System i

Sieci
Konfigurowanie TCP/IP

Wersja 6 wydanie 1

System i

Sieci
Konfigurowanie TCP/IP

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 63.

To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Konfigurowanie TCP/IP

Ten temat opisuje narzędzia i procedury dotyczące konfigurowania TCP/IP w systemie operacyjnym i5/OS.

Informacje te mogą być na przykład potrzebne podczas tworzenia opisu linii, interfejsu TCP/IP oraz trasy. Należy zapoznać się ze sposobem dostosowania konfiguracji TCP/IP 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 upewnić się, że zostały zainstalowane wszystkie niezbędne komponenty sprzętowe. Po zakończeniu czynności początkowych związanych z konfigurowaniem TCP/IP można przystąpić do rozszerzania możliwości systemu za pomocą aplikacji TCP/IP, protokołów oraz usług, zgodnie z własnymi potrzebami.

Informacje pokrewne

Sieć: aplikacje, protokoły i usługi TCP/IP

Sieć: rozwiązywanie problemów związanych z TCP/IP

Co nowego w wersji V6R1

Poniżej omówiono nowe lub znacznie zmienione informacje zawarte w sekcji dotyczącej konfigurowania TCP/IP.

Rozszerzenie obsługi IPv6

Następujące funkcje związane z konfiguracją TCP/IP aktualnie obsługują IPv6:

- Wirtualny adres IPv6
- Tabela hostów
- Serwer DNS

Udoskonalenia konfiguracji TCP/IP

Następujące funkcje konfiguracji TCP/IP zostały udoskonalone w tym wydaniu:

- Kreator łatwej konfiguracji (EZ-Setup) do konfigurowania TCP/IP został usunięty. Aby skonfigurować TCP/IP po raz pierwszy, należy użyć interfejsu znakowego.
- Aby przekształcić nazwy hostów i powiązane z nimi adresy IP, można skonfigurować i użyć serwera DNS zamiast tabeli hostów.
- Można skonfigurować bezstanową autokonfigurację adresu IPv6 i uruchomić interfejsy IPv6, kiedy system jest w stanie zastrzeżonym.
- Można utworzyć wirtualne interfejsy IPv4 lub IPv6.
- Jeśli TCP/IP zostało uruchomione bez uruchamiania IPv6, można uruchomić IPv6 w późniejszym czasie, bez konieczności zakończenia TCP/IP.

Udoskonalenia interfejsu znakowego

Do skonfigurowania i dostosowania TCP/IP można użyć nie tylko programu System i Navigator, ale także interfejsu znakowego:

- Konfigurowanie bezstanowego autokonfigurowania adresu IPv6
- Ręczne dodawanie, zmienianie i usuwanie interfejsów IPv4 oraz IPv6
- Uruchamianie i zatrzymywanie interfejsów IPv4 i IPv6
- Ręczne dodawanie, zmienianie i usuwanie tras IPv4 oraz IPv6
- Uruchamianie i zakończenie połączenia IPv4 lub IPv6

Udoskonalenia programu System i Navigator

Program System i Navigator udostępnia teraz bardziej spójne funkcje IPv4 i IPv6.

- Interfejsy bezstanowej autokonfiguracji IPv6 są teraz wyświetlone na liście w oknie interfejsów IPv6. Można je uruchamiać i zatrzymywać za pomocą menu wywoływanego.
- Preferowany wybór opisów linii jest dostępny na karcie Opcje w oknie Właściwości interfejsu IPv6.
- W oknie interfejsów IPv6 widoczna jest nowa kolumna o nazwie Status łącza (podłączone i odłączone).
- Można zmieniać interfejsy IPv4 i IPv6, kiedy są one aktywne.
- Okno Tabela hostów wyświetla zarówno adresy IPv4, jak i IPv6. Aby dodać, edytować lub usunąć nazwy hosta, które są powiązane z tą samą pozycją tabeli hostów, można wykonać te wszystkie działania jednocześnie.
- Menu Sąsiednia pamięć podręczna zostało przeniesione z drzewa nawigacji do menu wywoływanego indywidualnego interfejsu IPv6 lub linii IPv6.
- Ustawienia atrybutów IPv4 i IPv6 wykorzystują obecnie to samo okno, które zawiera ustawienia wspólnych właściwości IPv4 i IPv6.

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić odnalezienie miejsc, w których wprowadzono zmiany techniczne, użyto następujących symboli:

- symbol » służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol « służący do zaznaczania końca nowego lub zmienionego fragmentu.

Nowe i zmienione informacje w plikach PDF mogą być oznaczone symbolem | na lewym marginesie.

Plik PDF z informacjami dotyczącymi konfigurowania TCP/IP

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby przejrzeć lub pobrać ten dokument w wersji PDF, wybierz Konfigurowanie TCP/IP (około 980 kB).

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Odsyłacze pokrewne

“Informacje pokrewne dotyczące konfigurowania protokołu TCP/IP” na stronie 60
Informacje, które wiążą się z kolekcją tematów dotyczących konfigurowania TCP/IP można znaleźć w podręcznikach produktów, dokumentacji technicznej IBM (Redbooks), serwisach WWW i w innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Protokół IPv6

Protokół IPv6 odegra ważną rolę w przyszłości sieci Internet. Ten temat opisuje IPv6 i wyjaśnia, jak jest on zaimplementowany w systemie operacyjnym i5/OS.

Przegląd IPv6

Sekcja informuje o powodach wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyściach z 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. Protokół IPv6 jest aktualizacją wersji IPv4 protokołu i jako standard internetowy stopniowo zastępuje wersję poprzednią.

Duże możliwości adresowania IP

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. Ponieważ coraz więcej osób używa komputerów przenośnych, takich jak telefony komórkowe i 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.

Prostsza konfiguracja IP

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. Na przykład 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.

Zmiana adresów urządzeń

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 pozostaje niezmieniona, ponieważ tradycyjnie jest to część MAC adresu adaptera Ethernet. Nowy przedrostek IPv6 zostaje przypisany przez dostawcę usług internetowych, a następnie rozprowadzony wśród wszystkich końcowych hostów poprzez aktualizację routerów IPv6 w sieci oraz zezwolenie na rozpoznanie nowego prefiksu za pomocą bezstanowego autokonfigurowania protokołu IPv6.

Pojęcia pokrewne

“Dostępne funkcje IPv6” na stronie 14
IBM implementuje stopniowo IPv6 w systemie i5/OS. Funkcje IPv6 są przezroczyste dla istniejących aplikacji TCP/IP i współistnieją z funkcjami IPv4.

“Konfigurowanie IPv6” na stronie 26
Podane instrukcje umożliwiają skonfigurowanie obsługi funkcji IPv6 w systemie.

Odsyłacze pokrewne

“Porównanie protokołów IPv4 i IPv6” na stronie 6
Można się zastanawiać, czym protokół IPv6 różni się od protokołu IPv4. Korzystając z zamieszczonej tabeli można szybko porównywać różnice między protokołami IPv4 i IPv6 w zakresie podstawowych pojęć, funkcji IP oraz wykorzystania adresów IP.

Pojęcia związane z IPv6

Przed zaimplementowaniem IPv6 w systemie należy zrozumieć podstawowe pojęcia związane z IPv6, takie jak formaty adresów IPv6, typy adresów IPv6 oraz wykrywanie sąsiadów.

Pojęcia pokrewne

"Scenariusz: tworzenie sieci lokalnej IPv6" na stronie 15
Ten scenariusz pomoże zrozumieć sytuacje, w których protokół IPv6 można zastosować w celach biznesowych. Opisuje wymagania wstępne konfigurowania sieci LAN IPv6 oraz przedstawia etapy konfiguracji automatycznej konfiguracji bezstanowej IPv6 przy użyciu interfejsu znakowego.

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 IPv6 odwzorowanym na protokole IPv4, można podać w programie System i Navigator.

Typy adresów IPv6

W tej sekcji zawarto informacje o kategoriach różnych typów adresów IPv6, a także wyjaśniono sposób użycia każdej z nich.

Istnieją następujące podstawowe typy adresów IPv6:

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 adres dowolny idzie tylko do najbliższego interfejsu z tej grupy. i5/OS może wysyłać pakiety do adresów dowolnych, ale nie może być członkiem grupy adresów dowolnych.

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 system operacyjny i5/OS 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.

Uwaga: Stos TCP/IP systemu i5/OS nie obsługuje wykrywania sąsiadów w trybie routera.

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.

Zadania pokrewne

“Konfigurowanie bezstanowego autokonfigurowania adresu IPv6” na stronie 27
Skorzystanie z funkcji bezstanowego autokonfigurowania adresu IPv6 umożliwia automatyczne skonfigurowanie obsługi protokołu IPv6.

Porównanie protokołów IPv4 i IPv6

Można się zastanawiać, czym protokół IPv6 różni się od protokołu IPv4. Korzystając z zamieszczonej tabeli można szybko porównywać różnice między protokołami IPv4 i IPv6 w zakresie podstawowych pojęć, funkcji IP oraz wykorzystania adresów IP.

Wybierz odpowiedni atrybut z listy, aby porównać go z atrybutem przedstawionym w tabeli.

- Adres
- Przydzielanie adresu
- Czas życia adresu
- Maska adresu
- Przedrostek adresu
- Protokół ARP
- Zasięg adresu
- Typy adresów
- Śledzenie komunikacji
- Konfigurowanie
- System DNS
- Protokół DHCP
- Protokół FTP
- Fragmenty
- Tabela hostów
- Interfejs
- Protokół ICMP (Internet Control Message Protocol)
- Protokół IGMP (Internet Group Management Protocol)
- Nagłówek IP
- Opcje nagłówka IP
- Bajt protokołu nagłówka IP
- Bajt typu usługi (Type of Service) nagłówka IP
- Połączenie LAN
- Protokół L2TP (Layer Two Tunnel Protocol)
- Adres pętli zwrotnej
- Jednostka MTU

- Netstat
- Translacja adresu sieciowego (NAT)
- Tabela sieci
- Zapytanie o węzeł
- Routing OSPF
- Filtrowanie pakietów
- Przekazywanie pakietów
- Komenda PING
- Protokół PPP
- Ograniczenia portu
- Porty
- Adresy prywatne i publiczne
- Tabela protokołów
- Jakość usługi (QoS)
- Zmiana numerów
- Trasa
- Protokół routingu RIP
- Tabela usług
- Protokół SNMP
- Interfejs API gniazd
- Wybór adresu źródłowego
- Uruchamianie i zatrzymywanie
- Obsługa programu System i Navigator
- Telnet
- Śledzenie trasy
- Warstwy transportowe
- Adres nieokreślony (unspecified)
- Wirtualna sieć prywatna (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.

Opis	IPv4	IPv6
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. Zostawi 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	Pojęcie to ogólnie nie ma zastosowania do adresów IPv4, z wyjątkiem adresów przydzielanych za pomocą protokołu 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).
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 (Address Resolution Protocol) 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	Pojęcie to 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 adresów	Adresy IPv4 można podzielić na trzy podstawowe typy: pojedyncze, grupowe i rozgłoszeniowe.	Adresy IPv6 można podzielić na trzy podstawowe typy: pojedyncze, grupowe i dowolne (anycast). Opis znajduje się w sekcji Typy adresów IPv6.

Opis	IPv4	IPv6
Śledzenie komunikacji	Narzędzie śledzenia komunikacji umożliwia gromadzenie szczegółowych danych śledzenia pakietów TCP/IP (i innych), które trafiają do systemu i są z niego wysyłane.	Taka sama obsługa w przypadku IPv6.
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.
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.	Taka sama obsługa w przypadku IPv6.Obsługa IPv6 korzysta z typu rekordu AAAA (poczwórne A) i wyszukiwania odwrotnego (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 odwrotnego jest ip6.arpa, a w razie braku wyników używana jest domena ip6.int. (Patrz funkcja API getnameinfo() – Pobranie informacji o nazwie dla adresu gniazda).
Protokół DHCP	Protokół DHCP służy do dynamicznego uzyskiwania adresu IP i innych danych o konfiguracji. Serwer i5/OS obsługuje serwer DHCP dla protokołu IPv4.	Implementacja protokołu DHCP w serwerze i5/OS nie obsługuje protokołu IPv6.
Protokół FTP	Protokół FTP umożliwia wysyłanie i otrzymywanie plików w sieciach.	Implementacja protokołu FTP na serwerze i5/OS nie obsługuje protokołu 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	Konfigurowalna tabela definiująca powiązania adresów internetowych z nazwami hostów (na przykład 127.0.0.1 - 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).	Taka sama obsługa w przypadku IPv6.

Opis	IPv4	IPv6
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. Interfejsy IPv4 mogą być uruchamiane i zatrzymywane niezależnie od protokołu TCP/IP za pomocą komend STRTCPIFC i ENDTCPIFC oraz programu System i Navigator.	Taka sama obsługa w przypadku IPv6.
Protokół ICMP	Używany w IPv4 do przesyłania informacji o sieci.	Podobnie używany w IPv6, jednak ICMPv6 udostępnia kilka 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.	Protokół IGMP został w IPv6 zastąpiony przez protokół MLD (Multicast Listener Discovery). Protokół MLD działa z grubsza tak samo, jak IGMP w 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 pewną liczbę nagłówków 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 (Type of Service) nagłówka IP	Wykorzystywany przez usługi QoS i DiffServ do wyznaczenia klasy ruchu.	Wyznacza klasy ruchu IPv6 za pomocą innych kodów. Obecnie protokół IPv6 nie obsługuje TOS.
Połączenie LAN	Połączenie LAN jest używane przez interfejs IP w celu uzyskania dostępu do sieci fizycznej. Istnieje wiele typów, na przykład Token Ring i Ethernet. Czasami nazywane jest 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 (Layer Two Tunnel Protocol)	O protokole L2TP można myśleć, jak o wirtualnym połączeniu PPP, pracuje on poprzez dowolny obsługiwany typ linii.	Implementacja protokołu L2TP na serwerze i5/OS nie obsługuje aktualnie protokołu IPv6.

Opis	IPv4	IPv6
Adres pętli zwrotnej	Adres pętli zwrotnej to interfejs z adresem 127.*.*.* (zazwyczaj 127.0.0.1), wykorzystywany przez węzeł wyłącznie 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.
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.	Dla protokołu IPv6 dolna granica wielkości MTU wynosi 1280 bajtów. Oznacza to, że poniżej tego limitu protokół IPv6 nie fragmentuje pakietów. Aby wysłać pakiet IPv6 łączem o MTU mniejszym niż 1280, warstwa łącza musi w sposób przezroczysty dzielić i ponownie łączyć pakiety IPv6.
Netstat	Netstat to narzędzie do sprawdzania statusu połączeń TCP/IP, interfejsów lub tras. Dostępne za pośrednictwem programu System i Navigator i interfejsu znakowego.	Taka sama obsługa w przypadku IPv6.
Translacja adresu sieciowego (NAT)	Wbudowane w protokół TCP/IP podstawowe funkcje zapory firewall, z możliwością konfiguracji za pomocą programu System i 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	Konfigurowalna tabela w programie System i Navigator, która definiuje przypisanie nazwy sieciowej do adresu IP bez maski. Na przykład host Network 14, 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.
Routing OSPF	OSPF to protokół routingu, który w dużych sieciach systemów autonomicznych jest preferowany względem protokołu routingu RIP.	Taka sama obsługa w przypadku IPv6.
Filtrowanie pakietów	Filtrowanie pakietów stanowi podstawową funkcję zapory firewall wbudowaną w protokół TCP/IP. Konfiguracja tej funkcji odbywa się za pomocą programu System i Navigator.	Mechanizm filtrowania pakietów nie obsługuje protokołu IPv6.
Przekazywanie pakietów	Protokół TCP/IP i5/OS można skonfigurować w taki sposób, aby przekazywał otrzymywane pakiety IP dla nielokalnych adresów IP. Zazwyczaj interfejs dla połączeń przychodzących i interfejs dla połączeń wychodzących są połączone z innymi sieciami lokalnymi.	Przekazywanie pakietów jest w protokole IPv6 obsługiwane w ograniczonym zakresie. Stos TCP/IP systemu i5/OS nie obsługuje wykrywania sąsiadów w trybie routera.
Komenda PING	PING to podstawowe narzędzie TCP/IP do sprawdzania, czy host docelowy jest osiągalny. Dostępne za pośrednictwem programu System i Navigator i interfejsu znakowego.	Taka sama obsługa w przypadku IPv6.

Opis	IPv4	IPv6
Protokół PPP	Protokół PPP obsługuje interfejsy połączeń modemowych dla różnych modemów i typów linii.	Implementacja protokołu PPP na serwerze i5/OS nie obsługuje aktualnie protokołu IPv6.
Ograniczenia portu	Okna i5/OS umożliwiające klientom konfigurowanie wybranych numerów portów lub zakresu numerów portów dla protokołu TCP lub UDP, tak aby były one dostępne tylko dla określonego profilu.	Ograniczenia portu dla IPv6 są takie same jak te, które są dostępne w protokole IPv4.
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, oparte na wbudowanych projektowo określeń zasięgu (patrz Zasięg adresu).
Tabela protokołów	Tabela protokołów to konfigurowalna tabela w programie System i Navigator, definiująca przypisania nazw protokołów do określonych numerów protokołów, 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.
Jakość usługi (QoS)	Jakość usługi umożliwia zgłoszenie priorytetu pakietu i pasma dla aplikacji TCP/IP.	Implementacja usługi QoS na serwerze i5/OS nie obsługuje aktualnie protokołu IPv6.
Zmiana numerów	Zmiana numerów odbywa się poprzez ręczną zmianę konfiguracji, z możliwym wyjątkiem protokołu DHCP. Zmiana numerów w skali całego ośrodka lub organizacji jest ogólnie procesem trudnym i kłopotliwym, którego w miarę możliwości należy unikać.	Zmiana numerów stanowi ważny element projektowy protokołu IPv6 i jest wykonywana w dużej mierze automatycznie, zwłaszcza w ramach przedrostka /48.

Opis	IPv4	IPv6
Trasa	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.	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.
Tabela usług	Konfigurowalna tabela na serwerze i5/OS, zawierająca powiązania nazw usług z portami i protokołami, na przykład nazwa usługi FTP, 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.	Implementacja protokołu SNMP na serwerze i5/OS nie obsługuje aktualnie protokołu IPv6.
Interfejs 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 adresu IP.

Opis	IPv4	IPv6
Uruchamianie i zatrzymywanie	Do uruchamiania i zatrzymywania protokołu IPv4 służą odpowiednio komendy STRTCP i ENDTCP. Protokół IPv4 jest zawsze uruchamiany w chwili uruchomienia TCP/IP za pomocą komendy.	Do uruchamiania i zatrzymywania protokołu IPv6 służą odpowiednio komendy STRTCP i ENDTCP z parametrem STRIP6. Protokół IPv6 może nie zostać automatycznie uruchomiony wraz z TCP/IP. Protokół IPv6 można później uruchomić niezależnie. Interfejsy IPv6 są uruchamiane automatycznie, jeśli parametr AUTOSTART ma wartość *YES (wartość domyślna). Protokół IPv6 nie może być używany lub konfigurowany bez protokołu IPv4. Interfejs pętli zwrotnej IPv6 ::1, jest definiowany i aktywowany automatycznie podczas uruchamiania protokołu IPv6.
Obsługa z programu System i Navigator	Program System i Navigator stanowi kompletne rozwiązanie do konfigurowania protokołu TCP/IP.	Taka sama obsługa w przypadku IPv6.
Telnet	Usługa Telnet umożliwia zalogowanie się i korzystanie ze zdalnego komputera, tak jak przy połączeniu bezpośrednim.	Taka sama obsługa w przypadku IPv6.
Śledzenie trasy	Funkcja śledzenia trasy stanowi podstawowe narzędzie TCP/IP do określania ścieżki. Dostępne za pośrednictwem programu System i Navigator i interfejsu znakowego.	Taka sama obsługa w przypadku IPv6.
Warstwy transportowe	TCP, UDP, RAW.	Takie same warstwy transportowe znajdują się w protokole IPv6.
Adres nieokreślony (unspecified)	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.
Wirtualna sieć prywatna (VPN)	Sieć VPN (korzystająca z protokołu IPsec) umożliwia rozszerzenie zasięgu chronionych sieci prywatnych za pośrednictwem istniejących sieci publicznych.	Taka sama obsługa w przypadku IPv6. Więcej informacji można znaleźć w sekcji Sieć VPN.

Pojęcia pokrewne

“Przegląd IPv6” na stronie 3
Sekcja informuje o powodach wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyściach z użytkowania nowego protokołu.

Dostępne funkcje IPv6

IBM implementuje stopniowo IPv6 w systemie i5/OS. Funkcje IPv6 są przezroczyste dla istniejących aplikacji TCP/IP i współistnieją z funkcjami IPv4.

Najważniejsze opcje systemu i5/OS, na które ma wpływ protokół IPv6:

Konfigurowanie

- Domyślnie IPv6 jest uruchamiane przy uruchamianiu TCP/IP. Jeśli uruchomienie IPv6 przy uruchomieniu TCP/IP nie jest pożądane, należy w komendzie Uruchomienie TCP/IP (Start TCP/IP - STRTCP) podać wartość *NO dla parametru STRIP6. Można następnie uruchomić IPv6 w późniejszym czasie, podając w wydanej ponownie komendzie STRTCP parametr STRIP6 (*YES).
- Po skonfigurowaniu protokołu IPv6, pakiety IPv6 są wysyłane w sieci IPv6. Scenariusz opisujący konfigurowanie protokołu IPv6 w sieci znajduje się w sekcji "Scenariusz: tworzenie sieci lokalnej IPv6".
- Można skonfigurować wirtualne interfejsy IPv6 i wykonać automatyczną konfigurację bezstanową IPv6. Więcej informacji na temat tych opcji znajduje się w sekcji "Konfigurowanie IPv6" na stronie 26.
- Oprócz programu System i Navigator można teraz też używać interfejsu znakowego do konfigurowania i dostosowywania TCP/IP.

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 DNS obsługuje adresy AAAA i nową domenę IP6.ARPA przeznaczoną do wyszukiwania wstecz (IP-nazwa). Aplikacja może wybierać, czy akceptować adresy IP z systemu DNS (czy nie) i następnie skorzystać (lub nie) z IPv6 do komunikacji.

Rozwiązywanie problemów z 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

"Przegląd IPv6" na stronie 3
Sekcja informuje o powodach wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyściach z użytkowania nowego protokołu.

Scenariusz: tworzenie sieci lokalnej IPv6

Ten scenariusz pomoże zrozumieć sytuacje, w których protokół IPv6 można zastosować w celach biznesowych. Opisuje wymagania wstępne konfigurowania sieci LAN IPv6 oraz przedstawia etapy konfiguracji automatycznej konfiguracji bezstanowej IPv6 przy użyciu interfejsu znakowego.

Uwaga: W scenariuszu adresy IP x:x:x:x:x:x:x:x reprezentują adresy segmentowe IP.

Sytuacja

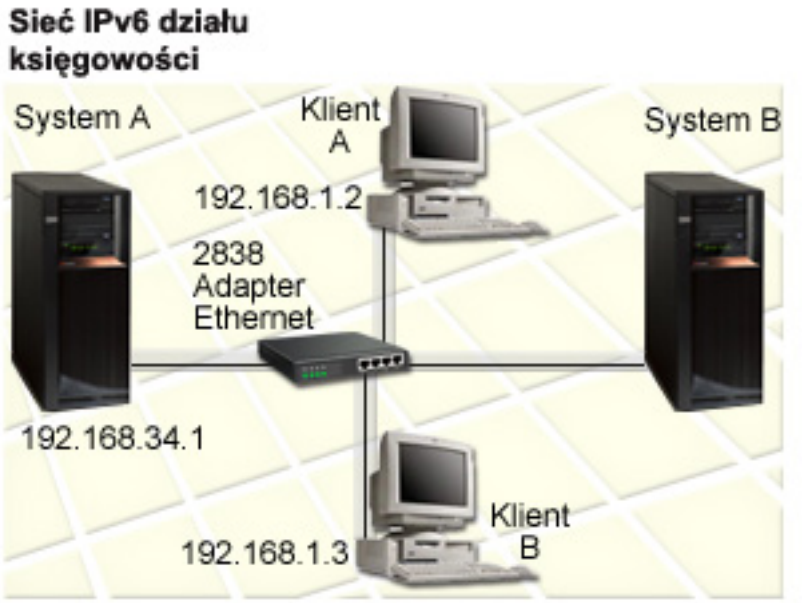
Działalność firmy najprawdopodobniej ulegnie znaczącemu rozwojowi. Dotyczy to zazwyczaj działu księgowości, który obecnie używa sieci IPv4. Ponieważ wykorzystanie IPv6 rozszerza możliwości adresacji IP, a IPv6 z czasem zastąpi IPv4 jako standard internetowy, jest bardzo ważne, aby wdrożyć IPv6 w działalności finansowej firmy. Zakupiona została już aplikacja księgowa klient-serwer, która wykorzystuje połączenia IPv6.

Cele

Po skonfigurowaniu systemu do użycia IPv6, dział księgowości firmy będzie mógł korzystać z aplikacji księgowej przez sieć IPv6.

Informacje szczegółowe

Działalność firmy wymaga, aby aplikacja księgowa zainstalowana na systemie A łączyła się z inną instancją aplikacji na systemie B. Pozwala to klientom uruchamiać aplikacje, współużytkować i przesyłać dane zapisane w obu systemach. Poniższy rysunek ilustruje konfigurację sieci w tym scenariuszu. Dwa produkty System i i dwie stacje robocze klienta są podłączone do sieci LAN standardu Ethernet w ośrodku za pomocą adapterów Ethernet.



- Zarówno system A jak i system B mają system operacyjny i5/OS w wersji 5, wydaniu 4 lub nowszej.
- System A ma aktualnie adres IPv4 192.168.34.1.
- Wymagane jest połączenie systemu A z systemem B, znajdującym się w zdalnej lokalizacji.
- Do sieci LAN IPv6 mają być podłączone dwie stacje robocze:
  - Klient A ma aktualnie adres IPv4 192.168.1.2.
  - Klient B ma aktualnie adres IPv4 192.168.1.3.

Wymagania wstępne i założenia

Ten scenariusz zakłada, że spełnione zostały następujące wymagania wstępne sprzętu w środowisku sieci:

- Ukończono konfigurację wszystkich kabli i sprzętu w sieci.
- Adapter Ethernet (w tym scenariuszu: 2838) został skonfigurowany.

Aby utworzyć sieć LAN IPv6, w systemie muszą być zainstalowane następujące komponenty oprogramowania:

- System i Access for Windows
- Program System i Navigator z komponentem sieci

Konfigurowanie

Przed rozpoczęciem konfigurowania IPv6 dla systemu należy wykonać następujące czynności:

- Należy skonfigurować TCP/IP z adresem IPv4.
- Należy skonfigurować opis linii Ethernet przy pierwszym konfigurowaniu TCP/IP.

Pojęcia pokrewne

| “Pojęcia związane z IPv6” na stronie 4
| Przed zaimplementowaniem IPv6 w systemie należy zrozumieć podstawowe pojęcia związane z IPv6, takie jak formaty adresów IPv6, typy adresów IPv6 oraz wykrywanie sąsiadów.

| **Zadania pokrewne**

| “Konfigurowanie TCP/IP po raz pierwszy” na stronie 21
| Podczas konfigurowania nowego systemu należy nawiązać połączenie sieciowe i skonfigurować początkowo protokół TCP/IP z IPv4.

| Uruchamianie stosu IPv6

| Należy najpierw uruchomić stos IPv6 za pomocą interfejsu znakowego. Usługi IPv6 nie będą dostępne, dopóki nie zostanie uruchomione IPv6.

| Sprawdź, czy stos IPv6 jest uruchomiony

| Zazwyczaj stos IPv6 jest uruchamiany przy pierwszym konfigurowaniu TCP/IP.

| Aby sprawdzić, czy stos IPv6 jest uruchomiony, wykonaj następujące czynności:

| 1. W wierszu komend wpisz NETSTAT i naciśnij klawisz Enter, aby uzyskać dostęp do menu Praca ze statusem sieci TCP/IP (Work with TCP/IP Network Status).
| 2. Wybierz opcję 10 (Wyświetlenie statusu stosu TCP/IP - Display TCP/IP stack status) i naciśnij klawisz Enter.
| 3. W podpowiedzi *status stosu IPv6* (IPv6 stack status) upewnij się, że ustawiona jest wartość Aktywny (Active).

| Uruchamianie stosu IPv6

| Jeśli status stosu IPv6 nie ma wartości Aktywny (Active), IPv6 nie zostało uruchomione.

| Aby uruchomić stos IPv6, wykonaj następujące czynności:

| 1. W wierszu komend wpisz STRTCP (komenda Uruchomienie TCP/IP - Start TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby wyświetlić listę dodatkowych parametrów.
| 2. W podpowiedzi *Uruchamianie IPv6* (Start IPv6) podaj wartość *YES i naciśnij klawisz Enter.

| **Uwaga:** Nie trzeba kończyć pracy TCP/IP, aby włączyć w późniejszym czasie IPv6.

| Konfigurowanie bezstanowego autokonfigurowania adresu IPv6

| Istnieje kilka sposobów konfigurowania IPv6 w systemie. W niniejszym temacie opisano, jak skonfigurować bezstanowe autokonfigurowanie adresu IPv6 za pomocą interfejsu znakowego.

| Ponieważ bezstanowe autokonfigurowanie adresu IPv6 tworzy automatycznie nowe interfejsy IPv6 dla danego opisu linii, należy skonfigurować istniejący opis linii Ethernet. W tym przykładzie wykorzystywana jest nazwa opisu linii Eth08.

| Aby skonfigurować bezstanowe autokonfigurowanie adresu IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

| **Uwaga:** Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

| 1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
| 2. W polu *Adres internetowy* (Internet address) wpisz *IP6SAC.
| 3. W polu *Opis linii* (Line description) wpisz Eth08 i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
| 4. Podaj wybrane wartości lub pozostaw domyślne wartości dla niektórych spośród parametrów opcjonalnych, posługując się poniższą tabelą.

Tabela 1. Wartości wejściowe do bezstanowego autokonfigurowania adresu IPv6

Nazwy parametrów	Wartości wejściowe
Maksymalna jednostka transmisji	*LIND
Identyfikator interfejsu	*LIND
Maksymalna ilość transmisji DAD	2
Rozszerzenia prywatności	*YES
Tekst opisu	Interfejs SAC IPv6 ETHLINE

5. Upewnij się, że wszystkie wartości są poprawnie podane i naciśnij klawisz Enter.

Bezstanowa autokonfiguracja adresu IPv6 została pomyślnie skonfigurowana.

Uruchamianie interfejsu IPv6

Po skonfigurowaniu bezstanowej autokonfiguracji adresu IPv6 należy uruchomić interfejs IPv6, aby sieć IPv6 mogła być wykorzystywana.

Aby rozpocząć bezstanową autokonfigurację adresu IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz *IP6SAC i naciśnij klawisz Enter.
3. W polu *Opis linii* (Line description) wpisz Eth08 i naciśnij klawisz Enter.

Bezstanowa autokonfiguracja adresu IPv6 została pomyślnie uruchomiona, a adres lokalny łącza IPv6 został przypisany do systemu.

Uwaga: Można przypisać jeden lub kilka globalnych adresów IPv6 w zależności od rozgłaszanych przedrostków routerów lokalnych.

Rozwiązywanie problemów dotyczących IPv6

Jeśli w systemie i5/OS skonfigurowano IPv6, można użyć kilku narzędzi do rozwiązywania problemów, które stosowane są w przypadku 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 pokrewne

Śledzenie komunikacji

Planowanie instalacji TCP/IP

Przed rozpoczęciem instalowania i konfigurowania systemu należy poświęcić parę chwil na zaplanowanie działań. Ten temat zawiera informacje pomocne podczas instalowania i konfigurowania protokołu TCP/IP w systemie operacyjnym i5/OS.

Wskazówki w tym temacie 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 o konfiguracji TCP/IP

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

Poniższa tabela przedstawia informacje wymagane do konfiguracji TCP/IP. Należy wydrukować tę stronę, a także zapisać informacje dotyczące konfiguracji swojego systemu oraz protokołu TCP/IP sieci, z którą jest nawiązywane połączenie. Informacje te będą potrzebne później, podczas konfigurowania protokołu TCP/IP.

Tabela 2. Informacje wymagane do konfiguracji TCP/IP

Wymagane informacje	Dla systemu użytkownika	Przykład
Rodzaj adaptera komunikacyjnego zainstalowanego w systemie (patrz instrukcje pod tabelą)		Ethernet
Nazwa zasobu		CMN01
Adres IP systemu		199.5.83.158
Maska podsieci systemu		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

Następujące informacje pomogą określić wartości z powyższej tabeli:

- Aby określić dane adaptera komunikacyjnego oraz nazwę zasobu (dwa pierwsze wiersze w tabeli), wykonaj następujące czynności:
  1. W wierszu komend wpisz GO HARDWARE i naciśnij klawisz Enter, aby uzyskać dostęp do menu Zasoby sprzętowe (Hardware Resources).
  2. Wybierz opcję 1 (Praca z zasobami komunikacyjnymi) 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.
- Jeśli jakiekolwiek pozostałe terminy nie są zrozumiałe dla użytkownika, należy zapoznać się z dokumentacją technicznąIBM (Redbooks):IBM i5/OS IP Networks: Dynamic  w celu uzyskania informacji o podstawowej instalacji i procedurach konfiguracji.

Zadania pokrewne

“Instalowanie TCP/IP” na stronie 20
W system operacyjny i5/OS wbudowano podstawową obsługę protokołu TCP/IP, która umożliwia podłączenie systemu do sieci.

Metody ochrony protokołu TCP/IP

Podczas planowania konfiguracji TCP/IP dla platformy System i 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 Signon values: Signon overview.

  Informacje pokrewne

  Serwery System i - bezpieczeństwo internetowe

  Planowanie ochrony TCP/IP

  Konfigurowanie ochrony TCP/IP

Instalowanie TCP/IP

W system operacyjny i5/OS wbudowano podstawową obsługę protokołu TCP/IP, która umożliwia podłączenie systemu do sieci.

Jeśli planowane jest używane protokołów aplikacyjnych opartych na TCP/IP, takich jak Telnet, FTP lub SMTP, należy dodatkowo zainstalować produkt IBM TCP/IP Connectivity Utilities for i5/OS. TCP/IP Utilities to osobny instalowany program licencjonowany.

Aby zainstalować w systemie program TCP/IP Utilities, wykonaj następujące czynności:

1. Włóż nośnik instalacyjny TCP/IP do odpowiedniego urządzenia w systemie.
   a. Jeśli jest to dysk CD-ROM, włóż go do urządzenia optycznego.
   b. 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 - Install licensed programs) i naciśnij klawisz Enter, aby zobaczyć listę programów licencjonowanych i ich elementów opcjonalnych.
4. Wpisz 1 (Instaluj - Install) w kolumnie opcji obok pozycji 5761TC1 (IBM TCP/IP Connectivity Utilities for i5/OS) i naciśnij klawisz Enter.
5. Na ekranie Potwierdzenie instalacji programów licencjonowanych (Confirm Install of Licensed Programs) naciśnij klawisz Enter.
6. Na ekranie Opcje instalacji (Install Options) wpisz wartości podane poniżej i naciśnij klawisz Enter, aby je zatwierdzić.

Tabela 3. Dostępne wartości na ekranie Opcje instalacji (Install Options)

Opcje instalacji	Opisy
Urządzenie instalacyjne (Urządzenie instalacyjne)	Jeśli instalowanie odbywa się z dysku CD-ROM, wpisz QOPT. Jeśli instalowanie odbywa się z napędu taśm, wpisz TAP01.
Instalowane obiekty (Objects to install)	Za pomocą tej opcji można określić, czy mają być instalowane programy, obiekty językowe, czy też oba typy elementów.
Niezaakceptowana umowa (Nonaccepted agreement)	Ta opcja ma zastosowanie tylko wtedy, jeśli umowa licencyjna oprogramowania nie została zaakceptowana wcześniej. Podaj wartość 2, aby został wyświetlony ekran umowy licencyjnej oprogramowania z opcją akceptacji lub odrzucenia.
Automatyczny IPL (Automatic IPL)	Opcja ta określa, czy system automatycznie wykona IPL po pomyślnym zakończeniu procesu instalacji.

Po pomyślnym zainstalowaniu oprogramowania IBM TCP/IP Connectivity Utilities for i5/OS zostanie wyświetlone menu Praca z programami licencjonowanymi (Work with Licensed Programs) lub ekran Wpisanie się (Sign On).

7. Wybierz opcję 50 (Wyświetlenie protokołu komunikatów), aby sprawdzić, czy oprogramowanie IBM TCP/IP Connectivity Utilities for i5/OS zostało zainstalowane pomyślnie. W przypadku wystąpienia błędu, w dolnej części ekranu Praca z programami licencjonowanymi (Work with Licensed Programs) będzie widoczny następujący komunikat:

   Nie zakończono funkcji Praca z programami licencjonowanymi (Work with licensed program function not complete).

   W razie wystąpienia programów należy ponowić próbę zainstalowania oprogramowania IBM TCP/IP Connectivity Utilities for i5/OS.

Uwaga: Inne programy licencjonowane, które można zainstalować to:

- IBM System i Access for Windows (5761–XE1): Ten program umożliwia konfigurowanie niektórych komponentów TCP/IP za pomocą programu System i Navigator.
- IBM HTTP Server for i5/OS (5761–DG1): Ten program umożliwia 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.

Odsyłacze pokrewne

“Zbieranie informacji o konfiguracji TCP/IP” na stronie 19
Należy zebrać podstawowe informacje konfiguracyjne wymagane podczas konfigurowania protokołu TCP/IP.

Konfigurowanie TCP/IP

Sekcja opisuje czynności wykonywane podczas konfigurowania TCP/IP po raz pierwszy lub podczas wykonywania dodatkowej konfiguracji IPv6. Podano tu instrukcje dotyczące konfigurowania TCP/IP w różnych sytuacjach.

Przed wykorzystaniem tych informacji do skonfigurowania TCP/IP należy upewnić się, że zostały zainstalowane wszystkie niezbędne komponenty sprzętowe.

Konfigurowanie TCP/IP po raz pierwszy

Podczas konfigurowania nowego systemu należy nawiązać połączenie sieciowe i skonfigurować początkowo protokół TCP/IP z IPv4.

Aby skonfigurować TCP/IP po raz pierwszy, należy użyć interfejsu znakowego. Jeśli na przykład potrzebna jest możliwość używania programu System i Navigator z komputera PC, a przed uruchomieniem programu System i Navigator wymagane jest podstawowe skonfigurowanie protokołu TCP/IP, do przeprowadzenia konfiguracji podstawowej trzeba użyć interfejsu znakowego.

Podczas konfigurowania systemu za pomocą interfejsu znakowego konieczne będzie częste otwieranie menu Konfigurowanie TCP/IP (Configure TCP/IP) w celu wybierania zadań konfiguracyjnych. Przed przystąpieniem do konfigurowania systemu należy poświęcić kilka chwil na zapoznanie się z tym menu, zgodnie z następującymi instrukcjami.

1. W wierszu komend wpisz GO TCPADM i naciśnij klawisz Enter, aby uzyskać dostęp do menu Administrowanie TCP/IP (TCP/IP Administration).
2. Wybierz opcję 1 (Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter, aby uzyskać dostęp do menu Konfigurowanie TCP/IP (Configure TCP/IP - CFGTCP).

Uwaga: Aby wykonać opisane tu czynności konfiguracyjne, trzeba posiadać uprawnienia specjalne *IOSYSCFG.

Pojęcia pokrewne

"Scenariusz: tworzenie sieci lokalnej IPv6" na stronie 15
Ten scenariusz pomoże zrozumieć sytuacje, w których protokół IPv6 można zastosować w celach biznesowych. Opisuje wymagania wstępne konfigurowania sieci LAN IPv6 oraz przedstawia etapy konfiguracji automatycznej konfiguracji bezstanowej IPv6 przy użyciu interfejsu znakowego.

"Dostosowywanie TCP/IP" na stronie 31
Za pośrednictwem programu System i Navigator i interfejsu znakowego można uzyskać dostęp do wielu opcji dostosowywania konfiguracji TCP/IP.

Odsyłacze pokrewne

"Planowanie konfiguracji IPv6" na stronie 26
Przed konfigurowaniem IPv6 w systemie należy skonfigurować protokół TCP/IP. Poniżej przedstawiono wymagania dotyczące sprzętu i oprogramowania oraz wymagania wstępne do konfigurowania IPv6 w systemie i5/OS.

Informacje pokrewne

Profile użytkowników

Uprawnienia specjalne *IOSYSCFG

Krok 1: konfigurowanie opisu linii (Ethernet)

Należy utworzyć opis linii Ethernet, będącej obiektem komunikacji dla TCP/IP.

W celu skonfigurowania opisu linii dla linii Ethernet wykonaj następujące czynności:

1. W wierszu komend wpisz CRTLINETH (komenda Tworzenie opisu linii - Create Line Description) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu tworzenia opisu linii (Ethernet).
2. W polu *Opis linii* (Line description) podaj nazwę linii (dowolną).
3. W polu *Nazwa zasobu* (Resource name) podaj nazwę zasobu.
4. Aby wyświetlić listę dodatkowych parametrów, naciśnij kilka razy klawisz Enter.
5. Podaj wartości dodatkowych parametrów, które mają być zmienione, a następnie naciśnij klawisz Enter, aby wprowadzić dane.

Krok 2: włączanie przesyłania datagramów IP

Jeśli pakiety IP mają być przesyłane między różnymi podsieciami, konieczne będzie włączenie przekazywania datagramów IP.

Aby włączyć przesyłanie datagramów IP, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 3 (Zmiana atrybutów TCP/IP - Change TCP/IP attributes) i naciśnij klawisz Enter.
3. W polu *Przesyłanie datagramów IP* (IP datagram forwarding) wpisz *YES i naciśnij klawisz Enter.

Krok 3: konfigurowanie interfejsu

Interfejs IPv4 należy skonfigurować poprzez przypisanie adresu IPv4 odpowiadającego adapterowi sieciowemu.

Aby skonfigurować interfejs TCP/IP, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Podaj opcję 1 (Praca z interfejsami TCP/IP - Work with TCP/IP interfaces) i naciśnij klawisz Enter.
3. W menu Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wpisz 1 (Dodaj - Add) w polu *Opcja* (Opt) i naciśnij klawisz Enter, aby uzyskać dostęp do menu Dodawanie interfejsu TCP/IP (Add TCP/IP Interface).
4. W polu *Adres internetowy* (Internet address) podaj poprawny adres IPv4, który zostanie przypisany systemowi.
5. W polu *Opis linii* (Line description) podaj nazwę linii zdefiniowaną w kroku 1.
6. W polu *Maska podsieci* (Subnet mask) wpisz poprawny adres IPv4 określający maskę podsieci i naciśnij klawisz Enter.
7. Aby uruchomić interfejs, wpisz opcję 9 (Uruchomienie - Start) obok skonfigurowanego interfejsu w menu Praca z interfejsami TCP/IP (Work with TCP/IP interfaces) i naciśnij klawisz Enter.

Krok 4: konfigurowanie trasy domyślnej

Dla każdej sieci zdalnej w systemie należy użyć niniejszych informacji, aby skonfigurować trasę domyślną.

Ponieważ sieć może składać się z wielu sieci połączonych ze sobą, należy zdefiniować przynajmniej jedną trasę dla systemu, aby mógł komunikować się ze zdalnym systemem w innej sieci. Pozycje routingu należy dodać także po to, aby zapewnić prawidłową pracę klientów TCP/IP łączących się z systemem 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. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 2 (Praca z trasami TCP/IP) i naciśnij klawisz Enter.
3. Wybierz opcję 1 (Dodaj) w polu *Opt* i naciśnij klawisz Enter, aby uzyskać dostęp do menu Dodanie trasy TCP/IP - Add TCP/IP Route (ADDTCPRTE).
4. Wpisz *DFTROUTE w polu *Cel trasy* (Route destination) i *NONE w polu *Maska podsieci* (Subnet mask).
5. W polu *Następny przeskok* (Next hop) podaj adres IP bramy na trasie i naciśnij klawisz Enter.

Krok 5: definiowanie domeny TCP/IP

Po określeniu pozycji routingu należy zdefiniować domenę lokalną i nazwy hostów, aby umożliwić komunikację w obrębie sieci, a następnie skorzystać z serwera DNS w celu powiązania adresów IP z nazwami hostów.

Domena lokalna i nazwa hosta tworzą nazwę podstawowa przypisaną systemowi. Są to informacje niezbędne podczas konfigurowania obsługi innych aplikacji sieciowych, na przykład obsługi poczty elektronicznej.

Jeśli pożądane jest stosowanie łatwych do zapamiętania nazw zamiast adresów IP, należy wprowadzić rozstrzyganie adresów IP za pomocą serwera DNS, tabeli hostów lub obu tych metod. Aby poinformować system o metodzie preferowanej, należy skonfigurować priorytet wyszukiwania nazw hostów.

Aby zdefiniować domenę TCP/IP, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).

2. Wybierz opcję 12 (Zmiana informacji domeny TCP/IP - Change TCP/IP domain information) i naciśnij klawisz Enter.
3. W polu *Nazwa hosta* (Host name) podaj nazwę zdefiniowaną wcześniej jako nazwa hosta lokalnego.
4. W polu *Nazwa domeny* (Domain name) podaj nazwę zdefiniowaną wcześniej jako nazwa domeny lokalnej.
5. W polu *Priorytet wyszukiwania nazwy hosta* (Host name search priority) ustaw jedną z następujących wartości:
   - Ustaw wartość *REMOTE (zalecana). Oznacza to, że system będzie w pierwszej kolejności automatycznie przeszukiwać nazwy hostów na serwerze DNS. System będzie wysyłać zapytania do kolejnych serwerów DNS aż do otrzymania odpowiedzi.
   - Ustaw wartość *LOCAL. Oznacza to, że system będzie w pierwszej kolejności przeszukiwać nazwy hostów w tabeli hostów.

   Uwaga: Jeśli priorytet wyszukiwania nazwy hosta ma wartość *LOCAL, należy w tabeli hostów zdefiniować pozycję odpowiadającą systemowi. Szczegółowe informacje można znaleźć w sekcji Krok 6: definiowanie tabeli hostów.
6. W polu *Serwer nazw domen* (Domain name server) wprowadź adres IP używanego serwera DNS i naciśnij klawisz Enter.

Po zdefiniowaniu informacji o domenie TCP/IP można modyfikować konfiguracje za pośrednictwem interfejsu znakowego lub programu System i Navigator.

Zadania pokrewne

“Modyfikacja domeny TCP/IP” na stronie 31
Możliwe jest modyfikowanie nazw domen i hostów lokalnych, dodawanie i usuwanie serwerów DNS, modyfikowanie priorytetu wyszukiwania nazwy hosta itd.

Informacje pokrewne

System DNS

Krok 6: definiowanie tabeli hostów

Może być potrzebna możliwość rozstrzygania adresów IP za pomocą nie tylko serwera DNS, lecz również tabeli hostów. Jeśli używany będzie wyłącznie serwer DNS, możesz ten krok zignorować.

Tabela hostów służy (podobnie jak serwer DNS) do przypisywania adresów IP do nazw hostów, co pozwala używać łatwych do zapamiętania nazw do identyfikacji systemu. Tabela hostów obsługuje zarówno adresy IPv4, jak i IPv6.

Aby zdefiniować tabelę hostów za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 10 (Praca z pozycjami tabeli hostów TCP/IP - Work with TCP/IP Host Table Entries) i naciśnij klawisz Enter.
3. Wpisz 1 (Dodaj - Add) w polu *Opcja* (Opt) i naciśnij klawisz Enter, aby uzyskać dostęp do menu Dodawanie pozycji tabeli hostów TCP/IP (Add TCP/IP Host Table Entry).
4. W polu *Adres internetowy* (Internet address) podaj adres IP zdefiniowany w kroku 3.
5. W polu *Nazwa hosta* (Host name) podaj pełną nazwę odpowiadającą hostowi lokalnemu i naciśnij klawisz Enter. Jeśli istnieje taka potrzeba, wprowadź znak plusa (+) obok pola *+: więcej wartości* (+ for more values), aby utworzyć miejsce na więcej niż jedną nazwę hosta.

   Uwaga: Dla jednej pozycji w tabeli hostów (adresu IP) można podać do 65 nazw hostów.
6. Powtórz czynności od 1 do 4 dla wszystkich pozostałych hostów w sieci, które mają być dostępne poprzez nazwę, i dodaj pozycję dla każdego z nich.

Po zdefiniowaniu tabeli hostów można modyfikować konfiguracje za pomocą interfejsu znakowego lub programu System i Navigator.

Zadania pokrewne

"Dostosowywanie pozycji w tabeli hostów" na stronie 32
Pozycje w tabeli hostów można dodawać, edytować i usuwać. Tabela hostów obsługuje zarówno adresy IPv4, jak i IPv6.

Krok 7: uruchamianie TCP/IP

Aby usługi TCP/IP były gotowe do użycia, należy uruchomić TCP/IP.

Aby uruchomić TCP/IP, wykonaj następujące czynności.

1. W wierszu komend wpisz STRTCP (komenda Uruchomienie TCP/IP - Start TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania TCP/IP.
2. Podaj wartość *YES, jeśli mają być opcjonalnie uruchamiane dodatkowe urządzenia. Jeśli nie ma takich urządzeń, podaj wartość *NO.
3. Naciśnij klawisz Enter, aby uruchomić TCP/IP.

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.

Aby zmienić konfigurację w razie konieczności zmiany ustawień sieci, można użyć programu System i Navigator lub interfejsu znakowego.

Pojęcia pokrewne

"Konfigurowanie IPv6" na stronie 26
Podane instrukcje umożliwiają skonfigurowanie obsługi funkcji IPv6 w systemie.

"Dostosowywanie TCP/IP" na stronie 31
Za pośrednictwem programu System i Navigator i interfejsu znakowego można uzyskać dostęp do wielu opcji dostosowywania konfiguracji TCP/IP.

Krok 8: testowanie połączenia TCP/IP

Aby przetestować połączenia TCP/IP po zakończeniu pierwszej konfiguracji TCP/IP, należy użyć niniejszej procedury.

Po pomyślnym zainstalowaniu licencjonowanego programu IBM TCP/IP Connectivity Utilities for i5/OS i skonfigurowaniu TCP/IP w systemie, należy sprawdzić, czy połączenie TCP/IP działa poprawnie.

Testowanie TCP/IP za pomocą wiersza komend

Aby przetestować połączenie TCP/IP z siecią, wykonaj następujące czynności:

1. Sprawdź, czy komunikacja TCP/IP została skonfigurowana i uruchomiona na wszystkich stacjach roboczych. Użyj dokumentacji udostępnionej przez dostawcę stacji roboczej.
2. Z poziomu stacji roboczej otwórz wiersz komend i wpisz komendę ping z adresem IP skonfigurowanego interfejsu. Jeśli na przykład adres IP to 192.168.34.1, wpisz:

```
ping 192.168.34.1
```

Może zostać wyświetlony komunikat potwierdzający, że pakiet został wysłany do systemu. Pozwala to sprawdzić, czy stacja robocza ma dostęp do systemu. Jeśli połączenie z siecią się nie powiedzie, zajrzyj do sekcji Rozwiązywanie problemów dotyczących TCP/IP, aby uzyskać więcej informacji.

Testowanie TCP/IP za pomocą programu System i Navigator

Można też użyć programu System i Navigator, aby przetestować połączenie TCP/IP:

- W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP** (*system* > Network > TCP/IP Configuration).
- Prawym przyciskiem myszy kliknij **Konfiguracja TCP/IP** i wybierz opcję **Narzędzia → Ping**.

| • Wykonaj czynności kreatora Ping, aby przetestować połączenie TCP/IP.

Konfigurowanie IPv6

Podane instrukcje umożliwiają skonfigurowanie obsługi funkcji IPv6 w systemie.

Protokół IPv6 pozwala korzystać z zalet następnej generacji sieci Internet. Protokół IPv6 można skonfigurować na istniejącej linii korzystając z funkcji bezstanowej autokonfiguracji adresów IPv6 lub poprzez ręczne skonfigurowanie interfejsów IPv6.

Pojęcia pokrewne

"Przegląd IPv6" na stronie 3
Sekcja informuje o powodach wymiany standardu IPv4 (Internet Protocol version 4) na IPv6 (Internet Protocol version 6) i korzyściach z użytkowania nowego protokołu.

Zadania pokrewne

"Krok 7: uruchamianie TCP/IP" na stronie 25
Aby usługi TCP/IP były gotowe do użycia, należy uruchomić TCP/IP.

Planowanie konfiguracji IPv6

| Przed konfigurowaniem IPv6 w systemie należy skonfigurować protokół TCP/IP. Poniżej przedstawiono wymagania
| dotyczące sprzętu i oprogramowania oraz wymagania wstępne do konfigurowania IPv6 w systemie i5/OS.

| Wymagania dotyczące sprzętu i oprogramowania

| Aby skonfigurować IPv6 na linii ethernetowej system musi spełniać następujące wymagania:
| • i5/OS wersja 5, wydanie 4 lub nowszy
| • System i Access for Windows
| • Program System i Navigator z komponentem sieci
| • Router z możliwością obsługi IPv6, aby wysyłać ruch IPv6 poza bezpośrednią sieć LAN.

| Wymagania wstępne konfiguracji

| Przed skonfigurowaniem IPv6 należy skonfigurować następujące elementy:
| • Należy skonfigurować TCP/IP przy użyciu IPv4. Więcej szczegółów zawiera sekcja Pierwsze konfigurowanie
| TCP/IP.
| • IPv6 musi być uruchomione. Aby sprawdzić, czy stos IPv6 jest uruchomiony, wykonaj następujące czynności:
| 1. W wierszu komend wpisz NETSTAT i naciśnij klawisz Enter, aby uzyskać dostęp do menu Praca ze statusem
| sieci TCP/IP (Work with TCP/IP Network Status).
| 2. Wybierz opcję 10 (Wyświetlenie statusu stosu TCP/IP - Display TCP/IP stack status) i naciśnij klawisz Enter.
| 3. W podpowiedzi *status stosu IPv6* (IPv6 stack status) upewnij się, że ustawiona jest wartość Aktywny (Active).
| 4. Jeśli status stosu IPv6 nie ma wartości Aktywny (Active), wykonaj następujące czynności, aby uruchomić IPv6:
| a. W wierszu komend wpisz STRTCP (komenda Uruchomienie TCP/IP - Start TCP/IP) i naciśnij klawisz F4
| (Podpowiedź), aby uzyskać dostęp do menu uruchamiania TCP/IP.
| b. W podpowiedzi *Uruchamianie IPv6* (Start IPv6) podaj wartość *YES i naciśnij klawisz Enter.

| **Uwaga:** Nie trzeba kończyć pracy TCP/IP, aby włączyć w późniejszym czasie IPv6.

| **Zadania pokrewne**

"Konfigurowanie TCP/IP po raz pierwszy" na stronie 21
Podczas konfigurowania nowego systemu należy nawiązać połączenie sieciowe i skonfigurować początkowo protokół TCP/IP z IPv4.

Konfigurowanie bezstanowego autokonfigurowania adresu IPv6

Skorzystanie z funkcji bezstanowego autokonfigurowania adresu IPv6 umożliwia automatyczne skonfigurowanie obsługi protokołu IPv6.

Funkcja bezstanowego autokonfigurowania adresu IPv6 automatycznie tworzy nowe interfejsy IPv6 dla wskazanego opisu linii i przypisuje do tych interfejsów adresy IPv6. Bezstanową autokonfigurację adresu IPv6 można przeprowadzić albo za pośrednictwem kreatora w programie System i Navigator, albo korzystając z interfejsu znakowego.

Konfigurowanie bezstanowego autokonfigurowania adresu IPv6 za pomocą programu System i Navigator

Aby skonfigurować bezstanowe autokonfigurowanie adresu IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → Linie** (*system* > Network > TCP/IP Configuration > Lines).
2. Kliknij prawym przyciskiem myszy jedną z linii w prawym panelu i wybierz kolejno **Bezstanowe autokonfigurowanie adresów IPv6 (IPv6 Stateless Address Autoconfiguration) → Konfiguruj (Configure)**.
3. Postępuj zgodnie z instrukcjami kreatora nowego interfejsu IPv6, aby dokończyć autokonfigurację.
4. Aby uruchomić interfejs IPv6 utworzony w procesie autokonfiguracji, kliknij prawym przyciskiem myszy nowo skonfigurowaną linię i wybierz kolejno opcje **Bezstanowe autokonfigurowanie adresów IPv6 (IPv6 Stateless Address Autoconfiguration) → Start (Uruchom)**.

   Uwaga: Aby upewnić się, że protokół IPv6 będzie uruchamiany automatycznie podczas uruchamiania protokołu TCP/IP, zaznacz opcję **Uruchom podczas uruchamiania TCP/IP** (Start when TCP/IP is started) na ekranie Konfigurowanie linii IPv6 (Configure Line for IPv6).

Jeśli status zmieni się na Aktywny, oznacza to, że bezstanowa autokonfiguracja adresów IPv6 została pomyślnie skonfigurowana i uruchomiona.

Konfigurowanie bezstanowego autokonfigurowania adresu IPv6 za pomocą interfejsu znakowego

Aby *skonfigurować* bezstanowe autokonfigurowanie adresu IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

Uwaga: Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz *IP6SAC.
3. W polu *Opis linii* (Line description) podaj nazwę linii (można użyć dowolnej nazwy) i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. Wprowadź ewentualne parametry opcjonalne i naciśnij klawisz Enter.

Aby *skonfigurować* bezstanowe autokonfigurowanie adresu IPv6, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz *IP6SAC i naciśnij klawisz Enter.
3. W polu *Opis linii* (Line description) podaj nazwę linii zdefiniowaną w poprzednich krokach konfiguracji, a następnie naciśnij klawisz Enter.

Bezstanowa autokonfiguracja adresów IPv6 została pomyślnie skonfigurowana i uruchomiona.

Pojęcia pokrewne

"Bezstanowe autokonfigurowanie adresu" na stronie 6
Bezstanowe autokonfigurowanie adresu automatyzuje niektóre zadania administratora.

Zadania pokrewne

"Uruchamianie konkretnego interfejsu TCP/IP" na stronie 30
Jeśli aplikacja korzystająca z gniazd wymaga konkretnego interfejsu IPv4 lub IPv6, należy ten interfejs uruchomić.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Ręczne tworzenie interfejsu IPv6

Protokół IPv6 można skonfigurować poprzez ręczne utworzenie interfejsu IPv6 w sieci LAN lub wirtualnego interfejsu IPv6. Do przeprowadzenia konfiguracji można wykorzystać program System i Navigator lub interfejs znakowy.

Tworzenie interfejsu IPv6 za pomocą programu System i Navigator

Aby utworzyć interfejs IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Kliknij prawym przyciskiem myszy pozycję **Interfejsy** i wykonaj jedną z następujących czynności:
   - Aby utworzyć interfejs IPv6 dla sieci lokalnej, wybierz kolejno **Nowy interfejs → Sieć lokalna**.
   - Aby utworzyć wirtualny interfejs IPv6, wybierz kolejno **Nowy interfejs → Wirtualny adres IP**.
3. Aby utworzyć nowy interfejs IPv6, postępuj zgodnie z instrukcjami zawartymi w kreatorze nowego interfejsu IPv6. Po zakończeniu procesu konfiguracji, nowy interfejs zostanie wyświetlony w oknie z prawej strony.

   Uwaga: Aby aktywować pozycję menu nowego interfejsu, należy posiadać uprawnienie specjalne *IOSYSCFG.
4. Aby uruchomić interfejs, kliknij prawym przyciskiem myszy nowy interfejs IPv6 na prawym panelu, a następnie wybierz opcję **Uruchom**.

   Można też zaznaczyć pole wyboru **Uruchamiaj wraz z TCP/IP**, aby się upewnić, że interfejs zostanie włączony automatycznie przy następnym uruchomieniu protokołu TCP/IP.

Konfigurowanie interfejsu IPv6 za pomocą interfejsu znakowego

Aby utworzyć zwykły interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

Uwaga: Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv6.
3. W polu *Opis linii* (Line description) podaj nazwę linii (można użyć dowolnej nazwy) i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Aby utworzyć wirtualny interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

Uwaga: Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv6.
3. W polu *Opis linii* (Line description) wpisz *VIRTUALIP i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. W polu *Preferowane opisy linii* (Preferred line descriptions) wykonaj jedną z następujących czynności:

- Jeśli nie chcesz na tym etapie określać żadnych preferowanych opisów linii, zaakceptuj domyślną wartość *NONE.
- Wpisz znak plusa (+) obok pola + *aby wyświetlić więcej wartości* (+ for more values) i naciśnij klawisz Enter. Następnie w menu Podaj więcej wartości dla parametru PREFLIND (Specify More Values for Parameter PREFLIND) podaj po kolei opisy linii (można użyć dowolnych nazw), a następnie naciśnij klawisz Enter.

Uwaga: Można wprowadzić maksymalnie 10 opisów linii w preferowanej kolejności użycia. Każdy opis linii musi być używany przez co najmniej jeden interfejs IPv6.

5. Upewnij się, że wszystkie pozostałe parametry opcjonalne zostały podane poprawnie i naciśnij klawisz Enter.

Aby uruchomić utworzony interfejs IPv6, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) podaj zdefiniowany wcześniej adres IPv6, a następnie naciśnij klawisz Enter.

Interfejs IPv6 został pomyślnie utworzony i uruchomiony.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Konfigurowanie TCP/IP, jeśli system znajduje się w stanie zastrzeżonym

Jeśli istnieje potrzeba skonfigurowania TCP/IP w momencie, gdy system operacyjny jest w stanie zastrzeżonym, należy wykonać czynności opisane w niniejszym temacie. Można użyć zarówno adresów IPv4, jak i IPv6 dla systemu.

Administrator sieci może napotkać sytuacje, w których użytkownikom nie można pozwolić na zmianę konfiguracji. Do tego wymagane jest przełączenie systemu operacyjnego w stan zastrzeżony. Aby skonfigurować TCP/IP w stanie zastrzeżonym, należy najpierw uruchomić TCP/IP przy użyciu specjalnych parametrów, a następnie uruchomić specyficzny interfejs IPv4 lub IPv6, aby umożliwić dostęp do systemu.

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

- Można uruchomić tylko te interfejsy, które nie są podłączone do opisu serwera sieci (NWSD), ani do opisu interfejsu sieci (NWID).
- Nie można uruchomić serwerów TCP/IP (komenda STRTCPSVR), ponieważ wymagają one aktywnych podsystemów.

Aby skonfigurować TCP/IP, podczas gdy system operacyjny znajduje się w stanie zastrzeżonym, wykonaj następujące czynności:

Uruchamianie TCP/IP z parametrami specjalnymi

Aby było możliwe konfigurowanie interfejsów IPv4 lub IPv6 w stanie zastrzeżonymi, należy podczas uruchamiania TCP/IP użyć parametrów specjalnych.

Aby uruchomić TCP/IP, gdy system znajduje się w stanie zastrzeżonym, wykonaj następujące czynności:

1. W wierszu komend wpisz STRTCP (komenda Uruchomienie TCP/IP - Start TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania TCP/IP.
2. Podaj *NO jako wartość parametrów Uruchomienie serwerów aplikacji (Start application servers), Uruchomienie interfejsów TCP/IP (Start TCP/IP interfaces) i Uruchomienie profili połączenia punkt z punktem (Start point-to-point profiles).
3. Podaj *YES jako wartość parametru Uruchomienie IPv6 (Start IPv6), dzięki czemu będzie możliwe konfigurowanie interfejsów IPv6 w stanie zastrzeżonym.
4. Naciśnij klawisz Enter, aby wprowadzić konfigurację.

Uwaga: Powyższe komendy powodują uruchomienie TCP/IP, ale bez uruchamiania serwerów aplikacji TCP/IP ani interfejsów IP.

Uruchamianie konkretnego interfejsu TCP/IP

Jeśli aplikacja korzystająca z gniazd wymaga konkretnego interfejsu IPv4 lub IPv6, należy ten interfejs uruchomić.

Po uruchomieniu TCP/IP w stanie zastrzeżonym można dokonać ręcznej konfiguracji interfejsów IPv4 i IPv6 lub w standardowy sposób przeprowadzić bezstanową autokonfigurację adresów IPv6. Można też skorzystać z istniejących interfejsów IPv4 lub IPv6, które zostały skonfigurowane wcześniej.

Aby uruchomić konkretny interfejs IPv4 lub IPv6, wykonaj następujące czynności:

1. Upewnij się, że uruchamiany interfejs albo określa wirtualny adres IP, albo korzysta z opisu linii *ELAN, *TRLAN lub *DDI.
   a. W wierszu komend wpisz komendę CFGTCP (Configure TCP/IP - Konfigurowanie TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Podaj opcję 1 (Praca z interfejsami TCP/IP - Work with TCP/IP interfaces) i naciśnij klawisz Enter.
   c. Sprawdź poprawność wartości w kolumnach Opis linii (Line Description) i Typ linii (Line Type):
      - Jeśli uruchamiany jest interfejs IPv4, upewnij się, że kolumna Opis linii (Line Description) zawiera wartość *VIRTUALIP lub kolumna Typ linii (Line Type) zawiera wartość *ELAN, *TRLAN lub *DDI.
      - Jeśli uruchamiany jest interfejs IPv6, upewnij się, że kolumna Opis linii (Line Description) zawiera wartość *VIRTUALIP lub kolumna Typ linii (Line Type) zawiera wartość *ELAN.
2. Upewnij się, że uruchamiany interfejs nie jest przyłączony do identyfikatora NWID ani opisu NWSD.
   a. W wierszu komend wpisz komendę DSPLIND (Display Line Description - Wyświetlenie opisu linii) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Wyświetlenie opisu linii (Display Line Description).
   b. W polu *Opis linii* (Line description) podaj nazwę linii interfejsu i naciśnij klawisz Enter.
   c. W menu Wyświetlenie opisu linii (Display Line Description) upewnij się, że wartość w kolumnie Nazwa zasobu (Resource name) nie jest równa *NWID ani *NWSD.

   Jeśli interfejs jest przyłączony do identyfikatora NWID lub opisu NWSD, zalecane jest wybranie innego interfejsu.
3. Uruchom interfejs.
   a. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
   b. W polu *Adres internetowy* (Internet address) wprowadź adres IPv4 lub IPv6 interfejsu, a następnie naciśnij klawisz Enter.

      Uwaga: Upewnij się, że w polu *Adres internetowy* (Internet address) nie jest podana wartość *AUTOSTART.

Zadania pokrewne

"Dodawanie interfejsów IPv4" na stronie 34
Do utworzenia interfejsów IPv4 w systemie, w tym interfejsów sieci lokalnej, interfejsów sieci rozległej oraz wirtualnych interfejsów IPv4 można użyć programu System i Navigator lub interfejsu znakowego.

"Dodawanie interfejsów IPv6" na stronie 37
Do utworzenia interfejsów IPv6 w systemie, w tym interfejsów sieci lokalnej oraz wirtualnych interfejsów IPv6 można użyć programu System i Navigator lub interfejsu znakowego.

"Konfigurowanie bezstanowego autokonfigurowania adresu IPv6" na stronie 27
Skorzystanie z funkcji bezstanowego autokonfigurowania adresu IPv6 umożliwia automatyczne skonfigurowanie obsługi protokołu IPv6.

Sprawdzanie działania interfejsu

Na koniec należy sprawdzić, czy uruchomiony interfejs jest aktywny.

Aby sprawdzić działanie interfejsu, należy wykonać komendę ping podając interfejs używanej aplikacji.

| Z poziomu stacji roboczej otwórz wiersz komend i wpisz komendę ping z adresem IP skonfigurowanego interfejsu.

W stanie zastrzeżonym działają tylko nieliczne narzędzia związane z protokołem TCP/IP. Dostępne są jednak narzędzia Ping i Netstat.

Informacje pokrewne

Ping

Netstat

Dostosowywanie TCP/IP

Za pośrednictwem programu System i Navigator i interfejsu znakowego można uzyskać dostęp do wielu opcji dostosowywania konfiguracji TCP/IP.

Po skonfigurowaniu TCP/IP można dostosowywać utworzoną konfigurację. W miarę rozrostu sieci może być konieczne modyfikowanie właściwości, dodawanie interfejsów lub dodawanie tras w systemie. Aby było możliwe korzystanie z aplikacji IPv6, należy w systemie skonfigurować obsługę protokołu IPv6. Ta sekcja stanowi punkt wyjścia do zarządzania konfiguracją TCP/IP. Do wykonania opisanych niezbędnych zadań można używać kreatorów programu System i Navigator lub interfejsu znakowego.

Zadania pokrewne

"Konfigurowanie TCP/IP po raz pierwszy" na stronie 21
Podczas konfigurowania nowego systemu należy nawiązać połączenie sieciowe i skonfigurować początkowo protokół TCP/IP z IPv4.

"Krok 7: uruchamianie TCP/IP" na stronie 25
Aby usługi TCP/IP były gotowe do użycia, należy uruchomić TCP/IP.

Zmiana ogólnych ustawień związanych z TCP/IP

Ogólne ustawienia związane z TCP/IP można wyświetlić i zmienić za pomocą programu System i Navigator lub interfejsu znakowego.

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.

Modyfikacja domeny TCP/IP

Możliwe jest modyfikowanie nazw domen i hostów lokalnych, dodawanie i usuwanie serwerów DNS, modyfikowanie priorytetu wyszukiwania nazwy hosta itd.

Do wyświetlania i modyfikowania danych domeny hosta można wykorzystać program System i Navigator lub interfejs znakowy.

Zmiana domeny TCP/IP za pomocą programu System i Navigator

Aby zmodyfikować dane domeny hosta za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** → **Sieć** → **Konfiguracja TCP/IP** (*system* > Network > TCP/IP Configuration).
2. Kliknij prawym przyciskiem myszy opcję **Konfiguracja TCP/IP** (TCP/IP Configuration) i wybierz **Właściwości** (Properties), aby otworzyć okno **Właściwości konfiguracyjne TCP/IP** (TCP/IP Configuration Properties).
3. Otwórz kartę **Informacje o domenie hosta** (Host Domain Information) i postępuj zgodnie z instrukcjami, aby dostosować dane domeny hosta.

Modyfikowanie domeny TCP/IP za pomocą interfejsu znakowego

Aby zmodyfikować dane domeny hosta za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 12 (Zmiana informacji domeny TCP/IP - Change TCP/IP domain information) i naciśnij klawisz Enter.
3. W menu Zmiana domeny TCP/IP (Change TCP/IP Domain) wprowadź niezbędne zmiany w nazwie hosta, nazwie domeny i serwerze DNS oraz określ odpowiednią listę wyszukiwania domeny i priorytet wyszukiwania nazw hostów.
4. Naciśnij klawisz Enter.

Zadania pokrewne

“Krok 5: definiowanie domeny TCP/IP” na stronie 23
Po określeniu pozycji routingu należy zdefiniować domenę lokalną i nazwy hostów, aby umożliwić komunikację w obrębie sieci, a następnie skorzystać z serwera DNS w celu powiązania adresów IP z nazwami hostów.

Dostosowywanie pozycji w tabeli hostów

Pozycje w tabeli hostów można dodawać, edytować i usuwać. Tabela hostów obsługuje zarówno adresy IPv4, jak i IPv6.

Do wyświetlania i dostosowywania wpisów w tabeli hostów można wykorzystać program System i Navigator lub interfejs znakowy.

Dostosowywanie pozycji w tabeli hostów za pomocą programu System i Navigator

Aby dostosować pozycje w tabeli hostów za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** → **Sieć** → **Konfiguracja TCP/IP** (*system* > Network > TCP/IP Configuration).
2. Kliknij prawym przyciskiem myszy pozycję **Konfiguracja TCP/IP** (TCP/IP Configuration) i wybierz **Tabela hostów** (Host Table), aby otworzyć okno Tabela hostów.

   W oknie Tabela hostów wyświetlane są nazwy hostów dla poszczególnych pozycji (zarówno dla adresów IPv4, jak i IPv6). Każda pozycja w tabeli hostów może zawierać do 65 nazw hostów.
3. W oknie Tabela hostów dodaj, zmień lub usuń wybrane pozycje tabeli hostów.

Dostosowywanie pozycji w tabeli hostów za pomocą interfejsu znakowego

Aby dostosować pozycje w tabeli hostów za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 10 (Praca z pozycjami tabeli hostów TCP/IP - Work with TCP/IP Host Table Entries) i naciśnij klawisz Enter.
3. Dostosuj zawartość tabeli hostów wykonując dowolne spośród następujących czynności:
   - Aby dodać pozycję do tabeli hostów, wpisz 1 (Dodaj - Add) w polu *Opcja* (Opt) w pierwszym wierszu, a następnie naciśnij klawisz Enter.
   - Aby zmienić nazwę hosta, wpisz 2 (Zmień - Change) obok wiersza, który chcesz zmienić, a następnie naciśnij klawisz Enter.
   - Aby usunąć pozycję z tabeli hostów, wpisz 4 (Usuń - Remove) obok wiersza, który chcesz usunąć, a następnie naciśnij klawisz Enter.
   - Aby zmienić nazwę pozycji w tabeli hostów, wpisz 7 (Zmień nazwę - Rename) obok wiersza, którego nazwę chcesz zmienić, a następnie naciśnij klawisz Enter.
4. Po wprowadzeniu wszystkich zmian naciśnij klawisz Enter.

Zadania pokrewne

“Krok 6: definiowanie tabeli hostów” na stronie 24
Może być potrzebna możliwość rozstrzygania adresów IP za pomocą nie tylko serwera DNS, lecz również tabeli hostów. Jeśli używany będzie wyłącznie serwer DNS, możesz ten krok zignorować.

Modyfikowanie właściwości IPv4

Program System i Navigator umożliwia przeglądanie i modyfikację ustawień IPv4.

Aby przeglądać i modyfikować właściwości IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Kliknij prawym przyciskiem myszy opcję **IPv4** i wybierz **Właściwości** (Properties), aby otworzyć okno Atrybuty TCP/IP (TCP/IP Attributes).
3. W górnej części okna otwórz jedną z następujących kart, aby zmienić dostępne właściwości:
   - Otwórz kartę **IPv4**, aby zmienić właściwości specyficzne dla protokołu IPv4.
   - Otwórz kartę **IPv6**, aby zmienić właściwości wspólne z protokołem IPv6.

Modyfikowanie właściwości IPv6

Program System i Navigator umożliwia przeglądanie i modyfikację ustawień IPv6.

Aby przeglądać i modyfikować właściwości IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Kliknij prawym przyciskiem myszy opcję **IPv6** i wybierz **Właściwości** (Properties), aby otworzyć okno Atrybuty TCP/IP (TCP/IP Attributes).
3. W górnej części okna otwórz jedną z następujących kart, aby zmienić dostępne właściwości:
   - Otwórz kartę **IPv6**, aby zmienić właściwości specyficzne dla protokołu IPv6.
   - Otwórz kartę **IPv4**, aby zmienić właściwości wspólne z protokołem IPv4.

Zmiana innych atrybutów TCP/IP

Możliwe jest wykonywanie dodatkowych czynności konfiguracyjnych dotyczących protokołu TCP/IP, takich jak zmiana dotyczących tego protokołu atrybutów protokołów UDP, ARP i innych.

Do przeprowadzenia dodatkowej konfiguracji TCP/IP można wykorzystać program System i Navigator lub interfejs znakowy.

Zmiana innych atrybutów TCP/IP za pomocą programu System i Navigator

Istnieją następujące sposoby uzyskania dostępu do stron atrybutów TCP/IP w programie System i Navigator:

- Aby uzyskać dostęp do okna Właściwości konfiguracyjne TCP/IP (TCP/IP Configuration Properties), wykonaj następujące czynności:
  1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP** (*system* > Network > TCP/IP Configuration).
  2. Kliknij prawym przyciskiem myszy opcję **Konfiguracja TCP/IP** (TCP/IP Configuration) i wybierz **Właściwości** (Properties), aby otworzyć okno **Właściwości konfiguracyjne TCP/IP** (TCP/IP Configuration Properties).
  3. Otwórz kartę **Jakość usługi** (Quality of Service), **Ograniczenia portów** (Port Restrictions), **Uruchamiane serwery** (Servers to Start) lub **SOCKS** i postępuj zgodnie z instrukcjami, aby zmodyfikować ustawienia.
- Aby uzyskać dostęp do okna Atrybuty TCP/IP (TCP/IP Attributes), wykonaj następujące czynności:
  1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv4 (or IPv6)** (*system* > Network > TCP/IP Configuration > IPv4/IPv6).

2. Kliknij prawym przyciskiem myszy opcję **IPv4 (lub IPv6)** i wybierz **Właściwości** (Properties), aby otworzyć okno Atrybuty TCP/IP (TCP/IP Attributes).
3. Otwórz kartę **Ogólne** (General) lub **Transporty** (Transports) i postępuj zgodnie z instrukcjami, aby dokonać zmiany ustawień.

Modyfikowanie innych atrybutów TCP/IP za pomocą interfejsu znakowego

Aby uzyskać dostęp do ekranu Zmiana atrybutów TCP/IP (Change TCP/IP Attributes) za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu uzyskania dostępu do menu Konfigurowanie TCP/IP (Configure TCP/IP).
2. Wybierz opcję 3 (Zmiana atrybutów TCP/IP - Change TCP/IP Attributes) i naciśnij klawisz Enter.
3. Zmień wybrane ustawienia i naciśnij klawisz Enter.

Dostosowywanie interfejsów IPv4

Może być konieczne dodanie interfejsów IPv4 do systemu bądź modyfikowanie, usuwanie, uruchamianie lub kończenie pracy istniejących interfejsów IPv4. Dostępne są szczegółowe instrukcje na temat wykonywania tych zadań.

Korzystając z programu System i Navigator lub interfejsu znakowego można dostosowywać interfejsy IPv4 poprzez wykonywanie dowolnych z poniższych zadań.

Dodawanie interfejsów IPv4

Do utworzenia interfejsów IPv4 w systemie, w tym interfejsów sieci lokalnej, interfejsów sieci rozległej oraz wirtualnych interfejsów IPv4 można użyć programu System i Navigator lub interfejsu znakowego.

Tworzenie interfejsu IPv4 za pomocą programu System i Navigator

Aby utworzyć interfejs IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Kliknij prawym przyciskiem myszy opcję **Interfejsy** (Interfaces) i wykonaj jedną z poniższych czynności:
   - Aby utworzyć interfejs sieci lokalnej, wybierz kolejno opcje **Nowy interfejs → Sieć LAN** (New Interface > Local Area Network).
   - Aby utworzyć interfejs sieci rozległej, wybierz kolejno opcje **Nowy interfejs → Sieć WAN** (New Interface > Wide Area Network).
   - Aby utworzyć interfejs wirtualny, wybierz kolejno opcje **Nowy interfejs → Wirtualny adres IP** (New Interface > Virtual IP).
3. Wykonaj czynności Kreatora nowego interfejsu IPv4, aby utworzyć interfejs IPv4. Po zakończeniu konfiguracji nowy interfejs zostanie wyświetlony w prawym panelu.

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

Tworzenie interfejsu IPv4 za pomocą interfejsu znakowego

Uwaga: Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby utworzyć normalny interfejs IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv4.

3. W polu *Opis linii* (Line description) podaj nazwę linii (można użyć dowolnej nazwy) i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Aby utworzyć wirtualny interfejs IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv4.
3. W polu *Opis linii* (Line description) wpisz *VIRTUALIP i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. W polu *Preferowane interfejsy* (Preferred interfaces) wykonaj jedną z następujących czynności:
   - Jeśli na tym etapie użytkownik nie chce podawać żadnych preferowanych interfejsów, należy pozostawić wartość domyślną *NONE.
   - Wpisz znak plusa (+) obok pola + *aby wyświetlić więcej wartości* (+ for more values) i naciśnij klawisz Enter. Następnie w menu Podaj więcej wartości dla parametru PREFIFC (Specify More Values for Parameter PREFIFC) podaj po kolei poprawne adresy IPv4, które odpowiadają preferowanym interfejsom IPv4, a następnie naciśnij klawisz Enter.

   Uwaga: Można podać maksymalnie 10 interfejsów IPv4 w kolejności preferencji. Każdy interfejs musi być normalnym interfejsem IPv4.
5. Upewnij się, że wszystkie pozostałe parametry opcjonalne zostały podane poprawnie i naciśnij klawisz Enter aby wprowadzić dane.

Zadania pokrewne

"Uruchamianie konkretnego interfejsu TCP/IP" na stronie 30
Jeśli aplikacja korzystająca z gniazd wymaga konkretnego interfejsu IPv4 lub IPv6, należy ten interfejs uruchomić.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Uruchamianie interfejsów IPv4

Można uruchomić interfejsy IPv4, które nie zostały uruchomione automatycznie przy utworzeniu lub które zostały wcześniej zakończone. Aby wykonać to zadanie można użyć programu System i Navigator lub interfejsu znakowego.

Uruchamianie interfejsu IPv4 za pomocą programu System i Navigator

Aby uruchomić interfejs IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv4 w prawym panelu.
3. Kliknij prawym przyciskiem myszy interfejs IPv4, który ma być uruchomiony i wybierz opcję **Uruchom** (Start).

   Jeśli status interfejsu zmieni się na Aktywny, interfejs IPv4 został pomyślnie uruchomiony.

Uruchamianie interfejsu IPv4 za pomocą interfejsu znakowego

Aby uruchomić interfejs IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wykonaj jedną z następujących czynności:
   - Aby uruchomić pojedynczy interfejs IPv4, podaj poprawny adres IPv4 i naciśnij klawisz Enter.
   - Aby wszystkie interfejsy mogły być uruchamiane automatycznie przy ich tworzeniu lub zmianie, wpisz *AUTOSTART i naciśnij klawisz Enter.

Modyfikowanie interfejsów IPv4

Właściwości istniejących interfejsów IPv4 można modyfikować za pomocą programu System i Navigator lub interfejsu znakowego.

Modyfikowanie interfejsu IPv4 za pomocą programu System i Navigator

Aby zmodyfikować istniejący interfejs IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv4 w prawym panelu.
3. Kliknij prawym przyciskiem myszy interfejs IPv4, który chcesz zmodyfikować i wybierz opcję **Właściwości** (Properties).
4. W oknie właściwości IPv4 podaj wartości właściwości, które chcesz zmienić.

   Niektóre właściwości interfejsu IPv4 można zmieniać, gdy ma on status aktywny.

Modyfikowanie interfejsu IPv4 za pomocą interfejsu znakowego

Uwaga: Aby użyć komendy CHGTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby zmodyfikować istniejący interfejs IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CHGTCPIFC (Change TCP/IP Interface - Zmiana interfejsu TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana interfejsu TCP/IP (Change TCP/IP Interface).
2. W polu *Adres internetowy* (Internet address) określ adres IPv4 interfejsu, który chcesz zmodyfikować, a następnie naciśnij klawisz Enter, aby zobaczyć listę parametrów opcjonalnych.
3. Wprowadź odpowiednie wartości wszelkich parametrów opcjonalnych, które chcesz zmienić, a dla parametrów, które mają pozostać bez zmian zachowaj domyślną wartość *SAME.
4. Upewnij się, że wszystkie parametry zostały podane poprawnie, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Kończenie pracy interfejsów IPv4

Może zaistnieć potrzeba zakończenia pracy skonfigurowanych wcześniej interfejsów IPv4. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Kończenie pracy interfejsu IPv4 za pomocą programu System i Navigator

Aby zakończyć pracę istniejącego interfejsu IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv4 w prawym panelu.
3. Kliknij prawym przyciskiem myszy interfejs IPv4, którego pracę chcesz zakończyć i wybierz opcję **Zatrzymaj** (Stop).

   Zmiana statusu interfejsu na Nieaktywne (Inactive) sygnalizuje pomyślne zakończenie pracy wybranego interfejsu IPv4.

Kończenie pracy interfejsu IPv4 za pomocą interfejsu znakowego

Aby zakończyć pracę istniejącego interfejsu IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ENDTCPIFC (End TCP/IP Interface - Zakończ pracę interfejsu TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zakończenie pracy interfejsu TCP/IP (End TCP/IP Interface).
2. W polu *Adres internetowy* (Internet address) podaj adres IPv4 interfejsu, którego pracę chcesz zakończyć, a następnie naciśnij klawisz Enter.

Usuwanie interfejsów IPv4

Może być konieczne usunięcie interfejsów IPv4, które zostały skonfigurowane. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Wymagania wstępne:

Należy zakończyć interfejs IPv4, zanim może on zostać usunięty. Oznacza to, że status interfejsu IPv4, który ma być usuwany, musi być nieaktywny. Więcej informacji na temat sposobu zakończenia interfejsu IPv4 znajduje się w sekcji “Kończenie pracy interfejsów IPv4” na stronie 36.

Usuwanie interfejsu IPv4 za pomocą programu System i Navigator

Aby usunąć istniejący interfejs IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv4 w prawym panelu.
3. Kliknij prawym przyciskiem myszy interfejs IPv4, który ma być usunięty i wybierz opcję **Usuń** (Delete).
4. W oknie potwierdzenia usunięcia kliknij **Yes** (Tak).

Usuwanie interfejsu IPv4 za pomocą interfejsu znakowego

Uwaga: Aby uruchomić komendę RMVTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby usunąć istniejący interfejs IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę RMVTCPIFC (Usuń interfejs TCP/IP - Remove TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu usuwania interfejsu TCP/IP.
2. W polu *Internet address* (Internet address) podaj adres IPv4 interfejsu, który ma zostać usunięty, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Dostosowywanie interfejsów IPv6

Może być konieczne dodanie interfejsów IPv6 do systemu bądź modyfikowanie, usuwanie, uruchamianie lub kończenie pracy istniejących interfejsów IPv6. Dostępne są szczegółowe instrukcje na temat wykonywania tych zadań.

Do dostosowywania interfejsów IPv6 można używać programu System i Navigator lub interfejsu znakowego.

Dodawanie interfejsów IPv6

Do utworzenia interfejsów IPv6 w systemie, w tym interfejsów sieci lokalnej oraz wirtualnych interfejsów IPv6 można użyć programu System i Navigator lub interfejsu znakowego.

Tworzenie interfejsu IPv6 za pomocą programu System i Navigator

Aby za pomocą programu System i Navigator utworzyć nowy interfejs IPv6, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).

2. Kliknij prawym przyciskiem myszy opcję **Interfejsy** (Interfaces) i wykonaj jedną z poniższych czynności:
   - Aby utworzyć interfejs sieci lokalnej, wybierz kolejno opcje **Nowy interfejs → Sieć LAN** (New Interface > Local Area Network).
   - Aby utworzyć interfejs wirtualny, wybierz kolejno opcje **Nowy interfejs → Wirtualny adres IP** (New Interface > Virtual IP).
3. Aby utworzyć nowy interfejs IPv6, postępuj zgodnie z instrukcjami zawartymi w kreatorze nowego interfejsu IPv6. Po zakończeniu konfiguracji nowy interfejs zostanie wyświetlony w prawym panelu.

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

Tworzenie interfejsu IPv6 za pomocą interfejsu znakowego

Uwaga: Aby uruchomić komendę ADDTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby utworzyć zwykły interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:
1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv6.
3. W polu *Opis linii* (Line description) podaj nazwę linii (można użyć dowolnej nazwy) i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Aby utworzyć wirtualny interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:
1. W wierszu komend wpisz komendę ADDTCPIFC (Dodaj interfejs TCP/IP -Add TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wpisz poprawny adres IPv6.
3. W polu *Opis linii* (Line description) wpisz *VIRTUALIP i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. W polu *Preferowane opisy linii* (Preferred line descriptions) wykonaj jedną z następujących czynności:
   - Jeśli na tym etapie użytkownik nie chce podawać żadnych preferowanych opisów linii, należy pozostawić wartość domyślną *NONE.
   - Wpisz znak plusa (+) obok pola + *aby wyświetlić więcej wartości* (+ for more values) i naciśnij klawisz Enter. Następnie w menu Podaj więcej wartości dla parametru PREFLIND (Specify More Values for Parameter PREFLIND) podaj po kolei opisy linii (można użyć dowolnych nazw), a następnie naciśnij klawisz Enter.

   Uwaga: Można wprowadzić maksymalnie 10 opisów linii w preferowanej kolejności użycia. Każdy opis linii musi być używany przez co najmniej jeden interfejs IPv6.
5. Upewnij się, że wszystkie pozostałe parametry opcjonalne zostały podane poprawnie i naciśnij klawisz Enter.

Zadania pokrewne

“Uruchamianie konkretnego interfejsu TCP/IP” na stronie 30
Jeśli aplikacja korzystająca z gniazd wymaga konkretnego interfejsu IPv4 lub IPv6, należy ten interfejs uruchomić.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Uruchamianie interfejsów IPv6

Można uruchomić interfejsy IPv6, które nie zostały uruchomione automatycznie przy utworzeniu lub które zostały wcześniej zakończone. Aby wykonać to zadanie można użyć programu System i Navigator lub interfejsu znakowego.

Uruchamianie interfejsu IPv6 za pomocą programu System i Navigator

Aby uruchomić interfejs IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv6 w prawym panelu.
3. Aby uruchomić interfejs, wykonaj jedną z następujących czynności:
   - W przypadku normalnych interfejsów IPv6, kliknij prawym przyciskiem myszy interfejs, który ma zostać uruchomiony i wybierz opcję **Uruchom** (Start).
   - W przypadku interfejsów utworzonych za pomocą bezstanowej autokonfiguracji adresu IPv6, kliknij prawym przyciskiem myszy interfejs, który ma zostać uruchomiony, a następnie wybierz opcję **Uruchom bezstanową autokonfigurację adresu** (Start stateless address autoconfiguration).

   Jeśli status interfejsu zmieni się na Aktywny, interfejs IPv6 został pomyślnie uruchomiony.

Uruchamianie interfejsu IPv6 za pomocą interfejsu znakowego

Aby uruchomić interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę STRTCPIFC (komenda Uruchomienie interfejsu TCP/IP - Start TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu uruchamiania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wykonaj jedną z następujących czynności:
   - Aby uruchomić normalny interfejs IPv6, podaj poprawny adres IPv6 i naciśnij klawisz Enter.
   - Aby uruchomić interfejs utworzony przy użyciu bezstanowej autokonfiguracji adresu IPv6, wykonaj następujące czynności:
     a. Wpisz *IP6SAC i naciśnij klawisz Enter.
     b. W polu *Opis linii* (Line description) podaj nazwę linii do bezstanowej autokonfiguracji adresu IPv6 i naciśnij klawisz Enter.
   - Aby wszystkie interfejsy mogły być uruchamiane automatycznie przy ich tworzeniu lub zmianie, wpisz *AUTOSTART i naciśnij klawisz Enter.

Modyfikowanie interfejsów IPv6

Właściwości istniejących interfejsów IPv6 można modyfikować za pomocą programu System i Navigator lub interfejsu znakowego.

Modyfikowanie interfejsu IPv6 za pomocą programu System i Navigator

Aby zmodyfikować istniejący interfejs IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Kliknij opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv6.
3. Kliknij prawym przyciskiem myszy interfejs IPv6, który chcesz zmodyfikować i wybierz opcję **Właściwości** (Properties), aby wyświetlić okno Właściwości interfejsu IPv6 (IPv6 Interface Properties).
4. W oknie Właściwości interfejsu IPv6 (IPv6 Interface Properties) podaj wartości właściwości, które chcesz zmienić.

   Uwagi:
   - Niektóre właściwości interfejsu IPv6 można zmieniać, gdy ma on status aktywny.
   - Jeśli modyfikowany jest wirtualny interfejs IPv6, istnieje możliwość zmiany preferowanych opisów linii na karcie **Opcje** (Options).

Modyfikowanie interfejsu IPv6 za pomocą interfejsu znakowego

Uwaga: Aby użyć komendy CHGTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby zmodyfikować istniejący interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CHGTCPIFC (Change TCP/IP Interface - Zmiana interfejsu TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana interfejsu TCP/IP (Change TCP/IP Interface).
2. W polu *Adres internetowy* (Internet address) wykonaj jedną z następujących czynności:
   - Aby zmodyfikować zwykły interfejs IPv6, podaj adres IPv6 interfejsu, który chcesz zmienić.
   - Aby zmodyfikować interfejs utworzony z wykorzystaniem bezstanowej autokonfiguracji adresów IPv6, wpisz *IP6SAC.
3. W polu *Opis linii* (Line description) podaj nazwę linii interfejsu, a następnie naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
4. Wprowadź odpowiednie wartości wszelkich parametrów opcjonalnych, które chcesz zmienić, a dla parametrów, które mają pozostać bez zmian zachowaj domyślną wartość *SAME.
5. Upewnij się, że wszystkie parametry zostały podane poprawnie, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Kończenie pracy interfejsów IPv6

Może zaistnieć potrzeba zakończenia pracy skonfigurowanych wcześniej interfejsów IPv6. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Kończenie pracy interfejsu IPv6 za pomocą programu System i Navigator

Aby zakończyć pracę istniejącego interfejsu IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv6 w prawym panelu.
3. Wykonaj jedną z poniższych czynności, aby zakończyć pracę interfejsu:
   - W przypadku zwykłych interfejsów IPv6, kliknij prawym przyciskiem myszy interfejs, którego pracę chcesz zakończyć i wybierz opcję **Zatrzymaj** (Stop).
   - W przypadku interfejsów utworzonych przez mechanizm bezstanowej autokonfiguracji adresów IPv6, kliknij prawym przyciskiem myszy interfejs, którego pracę chcesz zakończyć i wybierz opcję **Zatrzymaj bezstanową autokonfigurację adresów** (Stop stateless address autoconfiguration).

Kończenie pracy interfejsu IPv6 za pomocą interfejsu znakowego

Aby zakończyć pracę istniejącego interfejsu IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ENDTCPIFC (End TCP/IP Interface - Zakończ pracę interfejsu TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zakończenie pracy interfejsu TCP/IP (End TCP/IP Interface).
2. W polu *Adres internetowy* (Internet address) wykonaj jedną z następujących czynności:
   - Aby zakończyć pracę zwykłego interfejsu IPv6, wprowadź adres IPv6 interfejsu, którego pracę chcesz zakończyć, a następnie naciśnij klawisz Enter.
   - Aby zakończyć pracę interfejsu utworzonego z wykorzystaniem bezstanowej autokonfiguracji adresów IPv6, wpisz *IP6SAC, podaj nazwę linii interfejsu w polu *Opis linii* (Line description) i naciśnij klawisz Enter.

Usuwanie interfejsów IPv6

Może być konieczne usunięcie interfejsów IPv6, które zostały skonfigurowane. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Wymagania wstępne:

Należy zakończyć interfejs IPv6, zanim może on zostać usunięty. Oznacza to, że status interfejsu IPv6, który ma być usuwany, musi być nieaktywny. Więcej informacji na temat sposobu zakończenia interfejsu IPv6 znajduje się w sekcji “Kończenie pracy interfejsów IPv6” na stronie 40.

Usuwanie interfejsu IPv6 za pomocą programu System i Navigator

Aby usunąć istniejący interfejs IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić listę interfejsów IPv6 w prawym panelu.
3. Aby usunąć interfejs, wykonaj jedną z następujących czynności:
   - W przypadku normalnych interfejsów IPv6, kliknij prawym przyciskiem myszy interfejs, który ma zostać usunięty i wybierz opcję **Usuń** (Delete).
   - W przypadku interfejsów utworzonych za pomocą bezstanowej autokonfiguracji adresu IPv6, kliknij prawym przyciskiem myszy interfejs, który ma zostać zakończony, a następnie wybierz opcję **Usuń bezstanową autokonfigurację adresu** (Remove stateless address autoconfiguration).
4. W oknie potwierdzenia usunięcia kliknij **Yes** (Tak).

Usuwanie interfejsu IPv6 za pomocą interfejsu znakowego

Uwaga: Aby uruchomić komendę RMVTCPIFC, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby usunąć istniejący interfejs IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę RMVTCPIFC (Usuń interfejs TCP/IP - Remove TCP/IP Interface) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu usuwania interfejsu TCP/IP.
2. W polu *Adres internetowy* (Internet address) wykonaj jedną z następujących czynności:
   - Aby usunąć normalny interfejs IPv6, podaj adres IPv6 interfejsu, który ma zostać usunięty, a następnie naciśnij klawisz Enter.
   - Aby usunąć interfejs utworzony za pomocą bezstanowej autokonfiguracji adresu IPv6, wpisz komendę *IP6SAC i podaj nazwę linii interfejsu w oknie *Opis linii* (Line description), a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Dostosowywanie tras IPv4

Może być konieczne dodanie tras IPv4 do systemu bądź modyfikowanie lub usuwanie istniejących tras IPv4. Dostępne są szczegółowe instrukcje na temat wykonywania tych zadań.

Do dostosowywania tras IPv4 można używać programu System i Navigator lub interfejsu znakowego.

Dodawanie tras IPv4

Nowe trasy IPv4 dla systemu można utworzyć za pomocą kreatora w programie System i Navigator lub interfejsu znakowego.

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

Tworzenie nowej trasy IPv4 za pomocą programu System i Navigator

Aby utworzyć nową trasę IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Kliknij prawym przyciskiem myszy **Trasy** i wybierz **Nowa trasa**.
3. Wykonaj czynności Kreatora nowej trasy IPv4, aby skonfigurować nową trasę IPv4.

Tworzenie nowej trasy IPv4 za pomocą interfejsu znakowego

Aby utworzyć nową trasę IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ADDTCPRTE (Dodaj trasę TCP/IP - Add TCP/IP Route) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania trasy TCP/IP.

   Uwaga: Aby uruchomić komendę ADDTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.
2. W polu *Cel trasy* (Route destination) wykonaj jedną z następujących czynności:
   - Aby utworzyć domyślną trasę IPv4, wpisz *DFTROUTE i naciśnij klawisz Enter.

     Uwaga: Aby skonfigurować domyślną trasę IPv4, należy podać wartość *NONE parametru Maska podsieci.
   - Aby utworzyć normalną trasę IPv4, podaj adres IPv4 celu trasy i naciśnij klawisz Enter.

   Zostanie wyświetlona lista parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv4 bramy na trasie.
4. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Modyfikowanie tras IPv4

Właściwości istniejących tras IPv4 można modyfikować za pomocą programu System i Navigator lub interfejsu znakowego.

Modyfikowanie trasy IPv4 za pomocą programu System i Navigator

Aby zmienić właściwości istniejącej trasy IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Trasy** (Routes), aby wyświetlić listę tras IPv4.
3. Kliknij prawym przyciskiem myszy trasę IPv4, którą chcesz zmodyfikować i wybierz opcję **Właściwości** (Properties).
4. W oknie trasy IPv4 podaj wartości właściwości trasy IPv4, które chcesz zmienić.

Modyfikowanie trasy IPv4 za pomocą interfejsu znakowego

Aby zmienić właściwości istniejącej trasy IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CHGTCPRTE (Change TCP/IP Route - Zmiana trasy TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana trasy TCP/IP (Change TCP/IP Route).

   Uwaga: Aby użyć komendy CHGTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.
2. W polu *Cel trasy* (Route destination) wykonaj jedną z następujących czynności:
   - Aby zmienić domyślną trasę IPv4, wpisz *DFTROUTE i naciśnij klawisz Enter.

     Uwaga: Aby skonfigurować domyślną trasę IPv4, należy podać wartość *NONE parametru Maska podsieci.
   - Aby zmienić zwykłą trasę IPv4, podaj adres IPv4 celu trasy, który chcesz zmienić, a następnie naciśnij klawisz Enter.

   Zostanie wyświetlona lista parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv4 bramy na trasie.
4. Wprowadź odpowiednie wartości wszelkich innych parametrów opcjonalnych, które chcesz zmienić, a dla parametrów, które mają pozostać bez zmian, zachowaj domyślną wartość *SAME.
5. Upewnij się, że wszystkie parametry zostały podane poprawnie, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Usuwanie tras IPv4

Może być konieczne usunięcie tras IPv4, które zostały skonfigurowane. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Usuwanie trasy IPv4 za pomocą programu System i Navigator

Aby usunąć istniejącą trasę IPv4 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Trasy** (Routes), aby wyświetlić listę tras IPv4.
3. Kliknij prawym przyciskiem myszy trasę IPv4, która ma być usunięta i wybierz opcję **Usuń** (Delete).
4. W oknie potwierdzenia usunięcia kliknij Yes (Tak).

Usuwanie trasy IPv4 za pomocą interfejsu znakowego

Aby usunąć istniejącą trasę IPv4 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę RMVTCPRTE (Usuń trasę TCP/IP - Remove TCP/IP Route) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu usuwania trasy TCP/IP.

   Uwaga: Aby uruchomić komendę RMVTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.
2. W polu *Cel trasy* (Route destination) wykonaj jedną z następujących czynności:
   - Aby usunąć domyślną trasę IPv4, wpisz *DFTROUTE i naciśnij klawisz Enter.
   - Aby usunąć normalną trasę IPv4, podaj adres IPv4 celu trasy i naciśnij klawisz Enter.

   Zostanie wyświetlona lista parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv4 bramy na trasie.
4. Podaj dowolne inne parametry opcjonalne, które pomogą zidentyfikować trasę IPv4, która ma zostać usunięta, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Dostosowywanie tras IPv6

Może być konieczne dodanie tras IPv6 do systemu bądź modyfikowanie lub usuwanie istniejących tras IPv6. Dostępne są szczegółowe instrukcje na temat wykonywania tych zadań.

Korzystając z programu System i Navigator lub interfejsu znakowego można dostosowywać trasy IPv6 poprzez wykonywanie dowolnych z poniższych zadań.

Dodawanie tras IPv6

Trasy IPv6 dla systemu można utworzyć za pomocą kreatora w programie System i Navigator lub interfejsu znakowego. Można skonfigurować tylko jedną domyślną trasę IPv6.

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

Tworzenie trasy IPv6 za pomocą programu System i Navigator

Aby utworzyć trasę IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje **Sieć → Konfiguracja TCP/IP → IPv6** (Network > TCP/IP Configuration > IPv6).
2. Kliknij prawym przyciskiem myszy **Trasy** i wybierz **Nowa trasa**.

3. Aby utworzyć trasę IPv6, postępuj zgodnie z instrukcjami zawartymi w kreatorze nowej trasy IPv6.

Tworzenie trasy IPv6 za pomocą interfejsu znakowego

Uwaga: Aby uruchomić komendę ADDTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Aby utworzyć trasę IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ADDTCPRTE (Dodaj trasę TCP/IP - Add TCP/IP Route) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania trasy TCP/IP.
2. W polu *Cel trasy* (Route destination) podaj adres IPv6 celu trasy i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv6 bramy na trasie.
4. W polu *Opis linii skonsolidowanej* (Binding line description) podaj nazwę linii, z którą skonsolidowana będzie ta trasa.
5. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Aby utworzyć nową trasę domyślną IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę ADDTCPRTE (Dodaj trasę TCP/IP - Add TCP/IP Route) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu dodawania trasy TCP/IP.
2. W polu *Cel trasy* (Route destination) wpisz *DFT6ROUTE i naciśnij klawisz Enter, aby wyświetlić listę parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv6 bramy na trasie.
4. W polu *Długość przedrostka adresu* (Address prefix length) wpisz *DFT6ROUTE (to odpowiada wartości 0).
5. W polu *Opis linii skonsolidowanej* (Binding line description) podaj nazwę linii, z którą skonsolidowana będzie ta trasa.
6. Podaj dowolne inne parametry opcjonalne i naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Modyfikowanie tras IPv6

Właściwości istniejących tras IPv6 można modyfikować za pomocą programu System i Navigator lub interfejsu znakowego.

Modyfikowanie trasy IPv6 za pomocą programu System i Navigator

Aby zmienić właściwości istniejącej trasy IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Wybierz opcję **Trasy** (Routes), aby wyświetlić listę tras IPv6.
3. Kliknij prawym przyciskiem myszy trasę IPv6, którą chcesz zmodyfikować i wybierz opcję **Właściwości** (Properties).
4. W oknie Właściwości trasy IPv6 (IPv6 Route Properties) podaj odpowiednie wartości właściwości trasy IPv6.

Modyfikowanie trasy IPv6 za pomocą interfejsu znakowego

Aby zmienić właściwości istniejącej trasy IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CHGTCPRTE (Change TCP/IP Route - Zmiana trasy TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana trasy TCP/IP (Change TCP/IP route).

   Uwaga: Aby użyć komendy CHGTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

2. W polu *Cel trasy* (Route destination) wykonaj jedną z następujących czynności:
   - Aby zmienić domyślną trasę IPv6, wpisz *DFT6ROUTE i naciśnij klawisz Enter.

     Uwaga: Aby skonfigurować domyślną trasę IPv4, należy podać wartość *NONE parametru Maska podsieci.
   - Aby zmienić zwykłą trasę IPv6, podaj adres IPv6 celu trasy, który chcesz zmienić, a następnie naciśnij klawisz Enter.

   Zostanie wyświetlona lista parametrów opcjonalnych.
3. Wprowadź odpowiednie wartości wszelkich parametrów opcjonalnych, które chcesz zmienić, a dla parametrów, które mają pozostać bez zmian zachowaj domyślną wartość *SAME.
4. Upewnij się, że wszystkie parametry zostały podane poprawnie, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Usuwanie tras IPv6

Może być konieczne usunięcie tras IPv6, które zostały skonfigurowane. Do wykonania tej czynności można wykorzystać program System i Navigator lub interfejs znakowy.

Usuwanie trasy IPv6 za pomocą programu System i Navigator

Aby usunąć istniejącą trasę IPv6 za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system* → Sieć → Konfiguracja TCP/IP → IPv6** (*system* > Network > TCP/IP Configuration > IPv6).
2. Wybierz opcję **Trasy** (Routes), aby wyświetlić listę tras IPv6.
3. Kliknij prawym przyciskiem myszy trasę IPv6, która ma być usunięta i wybierz opcję **Usuń** (Delete).
4. W oknie potwierdzenia usunięcia kliknij Yes (Tak).

Usuwanie trasy IPv6 za pomocą interfejsu znakowego

Aby usunąć istniejącą trasę IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę RMVTCPRTE (Usuń trasę TCP/IP - Remove TCP/IP Route) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu usuwania trasy TCP/IP.

   Uwaga: Aby uruchomić komendę RMVTCPRTE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.
2. W polu *Cel trasy* (Route destination) wykonaj jedną z następujących czynności:
   - Aby usunąć domyślną trasę IPv6, wpisz *DFT6ROUTE i naciśnij klawisz Enter.
   - Aby usunąć normalną trasę IPv6, podaj adres IPv6 celu trasy i naciśnij klawisz Enter.

   Zostanie wyświetlona lista parametrów opcjonalnych.
3. W polu *Następny przeskok* (Next hop) podaj adres IPv6 bramy na trasie.
4. W polu *Opis linii skonsolidowanej* (Binding line description) podaj nazwę linii, z którą skonsolidowana jest ta trasa.
5. Podaj dowolne inne parametry opcjonalne, które pomogą zidentyfikować trasę IPv6, która ma zostać usunięta, a następnie naciśnij klawisz Enter.

Informacje pokrewne

Uprawnienia specjalne *IOSYSCFG

Kończenie połączeń TCP/IP

W niektórych sytuacjach może być konieczne zakończenie połączenia TCP/IP. W tej sekcji przedstawiono procedury umożliwiające zakończenie połączenia TCP IPv4 lub IPv6.

Aby zakończyć połączenie TCP IPv4 lub IPv6 za pomocą interfejsu znakowego, wykonaj następujące czynności:

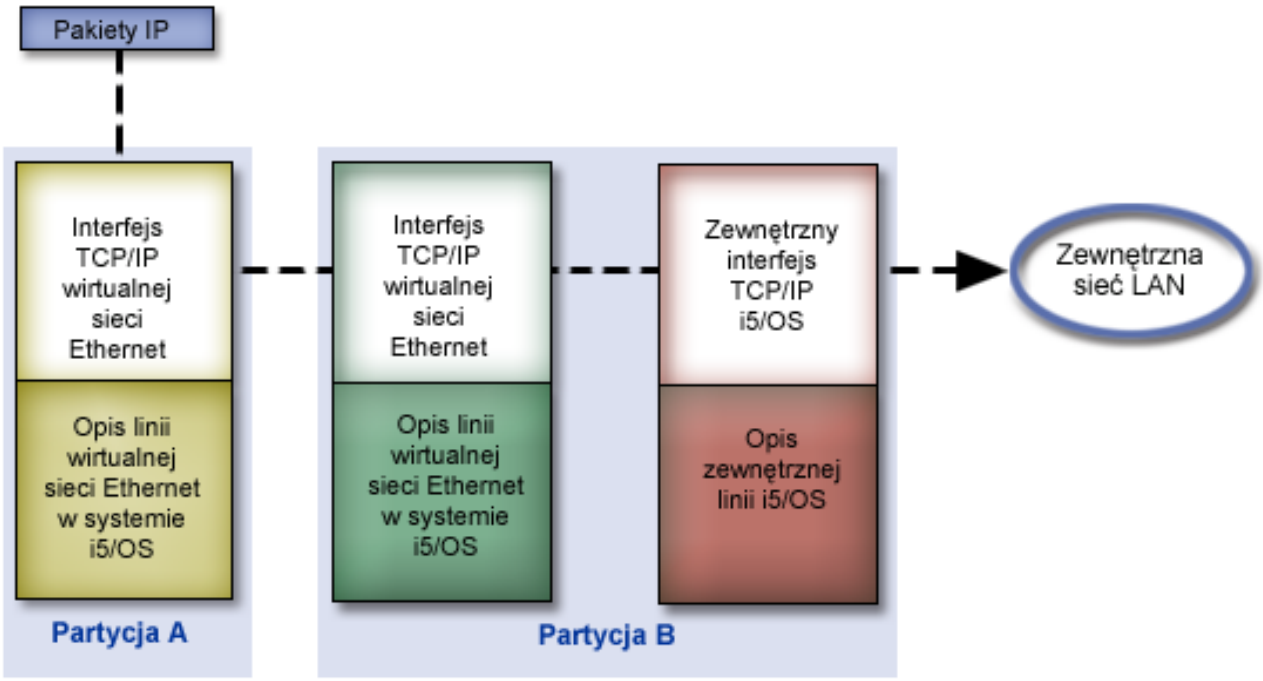
1. W wierszu komend wpisz komendę ENDTCPCNN (End TCP/IP Connection - Zakończenie połączenia TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zakończenie połączenia TCP/IP (End TCP/IP Connection).
2. W polu *Protokół* (Protocol) wpisz *TCP.
3. W polach *Lokalny adres internetowy* (Local internet address) i *Lokalny port* (Local port) wpisz odpowiednio poprawny adres IPv4 lub IPv6 i numer portu lokalnego hosta internetowego, a następnie naciśnij klawisz Enter.
4. W polach *Zdalny adres internetowy* (Remote internet address) i *Zdalny port* (Remote port) wpisz odpowiednio poprawny adres IPv4 lub IPv6 i numer portu zdalnego hosta internetowego, a następnie naciśnij klawisz Enter.

Połączenie TCP/IP zostało zakończone.

Łączenie wirtualnej sieci Ethernet z zewnętrznymi sieciami LAN za pomocą technik TCP/IP

Do połączenia wirtualnej sieci Ethernet z zewnętrzną siecią LAN można użyć różnych technik TCP/IP. Wirtualna sieć Ethernet może być używana jako rozwiązanie alternatywne dla karty sieciowej w komunikacji między partycjami.

Jeżeli do interpretacji zmian używana jest wirtualna sieć Ethernet, należy włączyć partycje w celu umożliwienia komunikacji z zewnętrzną fizyczną siecią LAN. Należy umożliwić ruch TCP/IP między wirtualną siecią Ethernet a zewnętrzną siecią LAN. Poniższy rysunek przedstawia przepływ logiczny pakietów IP.



Ruch IP zainicjowany w partycji A odbywa się wewnątrz wirtualnej sieci Ethernet od interfejsu na partycji A do interfejsu na partycji B. Po zaimplementowaniu technik TCP/IP używanych do łączenia wirtualnej sieci Ethernet z zewnętrznymi sieciami LAN 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 proxy ARP
- 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.

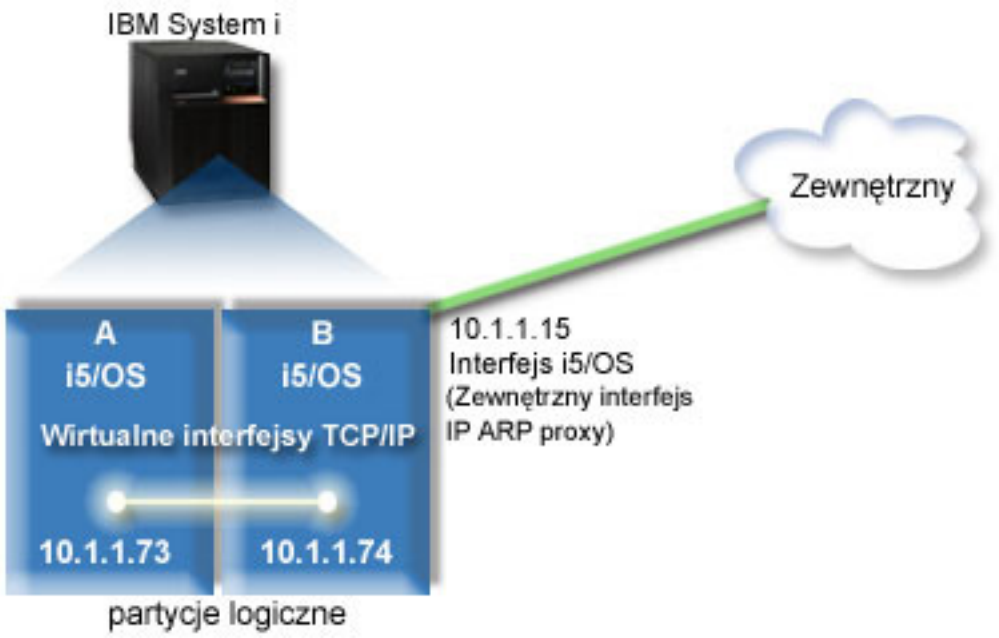
Funkcja ARP proxy jest wbudowana w stos TCP/IP. Wykorzystanie tej metody jest sugerowane, jeśli użytkownik ma odpowiednie adresy IP.

Uwaga: IPv6 nie jest obsługiwane przez metodę ARP.

Więcej informacji o przezroczystych podsieciach znajduje się w dokumentacji technicznej

- Podręcznik IBM i5/OS IP Networks: Dynamic
  Ta dokumentacja techniczna IBM (Redbook) informuje, jak zaprojektować sieć IP, która będzie samokonfigurująca się, odporna na błędy, bezpieczna i wydajna przy działaniu w systemie i5/OS.
- TCP/IP routing and workload balancing
  Ta kolekcja tematów 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: włączanie wirtualnej sieci Ethernet

Aby powiązać wirtualny interfejs z interfejsem zewnętrznym, należy najpierw włączyć partycje logiczne, które mają stanowić część wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890. W przypadku konfigurowania wirtualnej sieci
| Ethernet w modelach innych niż 8*xx* należy zapoznać się z instrukcjami w sekcji Wirtualna sieć Ethernet dla partycji
| logicznych systemu i5/OS Centrum informacyjnego IBM - sprzęt.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycji A) wpisz STRSST (komendę Uruchomienie narzędzi serwisowych - Start Service Tools) i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.
3. W oknie Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi - Work with System Partitions).
4. W oknie Praca z partycjami systemu (Work with System Partitions) wybierz opcję 3 (Praca z konfiguracją partycji - Work with Partition Configuration).
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 systemu możliwe są dwa sposoby wykonania tego kroku. Wybierz procedurę odpowiednią dla danego modelu.

Tworzenie opisów linii Ethernet w modelach 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach 8*xx*, dzięki czemu system będzie mógł
| korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie Praca z zasobami komunikacyjnymi (Work with Communication Resources) wybierz opcję 5 (Praca z opisami konfiguracji - Work with configuration descriptions) obok odpowiedniego portu wirtualnej sieci Ethernet, a następnie naciśnij klawisz Enter.
5. W oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

Tworzenie opisów linii Ethernet w modelach innych niż 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach innych niż 8*xx*, dzięki czemu system będzie
| mógł korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 515, 520, 525, 550, 570, 595 itp.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie 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 oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

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 wpisz komendę CHGTCPA (Change TCP/IP Attributes - Zmiana atrybutów TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana atrybutów TCP/IP (Change TCP/IP Attributes).
2. W polu *Przesyłanie datagramów IP* (IP datagram forwarding) wpisz *YES i naciśnij klawisz Enter.

Krok 4: tworzenie interfejsu w celu aktywowania ARP proxy

Aktywowanie ARP proxy wymaga utworzenia zewnętrznego interfejsu.

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 blok 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 (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu wyświetlenia okna 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 okna Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
   d. W polu *Adres internetowy* (Internet address) wpisz 10.1.1.15.
   e. W polu *Opis linii* (Line description) wpisz nazwę opisu linii, na przykład ETHLINE.
   f. W polu *Maska podsieci* (Subnet mask) wpisz 255.255.255.0.
3. Uruchom interfejs. W oknie Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.

Krok 5: tworzenie wirtualnych interfejsów TCP/IP

Wirtualne interfejsu TCP/IP należy zdefiniować zarówno na partycji A, jak i partycji B.

Aby utworzyć interfejs wirtualny na partycji A, wykonaj następujące czynności:

1. W wierszu komend partycji A wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu wyświetlenia okna 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 okna Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
4. W polu *Adres internetowy* (Internet address) wpisz 10.1.1.73.
5. W polu *Opis linii* wpisz nazwę opisu linii, na przykład ETHLINE.
6. W polu *Maska podsieci* (Subnet mask) wpisz 255.255.255.252.
7. W oknie Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wpisz obok interfejsu opcję 9 (Uruchom - Start), aby ten interfejs uruchomić.

Aby utworzyć interfejs wirtualny na partycji B, powtórz powyższe kroki w wierszu komend na partycji B. W kroku 4 wpisz w polu *Adres internetowy* (Internet address) wartość 10.1.1.74.

Krok 6: tworzenie listy preferowanych interfejsów

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

Tworzenie listy preferowanych interfejsów za pomocą programu System i Navigator

Aby utworzyć listę preferowanych interfejsów za pomocą programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń kolejno opcje ***system*** **→ Sieć → Konfiguracja TCP/IP → IPv4** (*system* > Network > TCP/IP Configuration > IPv4).
2. Wybierz opcję **Interfejsy** (Interfaces), aby wyświetlić na prawym panelu listę interfejsów.
3. Na liście interfejsów kliknij prawym przyciskiem myszy wirtualny adapter Ethernet, dla którego chcesz utworzyć listę interfejsów preferowanych, a następnie kliknij **Właściwości** (Properties).
4. Kliknij zakładkę **Zaawansowane** (Advanced) i wykonaj następujące czynności:
   a. Wybierz adresy interfejsów z listy dostępnych interfejsów i kliknij **Dodaj** (Add).

      Można również usunąć interfejs z listy preferowanych interfejsów w prawym panelu klikając **Usuń** (Remove) oraz przesunąć interfejs w górę lub w dół listy w celu dokonania zmiany kolejności klikając **Przesuń w górę** (Move up) lub **Przesuń w dół** (Move down).
   b. Zaznacz pole wyboru **Włącz ARP proxy**, aby aktywować listę.
   c. Kliknij przycisk **OK**, aby zapisać utworzoną listę preferowanych interfejsów.

Tworzenie listy preferowanych interfejsów za pomocą interfejsu znakowego

Aby utworzyć listę preferowanych interfejsów za pomocą interfejsu znakowego, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CHGTCPIFC (Change TCP/IP Interface - Zmiana interfejsu TCP/IP) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana interfejsu TCP/IP (Change TCP/IP Interface).
2. W polu *Adres internetowy* (Internet address) określ interfejs IPv4 wirtualnej sieci Ethernet, dla którego chcesz utworzyć listę preferowanych interfejsów, a następnie naciśnij klawisz Enter, aby zobaczyć listę parametrów opcjonalnych.
3. W polu *Preferowane interfejsy* (Preferred interfaces) wpisz znak plusa (+) obok pola *+: więcej wartości* (+ for more values) i naciśnij klawisz Enter.
4. Podaj w kolejności preferencji maksymalnie 10 preferowanych interfejsów IPv4. Pierwsza pozycja interfejsu odpowiada najsilniejszej preferencji dla tego interfejsu.
5. Naciśnij dwukrotnie klawisz Enter.

Uwagi:

1. Lista preferowanych interfejsów może zawierać tylko 10 interfejsów. Jeśli zostanie skonfigurowanych więcej niż 10, lista będzie skrócona do pierwszych 10 interfejsów.
2. 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 7: tworzenie trasy domyślnej

Utworzenie trasy domyślnej pozwala pakietom opuszczać wirtualną sieć Ethernet.

Aby utworzyć trasę domyślną, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę CFGTCP (Configure TCP/IP - Konfigurowanie TCP/IP) i naciśnij klawisz Enter.
2. Wybierz opcję 2 (Praca z trasami TCP/IP - Work with TCP/IP Routes) 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* (Next hop) 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 8: sprawdzanie komunikacji sieciowej

Na tym etapie można sprawdzić poprawność komunikacji sieciowej.

Aby sprawdzić poprawność komunikacji sieciowej, skorzystaj z 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.

Informacje pokrewne

Ping

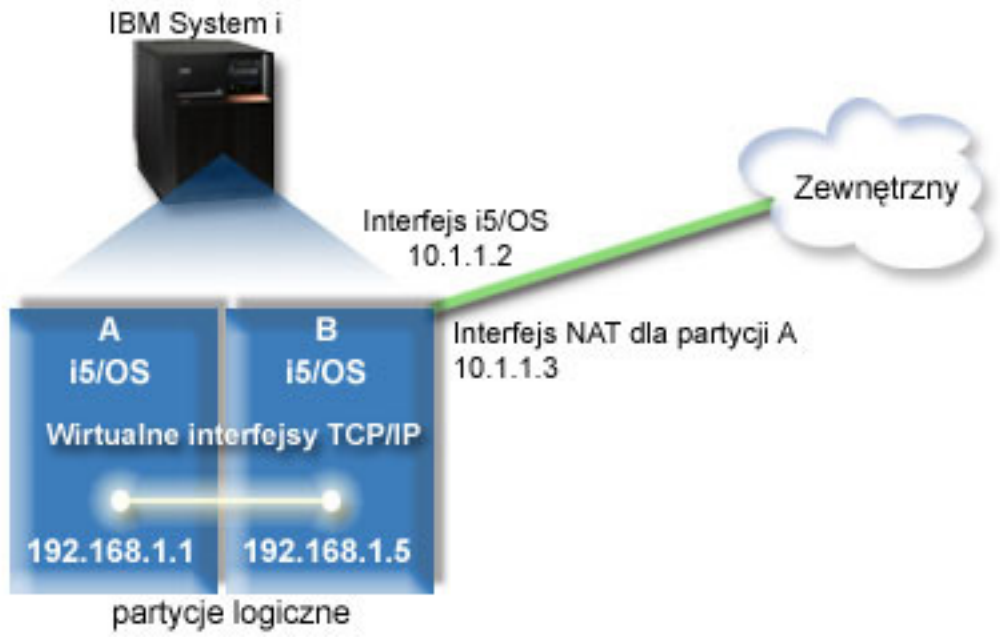
Metoda translacji adresu sieciowego (NAT)

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 wykorzystywane będą reguły pakietów IP, należy użyć programu System i Navigator do utworzenia i zastosowania reguł.

Uwaga: IPv6 nie jest obsługiwane przez metodę NAT.

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 systemu 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: włączanie wirtualnej sieci Ethernet

Aby powiązać wirtualny interfejs z interfejsem zewnętrznym, należy najpierw włączyć partycje logiczne, które mają stanowić część wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890. W przypadku konfigurowania wirtualnej sieci
| Ethernet w modelach innych niż 8*xx* należy zapoznać się z instrukcjami w sekcji Wirtualna sieć Ethernet dla partycji
| logicznych systemu i5/OS Centrum informacyjnego IBM - sprzęt.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycji A) wpisz STRSST (komendę Uruchomienie narzędzi serwisowych - Start Service Tools) i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.
3. W oknie Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi - Work with System Partitions).
4. W oknie 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 systemu możliwe są dwa sposoby wykonania tego kroku. Wybierz procedurę odpowiednią dla danego modelu.

Tworzenie opisów linii Ethernet w modelach 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach 8*xx*, dzięki czemu system będzie mógł
| korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie 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 oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

Tworzenie opisów linii Ethernet w modelach innych niż 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach innych niż 8*xx*, dzięki czemu system będzie
| mógł korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 515, 520, 525, 550, 570, 595 itp.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie 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 oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

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 wpisz komendę CHGTCPA (Zmiana atrybutów TCP/IP - Change TCP/IP Attributes) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana atrybutów TCP/IP (Change TCP/IP Attributes).
2. W polu *Przesyłanie datagramów IP* (IP datagram forwarding) wpisz *YES i naciśnij klawisz Enter.

Krok 4: tworzenie interfejsów

Aby umożliwić ruch między wirtualną siecią Ethernet i siecią zewnętrzną, należy utworzyć kilka interfejsów TCP/IP dla systemu.

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 systemem w obie strony:
   a. W wierszu komend partycji B wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu wyświetlenia okna 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 okna 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* (Subnet mask) wpisz 255.255.255.0.
   g. Uruchom interfejs. W oknie Praca z interfejsami TCP/IP (Work with TCP/IP Interfaces) wybierz opcję 9 (Uruchom) dla interfejsu.
2. Na partycji B utwórz i uruchom inny interfejs TCP/IP połączony z zewnętrzną siecią. Musi on używać tego samego opisu linii, którego używa istniejący zewnętrzny interfejs TCP/IP.

   Powtórz powyższe czynności, aby utworzyć interfejs. Podaj 10.1.1.3 jako *Adres internetowy* i użyj tych samych wartości w innych polach. Ten interfejs wykona ostatecznie translację adresu dla partycji.
3. Utwórz i uruchom interfejs TCP/IP i5/OS na partycji A dla wirtualnej sieci Ethernet:
   a. W wierszu komend partycji A wpisz CFGTCP (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu wyświetlenia okna 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 okna 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* (Subnet mask) wpisz 255.255.255.0.
   g. Uruchom interfejs. W oknie 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:

   Powtórz powyższe czynności na partycji B, aby utworzyć interfejs. Podaj 192.168.1.5 jako *Adres internetowy* i użyj tych samych wartości w innych polach.

Krok 5: tworzenie reguł pakietów

W programie System i 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 System i Navigator rozwiń kolejno opcje **system → Sieć → Strategie IP** (system > Network > IP Policies).
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Edytor reguł**.
3. Z menu **Kreatory** (Wizards) wybierz opcję **Translacja adresu** (Address Translation).
4. Wykonuj instrukcje kreatora, aby utworzyć reguły pakietów.***system***
   - 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 6: sprawdzanie komunikacji sieciowej

Na tym etapie można sprawdzić poprawność komunikacji sieciowej.

Aby sprawdzić komunikację sieciową, użyj 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.

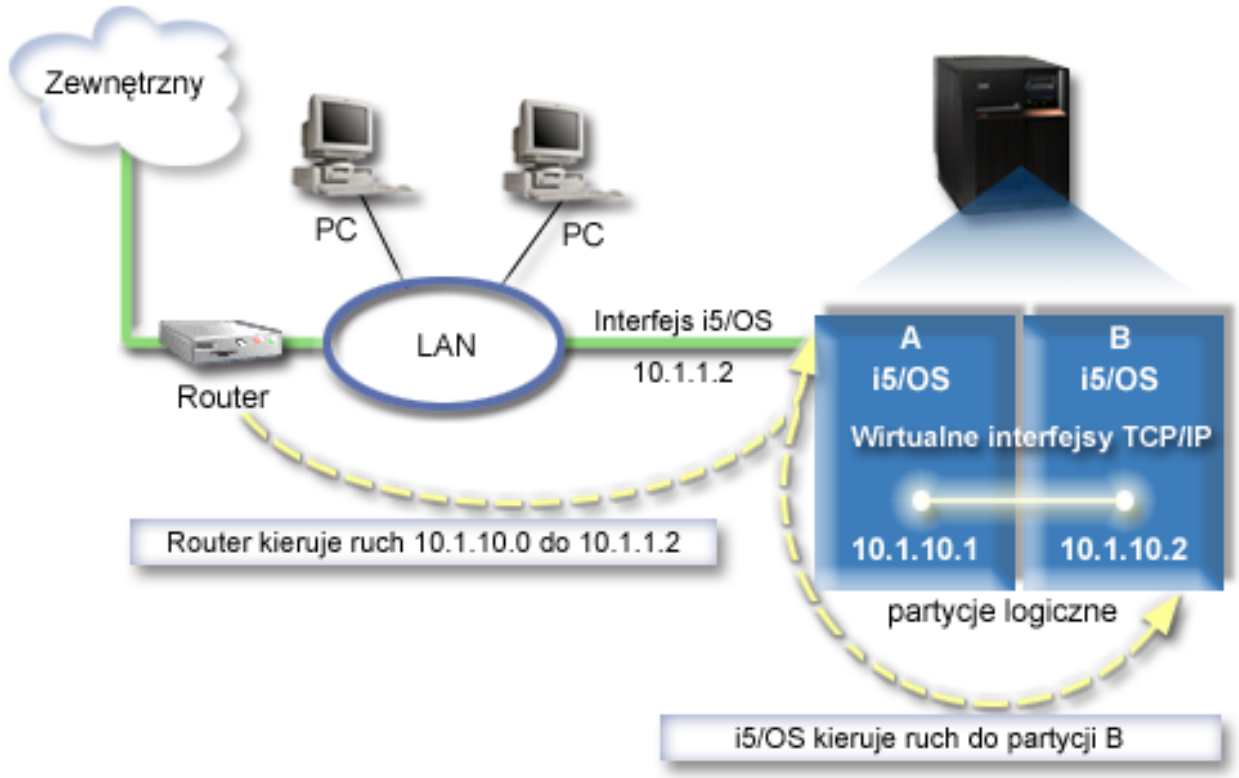
Informacje pokrewne

Ping

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 system i5/OS można ponadto użyć różnych technik routingu. Ta metoda nie jest trudna do skonfigurowania w systemie, ale w zależności od topologii sieci, jej zaimplementowanie może być niewygodne. Metoda routingu TCP/IP obsługuje zarówno IPv4, jak i IPv6. Poniższy rysunek ilustruje sieć IPv4:



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 systemu. 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 połączona jest platforma System i), 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: włączanie wirtualnej sieci Ethernet

Aby powiązać wirtualny interfejs z interfejsem zewnętrznym, należy najpierw włączyć partycje logiczne, które mają stanowić część wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890. W przypadku konfigurowania wirtualnej sieci
| Ethernet w modelach innych niż 8*xx* należy zapoznać się z instrukcjami w sekcji Wirtualna sieć Ethernet dla partycji
| logicznych systemu i5/OS Centrum informacyjnego IBM - sprzęt.

Aby aktywować wirtualną sieć Ethernet, wykonaj następujące czynności:

1. W wierszu komend partycji podstawowej (partycji A) wpisz STRSST (komendę Uruchomienie narzędzi serwisowych - Start Service Tools) i naciśnij klawisz Enter.
2. Wpisz ID użytkownika i hasło dla narzędzi serwisowych.

3. W oknie Narzędzia SST (System Service Tools - SST) wybierz opcję 5 (Praca z partycjami systemowymi - Work with System Partitions).
4. W oknie 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 systemu możliwe są dwa sposoby wykonania tej czynności. Wybierz procedurę odpowiednią dla danego modelu.

Tworzenie opisów linii Ethernet w modelach 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach 8*xx*, dzięki czemu system będzie mógł
| korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 800, 810, 825, 870 i 890.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie 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 oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

Tworzenie opisów linii Ethernet w modelach innych niż 8*xx*:

| Opisane kroki umożliwiają utworzenie opisu linii Ethernet w modelach innych niż 8*xx*, dzięki czemu system będzie
| mógł korzystać z wirtualnej sieci Ethernet.

| Ta procedura konfiguracji dotyczy modeli 515, 520, 525, 550, 570, 595 itp.

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 oknie Praca z zasobami komunikacyjnymi (Work with Communications Resources) wybierz opcję 7 (Wyświetlenie szczegółów zasobu - Display resource detail) 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 oknie Wyświetlanie szczegółów zasobu (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 oknie 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 oknie Praca z opisami konfiguracji (Work with Configuration Descriptions) wybierz opcję 1 (Utwórz) i naciśnij klawisz Enter, aby wyświetlić okno 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.

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 wpisz komendę CHGTCPA (Zmiana atrybutów TCP/IP - Change TCP/IP Attributes) i naciśnij klawisz F4 (Podpowiedź), aby uzyskać dostęp do menu Zmiana atrybutów TCP/IP (Change TCP/IP Attributes).
2. W polu *Przesyłanie datagramów IP* (IP datagram forwarding) wpisz *YES i naciśnij klawisz Enter.

Krok 4: tworzenie interfejsów

Aby umożliwić ruch między wirtualną siecią Ethernet i siecią zewnętrzną, należy utworzyć kilka interfejsów TCP/IP dla systemu.

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 (komendę Konfigurowanie TCP/IP - Configure TCP/IP) i naciśnij klawisz Enter w celu wyświetlenia okna 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 okna Dodawanie interfejsu TCP/IP (Add TCP/IP Interface - ADDTCPIFC).
d. W polu *Adres internetowy* wpisz 10.1.1.2.
e. W polu *Opis linii* (Line description) wpisz nazwę opisu linii, na przykład ETHLINE.
f. W polu *Maska podsieci* (Subnet mask) wpisz 255.255.255.0.

2. Uruchom interfejs. W oknie 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.

Korzyści z używania wirtualnej sieci Ethernet

Wirtualna sieć Ethernet zapewnia wydajną komunikację między partycjami logicznymi i korzyści płynące z utworzenia ekonomicznej sieci. Z wirtualnej sieci Ethernet można skorzystać w systemie operacyjnymi5/OS.

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 maksymalnie 16 wirtualnych sieci LAN. Od strony użytkowej wirtualna sieć Ethernet oferuje takie same możliwości, jak adapter Ethernet 1 Gb/s. Sieci lokalne Token Ring lub Ethernet 10 Mb/s i 100 Mb/s nie są obsługiwane, jeśli wykorzystywana jest wirtualna 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 systemu i komunikować się z zewnętrzną siecią LAN bez potrzeby instalowania dodatkowych fizycznych kart LAN. Jeśli system 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 systemu.
- 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

Informacje, które wiążą się z kolekcją tematów dotyczących konfigurowania TCP/IP można znaleźć w podręcznikach produktów, dokumentacji technicznej IBM (Redbooks), serwisach WWW i w innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Dokumentacja techniczna IBM (Redbooks)

- Podręcznik TCP/IP Tutorial and Technical Overview (około 7,5 MB)
- Podręcznik IBM i5/OS IP Networks: Dynamic (około 14,8 MB)

Serwisy WWW

- The Internet Engineering Task Force (IETF) (http://www.ietf.org/)
  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 wiadomości oraz wydarzenia związane z projektowaniem protokołu IPv6.

Inne informacje

- Aplikacje, protokoły i usługi TCP/IP: ta kolekcja tematów zawiera informacje o aplikacjach i usługach TCP/IP innych niż konfiguracyjne.
- Rozwiązywanie problemów dotyczących protokołu TCP/IP: ta kolekcja tematów zawiera informacje, które pomogą w rozwiązaniu problemów z połączeniami TCP/IP lub ruchem w sieci IPv4 i IPv6.
- Planning and setting up system security: ta kolekcja tematów zawiera informacje na temat planowania i konfigurowania ochrony dla produktów System i.

Odsyłacze pokrewne

“Plik PDF z informacjami dotyczącymi konfigurowania TCP/IP” na stronie 2
Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

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
USA

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
Tokio 106-0032, Japonia

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 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
USA

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

Licencjonowany program opisany w niniejszym dokumencie 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 możliwości 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/nazwiska sĄ fikcyjne i jakiekolwiek podobieästwo do istniejĄcych nazw/nazwisk i adres˜w jest ca?kowicie 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 dotyczące 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:

eServer
i5/OS
IBM
IBM (logo)
iSeries
Redbooks
System i

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

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

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation 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.

Drukowane w USA