System i

Sieci
Usługi zdalnego dostępu: połączenia PPP

Wersja 6 wydanie 1

System i

Sieci
Usługi zdalnego dostępu: połączenia PPP

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 67.

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

Usługi zdalnego dostępu: połączenia PPP

Protokół Point-to-Point (PPP) jest internetowym standardem przesyłania danych za pomocą łączy szeregowych.

Jest to protokół połączenia najczęściej używany przez dostawców usług internetowych (ISP). Umożliwia on pojedynczym komputerom uzyskanie dostępu do sieci. Sieci te następnie zapewniają dostęp do Internetu. Produkt System i obsługuje protokół PPP w ramach TCP/IP jako element obsługi łączności w sieci rozległej (WAN).

Protokół PPP łączy zdalny komputer z platformą System i, umożliwiając wymianę danych między różnymi miejscami. W ten sposób systemy zdalne połączone z danym systemem mogą uzyskać dostęp do jego zasobów oraz do innych komputerów należących do tej samej sieci. Za pomocą protokołu PPP można także skonfigurować połączenie systemu z Internetem. Kreator połączenia modemowego programu System i Navigator przeprowadza użytkownika przez proces tworzenia połączenia danego systemu z Internetem lub siecią wewnętrzną.

Plik PDF o usługach zdalnego dostępu (Remote Access Services)

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

Aby wyświetlić lub pobrać ten dokument w formacie PDF, wybierz Usługi zdalnego dostępu: połączenia PPP (około 940 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 związane z usługami zdalnego dostępu (Remote Access Services)” na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Pojęcia dotyczące protokołu PPP

Dzięki protokołowi PPP można połączyć platformę System i ze zdalnymi sieciami, komputerami PC, innymi platformami System i lub z dostawcą ISP. Aby w pełni korzystać z tego protokołu, należy poznać zarówno jego możliwości, jak i obsługę w systemie i5/OS.

Odsyłacze pokrewne

“Informacje związane z usługami zdalnego dostępu (Remote Access Services)” na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Co to jest protokół PPP

Protokół Point-to-Point Protocol (PPP) jest protokołem TCP/IP używanym do połączenia dwóch systemów komputerowych. Komputery używają protokołu PPP do komunikacji przez linię telefoniczną lub łączenia się z Internetem.

Połączenie PPP ma miejsce wtedy, kiedy dwa systemy połączone są fizycznie przy pomocy linii telefonicznej. Istnieje możliwość wykorzystania protokołu PPP do połączenia dwóch systemów. Na przykład ustanowienie połączenia PPP między oddziałem a centralą umożliwia przesyłanie danych przez sieć między tymi dwoma miejscami.

Umożliwia on współdziałanie programów zdalnego dostępu pochodzących od różnych producentów. Umożliwia również kilku protokołom komunikacyjnym wykorzystywanie tej samej fizycznej linii komunikacyjnej.

Poniższe standardy RFC (Request For Comment) opisują protokół PPP. Więcej informacji o standardach RFC zawiera serwis WWW RFC Editor  .

- RFC-1661 Point-to-Point Protocol (Protokół PPP)
- RFC-1662 PPP on HDLC-like framing (Protokół PPP na ramkach typu HDLC)
- RFC-1994 PPP CHAP (Protokół PPP CHAP)

Profile połączeń

Profile połączeń punkt z punktem definiują zestaw parametrów i zasobów dla określonych połączeń PPP. Profile, które korzystają z takich ustawień parametrów, można uruchomić w celu wykonywania połączeń wychodzących (rozpoczynania) lub nasłuchiwania (odbioru) połączeń PPP.

Do zdefiniowania zestawu parametrów połączenia PPP lub zestawów połączeń można użyć następujących dwóch typów profili:

- *Profile połączenia nadawcy* są połączeniami typu punkt z punktem inicjowanymi przez system lokalny i odbieranymi przez system zdalny. Przy pomocy tego obiektu można skonfigurować połączenia wychodzące.
- *Profile połączenia odbiorcy* są połączeniami typu punkt z punktem inicjowanymi przez system zdalny i odbieranymi przez system lokalny. Przy pomocy tego obiektu można skonfigurować połączenia przychodzące.

Profil połączenia określa sposób działania połączenia. Informacje zawarte w tych profilach odpowiadają na następujące pytania:

- Jakiego typu protokół jest używany (PPP lub Serial Line Internet Protocol - SLIP)?
- Czy system kontaktuje się z innym komputerem, inicjując połączenie (nadawca)? Czy system oczekuje na połączenie przychodzące z innego systemu (odbiorca)?
- Jaka linia komunikacyjna jest wykorzystywana przez połączenie?
- W jaki sposób system określa, którego adresu IP ma użyć?
- W jaki sposób system uwierzytelnia inny system? Gdzie system powinien przechowywać informacje dotyczące uwierzytelniania?

Profil połączenia jest logiczną reprezentacją następujących informacji dotyczących połączenia:

- typ profilu i linii,
- ustawienia dla połączeń multilink,
- numery zdalnych telefonów i opcje wybierania,
- uwierzytelnianie,
- ustawienia TCP/IP: adresy IP i routing, filtrowanie IP,
- zarządzanie pracą i dostosowanie połączenia,
- serwery nazw domen.

System przechowuje powyższe informacje konfiguracyjne w profilu połączenia. Dostarczają one systemowi kontekstu niezbędnego przy nawiązywaniu połączenia PPP z innym systemem. Profil połączenia zawiera następujące informacje:

- **Typ protokołu**. Istnieje możliwość wyboru między protokołem PPP a SLIP. Firma IBM zaleca używanie protokołu PPP, o ile jest to możliwe.
- **Wybór trybu**. Wybór trybu określa typ połączenia i tryb pracy dla danego profilu połączenia.

  Typ połączenia. Określa rodzaj linii, na której bazują połączenia, oraz czy jest to wybieranie (nadawca), czy odpowiadanie (odbiorca). Istnieje możliwość wyboru spośród poniższych typów połączenia:

  – Linia komutowana
  – Linia dzierżawiona (dedykowana)
  – Layer Two Tunneling Protocol (L2TP) (linia wirtualna)
  – Połączenie protokołu PPP przez sieć Ethernet (Point-to-Point Protocol over Ethernet - PPPoE, linia wirtualna)

  Protokół PPPoE obsługuje tylko profile połączeń nadawcy.
- **Tryb pracy**. Dostępne tryby pracy zależą od rodzaju połączenia.

Tabela 1. Tryby pracy dostępne dla profilu połączenia nadawcy

Typ połączenia	Dostępne tryby pracy
Linia komutowana	• Połączenie • Połączenie zamawiane (tylko inicjowanie) • Wybieranie na żądanie (dedykowany partner ma włączoną opcję odp.) • Połączenie zamawiane (zdalne węzły włączone)
Linia dzierżawiona	Inicjator
L2TP	• Inicjator • Inicjator wieloprzeskokowy • Zdalne inicjowanie
Protokół PPP przez sieć Ethernet	Inicjator

Tabela 2. Tryby pracy dostępne dla profilu połączenia odbiorcy

Typ połączenia	Dostępne tryby pracy
Linia komutowana	Odpowiedź
Linia dzierżawiona	Terminator
L2TP	Terminator (serwer sieciowy)

- **Konfiguracja linii**. Określa ona typ obsługi linii używanej przez połączenie.

  Wybór ten zależy od typu wyboru trybu. Dla linii dzierżawionych i komutowanych można wybrać:

  – Pojedyncza linia
  – Pula linii

  W przypadku wszystkich pozostałych typów połączeń (dzierżawione, L2TP, PPPoE) dostępna jest jedynie linia pojedyncza.

Odsyłacze pokrewne

“Wymagania sprzętowe i programowe” na stronie 31
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących ten protokół. Jeden z tych komputerów, platforma System i, może być albo nadawcą, albo odbiorcą.

Obsługa strategii dostępu dla grup

Obsługa strategii dostępu dla grup umożliwia administratorom sieci definiowanie strategii dla grup użytkowników w celu zarządzania zasobami. Poszczególni użytkownicy są przypisywani do strategii kontroli dostępu w momencie wpisywania się w sesji PPP lub L2TP.

Użytkownicy mogą być przypisywani do odpowiednich klas. Każda klasa ma własną unikalną strategię, definiującą ograniczenia dotyczące zasobów (na przykład liczba linii w wiązce połączenia multilink), atrybuty (na przykład przekazywanie IP) oraz stosowane reguły filtrowania pakietów IP. Obsługa strategii dostępu dla grup umożliwia na przykład administratorom sieci zdefiniowanie grupy Pracujący_z_domu, mającej pełny dostęp do sieci, oraz grupy Pracownicy_dostawcy, mającej dostęp do ograniczonego zestawu usług.

Odsyłacze pokrewne

"Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE" na stronie 10
Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

"Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP" na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Scenariusz: zdalny dostęp przez połączenia PPP

Scenariusze przedstawiają sposób działania protokołu PPP oraz implementacji środowiska PPP w sieci. Wprowadzono w nich również podstawowe pojęcia związane z protokołem PPP. Korzystać z nich mogą zarówno początkujący, jak i doświadczeni użytkownicy przed przystąpieniem do zadań planowania i konfiguracji.

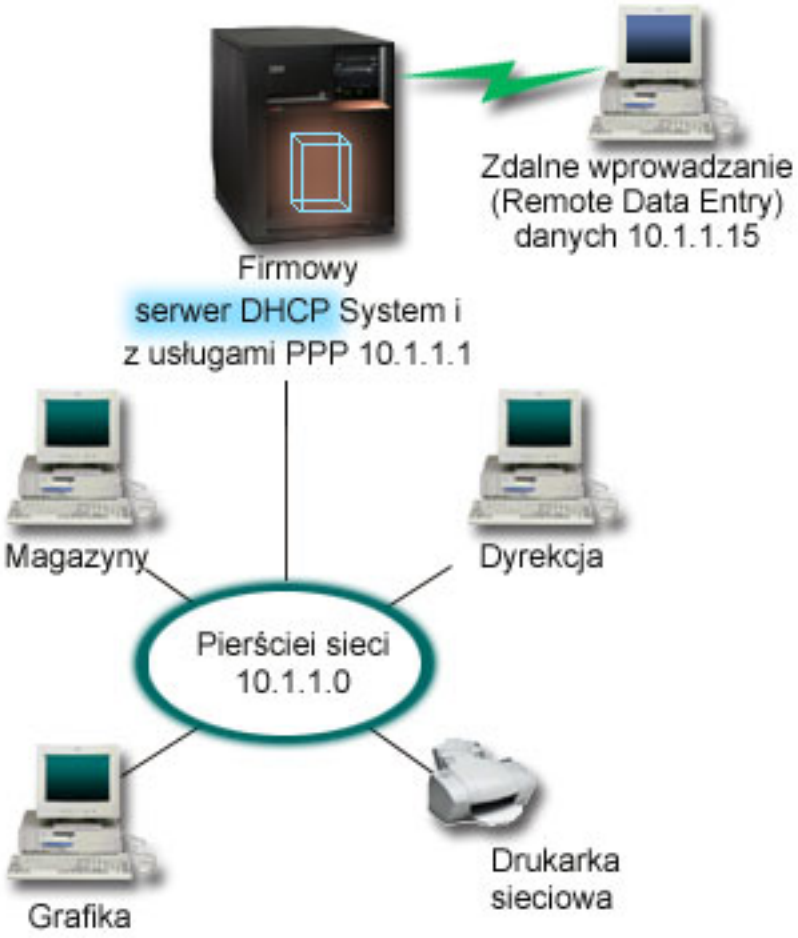
Odsyłacze pokrewne

"Informacje związane z usługami zdalnego dostępu (Remote Access Services)" na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Przykład: PPP i DHCP na jednym serwerze System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i na potrzeby sieci LAN i zdalnych klientów z połączeniem modemowym.

Często zachodzi potrzeba dopuszczenia do firmowej sieci LAN klientów łączących się zdalnie, na przykład za pośrednictwem łączy telefonicznych. Klienty z połączeniem modemowym mogą uzyskać dostęp do serwera System i za pomocą protokołu PPP. Aby uzyskać dostęp do sieci, klient z połączeniem modemowym wymaga informacji dotyczących adresu IP, tak samo jak klient podłączony bezpośrednio do sieci. Serwer DHCP System i może przekazywać adresy IP klientom z połączeniem modemowym za pośrednictwem protokołu PPP na takiej samej zasadzie, jak w przypadku innych klientów podłączonych bezpośrednio. Poniższy rysunek przedstawia sytuację, w której klient zdalny musi uzyskać dostęp do sieci firmowej, aby wykonać pewne czynności.



Rysunek 1. PPP i DHCP na jednym serwerze System i

Aby zdalny pracownik mógł podłączyć się do firmowej sieci, serwer System i musi skorzystać z usługi zdalnego dostępu RAS (Remote Access Service) i DHCP. Funkcja RAS umożliwia uzyskanie dostępu do serwera System i za pomocą modemu. Jeśli połączenie modemowe jest prawidłowo skonfigurowane, to bezpośrednio po jego nawiązaniu przez klienta serwer PPP wysyła do serwera DHCP żądanie dystrybucji danych TCP/IP do klienta zdalnego.

W tym przykładzie obsługa zarówno klientów w sieci LAN, jak i zdalnych klientów modemowych odbywa się według spójnej strategii dla jednej podsieci.

Parametry zlecające serwerowi DHCP dystrybucję danych IP dla klienta zdalnego są konfigurowane w profilu PPP. W ustawieniach TCP/IP profilu połączenia odbiorcy należy zmienić metodę przypisania zdalnego adresu IP z wartości Stały (Fixed) na DHCP. Aby umożliwić klientom modemowym komunikację z innymi klientami w sieci, na przykład z drukarką, należy również włączyć przekazywanie IP w ustawieniach TCP/IP profilu oraz we właściwościach konfiguracji (stosu) TCP/IP. Jeśli przekazywanie IP zostanie skonfigurowane tylko w profilu PPP, serwer System i nie będzie przekazywał pakietów IP. Konieczne jest włączenie przekazywania IP jednocześnie w profilu i w stosie.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP należącym do definicji podsieci serwera DHCP. W tym przykładzie adres lokalnego interfejsu w profilu PPP to 10.1.1.1. Adres ten powinien zostać wykluczony z puli zarządzanej przez serwer DHCP, aby nie został przypisany klientowi DHCP.

Planowanie konfiguracji DHCP dla klientów lokalnych i klientów PPP

Tabela 3. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracji	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 4. Podsieć dla klientów lokalnych i modemowych

Obiekt		**Wartość**
Nazwa podsieci		SiecGlowna
Zarządzane adresy		10.1.1.3 - 10.1.1.150
Okres dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracji	Opcje odziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.1.1 (lokalny adres interfejsu, podany w ustawieniach TCP/IP we właściwościach profilu połączenia odbiorcy w programie System i Navigator)

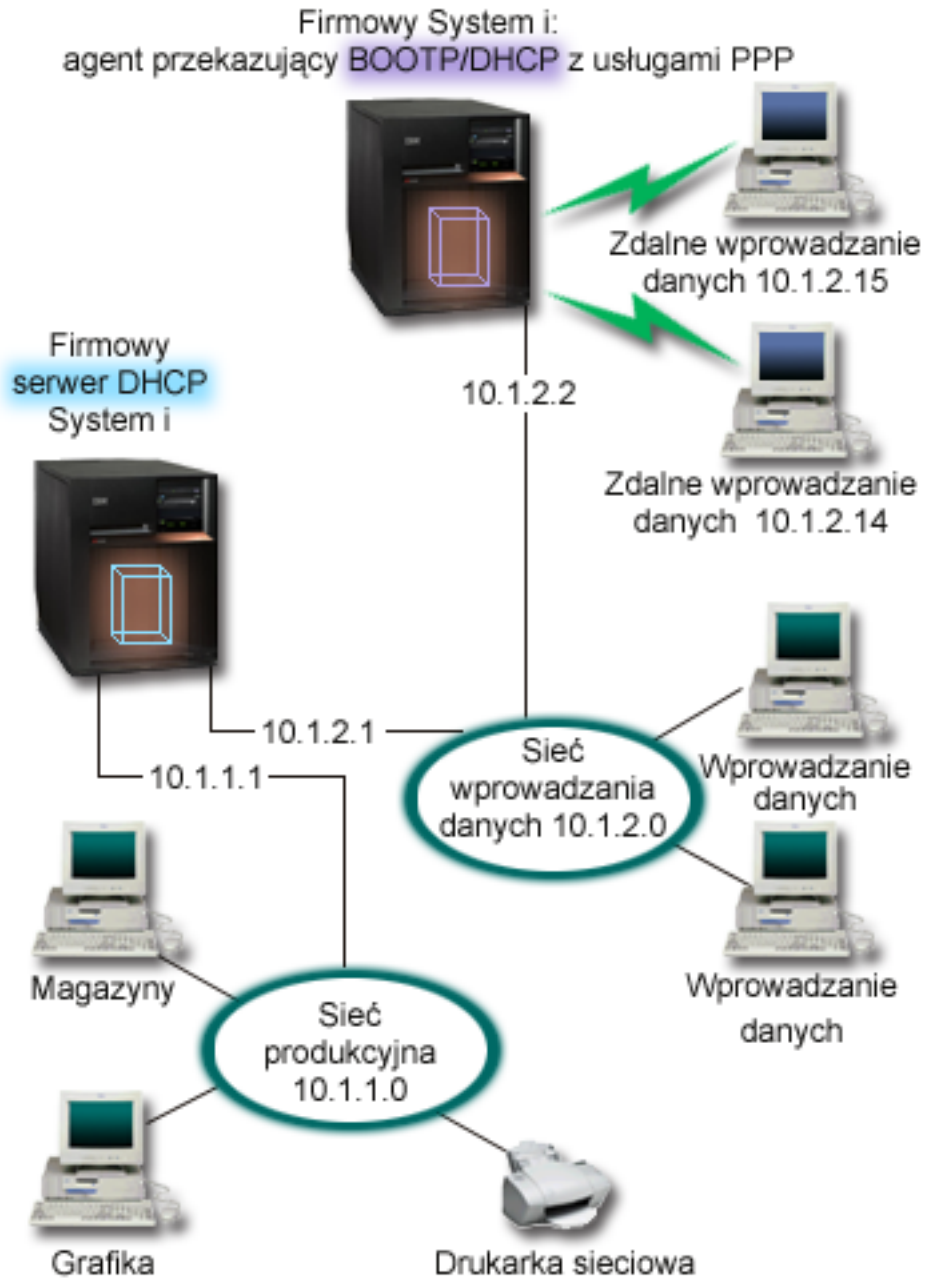
Pozostałe opcje konfiguracji

- W profilu połączenia PPP odbiorcy należy podać DHCP jako metodę określania zdalnego adresu IP.
  1. Należy włączyć możliwość nawiązania przez klientów sieci WAN połączenia z serwerem DHCP lub nawiązania połączenia przekazywanego, używając pozycji menu **Usługi** (Services) w menu Usługi zdalnego dostępu (Remote Access Services) programu System i Navigator.
  2. We właściwościach ustawień TCP/IP (TPC/IP Settings Properties) w profilu połączenia odbiorcy (Receiver Connection Profile) w programie System i Navigator jako metodę przypisywania adresów IP należy wybrać DHCP.
- We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator należy umożliwić zdalnemu komputerowi uzyskanie dostępu do innych sieci (przekazywanie IP).
- We właściwościach ustawień (Settings Properties) konfiguracji TCP/IP (TCP/IP Configuration) w programie System i Navigator należy włączyć przekazywanie datagramów IP.

Przykład: profile DHCP i PPP na różnych serwerach System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować dwa serwery System i, aby pełniły rolę serwera DHCP i agenta przekazującego BOOTP/DHCP na potrzeby dwóch sieci LAN i zdalnych klientów z połączeniem modemowym.

W przykładzie dotyczącym PPP i DHCP na jednym serwerze System i przedstawiono sposób korzystania z DHCP i PPP w jednym systemie w celu umożliwienia łączenia się z siecią klientom z połączeniem modemowym. Jednak z uwagi na fizyczną budowę sieci i ze względów bezpieczeństwa lepszym rozwiązaniem może być rozdzielenie serwerów PPP i DHCP lub zainstalowanie dedykowanego serwera PPP bez usług DHCP. Poniższy rysunek przedstawia sieć, w której klientów z połączeniem modemowym obsługują serwery PPP i DHCP umieszczone na różnych maszynach.



Rysunek 2. Profile DHCP i PPP na różnych serwerach System i

Zdalne klienty wprowadzania danych wybierają połączenie z serwerem PPP System i. Profil PPP na tym serwerze musi określać przypisywanie zdalnych adresów IP poprzez DHCP, jak w przykładzie dotyczącym PPP i DHCP na jednym serwerze System i. Profil PPP oraz właściwości stosu TCP/IP serwera PPP muszą mieć ustawione przekazywanie IP. Ponadto, ponieważ ten serwer działa w charakterze agenta przekazującego pakiety DHCP, musi być włączony agent przekazujący BOOTP/DHCP. Dzięki temu serwer zdalnego dostępu System i będzie mógł przekazywać pakiety DHCPDISCOVER do serwera DHCP. Serwer DHCP w odpowiedzi na te pakiety będzie udostępniał klientom modemowym dane konfiguracyjne TCP/IP za pośrednictwem serwera PPP.

Serwer DHCP jest odpowiedzialny za dystrybucję adresów IP w obu sieciach: 10.1.1.0 i 10.1.2.0. W sieci wprowadzania danych adresy z zakresu od 10.1.2.10 do 10.1.2.40 będą przypisywane przez serwer DHCP zarówno klientom z połączeniem modemowym, jak i klientom podłączonym bezpośrednio do sieci. Klientom z podsieci

wprowadzania danych potrzebny będzie jeszcze adres routera (opcja 3) 10.1.2.1, pozwalający nawiązać połączenie z siecią produkcyjną, przy czym serwer DHCP System i musi mieć także włączone przekazywanie IP.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP należącym do definicji podsieci serwera DHCP. W tym przykładzie adres lokalnego interfejsu w profilu PPP to 10.1.2.2. Adres ten powinien zostać wykluczony z puli zarządzanej przez serwer DHCP, aby nie został przypisany klientowi DHCP. Adres IP lokalnego interfejsu musi być adresem, pod który serwer DHCP może przesyłać pakiety odpowiedzi.

Planowanie konfiguracji DHCP dla serwera z agentem przekazującym DHCP

Tabela 5. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracji	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 6. Podsieć dla sieci produkcyjnej

Obiekt		**Wartość**
Nazwa podsieci		SiecProdukcyjna
Zarządzane adresy		10.1.1.3 - 10.1.1.150
Okres dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracji	Opcje odziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		brak

Tabela 7. Podsieć sieci wprowadzania danych

Obiekt		**Wartość**
Nazwa podsieci		WprowadzanieDanych
Zarządzane adresy		10.1.2.10 - 10.1.2.40
Okres dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracji	Opcja 3: router	10.1.2.1
	Opcje odziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.2.1 (router) 10.1.2.15 (adres IP lokalnego interfejsu dla zdalnego klienta wprowadzania danych) 10.1.2.14 (adres IP lokalnego interfejsu dla zdalnego klienta wprowadzania danych)

Inne ustawienia na platformie System i z usługą PPP

- Konfiguracja serwera TCP/IP agenta przekazującego BOOTP/DHCP

Obiekt	**Wartość**
Adres interfejsu	10.1.2.2
Przekazywanie pakietów pod adres IP serwera	10.1.2.1

- W profilu połączenia PPP odbiorcy należy podać DHCP jako metodę określania zdalnego adresu IP.

1. Należy włączyć możliwość nawiązania połączenia przez klientów sieci WAN z serwerem DHCP lub nawiązania połączenia przekazywanego, używając pozycji menu Usługi (Services) w menu Usługi zdalnego dostępu (Remote Access Services) w programie System i Navigator.
2. We właściwościach ustawień TCP/IP (TCP/IP Settings Properties) w profilu połączenia odbiorcy (Receiver Connection Profile) w programie System i Navigator jako metodę przypisywania adresów IP należy wybrać DHCP.

- We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator należy umożliwić zdalnemu komputerowi uzyskanie dostępu do innych sieci (przekazywanie IP). Chodzi tu o umożliwienie zdalnym klientom komunikowania się z siecią wprowadzania danych.
- We właściwościach ustawień (Settings Properties) konfiguracji TCP/IP (TCP/IP Configuration) w programie System i Navigator należy włączyć przekazywanie datagramów IP. Chodzi tu o umożliwienie zdalnym klientom komunikowania się z siecią wprowadzania danych.

Scenariusz: zabezpieczanie dobrowolnego tunelu L2TP za pomocą protokołu IPSec

Ten scenariusz przedstawia połączenie pomiędzy hostem w biurze oddziału a biurem centrali wykorzystujące protokół L2TP zabezpieczony protokołem IPSec. Adres IP biura oddziału jest przypisywany dynamicznie, natomiast biuro główne ma statyczny, globalny adres IP.

Sytuacja

Załóżmy, że przedsiębiorstwo ma niewielki oddział w innym regionie. W danym dniu roboczym oddział może wymagać dostępu do informacji poufnych na temat modelu System i w korporacyjnej sieci intranet. Obecnie przedsiębiorstwo wykorzystuje do tego celu drogie linie dzierżawione. Mimo że firma chce w dalszym ciągu oferować bezpieczny dostęp do swojego intranetu, przede wszystkim pragnie obniżyć koszty związane z linią dzierżawioną. Aby to zrobić, może utworzyć dobrowolny (voluntary) tunel L2TP (Layer 2 Tunnel Protocol), który rozszerzy sieć korporacyjną w taki sposób, że biuro oddziału będzie wyglądało jak część korporacyjnej podsieci. Ruch danych przez tunel L2TP będzie zabezpieczony przez sieć VPN.

W ramach dobrowolnego tunelu L2TP biuro oddziału ustanowi tunel bezpośrednio do sieciowego serwera L2TP (LNS) w sieci korporacyjnej. Funkcje koncentratora dostępu L2TP (LAC) rezydują po stronie klienta. Tunel jest przezroczysty dla dostawców ISP zdalnych klientów, więc dostawcy ci nie muszą obsługiwać protokołu L2TP. Więcej informacji na temat protokołu L2TP zawiera sekcja Protokół L2TP (Layer 2 Tunnel Protocol).

Ważne: W omawianym scenariuszu bramy bezpieczeństwa są podłączone bezpośrednio do Internetu. Nieuwzględnienie firewalli ma na celu uproszczenie scenariusza. Nie oznacza to jednak, że firewalle nie są konieczne. Należy liczyć się z zagrożeniami bezpieczeństwa systemu podczas każdego połączenia z Internetem.

Cele

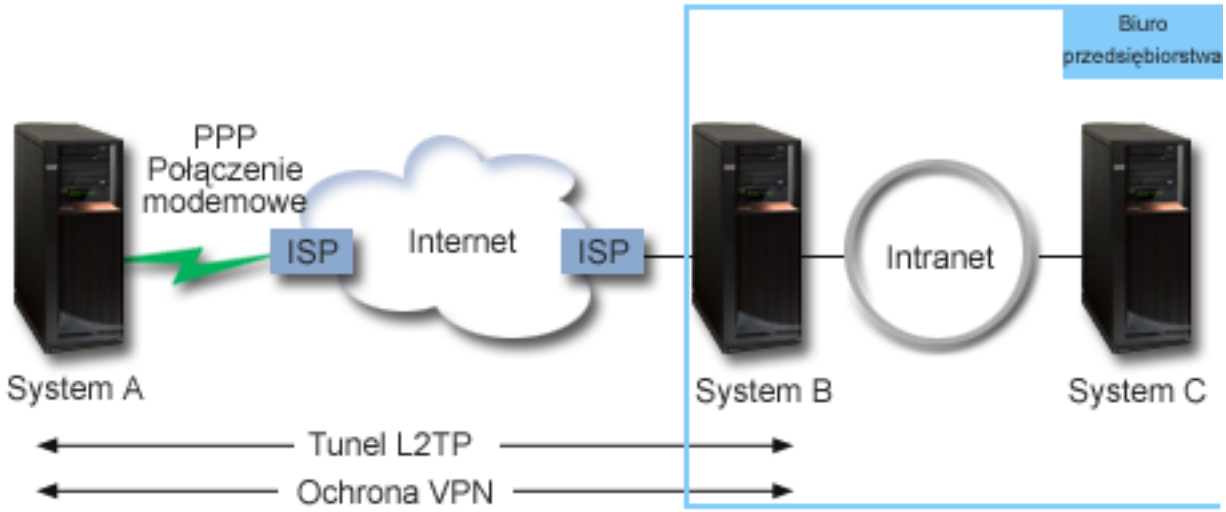
W tym scenariuszu system znajdujący się w oddziale firmy łączy się z siecią poprzez system bram przez tunel L2TP zabezpieczony siecią VPN.

Główne cele tego scenariusza to:

- System w biurze oddziału zawsze inicjuje połączenie z główną siedzibą firmy.
- System w biurze oddziału jest jedynym systemem w sieci oddziału, który potrzebuje dostępu do sieci korporacyjnej. Oznacza to, że działa on w sieci oddziału w roli hosta, a nie bramy.
- System korporacyjny jest hostem w sieci korporacyjnej.

Informacje szczegółowe

Poniższy rysunek ilustruje schemat sieci w tym scenariuszu:



System A

- Musi mieć dostęp do aplikacji TCP/IP we wszystkich systemach sieci korporacyjnej.
- Otrzymuje dynamicznie przypisywane adresy IP od dostawcy ISP.
- Musi być skonfigurowany do obsługi L2TP.

System B

- Musi mieć dostęp do aplikacji TCP/IP w systemie A.
- Adres IP podsieci to 10.6.0.0 z maską 255.255.0.0. Ta Podsieć reprezentuje punkt końcowy danych tunelu VPN w siedzibie głównej.
- Od strony Internetu ma adres IP 205.13.237.6. Stanowi on punkt końcowy połączenia. Oznacza to, że system B zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP. System B łączy się ze swoją podsiecią za pomocą adresu IP 10.6.11.1.

W terminologii protokołu L2TP *System A* działa jako inicjator L2TP, a *System B* - jako terminator L2TP.

Zadania konfiguracyjne

Zakładając, że protokół TCP/IP jest już skonfigurowany i działa, wykonaj następujące zadania:

Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE

Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

Sytuacja

Przedsiębiorstwo oczekuje szybszego połączenia z Internetem, więc jest zainteresowane połączeniem modemem DSL z lokalnym dostawcą ISP. Po wstępnym rozpoznaniu okazuje się, że dostawca ISP korzysta z PPPoE do łączenia się z klientami. Firma chciałaby skorzystać z połączenia PPPoE, aby zwiększyć szybkość połączenia z Internetem przez system.

Rysunek 3. Połączenie systemu z dostawcą ISP przy użyciu PPPoE

Rozwiązanie

Można obsługiwać połączenie PPPoE z dostawcą ISP przez dany system. System używa nowego rodzaju linii wirtualnej PPPoE, połączonej z fizyczną linią Ethernet, skonfigurowaną z adapterem Ethernet typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A lub 576A. Linia wirtualna obsługuje protokoły sesji PPP przez sieć LAN typu Ethernet połączoną z modemem DSL, który stanowi gateway do zdalnego dostawcy ISP. Gateway umożliwia użytkownikom sieci lokalnej uzyskanie szybkiego dostępu do Internetu przy użyciu połączenia PPPoE. Po nawiązaniu połączenia między systemem i dostawcą ISP użytkownicy sieci lokalnej mają dostęp do dostawcy ISP przez połączenie PPPoE i używają adresu IP przydzielonego systemowi. W celu zapewnienia dodatkowej ochrony, można zastosować dla linii wirtualnej PPPoE reguły filtrowania, które ograniczą pewną część ruchu przychodzącego.

Przykład konfiguracji

Aby ustawić przykładową konfigurację PPP z poziomu programu System i Navigator, wykonaj następujące czynności:

1. Skonfiguruj połączenie z dostawcą ISP.
2. Skonfiguruj profil połączenia nadawcy w swoim systemie.

   Należy wprowadzić poniższe informacje:

   - **Typ protokołu**: PPP
   - **Typ połączenia**: Protokół PPP przez sieć Ethernet
   - **Tryb pracy**: Inicjator
   - **Konfiguracja linii**: Pojedyncza linia
3. Na stronie Ogólne we Właściwościach nowego profilu połączenia punkt z punktem, wprowadź nazwę i opis profilu nadawcy. Nazwa ta odnosi się zarówno do profilu połączenia, jak i do linii wirtualnej PPPoE.
4. Kliknij przycisk **Połączenie**, aby otworzyć stronę Połączenie. Wybierz **Nazwę linii wirtualnej PPPoE** tego profilu połączenia. Po wybraniu linii program System i Navigator wyświetli okno dialogowe **właściwości linii** (line properties).

   a. Na stronie Ogólne wprowadź opis linii wirtualnej PPPoE.

b. Kliknij przycisk **Odsyłacz**, aby otworzyć stronę Odsyłacz. Z listy wyboru linii fizycznych wybierz używaną przez połączenie linię Ethernet i kliknij przycisk **Otwórz**. Jeśli chcesz zdefiniować nową linię Ethernet, wpisz nazwę linii i kliknij przycisk **Nowa**. Program System i Navigator wyświetli okno dialogowe **Właściwości linii Ethernet** (Ethernet line properties).

   Uwaga: Protokół PPPoE wymaga adaptera Ethernet typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A lub 576A.

   1) Na stronie Ogólne wprowadź opis linii Ethernet i sprawdź, czy w definicji linii podano odpowiednie zasoby sprzętowe.
   2) Kliknij przycisk **Odsyłacz**, aby otworzyć stronę Odsyłacz. Wprowadź właściwości fizycznej linii Ethernet. Więcej informacji na ten temat znajduje się w dokumentacji adaptera ethernet i w pomocy elektronicznej.
   3) Kliknij przycisk **Inne**, aby otworzyć stronę Inne. Określ poziom dostępu i uprawnienia użytkowników tej linii.
   4) Kliknij **OK**, aby powrócić do strony właściwości linii wirtualnej PPPoE.

c. Kliknij przycisk **Ograniczenia**, aby zdefiniować właściwości uwierzytelniania LCP lub przycisk **OK**, aby wrócić do strony Połączenie nowego profilu połączenia punkt z punktem.

d. Po powrocie do strony Połączenie ustaw adresowanie serwera PPPoE w oparciu o informacje dostarczone przez dostawcę ISP.

5. Jeśli dostawca ISP wymaga, aby system się uwierzytelnił, lub jeśli chcesz, aby system uwierzytelnił system zdalny, kliknij przycisk **Uwierzytelnianie** (Authentication), aby otworzyć stronę Uwierzytelnianie i wprowadź żądane informacje.
6. Kliknij przycisk **Ustawienia TCP/IP**, aby otworzyć stronę Ustawienia TCP/IP, a następnie określ parametry obsługi adresów IP dla tego profilu połączenia. Użyte ustawienie powinno zostać dostarczone przez dostawcę ISP. Aby umożliwić użytkownikom sieci LAN nawiązanie połączenia z dostawcą ISP z adresem IP przydzielonym systemowi, wybierz opcję **Ukryj adresy (pełne maskowanie)** (Hide addresses (Full masquerading)).
7. Kliknij przycisk **DNS**, aby otworzyć stronę DNS i wprowadź adres IP serwera DNS udostępnionego przez dostawcę ISP.
8. Kliknij **OK**, aby zakończyć.

Pojęcia pokrewne

“Obsługa strategii dostępu dla grup” na stronie 4
Obsługa strategii dostępu dla grup umożliwia administratorom sieci definiowanie strategii dla grup użytkowników w celu zarządzania zasobami. Poszczególni użytkownicy są przypisywani do strategii kontroli dostępu w momencie wpisywania się w sesji PPP lub L2TP.

Zadania pokrewne

“Tworzenie profilu połączenia” na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Odsyłacze pokrewne

“Konfigurowanie połączenia” na stronie 50
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

“Uwierzytelnianie systemu” na stronie 43
Połączenia PPP z platformą System i obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów nawiązujących połączenie z systemem, jak i połączeń wychodzących do dostawcy ISP lub innego systemu.

“Obsługa adresów IP” na stronie 41
Połączenia PPP umożliwiają dowolne zarządzanie adresami IP w zależności od rodzaju profilu połączenia.

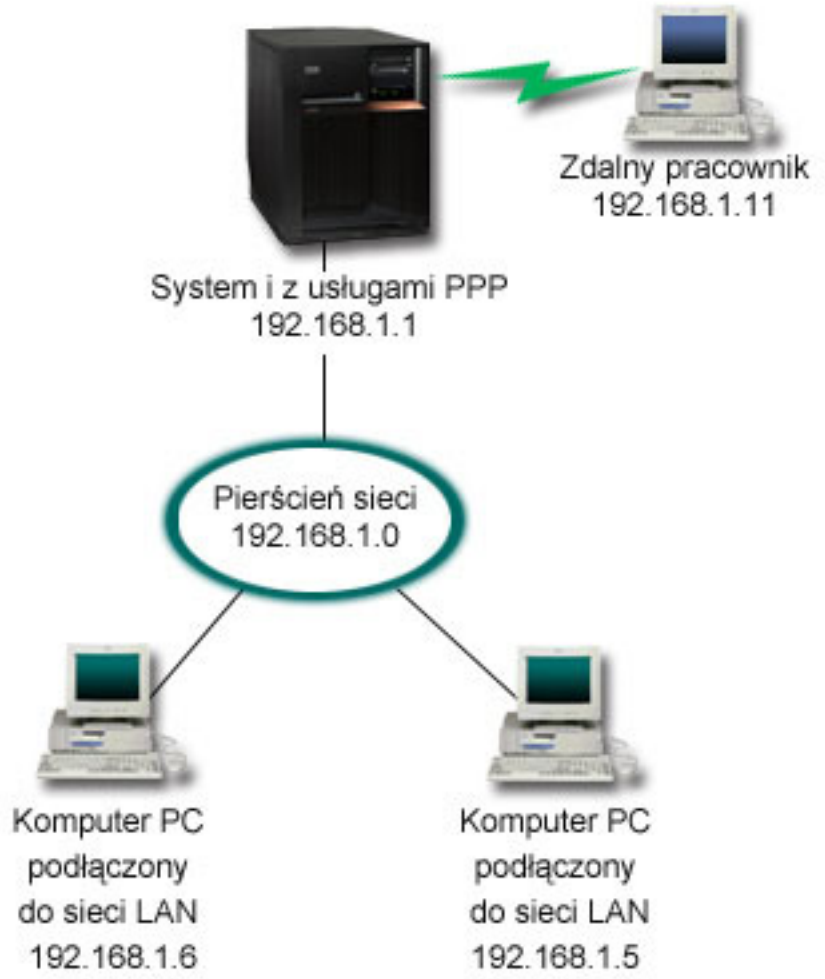
“Filtrowanie pakietów IP” na stronie 41
Filtrowanie pakietów IP ogranicza usługi dostępne dla poszczególnych użytkowników w momencie ich logowania się do sieci.

Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem

Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

Sytuacja

Administrator sieci przedsiębiorstwa musi zarządzać zarówno klientami sieciowymi, jak i systemem. Zamiast przychodzić do pracy w celu zdiagnozowania i rozwiązania problemów może on wykonać te zadania zdalnie, na przykład z domu. Dopóki firma nie ma stałego połączenia z Internetem, połączenie modemowe z systemem można nawiązać za pomocą modemu i protokołu PPP. Ponadto jedynym modemem, którego można użyć przy łączeniu, jest modem 7852-400 elektronicznego wsparcia klienta (ECS).



Rysunek 4. Łączenie z systemem klientów zdalnych korzystających z łącz komutowanych

Rozwiązanie

Domowy komputer PC z danym systememu można połączyć za pomocą modemu przy wykorzystaniu protokołu PPP. Jeśli do tego typu połączeń używany jest modem ECS, należy upewnić się, że jest on skonfigurowany do pracy zarówno w trybie synchronicznym, jak i asynchronicznym. Na rysunku przedstawiono system z usługami PPP,

połączony z siecią lokalną, zawierającą dwa komputery PC. Zdalny użytkownik łączy się telefonicznie z systemem. Jego system sam się uwierzytelnia i staje się częścią sieci przedsiębiorstwa (192.168.1.0). W tym przypadku klientowi łączącemu się telefonicznie łatwiej jest przydzielić statyczny adres IP.

Zdalny użytkownik uwierzytelnia się w systemie za pomocą protokołu Challenge Handshake Authentication Protocol (CHAP-MD5). System nie może użyć MS_CHAP, dlatego należy upewnić się, że klient PPP używa protokołu CHAP-MD5.

Jeśli zdalni użytkownicy mają mieć dostęp do sieci LAN, tak jak to opisano powyżej, należy włączyć zarówno przekazywanie IP na stosie TCP/IP, jak i profil odbiorcy PPP, a routing protokołu IP musi być należycie skonfigurowany. Jeśli istnieje potrzeba ograniczenia lub zabezpieczenia działań wykonywanych przez zdalnego klienta, do obsługi pakietów IP można wykorzystać reguły filtrowania.

Wcześniejszy rysunek przedstawia tylko jednego klienta połączenia modemowego, ponieważ modem elektronicznego wsparcia klienta może jednocześnie obsłużyć tylko jedno połączenie.

Przykład konfiguracji

Aby ustawić przykładową konfigurację PPP z poziomu programu System i Navigator, wykonaj następujące czynności:

1. Skonfiguruj Dial-up Networking i utwórz połączenie modemowe na zdalnym komputerze PC.
2. Skonfiguruj profil połączenia odbiorcy w swoim systemie.

   Należy wprowadzić poniższe informacje:

   - **Typ protokołu**: PPP
   - **Typ połączenia**: Linia komutowana
   - **Tryb pracy**: Odbieranie
   - **Konfiguracja linii**: może to być, w zależności od środowiska, linia pojedyncza lub pula linii.
3. Na stronie Ogólne we Właściwościach nowego profilu połączenia punkt z punktem wprowadź nazwę i opis profilu odbiorcy.
4. Kliknij przycisk **Połączenie**, aby otworzyć stronę Połączenie. Wybierz odpowiednią **Nazwę linii** lub utwórz nową, wpisując jej nazwę, i kliknij przycisk **Nowa**.
   a. Wyróżnij na stronie Ogólne istniejące zasoby sprzętowe, do których podłączony jest adapter 7852-400, i wybierz wartość **Asynchroniczne** w polu Ramki.
   b. Kliknij przycisk **Modem**, aby otworzyć stronę Modem. Z listy wyboru nazw wybierz modem **IBM 7852–400**.
   c. Kliknij **OK**, aby powrócić do strony Właściwości nowego profilu połączenia punkt z punktem.
5. Kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie.
   a. Wybierz opcję **Wymagana weryfikacja przez serwer iSeries tożsamości systemu zdalnego**.
   b. Zaznacz **Uwierzytelniaj lokalnie wykorzystując listę weryfikacji**, aby dodać nowego, zdalnego użytkownika do listy weryfikacji.
   c. Zaznacz **Zezwalaj na zaszyfrowane hasło (CHAP-MD5)**.
6. Kliknij przycisk **Ustawienia TCP/IP**, aby otworzyć stronę TCP/IP.
   a. Zaznacz lokalny adres IP 192.168.1.1.
   b. Dla zdalnego adresu IP wybierz opcję **Stały adres IP (Fixed IP address)**, podając początkowy adres 192.168.1.11.
   c. Zaznacz **Zezwalaj systemowi zdalnemu na dostęp do innych sieci (Allow remote system to access other networks)**.
7. Kliknij **OK**, aby zakończyć.

Pojęcia pokrewne

“Planowanie protokołu PPP” na stronie 31
Planowanie protokołu PPP obejmuje tworzenie połączeń PPP i administrowanie nimi.

Zadania pokrewne

“Tworzenie profilu połączenia” na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Odsyłacze pokrewne

“Protokół Challenge Handshake Authentication Protocol (CHAP) z MD5” na stronie 44
Protokół Challenge Handshake Authentication Protocol (CHAP-MD5) korzysta z algorytmu (MD-5) do obliczenia wartości znanej tylko systemowi uwierzytelniającemu i urządzeniu zdalnemu.

“Konfigurowanie połączenia” na stronie 50
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

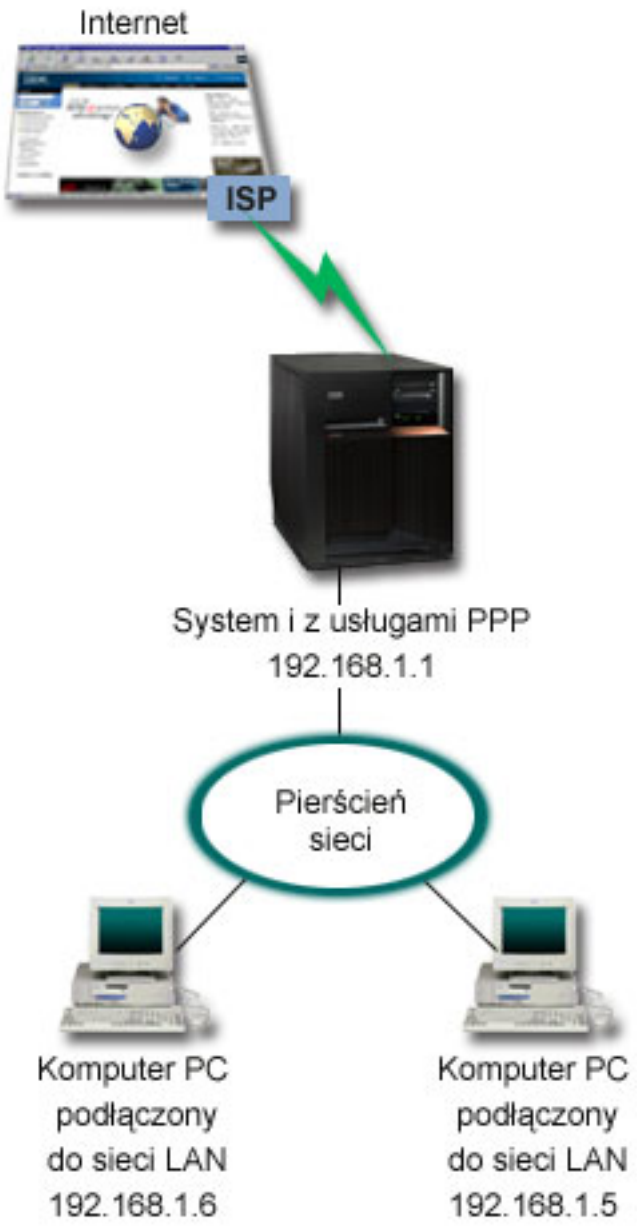
“Pula linii” na stronie 51
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP używające linii z puli linii. Podczas uruchamiania połączenia PPP system wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie system nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu

Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia systemu z dostawcą ISP mogą użyć modemu. Komputery PC przyłączone do sieci LAN mogą łączyć się z Internetem korzystając z systemu operacyjnego i5/OS jako bramy.

Sytuacja

Aplikacje używane w firmie wymagają, aby użytkownicy mieli dostęp do Internetu. Jeśli aplikacja nie wymaga wymiany dużej ilości danych, do połączenia systemu i klientów PC w sieci LAN z Internetem można użyć modemu. Poniższy rysunek przedstawia przykład takiej sytuacji.



Rysunek 5. Łączenie lokalnej sieci biurowej z Internetem przez modem

Rozwiązanie

Do połączenia systemu z dostawcą ISP można użyć modemu zintegrowanego (lub innego kompatybilnego). Aby ustanowić połączenie PPP z dostawcą ISP, należy utworzyć w systemie profil nadawcy PPP.

Po ustanowieniu połączenia między systemem i dostawcą ISP komputery PC w sieci LAN mogą komunikować się z Internetem używając tego systemu jako bramy. W profilu nadawcy należy upewnić się, czy opcja Ukryj adresy (Hide addresses) jest włączona. Umożliwia ona klientom sieci LAN z wewnętrznymi adresami IP komunikowanie się z Internetem.

Po połączeniu systemu i sieci LAN z Internetem należy zapoznać się z możliwymi zagrożeniami z tym związanymi. Współpraca z dostawcą ISP pomoże zapoznać się z jego strategią bezpieczeństwa. Dzięki temu stanie się możliwe podjęcie działań mających na celu zabezpieczenie sieci i systemu.

W zależności od tego, do czego wykorzystywany jest Internet, problemem może okazać się przepustowość.

Przykład konfiguracji

Aby ustawić przykładową konfigurację z poziomu programu System i Navigator, wykonaj następujące czynności:

1. Skonfiguruj profil połączenia nadawcy w swoim systemie.

   Należy wybrać następujące informacje:

   - **Typ protokołu**: PPP
   - **Typ połączenia**: Linia komutowana
   - **Tryb pracy**: Wybieranie
   - **Konfiguracja linii**: może to być, w zależności od środowiska, linia pojedyncza lub pula linii.
2. Na stronie Ogólne we Właściwościach nowego profilu połączenia punkt z punktem, wprowadź nazwę i opis profilu nadawcy.
3. Kliknij przycisk **Połączenie**, aby otworzyć stronę Połączenie. Wybierz odpowiednią Nazwę linii lub utwórz nową, wpisując jej nazwę, i kliknij **Nowa**.
   a. Na stronie Ogólne właściwości nowej linii wyróżnij istniejące zasoby sprzętowe. Jeśli zostanie zaznaczony zasób modemu wewnętrznego, typ modemu i typ ramki zostaną określone automatycznie.
   b. Kliknij **OK**, aby powrócić do strony Właściwości nowego profilu połączenia punkt z punktem.
4. Kliknij przycisk **Dodaj** i wpisz numer telefoniczny, aby połączyć się z serwerem dostawcy ISP. Należy uwzględnić wszystkie wymagane przedrostki.
5. Kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie, wybierz opcję **Zezwalaj zdalnemu systemowi na weryfikację tożsamości tego serwera iSeries**. Wybierz protokół uwierzytelniający i wprowadź informacje dotyczące nazwy użytkownika i hasła.
6. Kliknij przycisk **Ustawienia TCP/IP**, aby otworzyć stronę TCP/IP.
   a. Zaznacz **Przypisany do lokalnego adresu** zarówno dla lokalnego, jak i zdalnego adresu.
   b. Zaznacz **Dodaj system zdalny jako trasę domyślną**.
   c. Sprawdź **Ukryte adresy**, aby upewnić się, że wewnętrzny adres IP nie jest przekierowany do Internetu.
7. Kliknij przycisk **DNS**, aby otworzyć stronę DNS i wprowadź adres IP serwera DNS udostępnionego przez dostawcę ISP.
8. Kliknij **OK**, aby zakończyć.

Aby użyć profilu połączenia w celu połączenia się z Internetem, kliknij go prawym przyciskiem myszy w programie System i Navigator i wybierz **Start**. Jeśli status został zmieniony na **Aktywny**, połączenie powiodło się. Odśwież widok ekranu.

Uwaga: Należy upewnić się również, że w innych systemach w sieci zdefiniowano poprawnie routing, tak że generowany przez nie ruch TCP/IP związany z dostępem do Internetu jest wysyłany przez skonfigurowany system.

Pojęcia pokrewne

“Planowanie protokołu PPP” na stronie 31
Planowanie protokołu PPP obejmuje tworzenie połączeń PPP i administrowanie nimi.

Zadania pokrewne

“Tworzenie profilu połączenia” na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Odsyłacze pokrewne

“Pula linii” na stronie 51
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP używające linii z puli linii. Podczas uruchamiania połączenia PPP system wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie system nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

“Konfigurowanie połączenia” na stronie 50
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu

Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Protokołem PPP można połączyć ze sobą dwie sieci lokalne, ustanawiając połączenie między jednym systemem znajdującym się w centrali i drugim, znajdującym się w oddziale.

Sytuacja

Zakładamy, że sieci LAN w centrali i w oddziałach znajdują się w różnych miejscach. Każdego dnia oddział musi połączyć się z centralą, aby wymienić informacje znajdujące się w bazach danych. Ponieważ ilość przesyłanych danych nie wymusza zakupu stałego łącza, do połączenia obu sieci wykorzystywany jest modem.

Rysunek 6. Łączenie sieci korporacyjnej z sieciami zdalnymi za pomocą modemu

Rozwiązanie

Z pomocą protokołu PPP można połączyć ze sobą dwie sieci lokalne, ustanawiając połączenie między systemami, jak pokazano to na rysunku. W takim przypadku zakładamy, że oddział inicjuje połączenie z centralą. W systemie zdalnym konfigurowany jest profil nadawcy, a w systemie w centrali - profil połączenia odbiorcy.

Jeśli komputery znajdujące się w oddziale wymagają dostępu do sieci LAN (192.168.1.0), wówczas profil odbiorcy w centrali powinien mieć włączone przekazywanie IP i włączony routing adresów IP dla komputerów PC (w tym przykładzie oznaczonych jako: 192.168.2, 192.168.3, 192.168.1.6 i 192.168.1.5). Należy także uaktywnić przekazywanie IP dla stosu TCP/IP. Taka konfiguracja umożliwia podstawową komunikację TCP/IP między sieciami LAN. Przy rozstrzyganiu nazw hostów między sieciami LAN należy wziąć pod uwagę serwer DNS i względy bezpieczeństwa.

Przykład konfiguracji

Aby ustawić przykładową konfigurację z poziomu programu System i Navigator, wykonaj następujące czynności:

1. Skonfiguruj profil połączenia nadawcy w systemie zdalnym.

   Należy wybrać następujące informacje:

   - **Typ protokołu**: PPP
   - **Typ połączenia**: Linia komutowana
   - **Tryb pracy**: Wybieranie
   - **Konfiguracja linii**: może to być, w zależności od środowiska, linia pojedyncza lub pula linii.
2. Na stronie Ogólne we Właściwościach nowego profilu połączenia punkt z punktem, wprowadź nazwę i opis profilu nadawcy.
3. Kliknij przycisk **Połączenie**, aby otworzyć stronę Połączenie. Wybierz odpowiednią Nazwę linii lub utwórz nową, wpisując jej nazwę, i kliknij **Nowa**.
   a. Na stronie Ogólne we właściwościach linii wyróżnij istniejące zasoby sprzętowe i ustaw Ramki na **Asynchroniczne**.
   b. Kliknij przycisk **Modem**, aby otworzyć stronę Modem. Z listy wyboru nazw wybierz modem, którego używasz.
   c. Kliknij **OK**, aby powrócić do strony Właściwości nowego profilu połączenia punkt z punktem.
4. Kliknij przycisk **Dodaj** (Add) i wpisz numer telefonu do systemu znajdującego się w centrali. Należy podać wszystkie wymagane przedrostki.
5. Kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie, a następnie wybierz opcję **Zezwalaj zdalnemu systemowi na weryfikację tożsamości tego serwera iSeries**. Wybierz **Żądaj hasła szyfrowanego (CHAP-MD5)** (Require encrypted password (CHAP-MD5)) i wprowadź wymagane informacje dotyczące nazwy użytkownika i hasła.
6. Kliknij przycisk **Ustawienia TCP/IP**, aby otworzyć stronę Ustawienia TCP/IP.
   a. Z pola wyboru **Używaj stałych adresów IP** wybierz dla lokalnego adresu IP adres interfejsu LAN oddziału (192.168.2.1).
   b. Dla zdalnego adresu IP wybierz **Przypisany przez system zdalny**.
   c. W sekcji routingu zaznacz **Dodaj system zdalny jako trasę domyślną**.
   d. Kliknij **OK**, aby zakończyć.
7. Skonfiguruj profil połączenia odbiorcy w systemie w centrali.

   Należy wybrać następujące informacje:

   - **Typ protokołu**: PPP
   - **Typ połączenia**: Linia komutowana
   - **Tryb pracy**: Odbieranie
   - **Konfiguracja linii**: może to być, w zależności od środowiska, linia pojedyncza lub pula linii.

8. Na stronie Ogólne we Właściwościach nowego profilu połączenia punkt z punktem wprowadź nazwę i opis profilu odbiorcy.
9. Kliknij przycisk **Połączenie**, aby otworzyć stronę Połączenie. Wybierz odpowiednią Nazwę linii lub utwórz nową, wpisując jej nazwę, i kliknij **Nowa**.
   a. Na stronie Ogólne wyróżnij istniejące zasoby sprzętowe i ustaw Ramki na **Asynchroniczne**.
   b. Kliknij przycisk **Modem**, aby otworzyć stronę Modem. Z listy wyboru nazw wybierz modem, którego używasz.
   c. Kliknij **OK**, aby powrócić do strony Właściwości nowego profilu połączenia punkt z punktem.
10. Kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie.
    a. Zaznacz pole **Wymagana weryfikacja przez serwer iSeries tożsamości systemu zdalnego**.
    b. Dodaj nowego użytkownika do listy weryfikacji.
    c. Sprawdź uwierzytelnianie przy pomocy algorytmu CHAP-MD5.
11. Kliknij przycisk **Ustawienia TCP/IP**, aby otworzyć stronę Ustawienia TCP/IP.
    a. Jako lokalny adres IP wybierz w polu **wyboru** adres IP interfejsu centrali (192.168.1.1).
    b. Dla zdalnego adresu IP zaznacz **Bazuje na identyfikatorze użytkownika systemu zdalnego**. Zostanie wyświetlone okno dialogowe **Adresy IP zdefiniowane dla nazwy użytkownika**. Kliknąć przycisk **Dodaj**. Wypełnij pola związane z Nazwą użytkownika wywołującego, adresem IP i maską podsieci. W tym scenariuszu odpowiednie będą następujące ustawienia:
       - Nazwa użytkownika nawiązującego połączenie: Strona_zdalna
       - Adres IP: 192.168.2.1
       - Maska podsieci: 255.255.255.0

       Kliknij **OK**, a następnie kliknij **OK** ponownie, aby powrócić do strony Ustawienia TCP/IP.
    c. Zaznacz **Przekazywanie IP** (IP forwarding), aby inne systemy w tej sieci mogły używać systemu jako bramy.
12. Kliknij **OK**, aby zakończyć.

Zadania pokrewne

"Tworzenie profilu połączenia" na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Odsyłacze pokrewne

"Konfigurowanie połączenia" na stronie 50
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

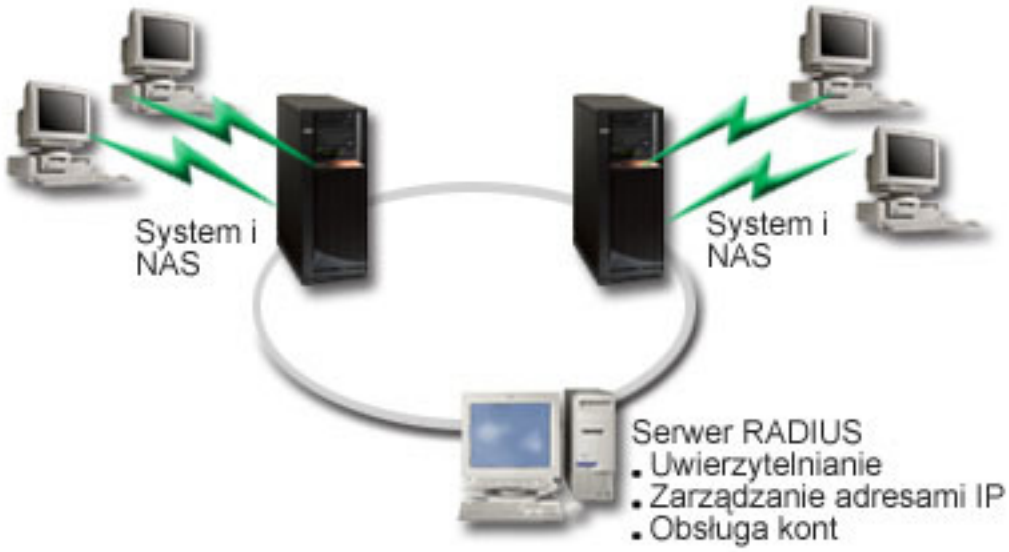
"Pula linii" na stronie 51
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP używające linii z puli linii. Podczas uruchamiania połączenia PPP system wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie system nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS

Serwer dostępu do sieci (Network Access Server - NAS) działający w systemie może kierować żądania uwierzytelnienia od klientów z połączeniem modemowym do odrębnego serwera RADIUS (Remote Authentication Dial In User Service). Po uwierzytelnieniu serwer RADIUS może również sterować adresami IP przydzielonymi użytkownikowi.

Sytuacja

W sieci firmowej pracują zdalni użytkownicy uzyskujący dostęp do dwóch systemów z sieci rozproszonej z połączeniem modemowym. Potrzebne jest scentralizowanie uwierzytelniania, usług i rozliczania, umożliwiające jednemu systemowi obsługę żądań sprawdzenia ID i haseł użytkowników oraz określenia adresów IP do nich przypisanych.



Rysunek 7. Uwierzytelnianie połączeń modemowych za pomocą serwera RADIUS

Rozwiązanie

Podczas próby nawiązania połączenia serwer NAS działający w systemie przekazuje dane dotyczące uwierzytelniania do sieciowego serwera RADIUS. Serwer ten, obsługujący wszystkie dane dotyczące uwierzytelniania dla sieci, przetwarza zgłoszenie dotyczące uwierzytelniania i odpowiada na nie. Jeśli użytkownik zostanie sprawdzony, odpowiednio skonfigurowany serwer RADIUS może przydzielić adres IP w sieci i uruchomić rozliczanie aktywności użytkownika i użycia zasobów. Do obsługi serwera RADIUS należy zdefiniować w systemie serwer RADIUS NAS.

Przykład konfiguracji

Aby ustawić przykładową konfigurację z poziomu programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń opcję **Sieć** (Network), kliknij prawym przyciskiem myszy **Usługi zdalnego dostępu** (Remote Access Services) i wybierz opcję **Usługi** (Services).
2. Na karcie **RADIUS** wybierz opcje **Włącz połączenie RADIUS Network Access Server** (Enable RADIUS Network Access Server connection) i **Włącz RADIUS dla uwierzytelniania** (Enable RADIUS for authentication). W zależności od wybranego rozwiązania RADIUS, można wybrać także obsługę rozliczenia połączenia i konfigurację adresu TCP/IP.
3. Kliknij przycisk **Ustawienia RADIUS NAS**.
4. Na stronie Ogólne wprowadź opis tego serwera.
5. Na stronie Serwer uwierzytelniania (i opcjonalnie Serwer rozliczania) kliknij **Dodaj** i wprowadź następujące dane:
   a. W polu **Lokalny adres IP** (Local IP address) wpisz adres IP interfejsu używanego do nawiązania połączenia z serwerem RADIUS.
   b. W polu **Adres IP serwera** (Server IP address) wpisz adres IP serwera RADIUS.
   c. W polu **Hasło** (Password) wpisz hasło używane do identyfikacji systemu na serwerze RADIUS.
   d. W polu **Port** wpisz port systemu, używany do komunikacji z serwerzem RADIUS. Wartością domyślną dla serwera uwierzytelniającego jest port 1812, a dla serwera rozliczającego port 1813.
6. Kliknij przycisk **OK**.
7. W programie System i Navigator rozwiń swój system i kolejno **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).

8. Wybierz profil połączenia, który będzie korzystał z serwera RADIUS do uwierzytelniania. Usługi RADIUS są dostępne tylko dla profili połączeń odbiorcy.
9. Na stronie Uwierzytelnianie wybierz opcję **Wymagane przez serwer iSeries do weryfikacji tożsamości systemu zdalnego**.
10. Wybierz **Uwierzytelnianie zdalne przy użyciu serwera RADIUS**.
11. Wybierz protokół uwierzytelniania (PAP lub CHAP-MD5). Protokół ten musi być także używany przez serwer RADIUS.
12. Wybierz **Use RADIUS for connection editing and accounting**.
13. Kliknij **OK**, aby zachować zmiany w profilu połączenia.

Niezbędne jest także skonfigurowanie serwera RADIUS, w tym obsługi protokołu uwierzytelniania, danych o użytkownikach, hasłach i rozliczeniu. Więcej informacji na ten temat powinien zapewnić dostawca serwera RADIUS.

Gdy użytkownicy łączą się, korzystając z tego profilu połączenia, system przekazuje dane dotyczące uwierzytelnienia do określonego serwera RADIUS. Po pomyślnym sprawdzeniu użytkownika zestawiane jest połączenie z zastosowaniem ograniczeń określonych w danych użytkownika o serwerze RADIUS.

Zadania pokrewne

“Udostępnianie usług RADIUS i DHCP profilom połączeń” na stronie 61
Poniżej przedstawiono procedurę udostępniania usług RADIUS i DHCP (Dynamic Host Configuration Protocol) profilom połączeń odbiorców.

Odsyłacze pokrewne

“Uwierzytelnianie systemu” na stronie 43
Połączenia PPP z platformą System i obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów nawiązujących połączenie z systemem, jak i połączeń wychodzących do dostawcy ISP lub innego systemu.

“Protokół RADIUS (Remote Authentication Dial In User Service) - przegląd” na stronie 45
RADIUS (Remote Authentication Dial In User Service) jest standardowym protokołem internetowym, który udostępnia usługi scentralizowanego uwierzytelniania, obsługi kont i zarządzania adresami IP w sieci rozproszonej z połączeniem modemowym dla użytkowników mających zdalny dostęp.

Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP

Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Sytuacja

W sieci jest kilka grup rozproszonych użytkowników, z których każda potrzebuje dostępu do innych zasobów firmowej sieci lokalnej. Grupa użytkowników wprowadzających dane potrzebuje dostępu do bazy danych oraz kilku innych aplikacji. Grupa osób z innych firm potrzebuje połączenia modemowego i dostępu do usług takich jak HTTP, FTP czy Telnet, ale ze względów bezpieczeństwa nie mogą mieć dostępu do innych usług TCP/IP i ruchu w sieci. Zdefiniowanie szczegółowych atrybutów połączenia i uprawnień dla każdego użytkownika wymaga dodatkowej pracy, a wprowadzenie ograniczeń sieciowych dla wszystkich użytkowników tego profilu połączenia nie zapewni wystarczającej kontroli. Potrzebne jest zdefiniowanie ustawień połączenia i uprawnień dla kilku odrębnych grup użytkowników stale łączących się z systemem połączeniem modemowym.

Rysunek 8. Zastosowanie ustawień połączenia do połączeń modemowych w oparciu o ustawienia strategii dla grupy

Rozwiązanie

Należy zastosować odrębne ograniczenia filtrowania IP dla dwóch różnych grup użytkowników. Aby to osiągnąć, należy utworzyć strategie dostępu do grup i reguły filtrowania IP. Strategie dostępu do grup odnoszą się do reguł filtrowania IP, dlatego najpierw należy utworzyć reguły filtrowania. W niniejszym przykładzie jest używany filtr PPP zawierający reguły filtrowania IP dla strategii dostępu dla grupy ″Partner handlowy IBM″. Reguły te zezwalają na korzystanie z usług HTTP, FTP i Telnet, ale ograniczają dostęp przez system do pozostałego ruchu TCP/IP oraz innych usług. Scenariusz ten pokazuje reguły filtrowania tylko dla grupy handlowców, można jednak skonfigurować podobne filtry dla grupy Wprowadzanie danych.

Ostatecznie, aby zdefiniować grupę, należy utworzyć strategie dostępu do grupy (po jednej dla każdej grupy). Strategia dostępu dla grupy umożliwia zdefiniowanie wspólnych atrybutów połączenia dla grupy użytkowników. Dodając strategię dostępu dla grupy do listy sprawdzania w systemie, można zastosować ustawienia połączenia podczas procesu uwierzytelniania. Strategia dostępu dla grupy określa kilka ustawień dla sesji użytkownika, włącznie z możliwością zastosowania reguł filtrowania IP, ograniczających adresy IP i usługi TCP/IP dostępne dla użytkownika podczas sesji.

Przykład konfiguracji

Aby ustawić przykładową konfigurację z poziomu programu System i Navigator, wykonaj następujące czynności:

1. Utwórz identyfikator filtru PPP i filtry reguł pakietów IP, które określą uprawnienia i ograniczenia dla tej strategii dostępu dla grupy.
   a. W programie System i Navigator rozwiń swój system i kolejno **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
   b. Kliknij **Profile połączenia odbiornika** i wybierz opcję Strategie dostępu dla grup.
   c. Prawym przyciskiem myszy kliknij nazwę predefiniowaną grupę w prawym panelu i wybierz opcję **Właściwości**.

      Uwaga: Aby utworzyć nową strategię dostępu dla grupy, kliknij prawym przyciskiem myszy **Strategie dostępu dla grupy** (Group Access Policies) i wybierz opcję **Nowa strategia dostępu dla grupy** (New Group Access Policies). Wypełnij kartę **Ogólne** (General). Następnie wybierz zakładkę **Ustawienia TCP/IP** (TCP/IP Settings) i przejdź do kroku e poniżej.
   d. Wybierz zakładkę **Ustawienia TCP/IP** (TCP/IP Settings) i kliknij **Zaawansowane** (Advanced).
   e. Wybierz **Użyj reguł pakietów IP** i kliknij **Edit Rules File (Edycja zbioru reguł)**. Zostanie uruchomiony edytor reguł pakietów IP i otworzony zbiór reguł pakietów filtrów PPP.

f. Otwórz menu **Insert** i wybierz **Filters**, aby dodać zestawy filtrów. Na karcie **Ogólne** (General) zdefiniuj zestawy filtrów, a na karcie **Usługi** (Services) - dozwolone usługi, na przykład HTTP. Poniższy zestaw filtrów, ″reguly_uslug″, zezwala na usługi HTTP, FTP i Telnet. Reguły filtrowania obejmują niejawne, domyślne instrukcje odmowy, ograniczające wszystkie niedozwolone usługi TCP/IP i ruch IP.

Uwaga: Adresy IP w tym przykładzie są poprawne w sieci i służą tylko jako przykład.

```
###Następujące 2 filtry zezwalają na ruch HTTP (przeglądarka WWW) w systemie i poza systemem.

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

###Następujące 4 filtry zezwalają na ruch FTP w systemie i poza systemem.

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF
###Następujące 2 filtry zezwalają na ruch telnet w systemie i poza systemem.

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

g. Otwórz menu **Insert** i wybierz opcję **Filter Interface**. Przy użyciu interfejsu filtru utwórz identyfikator filtru i dołącz zdefiniowane zestawy filtrów.

   1) Na karcie **Ogólne** (General) wpisz dozwolone_uslugi jako identyfikator filtru PPP.
   2) Na karcie **Zestawy filtrów** (Filter sets) wybierz zestaw filtrów **reguly_uslug** i kliknij przycisk **Dodaj** (Add).
   3) Kliknij przycisk OK. Do pliku reguł zostanie dodany następujący wiersz:

```
###Następujące instrukcje przypisują (wiążą) zestaw filtrów "reguly_uslug" z
identyfikatorem filtru PPP "dozwolone_uslugi".
Identyfikator filtru może zostać zastosowany na fizycznym interfejsie powiązanym z profilem
połączenia PPP lub strategią dostępu do grup.

FILTER_INTERFACE PPP_FILTER_ID = dozwolone_uslugi SET = reguly_uslug
```

h. Składuj zmiany i wyjdź. Jeśli zechcesz cofnąć zmiany, w interfejsie znakowym wpisz komendę RMVTCPTBL *ALL. Usunie ona z systemu wszystkie reguły filtrowania oraz translacje NAT.

i. W oknie dialogowym **Zaawansowane ustawienia TCP/IP** (Advanced TCP/IP settings) pozostaw puste pole **Identyfikator filtru PPP** (PPP filter identifier) i kliknij przycisk **OK**, aby wyjść. Następnie zastosuj utworzony identyfikator filtru do strategii dostępu dla grupy, nie do profilu połączenia.

2. Zdefiniuj nową strategię dostępu dla grupy dla tej grupy użytkowników.

a. W programie System i Navigator wybierz swój system i rozwiń kolejno **Sieć → Usługi zdalnego dostępu → Profile połączenia odbiorcy** (Network > Remote Access Services > Receiver Connection Profiles).
b. Kliknij prawym przyciskiem myszy ikonę **Strategia dostępu dla grupy** (Group Access Policy) i wybierz **Nowa strategia dostępu dla grupy** (New Group Access Policy). W programie System i Navigator zostanie wyświetlone okno dialogowe **Definiowanie nowej strategii dostępu dla grupy** (New Group Access Policy definition).
c. Na stronie Ogólne (General) wprowadź nazwę i opis strategii dostępu dla grupy.
d. Na stronie Ustawienia TCP/IP:
   - Wybierz **Dla tego połączenia użyj reguł pakietów IP** i wybierz identyfikator filtru PPP **dozwolone_uslugi**.
e. Wybierz **OK**, aby zapisać strategię dostępu dla grupy.

3. Zastosuj strategię dostępu dla grupy użytkowników powiązanych z tą grupą.
   a. Otwórz profil połączenia odbiorcy sterujący tymi połączeniami modemowymi.
   b. Na stronie Uwierzytelnianie (Authentication) profilu połączenia odbiorcy wybierz listę sprawdzania, która zawiera informacje uwierzytelniające użytkowników i kliknij przycisk **Otwórz** (Open).
   c. Z grupy Sprzedaż (Sales) wybierz użytkownika, dla którego chcesz zastosować strategię dostępu dla grupy, i kliknij **Otwórz** (Open).
   d. Kliknij **Zastosuj strategię grupy do użytkownika** (Apply a Group Policy to the user) i wybierz strategię dostępu dla grupy zdefiniowaną w kroku 2.
   e. Powtórz czynności dla każdego użytkownika grupy Sprzedaż.

Pojęcia pokrewne

“Konfigurowanie strategii dostępu dla grupy” na stronie 59
Folder **Strategie dostępu do grupy** w katalogu Profile połączenia odbiorcy zawiera opcje umożliwiające konfigurowanie parametrów połączenia dla grupy zdalnych użytkowników. Dotyczą one tylko połączeń PPP pochodzących ze zdalnych systemów i odbieranych w systemie lokalnym.

“Obsługa strategii dostępu dla grup” na stronie 4
Obsługa strategii dostępu dla grup umożliwia administratorom sieci definiowanie strategii dla grup użytkowników w celu zarządzania zasobami. Poszczególni użytkownicy są przypisywani do strategii kontroli dostępu w momencie wpisywania się w sesji PPP lub L2TP.

Zadania pokrewne

“Tworzenie profilu połączenia” na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

“Przypisywanie reguł filtrowania pakietów IP do połączeń PPP” na stronie 61
Dzięki zbiorowi reguł pakietów można ograniczyć dostęp użytkownika lub grupy użytkowników do adresów IP w sieci.

Odsyłacze pokrewne

“Lista weryfikacji” na stronie 46
Lista weryfikacji jest wykorzystywana do przechowywania identyfikatorów użytkowników i haseł dla zdalnych użytkowników.

“Uwierzytelnianie systemu” na stronie 43
Połączenia PPP z platformą System i obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów nawiązujących połączenie z systemem, jak i połączeń wychodzących do dostawcy ISP lub innego systemu.

Informacje pokrewne

Filtrowanie IP i translacja adresów sieciowych

Scenariusz: współużytkowanie modemu między partycjami logicznymi za pomocą protokołu L2TP

Między czterema partycjami logicznymi skonfigurowana jest wirtualna sieć Ethernet. Wybrane partycje logiczne mają współużytkować modem w celu uzyskania dostępu do zewnętrznej sieci LAN.

Sytuacja

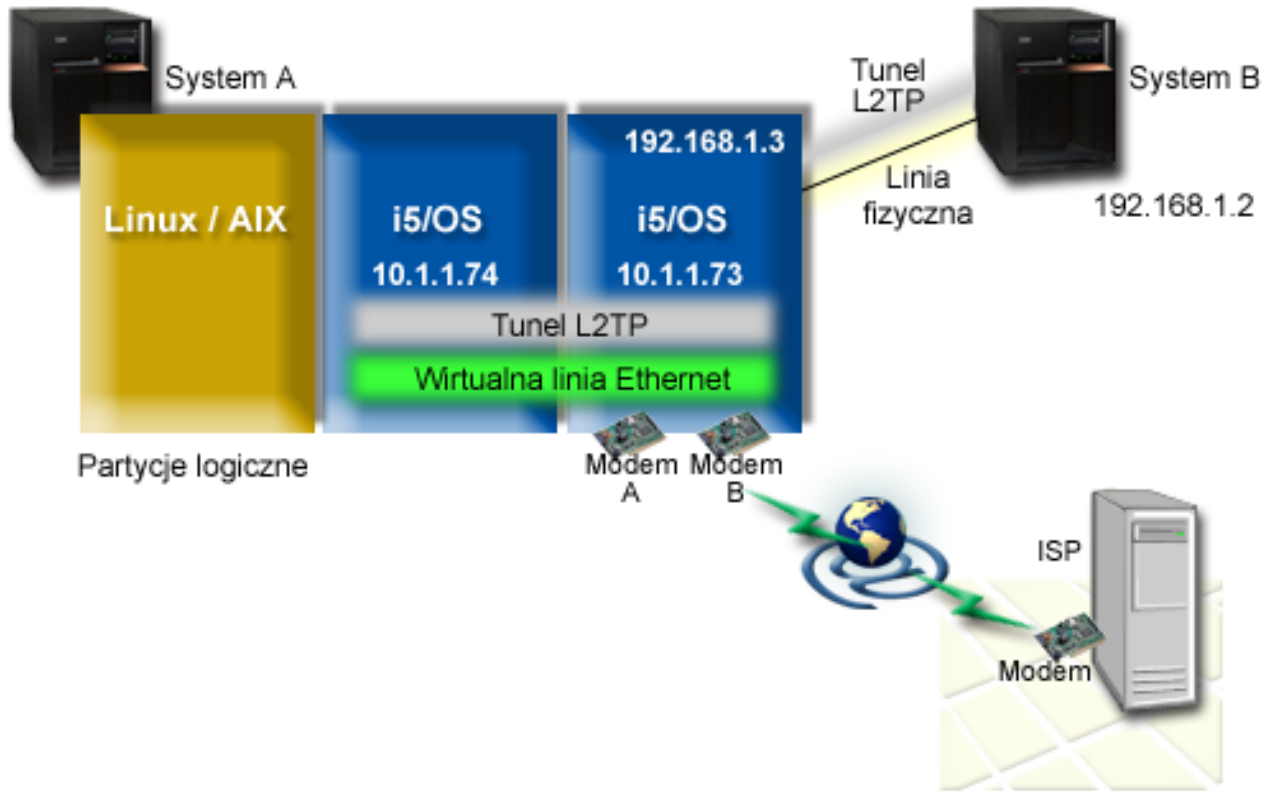
Użytkownik jest administratorem systemu w średniej wielkości przedsiębiorstwie. Nadszedł czas na modernizację sprzętu, ale przy okazji chciałby on zrobić trochę więcej: usprawnić jego działanie. Proces ten rozpocznie się od konsolidacji trzech dotychczasowych systemów w jeden system. W systemie są tworzone trzy partycje logiczne. Nowy system jest dostarczony z modemem wewnętrznym 2793. W tym egzemplarzu jest to jedyny procesor wejścia/wyjścia (IOP), który obsługuje protokół PPP. Dostępny jest również stary modem elektronicznego wsparcia klienta 7852–400.

Rozwiązanie

Wiele systemów i partycji może współużytkować te same modemy do obsługi połączeń komutowanych, dzięki czemu nie ma potrzeby, aby każdy system lub partycja miały własny modem. Jest to możliwe, jeśli używane są tunele L2TP i jeśli konfiguracja profili L2TP zezwala na połączenia wychodzące. W omawianej sieci tunele będą tworzone na bazie wirtualnej sieci Ethernet i sieci fizycznej. Linia fizyczna jest połączona z innym systemem, który współużytkuje modemy w danej sieci.

Informacje szczegółowe

Poniższy rysunek ilustruje schemat sieci w tym scenariuszu:



Rysunek 9. Wiele systemów współużytkujących jeden modem w celu nawiązywania połączeń komutowanych

Wymagania wstępne i założenia

System A musi spełniać następujące wymagania konfiguracyjne:

- System i5/OS wersja 5 wydanie 3 lub nowszy, zainstalowany na partycji, której przydzielono modemy z obsługą połączeń asynchronicznych.
- Sprzęt umożliwiający partycjonowanie.

- Programy System i Access for Windows i System i Navigator (komponent Konfigurowanie i obsługa aplikacji System i Navigator), wersja 5 wydanie 3 lub nowsze.
- W systemie utworzono co najmniej dwie partycje logiczne (LPAR). Na partycji, do której należy modem, musi być zainstalowany system i5/OS V5R3 lub nowszy. Na pozostałych partycjach mogą być zainstalowane systemy operacyjne OS/400 V5R2, i5/OS V5R3, Linux lub AIX. W tym scenariuszu na partycjach zainstalowano system operacyjny i5/OS lub Linux.
- Do obsługi komunikacji między partycjami utworzono wirtualną sieć Ethernet.

System B musi mieć zainstalowane programy licencjonowane i odpowiednie komponenty programu System i Navigator: System i Access for Windows i System i Navigator (komponent Konfigurowanie i obsługa aplikacji System i Navigator) V5R2 lub nowsze.

Informacje pokrewne

Partycje logiczne

Szczegóły scenariusza: współużytkowanie modemu między partycjami logicznymi za pomocą protokołu L2TP

Po spełnieniu wymagań wstępnych można rozpocząć konfigurowanie profili L2TP.

Etap 1: konfigurowanie profilu terminatora L2TP dla dowolnego interfejsu na partycji, do której należą modemy:

Aby utworzyć profil terminatora dla dowolnego interfejsu, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Usługi zdalnego dostępu** (*system* > Network > Remote Access Services).
2. Prawym przyciskiem myszy kliknij **Profile połączenia odbiorcy** i wybierz opcję **Nowy profil**.
3. Na stronie Konfiguracja wybierz następujące opcje i kliknij przycisk **OK**:
   - **Typ protokołu**: PPP
   - **Typ połączenia**: L2TP (linia wirtualna)
   - **Tryb pracy**: Terminator (serwer sieciowy)
   - **Typ usługi linii**: Linia pojedyncza
4. Wypełnij poniższe pola na karcie **Nowy profil - ogólne** (New Profile - General):
   - **Nazwa**: toExternal
   - **Opis**: Połączenie odbiornika dla połączeń wychodzących
   - Wybierz opcję **Uruchom profil z TCP**.
5. Wypełnij poniższe pola na karcie **Nowy profil - połączenie** (New Profile - Connection).
   - **Adres IP punktu końcowego lokalnego tunelu**: ANY
   - **Nazwa linii wirtualnej**: toExternal. Z tą linią nie jest powiązany żaden interfejs fizyczny. Linia wirtualna opisuje różne cechy tego profilu PPP. Po otwarciu okna Właściwości linii L2TP (L2TP Line Properties) kliknij zakładkę **Uwierzytelnianie** (Authentication) i wprowadź nazwę hosta swojego systemu. Kliknij przycisk **OK**, aby wrócić do karty **Połączenie** (Connection) w oknie Właściwości nowego profilu PPP (New PPP Profile Properties).
6. Kliknij opcję **Zezwolenie na ustanowienie połączenia wychodzącego**. Zostanie wyświetlone okno dialogowe **Właściwości wybierania dla połączenia wychodzącego**.
7. Wybierz na stronie Właściwości wybierania dla połączenia wychodzącego typ usługi linii.
   - **Typ usługi linii**: Pula linii
   - **Nazwa**: dialOut
   - Kliknij **Nowa**. Zostanie wyświetlone okno dialogowe **Właściwości nowej puli linii**.
8. Wybierz w oknie Właściwości nowej puli linii linie i modemy, dla których połączenia wychodzące mają być dozwolone, i kliknij przycisk **Dodaj**. Jeśli istnieje potrzeba zdefiniowania tych linii, wybierz opcję **Nowa linia**.

Interfejsy na partycji, do której należą te modemy, będą próbowały użyć którejkolwiek z otwartych linii w tej puli. Zostanie wyświetlone okno Właściwości nowej linii (New Line Properties).

9. Wpisz odpowiednie informacje w następujących polach zakładki **Właściwości nowej linii - ogólne**:
   - **Nazwa**: line1
   - **Opis**: Pierwsza linia i pierwszy modem w puli linii (modem wewnętrzny 2793)
   - **Zasoby sprzętu**: cmn03 (port komunikacyjny)
10. Na wszystkich pozostałych zakładkach zatwierdź wartości domyślne i kliknij **OK**, aby powrócić do okna Właściwości nowej puli linii.
11. Wybierz w oknie Właściwości nowej puli linii linie i modemy, dla których połączenia wychodzące mają być dozwolone, i kliknij **Dodaj**. Sprawdź, czy dla puli wybrany jest modem 2793.
12. Ponownie wybierz opcję **Nowa linia** (New Line), aby dodać modem elektronicznego wsparcia klienta 7852–400. Zostanie wyświetlone okno Właściwości nowej linii (New Line Properties).
13. Wpisz odpowiednie informacje w następujących polach zakładki **Właściwości nowej linii - ogólne**:
   - **Nazwa**: line2
   - **Opis**: druga linia i drugi modem w puli linii (zewnętrzny modem elektronicznego wsparcia klienta 7852-400).
   - **Zasoby sprzętu**: cmn04 (port V.24).
   - **Ramki**: Asynchroniczne
14. Na karcie **Właściwości nowej linii - modem** (New Line Properties - Modem) wybierz modem zewnętrzny (7852–400) i kliknij przycisk **OK**, aby powrócić do okna Właściwości nowej puli linii.
15. Wybierz pozostałe dostępne linie, które chcesz dodać do puli, i kliknij **Dodaj**. W sytuacji opisywanej w niniejszym przykładzie sprawdź, czy dwa nowe modemy dodane w powyższych czynnościach znajdują się na liście w polu **Wybrane linie dla puli** i kliknij przycisk **OK**, aby powrócić do okna Właściwości wybierania dla połączeń wychodzących.
16. W oknie Właściwości wybierania dla połączeń wychodzących wpisz Domyślne wybierane numery i kliknij przycisk **OK**, aby powrócić do okna Właściwości nowego profilu PPP.

    Uwaga: Mogą to być na przykład numery dostawcy ISP, ponieważ będą one często wybierane przez inne systemy korzystające z tych modemów. Jeśli w innych systemach podano numer telefonu *PRIMARY lub *BACKUP, wybrane zostaną numery podane tutaj. Jeśli w innych systemach jest podany konkretny numer telefonu, to właśnie on zostanie użyty.
17. Na karcie **Ustawienia TCP/IP** (TCP/IP Settings) wybierz następujące wartości:
   - **Lokalny adres IP**: Brak
   - **Zdalny adres IP**: Brak

    Uwaga: Jeśli chcesz użyć profilu do zakończenia sesji L2TP, musisz uzyskać lokalny adres IP reprezentujący system. W przypadku zdalnego adresu IP można wybrać pulę adresów, które znajdują się w tej samej podsieci, co dany system. Wszystkie sesje L2TP pobierają swoje adresy IP z tej puli.
18. Na karcie **Uwierzytelnianie** (Authentication) zatwierdź wszystkie wartości domyślne.

Konfigurowanie profilu terminatora L2TP na partycji z modemami dobiegło końca. Następnym krokiem jest skonfigurowanie zdalnego wybierania L2TP profilu nadawcy dla adresu 10.1.1.74.

Odsyłacze pokrewne

“Obsługa profili połączeń wielokrotnych” na stronie 53
Profile połączeń PPP, które obsługują połączenia wielokrotne, umożliwiają obsługiwanie wielu połączeń cyfrowych, analogowych oraz L2TP za pomocą jednego profilu połączenia.

Etap 2: konfigurowanie profilu nadawcy protokołu L2TP dla adresu 10.1.1.74:

Poniżej przedstawiono tworzenie profilu nadawcy protokołu L2TP:

1. W programie System i Navigator rozwiń **10.1.1.74 → Sieć → Usługi zdalnego dostępu** (10.1.1.74 > Network > Remote Access Services).

2. Prawym przyciskiem myszy kliknij **Profile połączenia inicjatora** i wybierz opcję **Nowy profil**.
3. Na stronie Konfiguracja wybierz następujące opcje i kliknij przycisk **OK**:
   - **Typ protokołu**: PPP
   - **Typ połączenia**: L2TP (linia wirtualna)
   - **Tryb pracy**: Zdalne wybieranie
   - **Typ usługi linii**: Linia pojedyncza
4. Na karcie **Ogólne** (General) wypełnij następujące pola:
   - **Nazwa**: toModem
   - **Opis**: połączenie inicjatora kierowane do partycji z modemem.
5. Na karcie **Połączenie** (Connection) wypełnij następujące pola:

   Nazwa linii wirtualnej: toModem. Z tą linią nie jest powiązany żaden interfejs fizyczny. Linia wirtualna opisuje różne cechy tego profilu PPP. Zostanie wyświetlone okno Właściwości linii L2TP.
6. Na karcie **Ogólne** (General) wprowadź opis linii wirtualnej.
7. Na karcie **Uwierzytelnianie** (Authentication) wpisz nazwę hosta lokalnego dla partycji i kliknij przycisk **OK**, aby powrócić do strony Połączenie.
8. W polu **Zdalne numery telefoniczne** dodaj wartości *PRIMARY i *BACKUP. Dzięki temu profil będzie korzystał z tych samych numerów telefonicznych, co profil terminatora na partycji, do której należą modemy.
9. W polu **Nazwa hosta lub adres IP zdalnego punktu końcowego tunelu** wpisz adres zdalnego punktu końcowego tunelu (10.1.1.73).
10. Na karcie **Uwierzytelnianie** (Authentication) wybierz **Zezwalaj systemowi zdalnemu na sprawdzenie tożsamości tego serwera iSeries** (Allow the remote system to verify the identity of this iSeries server).
11. W polu określającym protokół uwierzytelniania wybierz opcję **Wymaga szyfrowanego hasła (CHAP-MD5)**. Domyślnie opcja **Zezwól na rozszerzalny protokół uwierzytelniania** również jest zaznaczona.

    Uwaga: Protokół powinien być zgodny z protokołem używanym przez system, z którym będzie nawiązywane połączenie.
12. Wpisz nazwę użytkownika i hasło.

    Uwaga: Nazwa użytkownika i hasło powinny być zgodne z dowolną poprawną nazwą użytkownika i hasłem w systemie, z którym nawiązywane jest połączenie.
13. Przejdź do zakładki **Ustawienia TCP/IP** i sprawdź wymagane pola:
    - **Lokalny adres IP**: Przypisywany przez system zdalny
    - **Zdalny adres IP**: Przypisywany przez system zdalny
    - **Routing**: Nie jest wymagany dodatkowy routing
14. Kliknij przycisk **OK**, aby zapisać profil PPP.

Etap 3: konfigurowanie profilu zdalnego wybierania L2TP dla adresu 192.168.1.2:

Aby skonfigurować profil zdalnego wybierania L2TP dla adresu 192.168.1.2, powtórz czynności, które zawiera Etap 2, zmieniając adres zdalnego punktu końcowego tunelu na 192.168.1.3 (interfejs fizyczny, z którym łączy się System B).

Uwaga: Podane adresy są fikcyjne i zostały użyte jako przykład.

Etap 4: testowanie połączenia:

Po skonfigurowaniu obu systemów należy przetestować połączenia, aby upewnić się, że systemy współużytkują modemy w celu nawiązania połączenia z sieciami zewnętrznymi.

1. Sprawdź, czy profil terminatora L2TP jest aktywny.
   a. W programie System i Navigator rozwiń **10.1.1.73 → Sieć → Usługi zdalnego dostępu → Profile połączenia odbiorcy** (10.1.1.73 > Network > Remote Access Services > Receiver Connection Profiles).

b. W prawym panelu znajdź żądany profil (toExternal) i sprawdź, czy w polu **Status** jest wartość Aktywny (Active). Jeśli nie, kliknij go prawym przyciskiem myszy i wybierz opcję **Start**.

2. Uruchom profil zdalnego wybierania w systemie 10.1.1.74.
   a. W programie System i Navigator rozwiń **10.1.1.74 → Sieć → Usługi zdalnego dostępu → Profile połączenia nadawcy** (10.1.1.74 > Network > Remote Access Services > Originator Connection Profiles).
   b. W prawym panelu znajdź żądany profil (toModem) i sprawdź, czy w polu **Status** jest wartość Aktywny (Active). Jeśli nie, kliknij go prawym przyciskiem myszy i wybierz opcję **Start**.
3. Uruchom profil zdalnego wybierania w systemie B.
   a. W programie System i Navigator rozwiń **192.168.1.2 → Sieć → Usługi zdalnego dostępu → Profile połączenia nadawcy** (192.168.1.2 > Network > Remote Access Services > Originator Connection Profiles).
   b. W prawym panelu znajdź utworzony profil i sprawdź, czy w polu **Status** wyświetlona jest wartość Aktywny (Active). Jeśli nie, kliknij go prawym przyciskiem myszy i wybierz opcję **Start**.
4. Jeśli to możliwe, uruchom komendę ping z adresem dostawcy ISP lub innego punktu docelowego, aby sprawdzić, czy próbna nawiązania połączenia zakończyła się powodzeniem i czy oba profile są aktywne. Należy spróbować uruchomić komendę ping z obu adresów: 10.1.1.74 i 192.168.1.2.
5. Można również sprawdzić status połączenia.
   a. W programie System i Navigator rozwiń **system → Sieć → Usługi zdalnego dostępu → Profile połączenia nadawcy** (system > Network > Remote Access Services > Originator Connection Profiles).
   b. W prawym panelu kliknij prawym przyciskiem myszy utworzony profil i wybierz opcję **Połączenia**. W oknie Status połączenia wyświetlone są profile aktywne, nieaktywne, w trakcie łączenia i inne.

Planowanie protokołu PPP

Planowanie protokołu PPP obejmuje tworzenie połączeń PPP i administrowanie nimi.

Odsyłacze pokrewne

"Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem" na stronie 13
Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

"Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu" na stronie 15
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia systemu z dostawcą ISP mogą użyć modemu. Komputery PC przyłączone do sieci LAN mogą łączyć się z Internetem korzystając z systemu operacyjnego i5/OS jako bramy.

"Informacje związane z usługami zdalnego dostępu (Remote Access Services)" na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Wymagania sprzętowe i programowe

Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących ten protokół. Jeden z tych komputerów, platforma System i, może być albo nadawcą, albo odbiorcą.

Aby zdalne systemy miały dostęp do danego systemu, musi on spełnić wymienione poniżej wymagania wstępne.

- Program System i Navigator z obsługą protokołu TCP/IP.
- Jeden z dwóch profili połączeń:
  - Profil połączenia nadawcy do obsługi wychodzących połączeń PPP.
  - Profil połączenia odbiorcy do obsługi przychodzących połączeń PPP.
- Stacja robocza PC z zainstalowanym programem System i Access for Windows 95 lub nowszym z programem System i Navigator.
- Zainstalowany adapter.

Istnieje możliwość wyboru jednego z poniższych adapterów:

- 2699*: adapter wejścia/wyjścia (IOA) dwuliniowej sieci WAN.
- 2720*: adapter IOA PCI WAN/Twinaxial.
- 2721*: adapter IOA PCI dwuliniowej sieci WAN.
- 2745*: adapter IOA PCI dwuliniowej sieci WAN (zastępuje adapter IOA 2721).
- 2742*: dwuliniowy adapter IOA (zastępuje adapter IOA 2745).
- 2771: dwuportowy adapter WAN IOA ze zintegrowanym modemem V.90 na porcie 1 i standardowym interfejsem komunikacyjnym na porcie 2. Aby wykorzystać port 2 adaptera 2771, wymagany jest modem zewnętrzny lub adapter terminalu ISDN z odpowiednim kablem.
- 2772: dwuportowy zintegrowany modem V.90 WAN IOA.
- 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: adapter Ethernet do połączeń PPPoE.
- 2793/576C: dwuportowy adapter WAN IOA ze zintegrowanym modemem V.92 na porcie 1 i standardowym interfejsem komunikacyjnym na porcie 2. Aby użyć portu 2, wymagany jest modem zewnętrzny lub adapter terminalu ISDN z odpowiednim kablem.
- 2805: czteroportowy adapter WAN IOA ze zintegrowanym modemem analogowym V.92 (zastępuje modele 2761 i 2772)

***** Adaptery te wymagają zewnętrznego modemu V.90 (lub nowszego), adaptera terminalu ISDN i interfejsu RS-232 lub odpowiedniego kabla.

- Jeden z poniższych elementów, w zależności od typu połączenia i linii:
  - zewnętrzny lub wewnętrzny modem albo jednostka obsługi kanału (CSU)/jednostka obsługi danych (DSU).
  - adapter ISDN.
- Jeśli planowane jest połączenie z Internetem, należy uzgodnić z dostawcą usług internetowych warunki założenia konta dla połączeń telefonicznych. Dostawca ISP powinien podać numer telefonu oraz informacje dotyczące połączenia z Internetem.

Odsyłacze pokrewne

“Profile połączeń” na stronie 2
Profile połączeń punkt z punktem definiują zestaw parametrów i zasobów dla określonych połączeń PPP. Profile, które korzystają z takich ustawień parametrów, można uruchomić w celu wykonywania połączeń wychodzących (rozpoczynania) lub nasłuchiwania (odbioru) połączeń PPP.

“Modemy” na stronie 39
Do połączeń PPP można użyć zarówno modemów wewnętrznych, jak i zewnętrznych.

“CSU/DSU” na stronie 39
Urządzenie CSU (channel service unit - jednostka obsługi kanału) łączy terminal z linią cyfrową. Urządzenie DSU (data service unit - jednostka obsługi danych) pełni funkcje zabezpieczające i diagnostyczne dla linii telekomunikacyjnych. Najczęściej te dwa urządzenia występują jako jedno: CSU/DSU.

“Adaptery terminali ISDN” na stronie 39
Sieć ISDN udostępnia połączenie cyfrowe umożliwiające komunikację różnych aplikacji multimedialnych łączącą głos, dane i obrazy wideo.

Połączenia alternatywne

Protokół PPP może przesyłać datagramy przez szeregowe łącza typu punkt z punktem.

Protokół ten umożliwia współdziałanie sprzętu pochodzącego od różnych dostawców oraz wielu protokołów poprzez ujednolicenie komunikacji typu punkt z punktem. Warstwa łącza danych PPP wykorzystuje ramki typu HDLC (High-Level Data Link Control) do obudowania datagramów przesyłanych zarówno przez synchroniczne, jak i asynchroniczne łącza telekomunikacyjne PPP.

Protokół PPP obsługuje wiele typów linii, natomiast protokół SLIP (Serial Line Internet Protocol) obsługuje jedynie połączenia asynchroniczne. Protokół SLIP wykorzystywany jest głównie w łączach analogowych. Firmy

telekomunikacyjne oferują standardowe usługi, których koszt wzrasta wraz z ich jakością. Usługi te korzystają z istniejących urządzeń sieciowych firm telekomunikacyjnych, znajdujących się między klientem a centralą.

Przy pomocy protokołu PPP można ustanowić fizyczne połączenie między lokalnym a zdalnym hostem. Połączenia te zapewniają dedykowaną przepustowość. Zapewniają także różne szybkości przesyłania danych oraz obsługę różnych protokołów. Istnieje możliwość wyboru następujących połączeń:

Analogowe linie telefoniczne

Połączenia analogowe, wykorzystujące modemy do przesyłania danych poprzez linie dzierżawione lub komutowane, rozpoczynają cały szereg połączeń typu punkt z punktem.

Linie dzierżawione są stałymi połączeniami między dwoma określonymi punktami, podczas gdy linie komutowane oparte są na zwykłych liniach telefonicznych. Najszybsze współczesne modemy działają z nieskompresowaną szybkością 56 kb/s. W zależności od współczynnika szumu na kablu telefonicznym szybkość ta może być jednak mniejsza.

Szybkość modemów podawana w bitach na sekundę (b/s) najczęściej zwiększana jest przez producentów dzięki zastosowaniu algorytmów kompresji (CCITT V.42bis). Algorytm ten pozwala uzyskać aż czterokrotny stopień kompresji danych, ale stopień kompresji zależy głównie od rodzaju przesyłanych informacji i często nie przekracza 50%. Dane już skompresowane lub zaszyfrowane, przy zastosowaniu algorytmu V.42bis, mogą nawet powiększyć swoją objętość. Algorytmy X2 lub 56Flex zwiększają szybkość przesyłania danych dla analogowych linii telefonicznych do 56 kb/s. Jest to technologia hybrydowa, która wymaga, aby jeden koniec połączenia PPP był cyfrowy, a drugi analogowy. Jednak szybkość 56 kb/s osiągalna jest jedynie podczas przesyłania danych w kierunku zakończenia analogowego. Technologia ta wykorzystywana jest do połączeń z dostawcami ISP, po stronie których znajduje się cyfrowe zakończenie linii PPP oraz odpowiedni sprzęt. Najczęściej z modemem analogowym V.24 można połączyć się przez interfejs szeregowy RS-232, wykorzystując do tego celu protokół asynchroniczny z szybkością dochodzącą do 115,2 kb/s.

Standard V.90 jest końcowym rozwiązaniem dla zagadnień związanych z algorytmami K56flex/x2. Jest rezultatem kompromisu firm produkujących modemy obsługujące algorytmy x2 i K56flex. Dzięki potraktowaniu publicznej, komutowanej sieci telefonicznej jako sieci cyfrowej, technologia V.90 przyspiesza przesyłanie danych z Internetu do komputera z szybkością dochodzącą do 56 kb/s. Technologia ta różni się od innych standardów, dlatego, że używane jest cyfrowe kodowanie danych, a nie ich modulowanie, tak jak to robią modemy analogowe. Dane są przesyłane metodą asymetryczną, tzn. transmisja w kierunku przeciwnym (w większości przypadków naciskanie klawiszy i rozkazy myszy przesyłane z komputera do ośrodka centralnego wymagają mniejszej przepustowości) odbywa się ze zwykłą szybkością 33,6 kb/s. Dane z modemu przesyłane są w sposób analogowy, tak jak ma to miejsce w standardzie V.34. Dane przepływające w przeciwnym kierunku przesyłane są z pełną szybkością V.90.

Standard V.92 stanowi rozszerzenie standardu V.90 i umożliwia zwiększenie szybkości zwrotnej do 48 kb/s. Ponadto czas połączenia zostaje zredukowany dzięki ulepszeniom w procesie nawiązywania połączenia, a modemy obsługujące opcję wstrzymania (hold) mogą zostać połączone w czasie, gdy linia telefoniczna akceptuje połączenia przychodzące lub oczekuje na połączenie.

Usługa cyfrowa i usługi DDS (Digital Data Services)

Z protokołem PPP można używać usług cyfrowych i usług DDS.

Usługa cyfrowa

O usługach cyfrowych mówimy wtedy, gdy dane są przesyłane w postaci cyfrowej od komputera nadawcy przez firmę telekomunikacyjną, dostawcę usług internetowych i centralę, aż w końcu trafiają do komputera odbiorcy. Cyfrowe przesyłanie sygnałów zapewnia znacznie większą przepustowość i niezawodność niż sygnały analogowe. Eliminuje też wiele problemów, z którymi mają do czynienia modemy analogowe, takich jak szum, zmienne właściwości linii i tłumienie sygnałów.

Usługi DDS

Usługi Digital Data Services (DDS) należą do podstawowych usług cyfrowych. Połączenia DDS są stałymi, dzierżawionymi połączeniami działającymi z jednakową szybkością dochodzącą do 56 kb/s. Usługi te często oznaczane są jako DS0.

Aby połączyć się z DDS, należy użyć specjalnego urządzenia nazywanego *urządzeniem CSU/DSU* (Channel Service Unit/Data Service Unit - jednostka obsługi kanału/jednostka obsługi danych), będącego odpowiednikiem modemu przy połączeniach analogowych. Usługi DDS mają ograniczenia związane z odległością urządzeń CSU/DSU od centrali telefonicznej. Działają najlepiej, kiedy odległość ta jest mniejsza niż 9 km (30 000 stóp). Firmy telekomunikacyjne mogą zwiększyć tę odległość za pomocą odpowiednich urządzeń, ale usługi takie są wtedy znacznie droższe. Usługa DDS najlepiej nadaje się do połączenia dwóch ośrodków obsługiwanych przez tę samą centralę telefoniczną. W przypadku większych odległości, połączenia obejmujące różne centrale telefoniczne powodują zwiększenie opłat związanych z odległością, sprawiając, że usługa DDS staje się zbyt droga. Lepszym rozwiązaniem może być wówczas linia Switched-56. Najczęściej z urządzeniami CSU/DSU dla usług DDS można połączyć się za pomocą V.35, RS449 lub interfejsu szeregowego X.21, z użyciem protokołu synchronicznego o szybkości dochodzącej do 56 kb/s.

Odsyłacze pokrewne

"CSU/DSU" na stronie 39
Urządzenie CSU (channel service unit - jednostka obsługi kanału) łączy terminal z linią cyfrową. Urządzenie DSU (data service unit - jednostka obsługi danych) pełni funkcje zabezpieczające i diagnostyczne dla linii telekomunikacyjnych. Najczęściej te dwa urządzenia występują jako jedno: CSU/DSU.

"Linia Switched-56"
Kiedy nie ma potrzeby korzystania z łącza stałego, można zmniejszyć koszty używając cyfrowej usługi komutowanej, która ogólnie nazywana jest usługą *Switch-56 (SW56)*.

Linia Switched-56

Kiedy nie ma potrzeby korzystania z łącza stałego, można zmniejszyć koszty używając cyfrowej usługi komutowanej, która ogólnie nazywana jest usługą *Switch-56 (SW56)*.

Połączenie SW56 jest podobne do usługi DDS: urządzenie DTE łączy się z usługą cyfrową w podobny sposób, jak jednostka obsługi kanału/jednostka obsługi danych (CSU/DSU). Urządzenia CSU/DSU dla SW56 posiadają klawiaturę, z której wprowadza się numer telefonu zdalnego hosta. Usługa SW56 umożliwia zawiązanie cyfrowego połączenia telefonicznego z innym użytkownikiem SW56 znajdującym się w dowolnym miejscu w danym regionie lub w innym kraju.

Wywołania SW56 przekazywane są w sieci cyfrowej na duże odległości, tak jak ma to miejsce z cyfrowymi wywołaniami głosowymi. Usługa SW56 wykorzystuje te same numery telefonów, co lokalne systemy telefoniczne, dzięki czemu opłaty są takie same jak za połączenia głosowe.

Usługi SW56 dostępne są jedynie w sieciach na terenie Ameryki Północnej i ograniczone są do pojedynczych kanałów przesyłających wyłącznie dane. Są one alternatywą dla tych miejsc, gdzie niedostępne są usługi ISDN.

Najczęściej z urządzeniami CSU/DSU dla SW56 można połączyć się za pomocą modemu V.35 lub interfejsu szeregowego RS 449 z użyciem protokołu synchronicznego o szybkości przesyłania danych dochodzącej do 56 kb/s. Za pomocą jednostki wywołująco-odpowiadającej V.25bis przesyłanie danych oraz sterowanie połączeniem odbywa się przez pojedynczy interfejs szeregowy.

Odsyłacze pokrewne

"Usługa cyfrowa i usługi DDS (Digital Data Services)" na stronie 33
Z protokołem PPP można używać usług cyfrowych i usług DDS.

"Sieć cyfrowa z integracją usług" na stronie 35
Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W sieci ISDN można przesyłać zarówno głos, jak i dane, korzystając z tego samego połączenia.

Sieć cyfrowa z integracją usług

Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W sieci ISDN można przesyłać zarówno głos, jak i dane, korzystając z tego samego połączenia.

Istnieją różne typy usług ISDN, ale najpopularniejszą z nich jest usługa Basic Rate Interface (BRI). Składa się ona z dwóch kanałów B o szybkości 64 kb/s przesyłających dane użytkownika i jednego kanału D przesyłającego dane sygnałowe. Dwa kanały B mogą być ze sobą połączone w celu zwiększenia szybkości do 128 kb/s. Na niektórych obszarach firmy telekomunikacyjne mogą ograniczyć szybkość do 56 kb/s dla pojedynczego kanału B lub do 112 kb/s dla kanałów połączonych. Istnieje także fizyczne ograniczenie dotyczące odległości między użytkownikiem a przełącznikiem znajdującym się w centrali, która nie może przekraczać 5,4 km (18 000 stóp). Odległość tę można zwiększyć przez zastosowanie repeaterów. Do połączenia z usługą ISDN wykorzystuje się urządzenie zwane adapterem terminalu. Większość adapterów terminali ma wbudowane terminatory sieci (NT1) pozwalające na bezpośrednie podłączenie do gniazda telefonicznego. Najczęściej adaptery terminali łączone są z komputerem przy pomocy łącza asynchronicznego RS-232 i używają do konfigurowania i sterowania zbioru komend AT, podobnie jak typowe modemy analogowe. Każdy producent ustala własne rozszerzenia komend AT potrzebnych do ustawienia parametrów specyficznych dla usługi ISDN. W przeszłości wiele problemów wynikało z braku współpracy między adapterami terminali ISDN pochodzącymi od różnych producentów. Były one związane głównie z różnymi stopniami adaptacji protokołów w V.110 i V.120 oraz z odmiennymi schematami łączenia dwóch kanałów B.

Producenci skupiają się aktualnie na synchronicznym protokole PPP z połączeniem PPP multilink, umożliwiającym połączenie dwóch kanałów B. Niektórzy producenci adapterów terminalu łączą możliwości V.34 (modem analogowy) i swoich urządzeń. Dzięki temu użytkownicy z pojedynczą linią ISDN mogą obsługiwać zarówno ISDN, jak i zwykłe połączenia analogowe, korzystając z równoczesnego przesyłania danych i głosu. Z użyciem tej technologii adapter terminalu może służyć również jako system cyfrowy dla klientów V.92.

Najczęściej adapter terminalu ISDN podłącza się za pomocą interfejsu szeregowego RS-232 i protokołu asynchronicznego z szybkością dochodzącą do 230,4 kb/s. Jednak maksymalna szybkość transmisji protokołu asynchronicznego przez interfejs RS-232 wynosi 115,2 kb/s. Ogranicza to niestety maksymalną szybkość przesyłania do 11,5 kb/s, podczas gdy adapter z połączeniem multilink jest zdolny do przesyłania 14 lub 16 kB nieskompresowanych danych. Niektóre adaptery terminali obsługują protokół synchroniczny przez interfejs RS-232 z szybkością 128 kb/s, ale maksymalna szybkość transmisji systemu dla protokołu synchronicznego przez interfejs RS-232 wynosi 64 kb/s.

System ma możliwość obsługi protokołu asynchronicznego przez interfejs V.35 z szybkością dochodzącą do 230,4 kb/s. Jednak producenci adapterów terminali w większości przypadków nie oferują takiej konfiguracji. Konwerter interfejsu z RS-232 do V.35 mógłby stanowić rozwiązanie problemu, ale metoda ta nie została uwzględniona w systemie. Inną możliwością jest użycie adaptera terminalu z interfejsem V.35 obsługującym protokół synchroniczny z szybkością 128 kb/s. Chociaż tego typu adaptery terminali są produkowane, niewiele z nich oferuje synchroniczne połączenia PPP typu multilink.

Odsyłacze pokrewne

"Linia Switched-56" na stronie 34
Kiedy nie ma potrzeby korzystania z łącza stałego, można zmniejszyć koszty używając cyfrowej usługi komutowanej, która ogólnie nazywana jest usługą *Switch-56 (SW56)*.

"Adaptery terminali ISDN" na stronie 39
Sieć ISDN udostępnia połączenie cyfrowe umożliwiające komunikację różnych aplikacji multimedialnych łączącą głos, dane i obrazy wideo.

Połączenia liniami T1/E1 i linią częściową T1

Linie T1/E1 i linia częściowa T1 są dwoma z możliwych sposobów połączeń.

Linia T1/E1

Połączenie T1 scala ze sobą 24 kanały multipleksowe z podziałem czasu (TDM) o przepustowości 64 kb/s. Fizycznie jest to 4-żyłowy kabel wykonany w technologii miedzi. Jego całkowita przepustowość wynosi 1,544 Mb/s. Linia E1 w Europie i innych częściach świata łączy ze sobą 32 kanały o szybkości 64 kb/s o łącznej przepustowości 2,048 Mb/s.

Multipleksowanie czasowe TDM pozwala wielu użytkownikom na współużytkowanie cyfrowego nośnika przesyłania dzięki wykorzystaniu przydzielanych wcześniej odstępów czasowych. Wiele cyfrowych central wewnętrznych (PBX) korzysta z możliwości usługi T1, używając jednej linii T1 zamiast dwudziestu czterech par kabli biegnących od centrali PBX do firmy telekomunikacyjnej.

Należy również zaznaczyć, że linia T1 może być współużytkowana zarówno przez głos jak i dane. Usługa telefoniczna może wykorzystywać tylko część z 24 kanałów linii T1, pozostawiając pozostałe kanały wolne, np. na potrzeby połączenia z Internetem. Podczas współużytkowania linii T1 przez wiele form usług, do zarządzania dwudziestoma czterema kanałami DS0 potrzebny jest multiplekser T1. Dla pojedynczego połączenia, podczas którego przesyłane są tylko dane, linia będzie działa bez podziału na kanały (podział TDM nie będzie wykonywany). Można więc wykorzystać uproszczone urządzenie CSU/DSU. Najczęściej z urządzeniami T1/E1 CSU/DSU lub multiplekserem można połączyć się za pomocą modemu V.35 lub interfejsu szeregowego RS 449, wykorzystując przy tym protokół synchroniczny z szybkościami będącymi wielokrotnością 64 kb/s aż do 1,544 Mb/s lub 2,048 Mb/s. Urządzenia CSU/DSU lub multiplekser umożliwiają synchronizację w sieci.

Częściowa linia T1

Dzięki częściowej linii T1 (FT1) użytkownik może dzierżawić dowolną ilość kanałów 64 kb/s linii T1. Linia FT1 jest przydatna wszędzie tam, gdzie koszt całej linii T1 byłby zbyt duży w stosunku do aktualnie wykorzystywanej przez użytkowników przepustowości. Dzięki linii FT1 użytkownik płaci tylko za to, czego potrzebuje. Dodatkowo linia FT1 posiada jedną cechę, której nie ma pełna linia T1: multipleksowanie kanałów DS0 w centrali firmy telekomunikacyjnej. Zdalnym końcem połączenia FT1 jest przełącznik Digital Access Cross-Connect, który obsługiwany jest przez firmę telekomunikacyjną. Systemy, które współużytkują ten sam cyfrowy przełącznik, mogą przełączać się między kanałami DS0. Ten schemat działania jest popularny wśród dostawców ISP wykorzystujących pojedynczą linię T1 biegnącą od nich do cyfrowego przełącznika firmy telekomunikacyjnej. W takich przypadkach wielu klientów może być obsługiwanych przy pomocy usługi FT1. Najczęściej z urządzeniami T1/E1 CSU/DSU lub multiplekserem można połączyć się za pomocą modemu V.35 lub interfejsu szeregowego RS 449, wykorzystując protokół synchroniczny z niektórymi szybkościami będącymi wielokrotnościami 64 kb/s. Linia FT1 udostępnia część z 24 kanałów. Multiplekser T1 musi być tak skonfigurowany aby wykorzystywał tylko te odstępy czasowe, które przypisane są do usługi użytkownika.

Frame relay

Frame relay to protokół służący do wyboru trasy (routing) ramek w sieci, opierający się na polu adresu IP (identyfikator połączeniowy łącza) w ramce i umożliwiającym zarządzanie trasą lub połączeniem wirtualnym.

Sieci frame relay na terenie Stanów Zjednoczonych przesyłają dane z szybkościami T1 (1,544 Mb/s) i T3 (45 Mb/s). Są sposobem na wykorzystanie istniejących już linii T1 i T-3 należących do dostawców usług. Większość firm telekomunikacyjnych udostępnia usługę frame relay użytkownikom korzystającym z połączeń o szybkości od 56 kb/s do T1. W Europie szybkość frame relay waha się od 64 kb/s do 2 Mb/s. W Stanach Zjednoczonych usługa ta jest dość popularna, ponieważ jest stosunkowo tania. Jednak na niektórych obszarach została ona zastąpiona szybszą technologią, taką jak asynchroniczny tryb przesyłania (ATM).

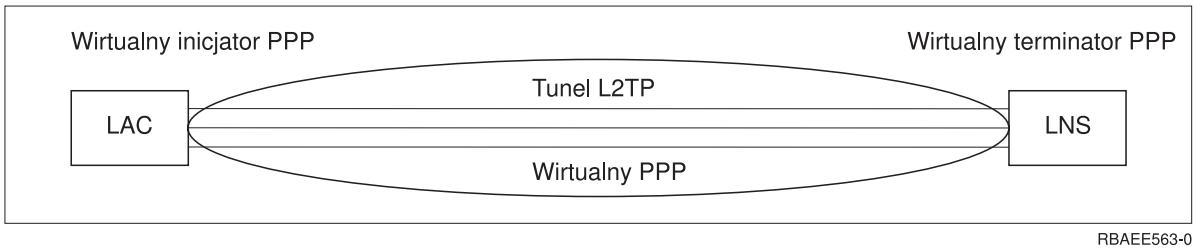
Konfigurowanie opisów linii L2TP dla połączeń PPP (tunelowanie)

Protokół L2TP jest protokołem tunelowym, który rozszerza protokół PPP o obsługę w warstwie łącza tuneli tworzonych między zgłaszającym klientem L2TP (koncentrator dostępu L2TP lub LAC) a serwerem docelowym L2TP (serwer sieciowy L2TP lub LNS).

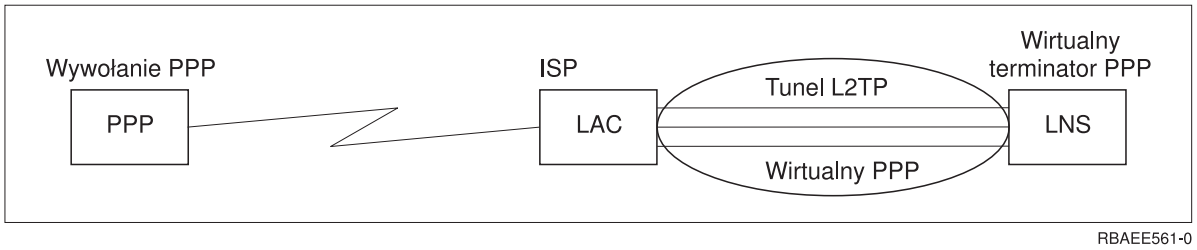
Protokół L2TP (Layer Two Tunneling Protocol)

Użycie tuneli L2TP umożliwia oddzielenie miejsca, w którym kończy się protokół połączenia telefonicznego, a zaczyna się dostęp do sieci. Z tego względu protokół L2TP jest nazywany również *wirtualnym PPP*.

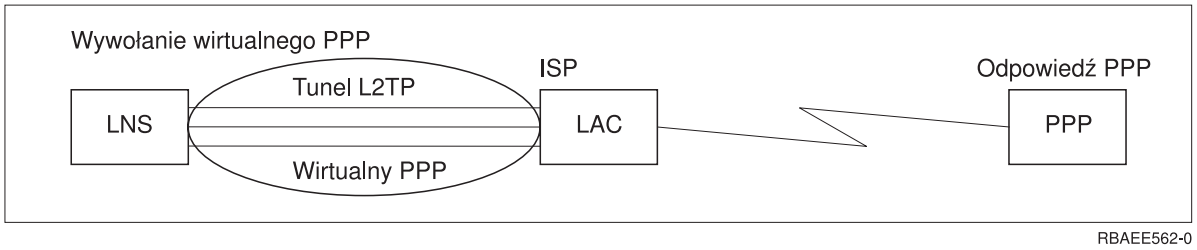
Poniżej znajdują się ilustracje obrazujące trzy różne implementacje tunelowania protokołu L2TP.



Rysunek 10. Wirtualny inicjator PPP lub wirtualny terminator PPP



Rysunek 11. Wybierający inicjator PPP lub wirtualny terminator PPP



Rysunek 12. Wywołanie wirtualnego PPP lub odpowiedź wirtualnego PPP

Protokół ten jest udokumentowany jako standard RFC-2661. Tunel L2TP może obejmować całą sesję PPP lub tylko jeden segment dwusegmentowej sesji. Można wyróżnić cztery modele tunelowania.

Informacje pokrewne

Scenariusz: zabezpieczanie dobrowolnego tunelu L2TP za pomocą protokołu IPSec

Edytor RFC

Tunel dobrowolny:

W tym modelu tunel dobrowolny jest tworzony przez użytkownika zazwyczaj za pomocą klienta obsługującego protokół L2TP.

W rezultacie użytkownik wysyła pakiety L2TP do dostawcy ISP, który następnie przekazuje je do serwera sieciowego L2TP (LNS). Przy tunelowaniu dobrowolnym dostawca ISP nie musi obsługiwać protokołu L2TP, a inicjator tunelu L2TP jest umieszczony w tym samym systemie co zdalny klient. W modelu tym tunel biegnie przez całą sesję PPP od klienta L2TP do serwera LNS.

Tunel wymuszony - połączenie przychodzące:

W tym modelu tunel jest tworzony bez ingerencji ze strony użytkownika oraz bez jego żadnego na to wpływu.

W wyniku tych działań użytkownik wysyła pakiety protokołu PPP do koncentratora dostępu L2TP dostawcy ISP. Dostawca ISP obudowuje pakiety w protokół L2TP i wysyła je w tunelu do serwera sieciowego L2TP (LNS). W

przypadku tunelowania wymuszonego dostawca ISP musi obsługiwać protokół L2TP. W niniejszym modelu tunel jest jedynie w segmencie sesji PPP między dostawcą ISP a serwerem LNS.

Tunel wymuszony - połączenie zdalne:

W modelu tym lokalny gateway (serwer sieciowy L2TP) inicjuje tunel do dostawcy ISP (LAC) i wymusza na nim połączenie lokalne z klientem odbierającym połączenie PPP.

Model ten jest przeznaczony dla zdalnych klientów odbierających połączenia PPP, którzy mają stałe połączenie telefoniczne z dostawcą ISP. Wykorzystuje się go, gdy firma z ustanowionym połączeniem z Internetem musi nawiązać połączenie z biurem wymagającym połączenia modemowego. W modelu tym tunel biegnie jedynie w segmencie sesji między serwerem LNS a dostawcą ISP.

Wieloprzeskokowe połączenia L2TP:

Połączenie wieloprzeskokowe L2TP (Layer Two Tunneling Protocol) jest sposobem na przekierowanie ruchu L2TP w imieniu klientów LAC i serwerów L2TP (LNS).

Połączenie to jest ustanawiane z użyciem bramy wieloprzeskokowej L2TP (systemu łączącego profile terminatora i inicjatora protokołu L2TP). Aby ustanowić połączenie, brama wieloprzeskokowa L2TP musi działać zarówno jako serwer LNS w celu ustawienia LNS, jak również jako LAC dla danego serwera LNS. Między klientem LAC a bramą wieloprzeskokową L2TP oraz między bramą a docelowym serwerem LNS ustanawiany jest tunel. Ruch pakietów L2TP pochodzących od klienta LAC jest przekierowywany przez bramę wieloprzeskokową L2TP do docelowego serwera LNS, a pakiety pochodzące z docelowego serwera LNS są przekierowywane do klienta LAC.

Obsługa PPPoE (DSL) dla połączeń PPP

Digital Subscriber Line (DSL) oznacza klasę technologii stosowaną do uzyskania większego pasma przy użyciu istniejącego wykonanego w technologii miedzi okablowania telefonicznego, uruchamianą między klientem a dostawcą ISP.

Ta technologia umożliwia symultaniczne przekazywanie głosu i szybkie przesyłanie danych przez pojedynczą parę miedzianego okablowania telefonicznego. Szybkości osiągane przez modemy zostały stopniowo zwiększone dzięki użyciu kompresji i innych technik, jednak najszybsze obecnie modemy (56 kb/s) osiągnęły teoretyczną górną granicę dla tej technologii. Technologia DSL umożliwia zwiększenie szybkości na liniach typu skrętka od centrali telefonicznej do domu, szkoły czy przedsiębiorstwa. Na niektórych obszarach osiągane są szybkości rzędu 2 Mb/s. Protokół PPP jest zazwyczaj używany w połączeniu z komunikacją szeregową, na przykład do połączeń modemowych. Wielu dostawców ISP stosujących technologię DSL korzysta obecnie z protokołu PPP przez sieć Ethernet (PPPoE) z uwagi na dodane opcje logowania się i zabezpieczające.

Modem DSL jest urządzeniem umieszczonym na jednym końcu linii telefonicznej wykonanej w technologii miedzi, umożliwiającym połączenie komputera (lub sieci LAN) z Internetem przez połączenie DSL. W przeciwieństwie do połączeń modemowych, takie rozwiązanie nie wymaga zazwyczaj dedykowanej linii telefonicznej (rozdzielacz POTS umożliwia symultaniczne współużytkowanie linii). Wprawdzie modemy DSL przypominają konwencjonalne modemy analogowe, ale zapewniają znacznie większą przepustowość.

Urządzenia łączące

Do obsługi połączeń PPP system używa modemów, adapterów terminali ISDN, adapterów sieci Token Ring, adapterów sieci Ethernet lub urządzeń CSU/DSU.

Są cztery rodzaje urządzeń łączących, których można użyć w środowisku PPP. Są to:

- Modemy
- CSU/DSU
- Adaptery terminali ISDN
- Adaptery ethernet (do połączeń PPPoE)

Modemy

Do połączeń PPP można użyć zarówno modemów wewnętrznych, jak i zewnętrznych.

Zestaw komend używanych przez modemy jest zazwyczaj opisany w ich dokumentacji. Komendy te używane są do resetowania i inicjowania modemu oraz do wybierania numeru zdalnego hosta. Każdy model modemu musi zostać zdefiniowany nim zostanie wykorzystany przez profil połączenia PPP ze względu na inny łańcuch komendy inicjującej go. W przypadku modemu wewnętrznego łańcuch ten jest już zdefiniowany.

System ma wiele predefiniowanych modeli modemów, a w programie System i Navigator można zdefiniować samodzielnie nowe modele. Istniejąca definicja może zostać wykorzystana jako baza do stworzenia nowej. Jeśli nie jest się pewnym, jakich komend używa modem, lub nie ma dostępu do dokumentacji, należy rozpocząć od definicji modemu Generic Hayes. Istniejących definicji nie można zmieniać. Jednak do istniejących komend inicjujących lub sekwencji wybierania można dodawać dodatkowe komendy.

Do połączeń PPP można użyć modemu elektronicznego wsparcia klienta (ECS) dostarczanego wraz z systemem. W starszych systemach modem elektronicznego wsparcia klienta był zewnętrznym modemem IBM 7852-400. Został on zastąpiony przez modem MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. W nowszych systemach jako modemu ECS można użyć modemu 2771, 2793 lub dowolnego innego obsługiwanego modemu wewnętrznego.

Odsyłacze pokrewne

“Wymagania sprzętowe i programowe” na stronie 31
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących ten protokół. Jeden z tych komputerów, platforma System i, może być albo nadawcą, albo odbiorcą.

CSU/DSU

Urządzenie CSU (channel service unit - jednostka obsługi kanału) łączy terminal z linią cyfrową. Urządzenie DSU (data service unit - jednostka obsługi danych) pełni funkcje zabezpieczające i diagnostyczne dla linii telekomunikacyjnych. Najczęściej te dwa urządzenia występują jako jedno: CSU/DSU.

Można powiedzieć, że urządzenia CSU/DSU są bardzo drogimi i wydajnymi modemami. Takie urządzenia wymagane są po obu stronach połączenia T-1 lub T-3. Muszą one pochodzić od tego samego producenta.

Odsyłacze pokrewne

“Wymagania sprzętowe i programowe” na stronie 31
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących ten protokół. Jeden z tych komputerów, platforma System i, może być albo nadawcą, albo odbiorcą.

“Usługa cyfrowa i usługi DDS (Digital Data Services)” na stronie 33
Z protokołem PPP można używać usług cyfrowych i usług DDS.

Adaptery terminali ISDN

Sieć ISDN udostępnia połączenie cyfrowe umożliwiające komunikację różnych aplikacji multimedialnych łączącą głos, dane i obrazy wideo.

Należy sprawdzić, czy adapter terminalu jest przygotowany do użycia w systemie.

W celu skonfigurowania adaptera terminalu wykonaj następujące kroki:

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. W oknie dialogowym **Właściwości nowego modemu** (New Modem Properties) wpisz poprawne wartości we wszystkich **polach** karty **Ogólne** (General). Upewnij się, czy jako urządzenie komunikacyjne podano adapter terminalu ISDN.
4. Wybierz zakładkę **Parametry dodatkowe**.
5. Na zakładce **Parametry dodatkowe** dodaj lub zmień właściwości ISDN, tak aby były zgodne z właściwościami wymaganymi przez adapter terminalu.

Zadania pokrewne

“Przykład: konfigurowanie adaptera terminalu ISDN” na stronie 56
Przykład przedstawia konfigurację adaptera terminalu sieci cyfrowej z integracją usług (ISDN).

Odsyłacze pokrewne

“Wymagania sprzętowe i programowe” na stronie 31
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących ten protokół. Jeden z tych komputerów, platforma System i, może być albo nadawcą, albo odbiorcą.

“Sieć cyfrowa z integracją usług” na stronie 35
Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W sieci ISDN można przesyłać zarówno głos, jak i dane, korzystając z tego samego połączenia.

Sugestie dotyczące adapterów terminali ISDN:

Istnieje kilka różnych adapterów terminali.

Zalecany zewnętrzny adapter terminalu ISDN lub modem ISDN to model **3Com/U.S. Robotics Courier I ISDN V.Everything**. Obsługuje on analogowe połączenia modemowe z użyciem protokołu V.90 (X2), protokołu V.92 oraz protokołu PPP typu multilink na linii ISDN, zarówno w trybie inicjującym, jak i w trybie odbierającym połączenie w systemie. Ponadto urządzenie to automatycznie obsługuje protokół CHAP (Challenge Handshake Authentication Protocol) dla połączeń PPP na linii ISDN. Dostępne są także następujące adaptery terminali ISDN: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA i ADtran ISU 2x64 Dual Port.

- **Połączenia inicjowane z systemu.** Na wezwania protokołu CHAP pochodzące ze strony odbierającej adapter terminalu Courier I odpowiada podczas negocjacji uwierzytelniania protokołu PAP z systemem. Odpowiedzi protokołu PAP nie są widoczne w połączeniu ISDN.
- **Połączenia odbierane przez system.** Adapter Courier I wymaga uwierzytelniania protokołu CHAP przez stronę wywołującą, jeśli konfiguracja odpowiedzi powoduje, że system otwiera uwierzytelnianie wezwaniem protokołu CHAP. Gdy system otwiera uwierzytelnianie według protokołu PAP, adapter terminalu Courier I przeprowadza uwierzytelnianie zgodnie z tym protokołem.

Jeśli używasz modemu Courier I wyprodukowanego przed rokiem 1999 w celu uzyskania najlepszej wydajności połączenia ISDN sprawdź, czy jest on połączony z systemem kablem V.35. Wraz z modemem Courier I dostarczane jest złącze RS-232 do kabla V.35, jednak starsze wersje tego kabla miały zły rodzaj złącza V.35. Jeśli zajdzie potrzeba wymiany złącza, należy kontaktować się z Biurem Obsługi Klienta firmy 3Com/US Robotics.

Uwaga: Zgodnie z informacjami od firmy 3Com/US Robotics wersja V.35 adaptera terminalu nie jest już dostępna u dostawców innych firm, jednak niektóre te wersje mogą wciąż być do nich dostarczane. Nadal zalecana jest wersja RS-232, mimo że zmniejsza ona wydajność systemu z powodu ograniczenia połączenia do 115.2 KB.

Upewnij się, że szybkość linii w systemie jest ustawiona na 230,4 kb/s.

Ograniczenia adaptera terminalu ISDN:

Przedstawione poniżej adaptery terminali zostały przetestowane. Są one zalecane jedynie do inicjowania zdalnych połączeń ISDN z systemu.

3Com Impact IQ ISDN:

Nie poleca się tego adaptera terminalu dla platformy System i z następujących powodów:

- Adapter terminalu nie obsługuje analogowych połączeń modemowych V.34, ale może to robić przy zewnętrznym połączeniu RJ-11.
- Adapter terminalu nie obsługuje połączeń V.90.
- Adapter terminalu nie może połączyć się z systemem z szybkością większą niż 115 200 b/s.
- Adapter terminalu nie obsługuje automatycznie protokołu CHAP. Jeśli S84 zostanie ustawione na 0, jest wykonywane uwierzytelnianie CHAP.

- System nie potrafi określić zakończenia połączenia na podstawie monitorowania sygnału DSR (Data Set Ready) z adaptera terminalu. Stanowi to potencjalne ryzyko naruszenia bezpieczeństwa systemu.

Motorola BitSurfr Pro ISDN:

Nie poleca się tego adaptera terminalu dla platformy System i z następujących powodów:

- Adapter terminalu nie obsługuje analogowych połączeń modemowych V.34, ale może to robić przy zewnętrznym połączeniu RJ-11.
- Adapter terminalu nie obsługuje połączeń V.90.
- Adapter terminalu nie może połączyć się z systemem z szybkością większą niż 115 200 b/s.
- Adapter terminalu nie obsługuje automatycznie protokołu CHAP. Jednak ustawienie @M2=C umożliwia wykonywanie uwierzytelniania CHAP.
- Adapter terminalu nie pozwala na automatyczne odbieranie połączeń PPP pojedynczych i typu multilink. Zdalny inicjujący adapter terminalu musi być ustawiony na ten sam typ protokołu (pojedynczy lub multilink), co adapter odbierający.
- Sprzętowy mechanizm sterowania przepływem nie współpracuje dobrze z tym adapterem terminalu. Powoduje to spadek wydajności przy wysyłaniu przez system danych w połączeniu PPP multilink.

Obsługa adresów IP

Połączenia PPP umożliwiają dowolne zarządzanie adresami IP w zależności od rodzaju profilu połączenia.

- Protokół DHCP umożliwia centralne zarządzanie przypisywaniem adresów IP w sieci. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami DHCP w sieci. Zapoznaj się z sekcją Dynamic Host Configuration Protocol.
- System DNS pomaga w zarządzaniu nazwami hostów i przypisanymi im adresami IP. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami DNS w sieci. Zapoznaj się z sekcją Domain Name System.
- Protokół BOOTP służy do powiązania klienckich stacji roboczych z systemem oraz przypisania im adresów IP. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami BOOTP w sieci. Zapoznaj się z sekcją Bootstrap Protocol.

  Odsyłacze pokrewne

  “Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE” na stronie 10
  Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

Filtrowanie pakietów IP

Filtrowanie pakietów IP ogranicza usługi dostępne dla poszczególnych użytkowników w momencie ich logowania się do sieci.

Filtrowanie pakietów umożliwia przyznawanie lub odmawianie dostępu w zależności od docelowego adresu IP i/lub portów. Definiując wiele zestawów reguł filtrowania pakietów, z których każdy ma własny, unikalny identyfikator filtrowania PPP, można utworzyć różne strategie. Reguły filtrowania pakietów mogą być przypisywane do poszczególnych profili połączeń odbiorcy lub za pomocą strategii dostępu dla grup do kategorii użytkowników. Reguły filtrowania pakietów nie są definiowane w protokole PPP, ale w opcji Reguły pakietów IP (IP Packet Rules) w programie System i Navigator.

W przypadku połączeń L2TP do zabezpieczenia ruchu w sieci należy użyć sieci VPN z filtrowaniem IPSec.

Odsyłacze pokrewne

“Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE” na stronie 10
Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

Informacje pokrewne

Filtrowanie IP i translacja adresów sieciowych

Korzystanie z sieci VPN (Virtual Private Networking)

Strategia zarządzania adresami IP

Przed rozpoczęciem konfigurowania profilu połączenia PPP należy zapoznać się ze strategią zarządzania adresami IP w sieci. Strategia ta wpływa na wiele decyzji w trakcie całego procesu konfiguracji, włącznie ze strategiami uwierzytelniania, założeniami dotyczącymi bezpieczeństwa i ustawieniami protokołu TCP/IP.

Profile połączenia nadawcy

Lokalne i zdalne adresy IP określone dla profilu nadawcy będą najczęściej zdefiniowane jako *Przypisane do systemu zdalnego*. Umożliwia to administratorom systemów zdalnych kontrolowanie adresów IP, które będą użyte podczas połączenia. Większość połączeń z dostawcami usług internetowych (ISP) będzie zdefiniowana w ten sposób, mimo iż wielu z nich oferuje stałe adresy IP za dodatkową opłatą.

Jeśli dla lokalnego albo zdalnego adresu IP zostanie zdefiniowany stały adres, należy upewnić się, że system zdalny akceptuje wcześniej zdefiniowane adresy IP. Zazwyczaj definiuje się adres lokalny jako stały adres IP, a adres zdalny jako przypisany do systemu zdalnego. System docelowy można zdefiniować w ten sam sposób. Gdy dwa systemy zostaną połączone, będą one wymieniać między sobą adresy, dzięki czemu możliwe będzie poznanie adresu systemu zdalnego. Jest to bardzo przydatne podczas tymczasowego łączenia.

Kolejnym elementem jest decyzja o uaktywnieniu maskowania adresów IP. Na przykład jeśli system łączy się z Internetem przez dostawcę ISP, sieć przyłączona za tym systemem również może mieć dostęp do Internetu. Zasadniczo system ukrywa adresy IP systemów w sieci znajdującej się za lokalnym adresem IP przypisanym przez dostawcę ISP, powodując, że cały ruch sieciowy IP sprawia wrażenie pochodzącego z tego systemu. Należy wziąć pod uwagę również dodatkowe kwestie dotyczące routingu w odniesieniu do obu systemów w sieci LAN (aby zapewnić przekazywanie ruchu internetowego do systemu), a także w odniesieniu do systemu, dla którego należy zaznaczyć pole wyboru **Podaj zdalny system jako domyślną trasę** (Add remote system as the default route).

Profile połączenia odbiorcy

Profile połączenia odbiorcy mają znacznie więcej opcji i możliwości dotyczących adresu IP niż profil połączenia nadawcy. Konfiguracja adresów IP zależy od planu zarządzania adresami IP dla danej sieci, określonych wymagań dotyczących wydajności i funkcjonalności połączenia oraz planu ochrony.

Lokalne adresy IP

Dla pojedynczego profilu odbiorcy można zdefiniować unikalny adres IP lub użyć istniejącego adresu IP systemu, aby określić ten koniec połączenia PPP. Dla profili odbiorcy, zdefiniowanych do obsługi wielu połączeń jednocześnie, należy użyć istniejącego adresu IP. Jeśli nie ma żadnych istniejących adresów IP, można w tym celu utworzyć wirtualny adres IP.

Zdalne adresy IP

Istnieje wiele opcji do przypisywania zdalnych adresów IP klientom PPP. Na stronie TCP/IP profilu połączenia odbiorcy mogą zostać określone następujące opcje.

Uwaga: Jeśli system zdalny ma stanowić część sieci lokalnej, należy skonfigurować routing adresów IP, wybrać adres IP z zakresu adresów dla systemów przyłączonych do sieci LAN i upewnić się, że zarówno dla profilu połączenia, jak i dla danego systemu, włączono przekazywanie IP.

Tabela 8. Opcje przypisania adresu IP dla profilu połączenia odbiorcy

Opcja	Opis
Stały adres IP	Pojedynczy adres IP jest definiowany dla zdalnych użytkowników i udostępniany im podczas połączenia. Adres ten jest adresem hosta (maska podsieci to 255.255.255.255) dostępnym jedynie profilom odbiorcy pojedynczego połączenia.
Pula adresów	Definiowany jest początkowy adres IP, a następnie określany jest zakres możliwych do przydzielenia dodatkowych adresów. Każdemu połączonemu użytkownikowi zostanie przydzielony unikalny adres IP ze zdefiniowanego wcześniej zakresu. Adres ten jest adresem hosta (maska podsieci to 255.255.255.255) dostępnym jedynie dla profili odbiorcy połączeń wielokrotnych.
Protokół RADIUS	Zdalny adres IP i związana z nim maska podsieci określane są przez serwer RADIUS. Jest to możliwe, gdy: • włączona jest obsługa protokołu Radius dla uwierzytelniania oraz adresowania IP z poziomu konfiguracji usług Remote Access Server, • włączone jest uwierzytelnianie dla profilu połączenia odbiorcy i zdefiniowane jest zdalne uwierzytelnianie przez serwer Radius.
DHCP	Zdalny adres IP określany jest bezpośrednio przez serwer DHCP lub pośrednio przez przekaźnik DHCP. Jest to możliwe jedynie wtedy, gdy obsługa DHCP jest włączona z poziomu konfiguracji usług Remote Access Serwer. Przydzielany jest wówczas adres IP hosta (maska podsieci to 255.255.255.255).
Bazujący na identyfikatorze użytkownika zdalnego systemu	Zdalny adres IP określany jest na podstawie identyfikatora użytkownika zdefiniowanego dla zdalnego systemu podczas jego uwierzytelniania. Pozwala to administratorowi na przypisanie użytkownikowi połączenia modemowego różnych adresów IP (i skojarzonych z nimi masek podsieci). Umożliwia to również zdefiniowanie dodatkowych tras związanych z poszczególnymi identyfikatorami użytkowników. Dzięki temu można dostosować środowisko do konkretnego zdalnego użytkownika. Aby funkcja ta działała prawidłowo, należy włączyć uwierzytelnianie.
Definiowanie dodatkowych adresów IP bazujących na identyfikatorze użytkownika zdalnego systemu	Opcja ta pozwala na zdefiniowanie adresów IP bazujących na identyfikatorze użytkownika zdalnego systemu. Jest ona wybierana automatycznie (i musi zostać użyta), jeśli metoda przypisania zdalnego adresu IP jest zdefiniowana jako **Bazujący na identyfikatorze użytkownika zdalnego systemu**. Opcja ta jest także dozwolona dla metod przypisywania adresów IP Stały adres IP i Pula adresów. Po połączeniu zdalnego użytkownika z systemem nastąpi próba określenia, czy dla tego użytkownika zdefiniowano konkretny adres IP. Jeśli tak, adres IP, maska oraz zestaw możliwych tras będą przydzielone dla tego połączenia. Jeśli użytkownik nie jest zdefiniowany, adres IP będzie domyślnym stałym adresem IP lub następnym kolejnym adresem IP z puli adresów.
Zezwolenie systemowi zdalnemu na zdefiniowanie własnego adresu IP	Opcja ta pozwala zdalnemu użytkownikowi na zdefiniowanie własnego adresu IP, jeśli negocjacja powiedzie się. W przeciwnym razie zdalny adres IP będzie określony jedną z metod przypisania zdalnego adresu IP. Opcja ta jest początkowo wyłączona i zanim zostanie uaktywniona należy dokładnie przeanalizować wszystkie okoliczności.
Kierowanie adresów IP	Jeśli klient z połączeniem modemowym potrzebuje dostępu do dowolnego z adresów IP w sieci lokalnej, do której należy system, zarówno ten klient, jak i system muszą mieć poprawnie skonfigurowany routing adresów IP.

Uwierzytelnianie systemu

Połączenia PPP z platformą System i obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów nawiązujących połączenie z systemem, jak i połączeń wychodzących do dostawcy ISP lub innego systemu.

System obsługuje kilka metod postępowania z informacjami o uwierzytelnianiu. Metody te obejmują zarówno proste listy sprawdzania w systemie zawierające spisy uprawnionych użytkowników z hasłami, jak i obsługę serwerów RADIUS. Serwery RADIUS przechowują szczegółowe dane o użytkownikach sieci. System ma również kilka opcji szyfrowania informacji o identyfikatorze użytkownika i jego haśle, od prostej wymiany haseł po obsługę protokołu CHAP-MD5. Preferencje dotyczące uwierzytelniania w systemie, włącznie z identyfikatorem użytkownika i hasłem

używanym do sprawdzania poprawności systemu przy połączeniach wychodzących, można określić na karcie **Uwierzytelnianie** (Authentication) profilu połączenia w programie System i Navigator.

Odsyłacze pokrewne

"Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE" na stronie 10
Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

"Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS" na stronie 21
Serwer dostępu do sieci (Network Access Server - NAS) działający w systemie może kierować żądania uwierzytelnienia od klientów z połączeniem modemowym do odrębnego serwera RADIUS (Remote Authentication Dial In User Service). Po uwierzytelnieniu serwer RADIUS może również sterować adresami IP przydzielonymi użytkownikowi.

"Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP" na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Protokół Challenge Handshake Authentication Protocol (CHAP) z MD5

Protokół Challenge Handshake Authentication Protocol (CHAP-MD5) korzysta z algorytmu (MD-5) do obliczenia wartości znanej tylko systemowi uwierzytelniającemu i urządzeniu zdalnemu.

Dzięki niemu identyfikator użytkownika i hasło są zawsze zaszyfrowane, co powoduje, że protokół CHAP jest bezpieczniejszy od protokołu Password Authentication Protocol (PAP). Protokół ten efektywnie chroni przed próbami dostępu metodą prób i błędów oraz odtwarzania. Uwierzytelnianie metodą protokołu CHAP może wystąpić wielokrotnie podczas połączenia.

System uwierzytelniający wysyła wezwanie do zdalnego urządzenia próbującego połączyć się z siecią. Zdalne urządzenie odsyła wartość wyliczoną przez wspólny algorytm (MD-5) używany przez obydwa urządzenia. System uwierzytelniający weryfikuje odpowiedź porównując ją z własnymi obliczeniami. Uwierzytelnienie zostaje potwierdzone, gdy wartości pasują do siebie, w przeciwnym razie połączenie zostaje przerwane.

Odsyłacze pokrewne

"Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem" na stronie 13
Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

"Protokół PAP (Password Authentication Protocol)" na stronie 45
Protokół Password Authentication Protocol (PAP) używa dwukierunkowego uzgadniania, zapewniając systemowi równorzędnemu prostą metodę ustalenia tożsamości.

Protokół EAP (Extensible Authentication Protocol)

Protokół Extensible Authentication Protocol (EAP) umożliwia zewnętrznym modułom uwierzytelniającym współdziałanie z protokołem PPP.

Protokół EAP jest rozszerzeniem protokołu PPP. Dzięki temu dostępny staje się standardowy mechanizm dla schematów uwierzytelniania, takich jak karty token (smart), protokół Kerberos, klucz publiczny oraz S/Key. Protokół EAP odpowiada na rosnące zapotrzebowanie na uwierzytelnianie za pomocą urządzeń zabezpieczających wyprodukowanych przez firmy zewnętrzne. Protokół ten chroni również bezpieczne sieci Virtual Private Network (VPN) przed atakami hakerów, którzy przy pomocy słowników próbują odgadnąć hasła. Protokół EAP stanowi ulepszenie protokołów PAP i CHAP.

W protokole EAP informacje uwierzytelniające nie są zawarte w informacji, lecz przesyłane są razem z nią. Pozwala to zdalnym systemom na negocjację wymaganego uwierzytelnienia przed odebraniem lub wysłaniem jakichkolwiek danych.

System nie obsługuje bezpośrednio protokołu EAP. Można jednak użyć zdalnego uwierzytelniania za pomocą serwera RADIUS, który obsługuje niektóre z opisanych wcześniej dodatkowych schematów uwierzytelniających.

Protokół PAP (Password Authentication Protocol)

Protokół Password Authentication Protocol (PAP) używa dwukierunkowego uzgadniania, zapewniając systemowi równorzędnemu prostą metodę ustalenia tożsamości.

Uzgadnianie jest przeprowadzane podczas ustanawiania połączenia. Po jego ustanowieniu zdalne urządzenie wysyła parę: identyfikator użytkownika i hasło do systemu uwierzytelniającego. W zależności od tego, czy przesłana para jest prawidłowa, system uwierzytelniający albo kontynuuje, albo kończy połączenie.

Uwierzytelnianie przy pomocy protokołu PAP wymaga, aby nazwa użytkownika i hasło było przesyłane do zdalnego systemu w sposób jawny. W protokole PAP identyfikator i hasło użytkownika nie są nigdy zaszyfrowane, w związku z czym istnieje możliwość ich śledzenia oraz ryzyko ataku hakera. Dlatego należy używać protokołu CHAP (Challenge Handshake Authentication Protocol), ilekroć jest to możliwe.

Odsyłacze pokrewne

"Protokół Challenge Handshake Authentication Protocol (CHAP) z MD5" na stronie 44
Protokół Challenge Handshake Authentication Protocol (CHAP-MD5) korzysta z algorytmu (MD-5) do obliczenia wartości znanej tylko systemowi uwierzytelniającemu i urządzeniu zdalnemu.

Protokół RADIUS (Remote Authentication Dial In User Service) - przegląd

RADIUS (Remote Authentication Dial In User Service) jest standardowym protokołem internetowym, który udostępnia usługi scentralizowanego uwierzytelniania, obsługi kont i zarządzania adresami IP w sieci rozproszonej z połączeniem modemowym dla użytkowników mających zdalny dostęp.

Model klient/serwer protokołu RADIUS zawiera serwer dostępu do sieci (Network Access Server - NAS), działający jako klient na serwerze RADIUS. System pracujący jako serwer NAS wysyła informacje dotyczące użytkownika i połączenia do wyznaczonego serwera RADIUS, używając standardu protokołu RADIUS zdefiniowanego w dokumencie RFC 2865.

Serwery RADIUS działają na podstawie przyjętych zgłoszeń o połączeniach użytkownika, uwierzytelniając go, a następnie zwracając wszystkie niezbędne informacje dotyczące konfiguracji do serwera NAS (systemu), który dzięki temu może zapewniać autoryzowane usługi uwierzytelnionym połączonym użytkownikom.

Jeśli serwer RADIUS jest niedostępny, system może przekierować żądania dotyczące uwierzytelnienia do serwera zastępczego. Umożliwia to międzynarodowym przedsiębiorstwom obsługę połączeń modemowych. Przydzielają one swoim użytkownikom unikalny identyfikator użytkownika potrzebny do wpisania się, bez względu na to, z którego miejsca nawiązano połączenie.

Kiedy zgłoszenie dotyczące uwierzytelniania zostaje odebrane przez serwer RADIUS, sprawdzana jest jego poprawność, a następnie serwer deszyfruje pakiet danych, aby uzyskać dostęp do nazwy i hasła użytkownika. Informacje wysyłane są dalej do odpowiedniego systemu zabezpieczającego, gdzie są przetwarzane. Systemem zabezpieczającym mogą być pliki haseł systemu UNIX, protokół Kerberos, specjalistyczny system ochrony dostępny w sprzedaży lub system stworzony na zamówienie firmy. Serwer RADIUS zwraca do systemu wszystkie usługi, do których jest uprawniony uwierzytelniony użytkownik, takie jak np. adres IP. Zgłoszenia protokołu RADIUS dotyczące kont obsługiwane są w podobny sposób. Informacje związane z obsługą kont użytkowników zdalnych mogą być przesyłane do wyznaczonych serwerów RADIUS. Standard protokołu RADIUS, który obsługuje konta, jest zdefiniowany w dokumencie RFC 2866. Serwer RADIUS obsługujący konta działa na bazie przyjętych zgłoszeń dotyczących kont rejestrując wszystkie informacje związane z tymi zgłoszeniami.

Odsyłacze pokrewne

“Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS” na stronie 21
Serwer dostępu do sieci (Network Access Server - NAS) działający w systemie może kierować żądania uwierzytelnienia od klientów z połączeniem modemowym do odrębnego serwera RADIUS (Remote Authentication Dial In User Service). Po uwierzytelnieniu serwer RADIUS może również sterować adresami IP przydzielonymi użytkownikowi.

Lista weryfikacji

Lista weryfikacji jest wykorzystywana do przechowywania identyfikatorów użytkowników i haseł dla zdalnych użytkowników.

Istnieje możliwość wykorzystania istniejącej listy lub utworzenia nowej przy pomocy strony uwierzytelniania profilu połączenia odbiorcy. Pozycje listy weryfikacji wymagają określenia typu protokołu uwierzytelniania przypisanego do identyfikatora użytkownika i hasła. Może to być protokół **szyfrowany - CHAP-MD5/EAP** lub **nieszyfrowany - PAP**.

Więcej informacji zawiera pomoc elektroniczna.

Odsyłacze pokrewne

“Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP” na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Uwagi dotyczące zakresu pasma przy połączeniu typu multilink

Do wykonania niektórych czynności często, ale nie zawsze, jest wymagana dodatkowa przepustowość.

Zakup specjalistycznego sprzętu oraz drogich linii komunikacyjnych może się nie opłacać. Protokół MP (Multilink Protocol) grupuje wiele fizycznych linii PPP w jedną linię wirtualną (wiązkę). Zostaje więc zwiększona całkowita efektywna przepustowość między dwoma systemami używającymi standardowych modemów i linii telefonicznych. W jednej wiązce MP można połączyć do sześciu linii. Aby ustanowić połączenie typu multilink, obie końcówki muszą obsługiwać protokół MP (Multilink Protocol). Protokół ten jest udokumentowany jako standard RFC-1990.

Przepustowość na żądanie

Zdolność dynamicznego dodawania i usuwania linii fizycznych pozwala systemowi zapewnić odpowiednią przepustowość wtedy, gdy jest ona potrzebna. Dzięki temu płaci się jedynie za przepustowość, która jest aktualnie wykorzystywana. Aby skorzystać z zalet przepustowości na żądanie, co najmniej jeden węzeł musi być w stanie monitorować wykorzystanie pasma w wiązce MP. Linie mogą być odpowiednio dodawane lub usuwane, gdy wykorzystanie pasma przekroczy wartości zdefiniowane w konfiguracji. Protokół BAP (Bandwidth Allocation Protocol) umożliwia węzłom negocjowanie dodawania i usuwania linii w ramach wiązki MP. Standard RFC-2125 opisuje zarówno protokół BAP (PPP Bandwidth Allocation Protocol), jak i BACP (Bandwidth Allocation Control Protocol).

Informacje pokrewne

Edytor RFC

Konfigurowanie protokołu PPP

Przed przystąpieniem do konfigurowania połączenia PPP należy skonfigurować środowisko dla tego protokołu.

Odsyłacze pokrewne

“Informacje związane z usługami zdalnego dostępu (Remote Access Services)” na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Tworzenie profilu połączenia

Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Profil połączenia jest logiczną reprezentacją następujących informacji dotyczących połączenia:

- typ profilu i linii,
- ustawienia dla połączeń multilink,
- numery zdalnych telefonów i opcje wybierania,
- uwierzytelnianie,
- ustawienia TCP/IP: adresy IP i routing,
- zarządzanie pracą i dostosowanie połączenia,
- serwery nazw domen.

Usługi zdalnego dostępu w katalogu Sieć zawiera następujące obiekty:

- Profile połączenia nadawcy
- Profile połączenia odbiorcy
- **Modemy**.

W celu utworzenia profilu połączenia wykonaj następujące kroki:

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Wybierz jedną z poniższych opcji:
   - Kliknij prawym przyciskiem myszy **Profile połączenia nadawcy** (Originator Connection Profiles), aby system rozpoczynał połączenie.
   - Kliknij prawym przyciskiem myszy **Profile połączenia odbiorcy** (Receiver Connection Profiles), aby system zezwalał na połączenia przychodzące z systemów zdalnych i od użytkowników.
3. Wybierz **Nowy profil**.
4. Na stronie Konfiguracja nowego profilu połączenia punkt z punktem wybierz typ protokołu.
5. Wybierz tryb.
6. Wybierz konfigurację łącza.
7. Kliknij przycisk **OK**.

   Zostanie wyświetlona strona Właściwości nowego profilu punkt z punktem, umożliwiająca ustawienie pozostałych wartości specyficznych dla sieci. Więcej informacji na ten temat zawiera pomoc elektroniczna.

   Zadania pokrewne

   “Przypisanie modemu do opisu linii” na stronie 57
   W temacie przedstawione zostały czynności związane z przypisaniem modemu do opisu linii.

   Odsyłacze pokrewne

   “Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE” na stronie 10
   Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

   “Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem” na stronie 13
   Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

   “Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu” na stronie 15
   Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia systemu z dostawcą ISP mogą użyć modemu. Komputery PC przyłączone do sieci LAN mogą łączyć się z Internetem korzystając z systemu operacyjnego i5/OS jako bramy.

"Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu" na stronie 18
Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Protokołem PPP można połączyć ze sobą dwie sieci lokalne, ustanawiając połączenie między jednym systemem znajdującym się w centrali i drugim, znajdującym się w oddziale.

"Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP" na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Typ protokołu: PPP lub Serial Line Internet Protocol (SLIP)

W połączeniach typu punkt z punktem protokół PPP zastąpił protokół SLIP (Serial Line Internet Protocol).

Protokół PPP umożliwia współdziałanie programów zdalnego dostępu pochodzących od różnych producentów. Dodatkowo umożliwia wielu sieciowym protokołom komunikacyjnym korzystanie z tej samej fizycznej linii komunikacyjnej.

Protokół SLIP nigdy nie stał się standardem internetowym, ponieważ ma kilka wad:

- Protokół SLIP nie ma standardowego sposobu na adresowanie IP między dwoma hostami, co uniemożliwia wykorzystanie nienumerowanych sieci.
- Protokół SLIP nie obsługuje wykrywania błędów oraz kompresji błędów. Funkcje te zostały zaimplementowane dopiero w protokole PPP.
- Protokół SLIP nie obsługuje uwierzytelniania systemu, podczas gdy protokół PPP obsługuje dwa sposoby uwierzytelniania.

Protokół SLIP jest wciąż używany, dlatego system operacyjny i5/OS go obsługuje. Jednakże firma IBMzaleca korzystanie z protokołu PPP podczas konfigurowania połączeń PPP. Protokół SLIP nie obsługuje połączeń multilink. W porównaniu z nim protokół PPP oferuje lepsze uwierzytelnianie oraz dzięki możliwościom kompresji lepszą wydajność.

Uwaga: Profile połączeń SLIP zdefiniowane dla linii typu ASYNC nie są już obsługiwane w tym wydaniu. Należy przeprowadzić ich migrację do profili SLIP lub PPP używających linii typu PPP.

Wybór trybu

Na wybór trybu dla profilu połączenia PPP składa się wybór typu połączenia oraz trybu pracy. Wybór trybu określa sposób użycia przez system nowego połączenia PPP.

W celu wybrania trybu wykonaj następujące kroki:

1. Wybierz jeden z poniższych typów połączenia:
   - Linia komutowana
   - Linia dzierżawiona
   - Layer Two Tunneling Protocol (L2TP) (linia wirtualna)
   - Połączenie protokołu PPP przez sieć Ethernet (Point-to-Point Protocol over Ethernet - PPPoE)
2. Wybierz tryb pracy odpowiedni dla połączenia PPP.
3. Zapisz wybrany typ połączenia i tryb pracy. Informacje te będą potrzebne podczas konfigurowania połączeń PPP.

Linia komutowana:

Jeśli do połączenia linią telefoniczną używasz modemu (wewnętrznego lub zewnętrznego) lub adaptera terminalu sieci cyfrowej z integracją usług (ISDN), wybierz połączenie linią komutowaną.

Połączenie na liniach komutowanych może pracować w następujących trybach:

Odpowiedź

Wybierz ten tryb pracy, aby umożliwić systemowi zdalnemu nawiązanie połączenia z danym systemem.

Połączenie

Wybierz ten tryb pracy, aby umożliwić systemowi nawiązywanie połączeń zewnętrznych z systemem zdalnym.

Połączenie na żądanie (tylko inicjowanie)

Wybierz ten tryb pracy, aby umożliwić systemowi nawiązanie automatycznego połączenia zewnętrznego z systemem zdalnym po wykryciu na łączu TCP/IP ruchu skierowanego do tego systemu. Połączenie zostanie przerwane, gdy transmisja się zakończy, a na łączu TCP/IP nie będzie ruchu przez ustalony czas.

Połączenie na żądanie (dedykowany węzeł z możliwością odpowiedzi)

Wybierz ten tryb pracy, aby umożliwić systemowi odpowiadanie na połączenia ze strony dedykowanego systemu zdalnego. Tryb ten umożliwia również systemowi wywołanie systemu zdalnego po wykryciu na łączu TCP/IP kierowanego do niego ruchu. Jeśli obydwa systemy używają systemu operacyjnego i5/OS i tego trybu pracy, ruch na łączu TCP/IP odbywa się na żądanie i nie jest konieczne utrzymywanie stałego fizycznego połączenia. Ten tryb pracy wymaga dedykowanego zasobu. Do poprawnego działania w tym trybie zdalny węzeł sieci musi inicjować połączenie.

Połączenie na żądanie (zdalne węzły włączone)

Wybór tego trybu pracy umożliwia zdalnym systemom inicjowanie lub odbieranie połączenia. Aby obsługiwać połączenia przychodzące, należy odnieść istniejący profil odpowiedzi do profilu połączenia PPP, który określa ten tryb pracy. Dzięki temu przy pomocy jednego profilu odbiorcy można obsługiwać wszystkie połączenia przychodzące z jednego lub wielu zdalnych węzłów. Natomiast połączenia wychodzące można obsługiwać przy pomocy osobnych profili na żądanie. Ten tryb pracy nie wymaga dedykowanego zasobu do obsługi połączeń przychodzących ze zdalnych węzłów.

Linia dzierżawiona:

Jeśli między systemem lokalnym i zdalnym znajduje się linia dedykowana, wybierz połączenie za pomocą linii dzierżawionej. W przypadku linii dzierżawionej do połączenia dwóch systemów nie jest wymagany modem ani adapter terminalu ISDN.

Za połączenie linią dzierżawioną między dwoma systemami uważa się linię stałą lub dedykowaną. Jest ona zawsze otwarta. Jeden koniec tej linii jest skonfigurowany jako inicjator, a drugi jako terminator.

Połączenie na linii dzierżawionej ma następujące tryby pracy:

Terminator

Wybór tego trybu pracy umożliwia zdalnemu systemowi uzyskanie dostępu do systemu poprzez linię dedykowaną. Ten tryb pracy odpowiada profilowi odbiorcy linii dzierżawionej.

Inicjator

Wybór tego trybu pracy umożliwia systemowi uzyskanie dostępu do systemu zdalnego poprzez linię dedykowaną. Ten tryb pracy odpowiada profilowi nadawcy połączeń linii dzierżawionej.

L2TP (linia wirtualna):

Ten typ połączenia należy wybrać, aby zapewnić połączenie między systemami używającymi protokołu L2TP.

Po ustanowieniu tunelu L2TP między danym systemem i systemem zdalnym jest tworzone połączenie protokołu PPP. Wykorzystanie tunelowania L2TP w połączeniu z ochroną IPSec daje możliwość wysyłania, kierowania i odbierania chronionych danych w sieci Internet.

Połączenie poprzez protokół L2TP (linia wirtualna) ma następujące tryby pracy:

Terminator

Wybór tego trybu pracy umożliwia zdalnemu systemowi nawiązanie połączenia z systemem użytkownika poprzez tunel L2TP.

Inicjator

Wybór tego trybu pracy umożliwia systemowi użytkownika nawiązanie połączenia ze zdalnym systemem poprzez tunel L2TP.

Zdalne inicjowanie

Wybór tego trybu pracy umożliwia systemowi użytkownika nawiązanie połączenia z innym systemem lub dostawcą ISP poprzez tunel L2TP i bezpośrednie zainicjowanie połączenia ze zdalnym klientem PPP z poziomu dostawcy ISP.

Inicjator wieloprzeskokowy

Wybór tego trybu pracy umożliwia systemowi nawiązanie połączenia wieloprzeskokowego.

Uwaga: Profil terminatora L2TP przypisanego do inicjatora wieloprzeskokowego musi mieć ustawione pole **Zezwól na połączenia wieloprzeskokowe** (Allow multi-hop connection) oraz pozycję na liście sprawdzania protokołu PPP przypisującą nazwę użytkownika PPP do profilu inicjatora wieloprzeskokowego.

Linia PPPoE:

Połączenia protokołu PPP przez sieć Ethernet (PPPoE) korzystają z linii wirtualnej do wysyłania danych PPP (przez adapter Ethernet) do modemu DSL dostarczonego przez dostawcę ISP. Modem ten jest podłączony również do sieci lokalnej opartej na protokole Ethernet.

Rozwiązanie takie zapewnia użytkownikom sieci lokalnej szybki dostęp do Internetu przez sesje PPP w systemie operacyjnym i5/OS. Po nawiązaniu połączenia między systemem i dostawcą ISP użytkownicy mogą rozpoczynać własne sesje do dostawcy ISP przez PPPoE.

Połączenia PPPoE są używane tylko przez profile połączeń nadawcy. Implikują one tryb pracy inicjatora i użycie tylko jednej linii.

Konfigurowanie połączenia

Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

Typ obsługi linii zależy od podanego typu połączenia.

Odsyłacze pokrewne

“Scenariusz: łączenie systemu z koncentratorem dostępu PPPoE” na stronie 10
Wielu dostawców ISP oferuje szybki dostęp do Internetu z użyciem protokołu PPP przez sieć Ethernet (PPPoE) i linii DSL (Digital Subscriber Line). Połączenie systemu z jednym z tych dostawców ISP zapewni połączenia o wysokiej przepustowości przy zachowaniu zalet korzystania z protokołu PPP.

“Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem” na stronie 13
Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

“Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu” na stronie 15
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia systemu z dostawcą ISP mogą użyć modemu. Komputery PC przyłączone do sieci LAN mogą łączyć się z Internetem korzystając z systemu operacyjnego i5/OS jako bramy.

"Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu" na stronie 18
Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Protokołem PPP można połączyć ze sobą dwie sieci lokalne, ustanawiając połączenie między jednym systemem znajdującym się w centrali i drugim, znajdującym się w oddziale.

Pojedyncza linia:

Ten typ obsługi linii należy wybrać, aby zdefiniować linię PPP powiązaną z modemem analogowym. Opcja ta jest również używana dla linii dzierżawionych, w których modem nie jest potrzebny. Profil połączenia PPP zawsze używa tego samego zasobu portu komunikacyjnego serwera i5/OS.

Pojedyncza linia analogowa może w razie potrzeby zostać skonfigurowana jako współużytkowana przez profil odbiorcy i profil wybierający. Współużytkowanie zasobu dynamicznego jest nową funkcją rozszerzającą użyteczność zasobu. W wersjach wcześniejszych niż V5R2 zasób modemowy był zajęty tak długo, jak długo działał profil z niego korzystający. Ograniczało to wykorzystanie przez użytkownika jednego zasobu na sesję, nawet jeśli zasób był w stanie pasywnego oczekiwania. Obecnie stosowane są nowe reguły współużytkowania przy dostępie do określonych zasobów. Rozpatrzmy dwa przypadki: w pierwszym profil wybierający został uruchomiony przed profilem odbierającym, w drugim profil odbierający został uruchomiony przed profilem wybierającym. Zakładamy, że współużytkowanie zasobów zostało włączone. W pierwszym przypadku uruchomiony profil wybierający połączy się pomyślnie. Profil odbierający, który został uruchomiony jako drugi, będzie oczekiwał, aż linia stanie się dostępna. Po zakończeniu połączenia wybieranego profil odbierający zażąda linii i zostanie uruchomiony. W drugim przypadku, uruchomiony profil odbierający będzie czekał na połączenia przychodzące. Jeśli nie nadejdzie połączenie przychodzące, profil wybierający, uruchomiony jako drugi, ″pożyczy″ linię od profilu odbierającego, który ją ″wypożyczy″. Następnie zostanie nawiązane połączenie wychodzące. Po zakończeniu połączenia profil wybierający odda linię do profilu odbierającego, który ponownie będzie gotów do przyjmowania połączeń przychodzących. Aby włączyć funkcję współużytkowania, kliknij zakładkę **modem** w opisie linii komutowanej i wybierz opcję **Włącz dynamiczne współużytkowanie zasobów** (Enable Dynamic Resource Sharing).

Obsługa linii pojedynczej jest używana również dla typów połączeń L2TP (linia wirtualna) i PPPoE (linia wirtualna). W przypadku typów połączeń L2TP (linia wirtualna) nie są wykorzystywane żadne sprzętowe zasoby portu komunikacyjnego. Inaczej mówiąc, pojedyncza linia użyta z połączeniem L2TP jest *wirtualna*, co oznacza, że nie wymaga do ustanowienia tunelu fizycznego ze sprzętu PPP. Pojedyncza linia używana w połączeniu PPPoE jest także wirtualna, dostarcza mechanizmu pozwalającego na traktowanie fizycznej linii Ethernet jako obsługującej zdalne połączenia linii PPP. Wirtualna linia PPPoE jest połączona z fizyczną linią Ethernet i używana do obsługi przesyłania danych protokołem PPP przez połączenie LAN Ethernet z modemem DSL.

Pula linii:

Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP używające linii z puli linii. Podczas uruchamiania połączenia PPP system wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie system nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

Puli linii można używać po to, aby nie definiować poszczególnych opisów linii dla profilu połączenia. W puli linii można określić jeden lub więcej opisów linii.

Pula linii umożliwia pojedynczemu profilowi połączenia obsłużenie wielokrotnych analogowych połączeń przychodzących lub pojedynczych połączeń wychodzących. Po zakończeniu połączenia PPP linia jest zwracana do puli linii.

W przypadku używania puli linii do obsługi jednoczesnych analogowych połączeń przychodzących, należy wskazać maksymalną liczbę połączeń przychodzących. Wartość tę należy podać podczas konfigurowania profilu połączenia na karcie **Połączenia** (Connections) okna dialogowego **Właściwości nowego profilu punkt z punktem** (New Point-to-Point Profile Properties). Aby wykorzystać pule linii dla pojedynczych połączeń ze zwiększonym pasmem, należy użyć ustawień protokołu multilink.

Zalety korzystania z puli linii:

- Nie trzeba przypisywać zasobu linii do połączenia PPP, dopóki nie zostanie on uruchomiony.

  W przypadku połączeń PPP wykorzystujących określoną linię, kiedy linia ta jest niedostępna, połączenie zostaje zakończone, chyba że włączone jest dynamiczne współużytkowanie zasobu. W przypadku połączeń korzystających z puli linii, podczas uruchamiania profilu musi być dostępna przynajmniej jedna linia z puli.

  Ponadto, jeśli zasoby zostały skonfigurowane jako współużytkowane (włączone współużytkowanie zasobu dynamicznego), zasób jest łatwiej dostępny dla połączeń wychodzących.
- Użycie profili połączeń na żądanie z pulą linii pozwala bardziej efektywnie wykorzystywać zasoby.

  System wybiera linię z puli tylko podczas połączenia na żądanie. Inne połączenia mogą wykorzystać tę linię w późniejszym czasie.
- Możliwe jest uruchomienie większej liczby połączeń PPP niż to wynika z zasobów, które mają je obsłużyć.

  Jeśli, na przykład, środowisko wymaga czterech unikalnych typów połączeń, ale w dowolnym momencie potrzebne są co najwyżej dwie linie, problem ten można rozwiązać wykorzystując pulę linii. Należy utworzyć cztery profile połączeń na żądanie i przypisać każdy z nich do puli zawierającej dwa opisy linii. Każda linia będzie mogła być użyta przez każdy z czterech profili, co pozwoli na to, aby w dowolnym momencie dwa połączenia były aktywne. Dzięki wykorzystaniu puli linii nie są potrzebne cztery osobne linie.

  Oprócz tego, jeśli środowisko stanowi kombinację klienta i serwera protokołu PPP, linie te mogą być współużytkowane (włączone współużytkowanie zasobu dynamicznego), zarówno gdy są używane jako linie pojedyncze, jak i gdy są umieszczone w puli linii. Profil uruchamiany jako pierwszy nie zatwierdza zasobu, dopóki połączenie nie jest aktywne. Na przykład jeśli uruchomiony zostaje serwer PPP oczekujący na połączenia przychodzące, może on ″wypożyczyć″ linię, z której korzysta, dla klienta PPP, który uruchamia się i ″pożycza″ współużytkowaną linię od serwera PPP.

Konfigurowanie puli linii

Pule linii definiuje się w profilu połączenia. Podstawowa konfiguracja puli linii została opisana w poniższych krokach:

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Utwórz profil połączenia służący do nawiązywania lub odbierania połączeń. Wybierz jedną z poniższych opcji:
   - Kliknij prawym przyciskiem myszy **Profile połączenia nadawcy** (Originator Connection Profiles), aby system rozpoczynał połączenie z systemem zdalnym.
   - Kliknij prawym przyciskiem myszy **Profile połączenia odbiorcy** (Receiver Connection Profiles), aby system zezwalał na połączenia przychodzące z systemów zdalnych i od użytkowników.
3. Wybierz **Nowy profil**.
4. W przypadku profilu inicjatora (nawiązywanie połączenia) wybierz: PPP, Linia komutowana i Tryb pracy (zazwyczaj wybieranie). Jako konfigurację łącza wybierz **Pula linii**. Kliknij przycisk **OK** - program System i Navigator otworzy okno właściwości dla tego profilu połączenia.

   Uwaga: Podczas tworzenia profili połączenia odbiorcy można również wybrać pulę linii. Opcja Pula linii (Line pool) może być wyświetlona lub nie, w zależności od wartości wpisanych w następujących polach: typ protokołu, typ połączenia i tryb pracy.
5. Na stronie Ogólne nazwij profil i wpisz jego opis.
6. Na stronie Połączenie wpisz nazwę puli linii i kliknij **Nowa**. Spowoduje to wyświetlenie okna dialogowego **Właściwości nowej puli linii**, w którym wyświetlone będą wszystkie dostępne dla tego systemu linie i modemy.
7. Wybierz linie, których chcesz użyć, i dodaj je do puli. Możesz także kliknąć opcję **Nowa linia**, aby zdefiniować nową.
8. Kliknij **OK**, aby zapisać tę pulę linii, i wróć do właściwości nowego profilu połączenia punkt z punktem.
9. Wpisz niezbędne informacje na pozostałych stronach (na przykład ustawienia TCP/IP i Uwierzytelnianie).
10. Profil połączenia sprawdza po kolei listę dostępnych linii (w puli) aż znajdzie dostępny zasób. Do obsługi połączenia będzie wykorzystywana znaleziona linia. Aby uzyskać więcej informacji, użyj pomocy programu System i Navigator.

Odsyłacze pokrewne

"Scenariusz: łączenie zdalnych klientów korzystających z łącz komutowanych z systemem" na stronie 13
Zdalni użytkownicy, tacy jak telepracownicy lub klienci korzystający z komputerów przenośnych, wymagają częstego dostępu do sieci LAN. Klienci korzystający z połączeń komutowanych uzyskują dostęp do systemu dzięki protokołowi Point-to-Point Protocol (PPP).

"Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu" na stronie 15
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia systemu z dostawcą ISP mogą użyć modemu. Komputery PC przyłączone do sieci LAN mogą łączyć się z Internetem korzystając z systemu operacyjnego i5/OS jako bramy.

"Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu" na stronie 18
Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Protokołem PPP można połączyć ze sobą dwie sieci lokalne, ustanawiając połączenie między jednym systemem znajdującym się w centrali i drugim, znajdującym się w oddziale.

Obsługa profili połączeń wielokrotnych:

Profile połączeń PPP, które obsługują połączenia wielokrotne, umożliwiają obsługiwanie wielu połączeń cyfrowych, analogowych oraz L2TP za pomocą jednego profilu połączenia.

Jest to przydatne, gdy wielu użytkowników potrzebuje połączenia z systemem. Nie trzeba wtedy określać osobnych profili połączeń PPP do obsługi każdej linii PPP. Opcja ta jest szczególnie przydatna w przypadku zintegrowanego modemu 4-portowego 2805, w którym cztery linie są dostępne z jednego adaptera.

Dla linii analogowych obsługiwanych przez profile połączeń wielokrotnych wszystkie linie w danej puli mogą być wykorzystane, aż do maksymalnej liczby połączeń. Dla każdej linii zdefiniowanej w puli jest uruchamiany osobny wątek profilu połączenia. Wszystkie wątki profilu połączenia czekają na połączenia przychodzące na odpowiednich liniach.

Lokalny adres IP dla profili połączeń wielokrotnych

Dla profilu połączenia wielokrotnego można użyć lokalnego adresu IP, pod warunkiem że istnieje i jest zdefiniowany w systemie. Istniejący adres IP można wybrać z rozwijanej listy lokalnych adresów IP. Zdalni użytkownicy będą mieli dostęp do zasobów sieci lokalnej, jeśli jako lokalny adres IP profilu PPP zostanie wybrany lokalny adres IP. Trzeba ponadto zdefiniować adresy IP ze zdalnej puli adresów IP, tak aby były w tej samej sieci co adresy lokalne IP.

Jeśli nie ma lokalnego adresu IP albo użytkownicy zdalni nie powinni mieć dostępu do sieci LAN, dla systemu należy zdefiniować wirtualny adres IP. Wirtualny adres IP jest zwany również interfejsem bezobwodowym. Profile połączeń PPP mogą używać takich adresów jako swoich lokalnych adresów IP. Ponieważ taki adres IP nie jest związany z fizyczną siecią, ruch do innych sieci dołączonych do systemu nie jest przekazywany automatycznie.

W celu utworzenia wirtualnego adresu IP, wykonaj poniższe czynności:

1. W programie System i Navigator rozwiń swój system, a następnie wybierz opcje **Sieć → Konfiguracja TCP/IP → IPV4 → Interfejsy** (Network > TCP/IP configuration > IPV4 > Interfaces).
2. Kliknij prawym przyciskiem myszy opcję **Interfejsy** i wybierz **Nowy interfejs → Wirtualny adres IP** (New Interface > Virtual IP).
3. Aby utworzyć nowy interfejs dla wirtualnego adresu IP, wykonuj instrukcje kreatora interfejsu. Profil połączenia PPP będzie mógł używać wirtualnego adresu IP od razu po jego utworzeniu. Aby użyć tego adresu z profilem, wybierz go z listy rozwijanej w polu **Lokalny adres IP** (Local IP address) na stronie Ustawienia TCP/IP (TCP/IP Settings).

   Uwaga: Wirtualny adres IP musi być aktywny przed uruchomieniem profilu połączenia wielokrotnego, w przeciwnym razie profil się nie uruchomi. Aby uaktywnić adres IP po utworzeniu interfejsu, należy wybrać opcję uruchomienia adresu IP podczas korzystania z kreatora interfejsu.

Pule zdalnych adresów IP dla profili połączeń wielokrotnych

Z profilami połączeń wielokrotnych można także używać pul zdalnych adresów IP. Typowy profil pojedynczego połączenia PPP pozwala na określenie tylko jednego zdalnego adresu IP, który jest udostępniany systemowi wywołującemu podczas nawiązywania połączenia. Ponieważ wielu wywołujących może teraz łączyć się równocześnie, pula zdalnych adresów IP jest stosowana do zdefiniowania adresu początkowego oraz zakresu dodatkowych adresów IP udostępnianych systemowi wywołującemu.

Ograniczenia pul linii

W połączeniach wielokrotnych występują następujące ograniczenia:

- Dana linia może być jednocześnie tylko w jednej puli linii. Po usunięciu linii z puli, może ona być wykorzystana przez inną pulę linii.
- Podczas uruchamiania wielu profili połączeń korzystających z puli linii wszystkie linie z puli zostaną użyte, aż do maksymalnej liczby połączeń określonej w profilu. Gdy nie ma wolnych linii, żadne nowe połączenie nie powiedzie się. Ponadto, kiedy nie ma dostępnych linii w puli, a jest uruchamiany inny profil, to zostanie on zakończony.
- Po uruchomieniu profilu pojedynczego połączenia, który ma pulę linii, system wykorzystuje tylko jedną linię z puli. Jeśli zostanie uruchomiony profil połączenia wielokrotnego korzystający z tej samej puli linii, pozostałe linie z puli są dostępne.

  Zadania pokrewne

  “Etap 1: konfigurowanie profilu terminatora L2TP dla dowolnego interfejsu na partycji, do której należą modemy” na stronie 28
  Aby utworzyć profil terminatora dla dowolnego interfejsu, wykonaj następujące czynności:

Pule zdalnych adresów IP:

System może korzystać z pul zdalnych adresów IP dla dowolnego odbierającego lub kończącego profilu PPP używanego do obsługi połączeń przychodzących typu multilink.

Dotyczy to protokołu L2TP oraz puli linii z maksymalną liczbą połączeń większą niż jedno. Funkcja ta umożliwia systemowi przypisanie unikalnego zdalnego adresu IP do każdego połączenia przychodzącego.

Pierwszy system, który ma być połączony, otrzymuje adres IP zdefiniowany w polu Początkowy adres IP. Jeśli adres IP jest już używany, systemowi przypisywany jest następny adres z zakresu. Zakładając na przykład, że początkowym adresem IP jest 10.1.1.1, a Liczba adresów IP wynosi 5, adresami w puli zdalnych adresów IP są 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4, i 10.1.1.5. Maska podsieci zdefiniowana dla puli zdalnych adresów ma zawsze postać 255.255.255.255.

Użycie puli zdalnych adresów IP wiąże się z poniższymi ograniczeniami:

- Do tej samej puli adresów może odnosić się więcej niż jeden profil połączenia. Jeśli wszystkie adresy IP w puli są używane, każde żądanie kolejnego połączenia będzie odrzucane, dopóki inne połączenie się nie zakończy i adres IP nie będzie dostępny.
- Aby przydzielić określone adresy IP niektórym zdalnym systemom, a innym systemom umożliwić korzystanie z puli, wykonaj poniższe czynności:
  1. Korzystając z zakładki **Uwierzytelnianie**, włącz uwierzytelnianie zdalnego systemu tak, aby została podana nazwa użytkownika zdalnego systemu.
  2. Zdefiniuj pulę zdalnych adresów dla wszystkich żądań połączeń przychodzących, które nie wymagają określonych adresów IP.
  3. Zdefiniuj zdalny adres IP dla określonego użytkownika zaznaczając **Zdefiniuj dodatkowy adres IP na podstawie identyfikatora użytkownika zdalnego systemu**, a następnie kliknij **Adresy IP zdefiniowane na podstawie nazwy użytkownika**.

W momencie łączenia się zdalnego użytkownika system sprawdzi, czy został dla niego zdefiniowany określony adres IP. Jeśli tak, adres taki jest udostępniany zdalnemu systemowi, w przeciwnym razie pobierany jest adres z puli zdalnych adresów IP.

Konfigurowanie modemu do połączeń PPP

Modem umożliwia nawiązywanie połączęń analogowych (na liniach dzierżawionych i komutowanych). Na potrzeby analogowych połączeń PPP można użyć modemu zewnętrznego, modemu wewnętrznego albo adaptera terminalu sieci cyfrowej z integracją usług (ISDN).

Odsyłacze pokrewne

"Rozwiązywanie problemów z protokołem PPP" na stronie 64
W przypadku wystąpienia problemów z połączeniem z wykorzystaniem protokołu PPP można użyć listy kontrolnej w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy ustalaniu objawu błędu oraz rozwiązywaniu problemów z połączeniem PPP.

Konfigurowanie nowego modemu

Nowy modem można skonfigurować, używając istniejącego opisu modemu lub w oparciu o opis modemu wykorzystywany wcześniej.

Aby skonfigurować nowy modem, wykonaj poniższe czynności.

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. Na karcie **Ogólne** (General) wpisz poprawne wartości we wszystkich polach.
4. Opcjonalnie: kliknij zakładkę **Parametry dodatkowe** (Additional Parameters) i dodaj wszystkie konieczne komendy inicjowania modemu.
5. Kliknij **OK**, aby zapisać wprowadzone dane, i zamknij stronę Właściwości nowego modemu.

Z użyciem istniejącego opisu modemu

Aby określić, czy można użyć istniejącego opisu modemu, wykonaj następujące kroki:

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Wybierz **Modemy**.
3. Przejrzyj listę modemów, aby znaleźć nazwę producenta i model zainstalowanego modemu.

   Uwaga: Jeśli modem jest wyświetlany na liście modemów domyślnych, nie trzeba wykonywać żadnych innych czynności.
4. Kliknij prawym przyciskiem opis modemu najbardziej zbliżony do posiadanego modelu i wybierz opcję **Właściwości**, aby obejrzeć łańcuchy komend.
5. Korzystając z podręcznika użytkownika modemu, podaj właściwy łańcuch komend dla posiadanego modemu.

   Jeśli łańcuch komend spełnia wymagania posiadanego modemu, użyj modemu domyślnego. W przeciwnym razie należy utworzyć opis modemu i dodać go do listy modemów.

Tworzenie opisu modemu w oparciu o istniejący opis modemu

Aby utworzyć opis modemu w oparciu o istniejący opis modemu, wykonaj następujące czynności:

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Wybierz **Modemy**.
3. Na liście modemów kliknij prawym przyciskiem myszy opcję **Ogólny Hayesa** i wybierz **Nowy modem na podstawie**.

4. W oknie dialogowym **Nowy modem** zmień łańcuchy komend, aby dopasować dane do wymagań modemu.

Odsyłacze pokrewne

"Rozwiązywanie problemów z protokołem PPP" na stronie 64
W przypadku wystąpienia problemów z połączeniem z wykorzystaniem protokołu PPP można użyć listy kontrolnej w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy ustalaniu objawu błędu oraz rozwiązywaniu problemów z połączeniem PPP.

Ustawianie łańcuchów komend modemu

W podręczniku użytkownika modemu można znaleźć równoważne łańcuchy komend. W opisie modemu należy użyć ustawień zalecanych przez producenta.

Tabela 9. Modemy zdefiniowane w systemie i łańcuchy komend

Właściwość modemu	**Łańcuch komendy poprawny dla większości modemów**
Zresetowanie modemu do ustawień fabrycznych	AT&F lub AT&Z
Inicjowanie modemu:	
Wyświetlenie słownych kodów wyniku	Q0 i V1
Normalne tryby CD i DTR	&C1 i &D2
Wyłączenie trybu echa	E0
Wykrywanie sygnału nośnego sygnałem DSR	&S1
Włączenie sprzętowego sterowania przepływem (RTS/CTS)	
Włączenie korekcji błędów i, opcjonalnie, kompresji (V.42/V.42 bis)	
Włączenie stałej szybkości linii DTE-DCE 115,2 kb/s (lub maksymalnej dozwolonej przez modem)	
(Opcjonalnie) Włączenie czasu nieaktywności, o ile modem obsługuje tę funkcję	
Tryb odpowiedzi modemu:	
Odpowiedź po *n* dzwonkach	S0=*n*, gdzie *n* = 1 lub 2
Rozłącz przy braku sygnału nośnego (połączenia) po *m* sekundach	S7=*m*
Tryb wybierania numeru	ATDT dla wybierania tonowego lub ATDP dla wybierania impulsowego

Przykład: konfigurowanie adaptera terminalu ISDN

Przykład przedstawia konfigurację adaptera terminalu sieci cyfrowej z integracją usług (ISDN).

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. Na karcie **Ogólne** (General) wpisz poprawne wartości we wszystkich **polach**.
4. Opcjonalne: Kliknij zakładkę **Parametry ISDN** (ISDN Parameters), aby dodać wszystkie konieczne komendy inicjowania modemu.

   W przypadku adapterów terminali ISDN komendy i parametry na tej liście są wysyłane do adaptera terminalu tylko w następujących sytuacjach:

   - kiedy komendy lub parametry na liście są zmieniane albo dodawane,
   - w wyniku różnych wykonywanych przez system działań związanych z odtwarzaniem po błędach.

   W związku z tym komendy te powinny ograniczać się do niżej wymienionych czynności:

   - ustawianie typu i wersji węzła komutacyjnego ISDN dostarczanych przez lokalną firmę telekomunikacyjną,
   - ustawianie numerów telefonów i identyfikatorów SPID dostarczanych przez lokalną firmę telekomunikacyjną,
   - ustawianie identyfikatorów TEI (Terminal Entry ID) dostarczanych przez lokalną firmę telekomunikacyjną,

- ustawianie protokołu kanału B (PPP od asynchronicznego do synchronicznego),
- inne ustawienia modemu o zmiennej długości parametrów, wymagające znaku powrotu karetki do oznaczenia długości parametru,
- zachowanie i aktywowanie nowych ustawień, tak aby były one przywracane po zresetowaniu lub wyłączeniu systemu,
- komenda testowania interfejsu stanu aktywnego *U* (ATD*x*), która pozwala systemowi określić moment synchronizacji z przełącznikiem ISDN centrali telefonicznej. *X* może określać dowolną cyfrę dozwoloną w numerach telefonów, ze znakami # i * włącznie.

5. Kliknij **Dodaj**, aby dodać komendy modemu. W oknie tym można dodać do listy komend komendę modemu z parametrem lub bez oraz opis. Gdy modem jest powiązany z opisem linii, każdej komendzie podanej bez parametru można przypisać określony parametr.
6. Kliknij **OK**, aby zapisać wprowadzone dane, i zamknij stronę Właściwości nowego modemu.

Odsyłacze pokrewne

"Adaptery terminali ISDN" na stronie 39
Sieć ISDN udostępnia połączenie cyfrowe umożliwiające komunikację różnych aplikacji multimedialnych łączącą głos, dane i obrazy wideo.

Przypisanie modemu do opisu linii

W temacie przedstawione zostały czynności związane z przypisaniem modemu do opisu linii.

1. W programie System i Navigator wybierz swój system i rozwiń kolejno **Sieć → Usługi zdalnego dostępu → Profile połączenia nadawcy lub Profile połączenia odbiorcy** (Network > Remote Access Services > Originator Connection Profiles or Receiver Connection Profiles).
2. Wybierz jedną z poniższych opcji:
   - Aby pracować z istniejącym profilem połączenia, kliknij prawym przyciskiem myszy profil połączenia i wybierz **Właściwości**.
   - Aby pracować z nowym profilem połączenia, utwórz go.
3. Na stronie Właściwości nowego profilu PPP wybierz zakładkę **Połączenie** i kliknij **Nowe**.
   - Wprowadź nazwę konfiguracji łącza.
   - Kliknij **Nowa**, aby otworzyć okno Właściwości nowej linii.
4. W oknie Właściwości nowej linii kliknij zakładkę **Modem** i wybierz z listy modem. Wybrany modem zostanie przypisany do opisu tej linii. Modemy wewnętrzne powinny mieć wybrane już odpowiednie definicje. Więcej informacji zawiera pomoc elektroniczna.

Można tak skonfigurować profil połączenia nadawcy, aby ten pożyczał linię PPP i modem przypisane do profilu połączenia odbiorcy oczekującego na połączenia przychodzące. Po zakończeniu połączenia linia PPP i modem są oddawane profilowi połączenia odbiorcy. Aby włączyć tę nową funkcję, wybierz opcję **Włącz dynamiczne współużytkowanie zasobów** (Enable dynamic resource sharing) na karcie **Modem** okna konfiguracji linii PPP. Linie PPP można konfigurować na karcie **Połączenie** (Connection) w profilu połączenia nadawcy lub odbiorcy.

Zadania pokrewne

"Tworzenie profilu połączenia" na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie w systemie profilu połączenia.

Konfigurowanie zdalnego komputera PC

Aby połączyć się z platformą System i z komputera osobistego (PC) z dowolnym 32-bitowym systemem operacyjnym Windows, należy sprawdzić poprawność instalacji i konfiguracji modemu oraz czy zainstalowano protokół TCP/IP oraz Dial-Up Networking.

Informacje na temat konfigurowania Dial-Up Networking dla komputera PC zawiera dokumentacja systemu Microsoft Windows. Upewnij się, czy zostały wprowadzone następujące informacje:

- Jako typ połączenia modemowego powinno być ustawione **PPP**.

- Jeśli używasz haseł szyfrowanych, sprawdź, czy w tym celu stosowany jest protokół CHAP-MD5 (protokół MS-CHAP nie jest obsługiwany przez system operacyjny i5/OS). Niektóre wersje systemu Windows nie obsługują bezpośrednio protokołu MD-5 CHAP, ale można go skonfigurować z pomocą firmy Microsoft.
- W przypadku haseł niezaszyfrowanych (lub niezabezpieczonych) automatycznie używany jest protokół Password Authentication Protocol (PAP). System nie obsługuje żadnego innego typu protokołu niezabezpieczonego.
- Zwykle adresowanie IP jest definiowane przez system zdalny lub system operacyjny i5/OS. Jeśli chcesz użyć alternatywnych metod adresowania IP (na przykład definiować własne adresy IP), sprawdź, czy konfiguracja systemu umożliwia obsługę danej metody.
- Adres IP serwera DNS, jeśli istnieje.

Konfigurowanie dostępu do Internetu poprzez AT&T Global Network

W przypadku komunikacji z siecią AT&T Global Network wymagane są specjalne profile.

W celu skorzystania z tej usługi można użyć kreatora AT&T Global Network Dial Connection, który pomoże skonfigurować profil połączenia wybierającego sieć AT&T Global Network. Kreator prowadzi użytkownika przez mniej więcej osiem paneli, a cała procedura trwa około dziesięciu minut. Działanie kreatora można w dowolnym momencie anulować bez zapisywania jakichkolwiek danych.

Połączenie z AT&T Global Network może być wykorzystywane przez następujące typy aplikacji:

- **Mail Exchange**: umożliwia okresowe pobieranie poczty z jednego konta AT&T Global Network i wysyłanie jej do systemu w celu dostarczenia użytkownikom programu Lotus Mail lub protokołu SMTP (Simple Mail Transfer Protocol).
- **Dial-up Networking**: umożliwia korzystanie z innych aplikacji obsługujących połączenia telefoniczne z siecią AT&T Global Network, tak jak przy standardowym trybie dostępu do Internetu.

Profile połączeń z siecią AT&T Global Network wymagają takiej samej obsługi, jak wszystkie inne profile połączeń PPP.

Aby użyć kreatora połączenia AT&T Global Network Dial Connection, niezbędny jest jeden z poniższych adapterów:

- 2699: adapter I/O Two-line WAN
- 2720: adapter I/O PCI WAN/Twinaxial
- 2721: adapter I/O PCI Two-line WAN
- 2745: adapter I/O PCI Two-line WAN (zastępuje adapter 2721)
- 2771: dwuportowy adapter WAN IOA ze zintegrowanym modemem V.90 na porcie 1 i standardowym interfejsem komunikacyjnym na porcie 2. Aby wykorzystać port 2 adaptera 2771, wymagany jest modem zewnętrzny lub adapter terminalu ISDN z odpowiednim kablem.
- 2772: dwuportowy zintegrowany modem V.90 WAN IOA
- 2793/576C: dwuportowy adapter WAN IOA ze zintegrowanym modemem V.92 na porcie 1 i standardowym interfejsem komunikacyjnym na porcie 2 (zastępuje model 2771).
- 2805: czteroportowy adapter WAN IOA ze zintegrowanym modemem analogowym V.92 (zastępuje modele 2761 i 2772).

Aby uruchomić kreatora AT&T Global Network Dial Connection, należy zebrać następujące informacje o lokalnym środowisku:

- dla aplikacji wymieniających pocztę lub obsługujących sieciowe połączenia przez linię telefoniczną informacje o koncie w sieci AT&T Global Network (numer konta, identyfikator użytkownika i hasło),
- dla aplikacji wymieniających pocztę, adresy IP serwerów poczty i serwera nazw domen,
- nazwę modemu używanego przy połączeniach poprzez pojedynczą linię.

Aby uruchomić kreatora połączenia AT&T Global Network Dial Connection, wykonaj poniższe kroki:

1. W programie System i Navigator rozwiń swój system i kolejno **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Prawym przyciskiem myszy kliknij **Profile połączenia inicjatora** i wybierz opcję **Nowe połączenie AT&T Global Network Dial Connection**.
3. Po uruchomieniu kreatora połączenia telefonicznego z siecią AT&T Global Network kliknij opcję **Pomoc** w celu uzyskania informacji niezbędnych do wypełnienia panelu.

Kreatory połączeń

Kreatory połączeń ułatwiają konfigurowanie profilu połączenia.

Kreator nowego połączenia telefonicznego

Poniższy kreator zawiera opis konfiguracji profilu połączenia modemowego w celu uzyskania dostępu do usług dostawcy ISP lub sieci intranet. Aby podać wszystkie dane wymagane przez kreatora, potrzebne są informacje od administratora sieci lub dostawcy ISP. Więcej informacji na temat tego kreatora można znaleźć w pomocy elektronicznej.

Kreator połączenia uniwersalnego IBM

Kreator zawiera opis czynności związanych z konfigurowaniem profilu, którego może użyć oprogramowanie elektronicznego wsparcia klienta do połączenia z firmą IBM. Obsługa usług elektronicznych monitoruje dane środowisko i5/OS w celu wskazania indywidualnych poprawek dla systemu i sytuacji.

Informacje pokrewne

Połączenie uniwersalne

Konfigurowanie strategii dostępu dla grupy

Folder **Strategie dostępu do grupy** w katalogu Profile połączenia odbiorcy zawiera opcje umożliwiające konfigurowanie parametrów połączenia dla grupy zdalnych użytkowników. Dotyczą one tylko połączeń PPP pochodzących ze zdalnych systemów i odbieranych w systemie lokalnym.

Aby skonfigurować nową strategię dostępu dla grupy, wykonaj następujące czynności:

1. W programie System i wybierz swój system i rozwiń kolejno **Sieć → Usługi zdalnego dostępu → Profile połączenia odbiorcy** (Network > Remote Access Services > Receiver Connection Profiles).
2. Kliknij prawym przyciskiem myszy opcję **Strategie dostępu do grupy** i wybierz opcję **Nowa strategia dostępu do grupy**.
3. Na karcie **Ogólne** (General) wpisz nazwę i opis nowej strategii dostępu do grupy.
4. Kliknij zakładkę **Multilink** i skonfiguruj połączenie typu multilink.

   Konfigurowanie połączenia typu multilink określa połączenie wielu linii fizycznych w jedną wiązkę. W pojedynczej wiązce może być od 1 do 6 linii. Ustawienia typu linii nie są znane aż do momentu nawiązania połączenia. Wartością domyślną jest zawsze 1. Strategia dostępu do grupy może zwiększyć lub ograniczyć możliwości protokołu multilink dla określonego użytkownika.

   Maksymalna liczba łączy dla pakunku określa maksymalną liczbę łączy (lub linii) tworzących pojedynczą linię logiczną. Maksymalna liczba linii nie może być większa niż liczba wolnych linii dostępnych w momencie zastosowania strategii dostępu do grupy wobec sesji z profilem PPP.

   Sprawdź **Wymagany protokół przydziału szerokości pasma**, jeśli połączenie ma zostać ustanowione tylko w przypadku, gdy zdalny system obsługuje protokół BACP (Bandwidth Allocation Protocol). Jeśli system nie będzie obsługiwał tego protokołu, możliwe będzie tylko pojedyncze łącze.
5. Kliknij zakładkę **Ustawienia TCP/IP**, aby włączyć jedną z następujących opcji:

   Zezwól, aby zdalny system miał dostęp do innych sieci (przekazywanie IP). Ta opcja określa, czy przekazywanie IP jest pożądane. Wybranie tej opcji powoduje, że system będzie działał jako router dla danego

połączenia. Dzięki temu datagramy IP nieprzeznaczone dla tego systemu będą przekazywane dalej. Jeśli opcja ta nie zostanie wybrana, protokół IP będzie odrzucał te datagramy z systemu zdalnego, których punktem docelowym nie będzie żaden adres lokalny w danym systemie.

Brak zezwolenia użytkownika na przesyłanie datagramów IP może wynikać z konieczności ochrony systemu. Z drugiej strony dostawcy ISP zazwyczaj udostępniają przekazywanie IP. Należy zauważyć, że funkcja ta działa tylko wtedy, gdy włączone jest przesyłanie dużych datagramów IP. W przeciwnym razie, nawet pomimo zaznaczenia tej opcji, funkcja jest ignorowana. Ustawienie przekazywania datagramów IP dla całego systemu można sprawdzić na karcie **Ogólne** (General) na stronie Właściwości IPv4 (IPv4 Properties).

Żądaj kompresji nagłówka TCP/IP (VJ). Opcja ta określa, czy informacje znajdujące się w nagłówku mają być kompresowane przez protokół IP po nawiązaniu połączenia. Na ogół kompresja zwiększa wydajność. Jest to szczególnie istotne w przypadku ruchu interakcyjnego lub wolnych linii do transmisji szeregowej. Kompresja nagłówka jest zgodna z metodą Van Jacobsona (VJ) zdefiniowaną w standardzie RFC 1332. W przypadku połączeń PPP kompresja jest negocjowana po ustanowieniu połączenia. Jeśli drugi koniec połączenia nie obsługuje kompresji VJ, wówczas system ustanawia połączenie, które nie używa kompresji.

Dla tego połączenia użyj reguł pakietów IP. Opcja ta określa, czy w przypadku danej strategii dostępu do grupy zastosować reguły filtrowania. Reguły filtrowania sterują ruchem pakietów IP w sieci. Można użyć tego komponentu filtrowania pakietów IP do zabezpieczenia systemu przez filtrowanie pakietów zgodnie z określonymi regułami. Reguły te są ustalane na podstawie informacji zawartych w nagłówku pakietu.

Stosowanie strategii dostępu do grupy w przypadku zdalnych użytkowników

W przypadku zdalnego dostępu strategię dostępu do grupy można zastosować dopiero po zakończeniu ustawiania właściwości PPP nowego profilu połączenia odbiorcy.

Aby zastosować strategię dostępu do grupy w przypadku zdalnego połączenia, należy wykonać następujące czynności:

1. Kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie.
2. Kliknij opcję **Wymagana weryfikacja przez serwer iSeries tożsamości systemu zdalnego**.
3. Wybierz **Uwierzytelnianie lokalne za pomocą listy weryfikacji**.
4. Jeśli lista weryfikacji już istnieje, wybierz ją z listy i kliknij polecenie **Otwórz**. Jeśli dopiero ją tworzysz, wpisz nazwę nowej listy weryfikacji i kliknij **Nowa**.
5. Kliknij **Dodaj**, aby dodać nowego użytkownika do listy weryfikacji.
6. W oknie dialogowym Dodawanie użytkownika:
   a. Wybierz protokół uwierzytelniania zdefiniowany dla nazwy użytkownika.
   b. Wpisz nazwę użytkownika i hasło.

      Uwaga: Ze względów bezpieczeństwa zaleca się nieużywanie tego samego hasła co w przypadku protokołu CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) oraz PAP (Password Authentication Protocol).

   c. Zaznacz pole **Przypisanie użytkownikowi strategii dostępu do grupy**, z rozwijanej listy wybierz strategię dostępu do grupy, a następnie kliknij **Otwórz**.

   Właściwości strategii dostępu do grupy można zmodyfikować lub pracować z istniejącymi ustawieniami.
7. Kliknij **OK**, aby zakończyć konfigurację i powrócić do strony Właściwości PPP.

Odsyłacze pokrewne

“Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP” na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Informacje pokrewne

Filtrowanie IP i translacja adresów sieciowych

Przypisywanie reguł filtrowania pakietów IP do połączeń PPP

Dzięki zbiorowi reguł pakietów można ograniczyć dostęp użytkownika lub grupy użytkowników do adresów IP w sieci.

W temacie Filtrowanie pakietów IP i translacja adresów sieciowych Centrum informacyjnego omówiono sposób tworzenia reguł pakietów IP, które można zastosować do profili połączeń PPP.

Istniejące reguły filtrowania pakietów IP można obejrzeć na dwa sposoby:

- Poziom profilu połączenia
  1. Po wypełnieniu **Właściwości PPP** dla **Profilu połączenia odbiorcy** wybierz stronę Ustawienia TCP/IP i kliknij **Zaawansowane**.
  2. Zaznacz pole **Dla tego połączenia użyj reguł pakietów IP** i wybierz z listy identyfikator filtru PPP.
  3. Kliknij **OK**, aby zatwierdzić filtr PPP dla danego profilu połączenia.
- Poziom użytkownika
  1. Otwórz istniejącą strategię dostępu dla grupy lub utwórz nową.
  2. Kliknij Ustawienia TCP/IP.
  3. Zaznacz pole **Dla tego połączenia użyj reguł pakietów IP** i wybierz z listy identyfikator filtru PPP.
  4. Kliknij **OK**, aby zatwierdzić filtr PPP.

Odsyłacze pokrewne

"Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP" na stronie 23
Strategia dostępu dla grupy rozpoznaje odrębne grupy użytkowników dla danego połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień bezpieczeństwa dla całej grupy. W połączeniu z filtrowaniem IP strategia umożliwia zezwolenie na dostęp lub ograniczenie dostępu do określonych adresów IP w sieci.

Udostępnianie usług RADIUS i DHCP profilom połączeń

Poniżej przedstawiono procedurę udostępniania usług RADIUS i DHCP (Dynamic Host Configuration Protocol) profilom połączeń odbiorców.

1. W programie System i Navigator wybierz swój system i rozwiń **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services).
2. Kliknij prawym przyciskiem myszy **Usługi zdalnego dostępu** i wybierz **Usługi**.
3. Wybierz zakładkę **Klient WAN DHCP**. Włączy to automatycznie usługę DHCP i wykryje, który serwer DHCP i jacy agenci przekazujący (jeśli istnieją) działają w systemie.
4. Aby włączyć usługi RADIUS, wybierz zakładkę **RADIUS**.
   a. Zaznacz pole **Włącz połączenie z RADIUS Network Access Server**.
   b. Zaznacz **Włącz RADIUS dla uwierzytelniania**.
   c. W zależności od zastosowanego rozwiązania RADIUS można również wybrać rozliczanie RADIUS i konfigurację adresu TCP/IP.
5. Kliknij przycisk **Ustawienia NAS RADIUS**, aby skonfigurować połączenie z serwerem RADIUS.
6. Kliknij **OK**, aby wrócić do programu System i Navigator.

Odsyłacze pokrewne

"Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS" na stronie 21
Serwer dostępu do sieci (Network Access Server - NAS) działający w systemie może kierować żądania uwierzytelnienia od klientów z połączeniem modemowym do odrębnego serwera RADIUS (Remote Authentication Dial In User Service). Po uwierzytelnieniu serwer RADIUS może również sterować adresami IP przydzielonymi użytkownikowi.

Zarządzanie protokołem PPP

W tym temacie znajdują się informacje dotyczące zadań zarządzania protokołem PPP, które można wykonać w systemie.

Odsyłacze pokrewne

“Informacje związane z usługami zdalnego dostępu (Remote Access Services)” na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Ustawianie właściwości dla profili połączeń PPP

Podczas tworzenia profilu połączenia w oknie Konfigurowanie profilu połączenia PPP, należy wybrać protokół, typ połączenia oraz tryb pracy nowego profilu połączenia.

Po wprowadzeniu tych informacji wyświetlona zostanie strona z właściwościami profilu połączenia. Zawartość tej strony oraz kolejność zakładek jest uzależniona od wprowadzonych informacji. Właściwości profili połączeń inicjatora i odbiorcy różnią się od siebie.

Z poniższych wskazówek można skorzystać po wprowadzeniu wszystkich informacji w oknie Właściwości nowego profilu połączenia PPP. Wybrane na każdej stronie ustawienia zależą od lokalnego środowiska i typu konfigurowanego połączenia. W pomocy elektronicznej programu System i Navigator znajduje się opis wszystkich opcji wyświetlonych w oknie. Więcej informacji można również znaleźć w procedurach i przykładach połączeń PPP.

Monitorowanie aktywności połączeń PPP

Podgląd profilu połączenia i protokołu sesji można uzyskać w programie System i Navigator.

Zadania połączeń PPP:

- Do zarządzania poszczególnymi wątkami połączeń PPP są używane dwa zadania sterujące połączeniami PPP. Zadania te są uruchamiane w podsystemie QSYSWRK:
  - QTPPPCTL - Główne zadanie sterujące połączeniem PPP. Jest to zadanie zarządzające wszystkimi wątkami połączeń PPP.
  - QTPPPL2TP - serwer L2TP. Zadanie zarządzające ustanawianiem tunelu L2TP. Jest ono uruchamiane, tylko jeśli uruchomiony jest profil L2TP.
- Wątki połączeń PPP działają w podsystemie QTPPPCTL z nazwą użytkownika QTCP.
- Zadania połączeń SLIP są uruchamiane w podsystemie QSYSWRK pod nazwą użytkownika QTCP. Istnieją dwa typy nazw zadań połączeń SLIP:
  - QTPPDIAL*nn* to zadania połączeń wychodzących, gdzie *nn* jest dowolną liczbą od 1 do 99.
  - QTPPANS*nnn* to zadania połączeń przychodzących, gdzie *nnn* jest dowolną liczbą od 1 do 999.

Praca z profilami połączeń:

1. W programie System i Navigator rozwiń swój system i kolejno **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services). Wybierz **Profil połączenia nadawcy** lub **Profil połączenia odbiorcy**.
2. W kolumnie Profil kliknij prawym przyciskiem dowolną nazwę profilu i wybierz jedną z poniższych opcji:
   - **Połączenia** otwiera okno z informacjami o wszystkich połączeniach przypisanych do tego profilu. W informacjach tych zawarte są dane o połączeniu bieżącym oraz połączeniach poprzednich. Dostępne są opcje umożliwiające wyświetlenie danych wyjściowych zadania, szczegółowych informacji o połączeniu, protokołów połączeń oraz protokołów komunikatów dla każdego z połączeń.
   - **Właściwości** otwiera stronę Właściwości w celu wyświetlenia bieżących właściwości połączenia.

Wyświetlanie informacji o połączeniu:

1. W programie System i Navigator rozwiń swój system i kolejno **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services). Wybierz opcję **Profil połączenia nadawcy** lub **Profil połączenia odbiorcy**.
2. W kolumnie Profil kliknij prawym przyciskiem myszy dowolną nazwę profilu połączenia o statusie innym niż Nieaktywny i wybierz **Połączenia**, aby wyświetlić informacje o połączeniu.

   Wyświetlone zostaną wszystkie połączenia dla danego profilu (bieżące oraz poprzednie). Bieżący status połączenia jest wskazywany w polu statusu. Informacje dodatkowe, takie jak identyfikator połączonego użytkownika, ID wątku, lokalny i zdalny adres IP oraz nazwa zadania PPP zostaną wyświetlone w zależności od statusu zadania PPP.
3. Aby przejrzeć dane wyjściowe zadania, szczegółowe informacje o połączeniu, protokoły połączeń lub protokoły komunikatów, kliknij prawym przyciskiem myszy połączenie w celu aktywowania odpowiednich przycisków.
4. Aby wyświetlić podsystem QTPPPCTL, kliknij przycisk **Zadania** (Jobs). W oknie połączeń kliknij prawym przyciskiem myszy nazwę zadania i wybierz polecenie **Dane wyjściowe drukarki** lub **Protokół zadania**; wyświetlone zostaną informacje o wszystkich wątkach połączeń powiązanych z QTPPPCTL.
5. Aby przejrzeć informacje szczegółowe o połączeniu, kliknij **Informacje szczegółowe**. Informacje te mogą zostać wyświetlone tylko dla połączeń aktywnych. Wyświetlone zostanie okno dialogowe z dodatkowymi informacjami o danym połączeniu.
6. Aby wyświetlić protokoły połączeń, kliknij przycisk **Protokół połączenia**.
7. Aby wyświetlić protokoły komunikatów, kliknij przycisk **Protokół komunikatu**.

Praca z danymi wyjściowymi PPP z systemu:

Aby pracować z danymi wyjściowymi PPP, w wierszu komend wpisz komendę WRKTCPPTP:

- Aby pracować ze wszystkimi aktywnymi zadaniami PPP (łączenie z QTPPPCTL oraz QTPPPL2TP), naciśnij klawisz F14 (Praca z zadaniami aktywnymi).
- Aby pracować z danymi wyjściowymi pojedynczego profilu połączenia, wybierz **opcję 8** (praca z danymi wyjściowymi) dla danego profilu.
- Aby wydrukować konfigurację profilu PPP, wybierz **opcję 6** (Drukuj) dla danego profilu. Następnie za pomocą komendy WRKSPLF przejrzyj wydruk.

Status połączenia:

Status profilu połączenia jest wyświetlany w polu **Status** każdego profilu znajdującego się na liście profili połączeń w opcji **Sieć → Usługi zdalnego dostępu** (Network > Remote Access Services) po wybraniu profilu nadawcy lub odbiorcy. Status indywidualnego połączenia można zobaczyć w oknie Połączenia.

Tabela 10. Opis statusu podstawowego

Opis statusu podstawowego	**Objaśnienie**
Oczekiwanie na żądania połączenia	Profil odbiorcy jest gotowy do połączenia
Oczekiwanie na połączenie przychodzące	System jest gotowy do połączenia
Łączenie	Trwa proces łączenia ze zdalnym systemem
Aktywne/Aktywne połączenia	Połączenie zostało nawiązane i zadanie jest wykonywane
Nieaktywny	Dla tego profilu połączenia nie ma w danej chwili uruchomionych zadań
Zakończone	Informacje dostępne
Terminator wieloprzeskokowy uruchamia inicjator wieloprzeskokowy	Trwa nawiązywanie połączenia wieloprzeskokowego
Połączenie wieloprzeskokowe jest aktywne	Połączenie wieloprzeskokowe zostało nawiązane pomyślnie

Tabela 11. Opis statusu dodatkowego

Opis statusu dodatkowego	Objaśnienie
Inicjowanie modemu	Inicjowanie modemu podczas uruchamiania połączenia modemowego
Oczekiwanie na połączenie modemowe	Serwer PPP jest w stanie nasłuchu
WYBIERANIE xxx-xxxx	Numer wybrany przez klienta połączenia modemowego
Wykryto połączenie przychodzące	Serwer PPP wykrył połączenie przychodzące
Modem połączony	Pomyślnie zakończono uzgadnianie PPP
Działające	Połączenie PPP jest aktywne
Połączenie zakończone	Połączenie zakończone przez węzeł sieci
Zatrzymane	Zakończył się profil lub zadanie
Niepowodzenie uwierzytelniania	Połączenie PPP nie powiodło się z powodu problemów z uwierzytelnianiem
Przekroczenie czasu nieaktywności połączenia	Połączenie PPP nie powiodło się z powodu przekroczenia czasu nieaktywności
Uzgadnianie adresów IP	Połączenie PPP zakończone z powodu problemów z uzgadnianiem IP
Brak odpowiedzi zdalnego modemu	Połączenie PPP nie powiodło się z powodu braku odpowiedzi z drugiej strony
Odrzucenie protokołu	Połączenie PPP nie powiodło się, niepowodzenie w uzgadnianiu NCP
Niepowodzenie ponownej próby	Połączenie PPP nie powiodło się z powodu przekroczenia licznika ponowień
Z węzła sieci otrzymano potwierdzenie sesji PPPoE	Uzgadnianie PPPoE zakończyło się pomyślnie
Nawiązano połączenie L2TP	Komunikat o zestawieniu tunelu L2TP

Rozwiązywanie problemów z protokołem PPP

W przypadku wystąpienia problemów z połączeniem z wykorzystaniem protokołu PPP można użyć listy kontrolnej w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy ustalaniu objawu błędu oraz rozwiązywaniu problemów z połączeniem PPP.

Bieżące oraz pokrewne informacje dotyczące poprawek PTF oraz rozwiązywania problemów są dostępne w serwisie WWW TCP/IP for i5/OS. Serwis ten zawiera najnowsze informacje uzupełniające lub zastępujące informacje zawarte w niniejszym temacie.

1. Wymagany materiał pomocniczy:
   - Typ zdalnego hosta, system operacyjny i poziom.
   - Poziom systemu operacyjnego serwera i5/OS.
   - Wszystkie zbiory wyjściowe zapisywane w kolejce wyjściowej pod tą samą nazwą, co profil.
   - Protokoły zadań podsystemów QTPPPCTL i QTPPPL2TP (dla profili L2TP).
   - Skrypt połączenia używany w danym środowisku.
   - Status profilu połączenia przed i po nieudanym połączeniu.
2. Zalecany materiał pomocniczy:
   - Opis linii.
   - Profil połączenia.

     Ustawienia profilu można wydrukować przy pomocy opcji 6 WRKTCPPTP.

- Typ i model modemu.
- Łańcuchy komend modemu.
- Śledzenie komunikacji.

Dokumentacja techniczna ITSO Redbook V4 TCP/IP for AS/400: More Cool Things Than Ever  zawiera informacje o problemach z protokołem PPP opisanych poniżej. Zawiera również szczegółowe informacje na temat rozwiązywania problemów.

Aby określić rodzaj problemu i znaleźć jego rozwiązanie, zapoznaj się z listą kontrolną przedstawioną w tabeli poniżej.

Tabela 12. Problemy z protokołem PPP opisane w dokumentacji technicznej (redbook) ITSO

Problem	Rozwiązanie
Konfiguracja sprzętowa modemu Błędna konfiguracja zworek i innych ustawień sprzętowych.	Sprawdź, czy modem został skonfigurowany dla odpowiedniego typu ramek. Dopuszczalne ustawienia to *Asynchroniczne* lub *Synchroniczne*. Informacje na ten temat można znaleźć w podręczniku modemu.
Komendy AT modemu Użyty modem nie występuje na predefiniowanej liście modemów programu System i Navigator.	Utwórz nowy modem.
Hasła i użytkownicy PPP Podczas próby połączenia PPP występują błędy związane z nazwą użytkownika i hasłem.	• Sprawdź, czy identyfikator użytkownika i hasło wprowadzono z uwzględnieniem małych i wielkich liter. • Sprawdź, czy protokół uwierzytelniania używany przez węzły sieci jest ten sam. • Nie używaj protokołu PAP na węźle, jeśli na drugim węźle został skonfigurowany protokół CHAP.
Linie PPP dla uruchomionego profilu połączenia Linie PPP są używane przez te same zasoby sprzętowe.	Zablokuj inne linie używające tych samych zasobów sprzętowych.
Protokół PPP Występują błędy związane z błędną konfiguracją protokołu PPP.	W niektórych sytuacjach, gdy węzły nie mogą komunikować się ze sobą w związku z błędami konfiguracyjnymi, może być konieczne sprawdzenie niższych poziomów protokołu PPP. Jeśli protokół PPP oraz protokół zadania PPP nie wykazują żadnych problemów, można wykorzystać funkcję śledzenia.

Pojęcia pokrewne

“Konfigurowanie modemu do połączeń PPP” na stronie 55
Modem umożliwia nawiązywanie połączeń analogowych (na liniach dzierżawionych i komutowanych). Na potrzeby analogowych połączeń PPP można użyć modemu zewnętrznego, modemu wewnętrznego albo adaptera terminalu sieci cyfrowej z integracją usług (ISDN).

“Konfigurowanie nowego modemu” na stronie 55
Nowy modem można skonfigurować, używając istniejącego opisu modemu lub w oparciu o opis modemu wykorzystywany wcześniej.

Odsyłacze pokrewne

“Informacje związane z usługami zdalnego dostępu (Remote Access Services)” na stronie 66
Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Informacje związane z usługami zdalnego dostępu (Remote Access Services)

Dokumentacja techniczna IBM (Redbooks) i serwisy WWW zawierają informacje związane z kolekcją tematów o usługach zdalnego dostępu (Remote Access Services - RAS). Wszystkie pliki PDF można wyświetlić lub wydrukować.

Dokumentacja techniczna IBM (Redbooks)

- Podręcznik IBM i5/OS IP Networks: Dynamic!
- V4 TCP/IP for AS/400: More Cool Things Than Ever

Serwisy WWW

Najnowsze poprawki PTF oraz informacje o konfiguracji protokołów PPP i L2TP można znaleźć korzystając z odsyłacza PPP w serwisie WWW TCP/IP for i5/OS . Serwis ten zawiera najnowsze informacje uzupełniające lub zastępujące informacje zawarte w niniejszej kolekcji tematów.

Odsyłacze pokrewne

“Plik PDF o usługach zdalnego dostępu (Remote Access Services)” na stronie 1
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.

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 podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

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

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

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

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

Informacje 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:

AIX
AS/400
eServer
i5/OS
IBM
IBM (logo)
iSeries
Lotus
OS/400
Redbooks
System i

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi 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.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i 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 lub 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