router z możliwością obsługi IPv6.
- Skonfigurowany protokół TCP/IP (korzystający z IPv4) na oddzielnym adapterze fizycznym, ponieważ na serwerze musi być uruchomiony protokół TCP/IP. Jeśli jeszcze nie skonfigurowałeś serwera dla IPv4, to przed konfiguracją linii dla IPv4 zapoznaj się z sekcją Konfigurowanie po raz pierwszy protokołu TCP/IP.

Aby utworzyć skonfigurowany tunel (TNLCFG64):
- System operacyjny OS/400 wersja 5 wydanie 2 lub nowsze.
- Program iSeries Access for Windows i iSeries Navigator
  - komponent sieciowy programu iSeries Navigator.
- Przed skonfigurowaniem tunelu dla IPv6 należy skonfigurować TCP/IP (korzystając z IPv4). Jeśli jeszcze nie skonfigurowałeś serwera dla IPv4, przeczytaj sekcję Konfigurowanie po raz pierwszy protokołu TCP/IP.

Instrukcje dotyczące kreatora znajdziesz w sekcji Konfigurowanie protokołu IPv6 za pomocą kreatora Konfiguracja IPv6.

Konfigurowanie protokołu IPv6 za pomocą kreatora Konfiguracja IPv6

Aby skonfigurować IPv6 na serwerze, należy zmienić konfigurację serwera za pomocą kreatora **Konfiguracja IPv6** w programie iSeries Navigator. Protokół IPv6 można konfigurować tylko z programu iSeries Navigator, nie można tego zrobić korzystając z interfejsu znakowego.

Uwaga: można skonfigurować opis linii Ethernet dla IPv6 za pomocą komendy Utworzenie opisu linii (Ethernet) (Create Line Desc (Ethernet) - CRTLINETH) w interfejsie znakowym, jednak należy przy tym podać szesnastkowy adres grupowy 333300000001. Następnie aby zakończyć konfigurowanie IPv6, należy użyć kreatora **Konfiguracja IPv6**.

Kreator wymaga następujących danych wejściowych:

Aby skonfigurować linię Ethernet dla IPv6:
Konfiguracja umożliwia wysyłanie pakietów IPv6 przez sieć lokalną IPv6. Kreator wymaga podania nazwy sprzętowego zasobu komunikacyjnego na serwerze, na którym będzie konfigurowany protokół IPv6; na przykład CMN01. Musi to być adapter Ethernet 2838 lub 2849, jeszcze nie skonfigurowany dla IPv4. Scenariusz pokazujący, kiedy konfigurować linię Ethernet dla IPv6, zawiera sekcja Tworzenie sieci lokalnej IPv6.

Aby utworzyć skonfigurowany tunel (TNLCFG64):
Ten typ konfiguracji umożliwia wysyłanie pakietów IPv6 przez sieć IPv4. Kreator wymaga adresu IPv4 lokalnego punktu końcowego i adresu IPv6 dla interfejsu lokalnego powiązanego z tunelem. Scenariusze pokazujące dwie przykładowe sytuacje, w których warto skonfigurować tunele dla IPv6, znajdują się w sekcjach Wysyłanie pakietów IPv6 przez sieć lokalną IPv4 i Wysyłanie pakietów IPv6 przez sieć rozległą IPv4.

Aby skorzystać z kreatora **Konfiguracja IPv6**, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **serwer —> Sieć —> Konfiguracja TCP/IP**.
2. Kliknij prawym przyciskiem myszy **IPv6** i wybierz **Konfiguracja IPv6**.
3. Aby skonfigurować protokół IPv6 na serwerze, wykonuj kolejne instrukcje kreatora.

Rozdział 7. Dostosowanie konfiguracji TCP/IP za pomocą programu 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.

Wybierz temat z listy, aby dostosować konfigurację za pomocą programu iSeries Navigator. Tematy te stanowią punkt wyjścia do zarządzania konfiguracją TCP/IP za pomocą programu iSeries Navigator.

Zmiana ustawień TCP/IP

Konfigurowanie protokołu IPv6

Dodawanie interfejsów IPv4

Dodawanie interfejsów IPv6

Dodawanie tras IPv4

Dodawanie tras IPv6

Zmiana ustawień 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, na przykład warstwy transportowej.

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 odpowiednią zakładkę.

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 protokołu IPv6

W sekcji Protokół IPv6 znajduje się krótki przegląd informacji na temat tego protokołu.

Aby skonfigurować IPv6, należy zmienić konfigurację serwera za pomocą kreatora **Konfiguracja IPv6**. Przed użyciem kreatora zapoznaj się z instrukcją i wymaganiami dodatkowymi znajdującymi się w sekcji Konfigurowanie protokołu IPv6.

Dodawanie interfejsów 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

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

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

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.

Rozdział 8. Rozwiązywanie problemów dotyczących protokołu IPv6

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.

Rozdział 9. Informacje związane z konfigurowaniem protokołu TCP/IP

W momencie gdy serwer zaczyna działać, powstaje pytanie, jak wykorzystać wszystkie jego możliwości. Poniżej wymienione zostały podręczniki i spis dokumentacji technicznej IBM (w formacie PDF) oraz tematów Centrum informacyjnego, związanych z konfigurowaniem TCP/IP. Pliki PDF można przeglądać lub drukować. Odnośniki te pomogą w wykonaniu większości zadań związanych z konfigurowaniem TCP/IP na serwerze iSeries:

Podręczniki

- **TCP/IP Configuration and Reference** (około 100 stron)
  Książka o konfigurowaniu protokołu TCP/IP i działaniu sieci oraz o zarządzaniu nią.

- **Wskazówki i narzędzia dotyczące ochrony iSeries** (około 254 stron)
  Książka przedstawia najprostsze zalecenia dotyczące opcji ochrony serwera iSeries, które pomogą chronić serwer.

Dokumentacja techniczna

- **TCP/IP Tutorial and Technical Overview**
  Dokumentacja techniczna o podstawach protokołu TCP/IP.

- **TCP/IP for AS/400 : More Cool Things Than Ever**
  Dokumentacja techniczna zawierająca obszerny spis powszechnych aplikacji i usług protokołu TCP/IP.

IPv6

- **The Internet Engineering Task Force (IETF)** (http://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 związane z protokołem IPv6 i odnośniki do źródeł protokołu IPv6.

- **IPv6 Forum** (http://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.

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

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

Program Adobe Acrobat Reader, potrzebny do przeglądania i drukowania plików PDF można pobrać z serwisu Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .