Systemy IBM - iSeries

Sieci
Usługi zdalnego dostępu: połączenia PPP

Wersja 5 Wydanie 4

Systemy IBM - iSeries

Sieci
Usługi zdalnego dostępu: połączenia PPP

Wersja 5 Wydanie 4

Uwaga

Przed korzystaniem z poniższych informacji oraz produktu, którego dotyczą, należy przeczytać informacje znajdujące się w sekcji “Uwagi”, na stronie 67.

Wydanie siódme (luty 2006)

Niniejsze wydanie dotyczy wersji 5, wydania 4, modyfikacji 0 systemu operacyjnego i5/OS (numer produktu 5722–SS1) oraz wszelkich kolejnych wersji i modyfikacji tego produktu, o ile nowe wydania nie wskazują inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Zdalne usługi dostępu: połączenia PPP

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

Jest to protokół połączenia najczęściej używany przez dostawców usług internetowych (ISP). Protokół PPP pozwala indywidualnym komputerom na dostęp do sieci, umożliwiając połączenie z Internetem. Serwer IBM iSeries obsługuje protokół PPP w ramach TCP/IP jako element obsługi łączności w sieci rozległej (WAN).

Protokół PPP łączy zdalny komputer z serwerem iSeries, umożliwiając wymianę danych między różnymi miejscami. W ten sposób systemy zdalne połączone z serwerem iSeries mają dostęp do zasobów serwera oraz do innych komputerów należących do tej samej sieci. Za pomocą protokołu PPP można także skonfigurować serwer iSeries w taki sposób, aby połączyć go z Internetem. Kreator połączenia modemowego programu iSeries Navigator przeprowadza przez proces tworzenia połączenia serwera iSeries z Internetem lub siecią wewnętrzną.

Co nowego w wersji V5R4

W poniższym temacie omówione są zmiany w funkcjach połączeń PPP usługi Remote Access Service dokonane w wersji V5R4 systemu.

Zmiany funkcji

- **Protokół połączeń**

  Protokoły połączeń stanowią istotne zapisy danych wysyłanych i odbieranych przez modem podczas sesji PPP. Są zapisywane i usuwane w oparciu o wartość parametru OUTPUT (*ERROR, *PRINT lub *NONE) komendy Uruchomienie połączenia modemowego TCP/IP (Start TCP/IP Point-to-Point - STRTCPPTP).

  W poprzednich wersjach systemu nazwy protokołów połączeń miały postać ″protokół połączenia*nnnnnn*″, gdzie *nnnnnn* oznaczało numer zadania *nnnnnn*/QTCP/QTPPPSSN.

  W wersji V5R4 wszystkie sesje PPP są uruchamiane w wątku *nnnnnn*/QTCP/QTPPPCTL. Nazwy zbiorów buforowych protokołów połączeń mają postać ″CL*mmmmmmmm*″, gdzie *mmmmmmmm* oznacza ID wątku. Umożliwia to dopasowywanie komunikatów sesji w protokole zadania QTPPPCTL (zawierają one pole Wątek.... 00000028) do odpowiednich protokołów połączeń.

- **QTPPPSSN i QTPPPL2SSN**

  – Zadania QTPPPSSN i QTPPPL2SSN (L2TP) są zadaniami sesji PPP w wersjach systemu IBM i5/OS wcześniejszych niż V5R4. Były one uruchamiane i kończone za pomocą komend STRTCPPTP oraz Zakończenie połączenia modemowego TCP/IP (End Point-to-Point TCP/IP - ENDTCPPTP) lub za pomocą komendy QTPPPL2TP podczas ustanawianiu lub zamykania tunelu. Można je również było uruchomić lub zakończyć automatycznie podczas rozpoczynania lub kończenia połączeń przez protokół multilink.

    Począwszy od wersji V5R4, protokół PPP nie używa zadań QTPPPSSN i QTPPPL2SSn. Sesje są uruchamiane jako wątki zadania QTPPPCTL.

  – W wersjach systemu i5/OS wcześniejszych niż V5R4 opcja 14 (Praca z zadaniem) komendy Praca z profilami TCP/IP połączenia modemowego (Work with Point-to-Point TCP/IP Profiles - WRKTCPPTP) powodowała wyświetlenie zadania aktywnej sesji. Czasami powodowała ona uruchomienie zadania QTPPPL2TP, jeśli nie istniała aktywna sesja PPP dla profilu L2TP.

    W wersji V5R4 opcja 14 komendy WRKTCPPTP powoduje wyświetlenie zadania QTPPPCTL, jeśli jest dla niego aktywny wątek sesji.

- **Protokół komunikatów**

  W wersji V5R4 wprowadzony został nowy zbiór buforowy protokołu komunikatów dla komunikatów sesji. Zawiera on komunikaty wątku sesji, komunikaty wątku początkowego będące wynikiem działań wykonanych dla sesji oraz komunikaty procesów potomnych.

Nazwa zbioru buforowego protokołu komunikatów ma postać ″ML*mmmmmmmm*″, gdzie *mmmmmmmm* oznacza ID wątku. Umożliwia to dopasowywanie do siebie protokołów połączeń, protokołów komunikatów i komunikatów sesji w protokole zadania QTPPPCTL (zawierają one pole Wątek.... 00000028).

- **QTPPPCTL i QTPPPL2TP**

  W wersji V5R4 zadanie QTPPPCTL uruchamia uruchamia sesje jako wątki, zamiast oddzielnych procesów, używając wielokrotnych wątków systemowych (QTPPPSSN I QTPPPL2SSN).

  Zadanie QTPPPCTL uruchamia sesję dodatkową oraz wątki połączeń w celu zastąpienia starych zadań połączeń i sesji QTPPPSSN oraz QTPPPL2SSN.

  Zadanie QTPPPCTL jest wartością zwracaną w aplikacyjnych interfejsach programistycznych (API) i interfejsie GUi programu iSeries Navigator przez żądania zadań sesji.

- **Adaptery ethernet**

  W wersji V5R4 lista adapterów ethernet obsługujących połączenia PPPoE została poszerzona o adaptery 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 i 573A.

- **PPPoE**

  W wersji V5R4 połączenia PPPoE mogą współużytkować adapter z połączeniami IPv4 i IPv6.

Jak zobaczyć, co jest nowe lub zmienione

Aby zmiany techniczne były lepiej widoczne, w niniejszych informacjach zastosowano następujące znaki:

- Symbol » oznacza początek nowych lub zmienionych informacji.
- Symbol « oznacza koniec nowych lub zmienionych informacji.

Więcej informacji dotyczących nowych lub zmienionych funkcji systemu można znaleźć w temacie Informacje dla użytkowników.

Drukowalne pliki PDF

Poniższy temat umożliwia wyświetlenie i wydrukowanie pliku PDF zawierającego poniższe informacje.

Aby wyświetlić lub pobrać dokument w formacie PDF, należy wybrać Usługi zdalnego dostępu: połączenia PPP (około 940 kB).

Inne informacje

Można również wyświetlać lub drukować następujące informacje:

- Podręczniki:
  - Najnowsze poprawki PTF i najnowsze informacje o konfiguracji protokołów PPP i L2TP dostępne są poprzez odsyłacz PPP na stronie iSeries server TCP/IP home page. Odsyłacz do danych, które uzupełniają lub zastępują informacje zawarte w tej kolekcji tematów.
- Dokumentacja techniczna IBM Redbooks:
  - Dokumentacja techniczna (redbook) ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) zawiera informacje dotyczące usług i aplikacji TCP/IP.
  - Dokumentacja techniczna (redbook) ITSO iSeries IP Networks: Dynamic! (SG24-6718) w opisuje usługi i aplikacje TCP/IP.

Zapisywanie plików PDF

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

1. W oknie przeglądarki kliknij prawym przyciskiem myszy wybrany dokument (jeden z powyższych odsyłaczy).

2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w ma zostać zapisany plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do wyświetlenia lub wydrukowania zawartości plików PDF niezbędny jest program Adobe Reader. Jego kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Pojęcia dotyczące protokołu PPP

Dzięki protokołowi PPP można połączyć serwer iSeries ze zdalnymi sieciami, komputerami PC, innymi serwerami iSeries lub z dostawcą ISP. Aby w pełni wykorzystywać ten protokół, należy poznać zarówno jego możliwości, jak i jego obsługę na serwerze iSeries.

Odsyłacze pokrewne

"Informacje pokrewne dotyczące protokołu PPP" na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Co to jest protokół PPP

Protokół Point-to-Point Protocol (PPP) jest to protokół TCP/IP używany do połączenia dwóch systemów komputerowych. Komputery wykorzystują protokół **PPP**, lub inaczej **protokół typu punkt z punktem (Point-to-Point)**, 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.

Protokół PPP jest internetowym standardem. Jest też najczęściej używanym przez dostawców usług internetowych protokołem połączeniowym. Można go wykorzystać do połączenia z dostawcą ISP, który umożliwia dostęp do Internetu.

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 dotyczących standardów RFC można znaleźć na stronie WWW RFC Editor.

- RFC1661 Protokół Point-to-Point
- RFC1662 Protokół PPP na ramkach typu HDLC
- RFC1994 Protokół PPP CHAP

Profile połączeń

Profile połączeń punkt z punktem definiują zestaw parametrów i zasobów dla określonych połączeń PPP. Profile, które wykorzystują takie ustawienia parametrów, można uruchomić podczas dodzwaniania (rozpoczynania) lub nasłuchiwania (odbioru) połączeń PPP.

Istnieją dwa rodzaje profili, które umożliwiają użytkownikom definiowanie zestawów charakterystyk połączenia PPP lub zestawu połączeń.

- **Profile połączenia nadawcy** są połączeniami typu punkt z punktem, które są inicjowane z lokalnego serwera iSeries i odbierane przez system zdalny. Przy pomocy tego obiektu można skonfigurować połączenia wychodzące.
- **Profile połączenia odbiorcy** są połączeniami typu punkt z punktem, które są inicjowane ze zdalnego systemu i odbierane przez lokalny serwer iSeries. Przy pomocy tego obiektu można skonfigurować połączenia przychodzące.

Profile połączeń określają, w jaki sposób powinno funkcjonować połączenie PPP. Informacje zawarte w tych profilach odpowiadają na następujące pytania:

- Jakiego typu protokół połączeniowy jest używany? (PPP lub Serial Line Internet Protocol - SLIP)
- Czy serwer iSeries łączy się z innym komputerem, inicjując połączenie telefoniczne (nadawca)? Czy serwer iSeries oczekuje na połączenie telefoniczne pochodzące z innego systemu (odbiorca)?
- Jaka linia komunikacyjna jest wykorzystywana przez połączenie?
- W jaki sposób serwer iSeries określa adres IP, którego należy użyć?
- W jaki sposób serwer iSeries powinien uwierzytelniać inny system? Gdzie powinny być przechowywane przez serwer iSeries 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.

Serwer iSeries przechowuje informacje konfiguracyjne w profilu połączenia. Informacje te dostarczają wymaganego przez serwer iSeries kontekstu umożliwiając ustanowienie połączenia PPP z innym systemem komputerowym. Profil połączenia zawiera następujące informacje:

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

  Typ połączenia określa rodzaj linii, z której korzysta połączenie, oraz czy jest to **wybieranie** (nadawca), czy **odpowiadanie** (odbiorca). Istnieje możliwość wyboru spośród poniższych typów połączenia:
  - Linia komutowana
  - Linia dzierżawiona (dedykowana)
  - L2TP (linia wirtualna)
  - PPPoE (linia wirtualna).

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

  Tabela zawierająca informacje o profilach połączenia nadawcy:

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 zawierająca informacje o profilach połączenia odbiorcy:

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 32
  Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących protokół PPP. Jeden z tych komputerów, serwer iSeries, może być zarówno inicjatorem, jak i odbiorcą.

Obsługa strategii dostępu do grupy

Obsługa strategii dostępu do grupy umożliwia administratorom sieci definiowanie użytkownika na podstawie strategii. Jest to pomocne przy zarządzaniu zasobami i umożliwia przypisywanie strategii sterowania dostępem indywidualnym użytkownikom podczas logowania do sieci poprzez sesje PPP lub L2TP.

Użytkownicy mogą być przypisywani do specyficznych klas, z których każda ma własną, unikalną strategię. Każda strategia dostępu do grupy definiuje ograniczenia dotyczące zasobów, jak na przykład liczbę linii w wiązce połączenia multilink, przekazywanie IP oraz stosowane reguły filtrowania pakietów IP. Dzięki obsłudze strategii dostępu do grupy administratorzy sieci mogą zdefiniować na przykład grupę Pracujący_z_domu, która umożliwia grupie użytkowników pełny dostęp do sieci oraz grupę Pracownicy_dostawcy mającą dostęp do ograniczonego zestawu usług.

Odsyłacze pokrewne

“Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE” na stronie 11
Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

“Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP” na stronie 24
Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

Scenariusze

Scenariusze opisane w poniższym temacie pomagają zrozumieć, jak działa protokół PPP oraz w jaki sposób można implementować środowisko PPP w sieci. Scenariusze te przedstawiają podstawowe zagadnienia związane z protokołem PPP. Mogą być wykorzystane zarówno przez początkujących, jak i doświadczonych użytkowników zanim zaczną oni planowanie i konfigurowanie zadań.

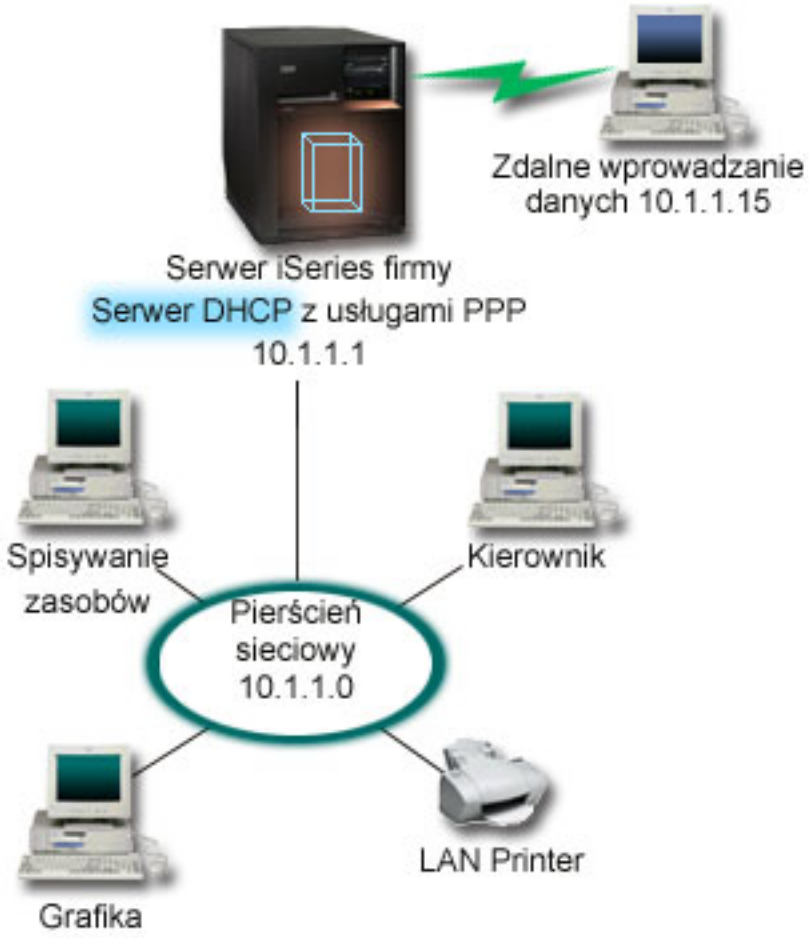
Odsyłacze pokrewne

“Informacje pokrewne dotyczące protokołu PPP” na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Przykład: protokoły PPP i DHCP działające na jednym serwerze iSeries

Informacje przedstawiające sposób konfigurowania serwera iSeries jako serwera DHCP dla sieci lokalnej i zdalnego klienta łączącego się przez połączenie komutowane.

Zdalni użytkownicy, tacy jak użytkownicy wykorzystujący połączenia komutowane, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP. Aby uzyskać dostęp do sieci, klienci z połączeniem komutowanym będą potrzebowali informacji o adresie IP, tak jak klienci bezpośrednio przyłączeni do sieci. Serwer DHCP iSeries może rozprowadzić dane IP między klientów z połączeniami komutowanymi PPP tak samo, jak między pozostałych klientów. Poniższa ilustracja przedstawia użytkownika zdalnego, którego praca wymaga połączenia komutowanego z siecią firmy.



Rysunek 1. Protokoły PPP i DHCP działające na jednym serwerze iSeries

Aby umożliwić pracownikowi zdalnemu efektywną pracę w sieci firmy, serwer iSeries używa kombinacji usługi Remote Access Service i protokołu DHCP. Funkcja Remote Access Service umożliwia dostęp do serwera iSeries przez połączenie komutowane. Poprawnie skonfigurowany serwer PPP wysyła do serwera DHCP żądanie dostarczenia do pracownika informacji TCP/IP po ustanowieniu przez niego połączenia komutowanego.

W poniższym przykładzie pojedyncza strategia podsieci DHCP odpowiada zarówno za klientów w siedzibie przedsiębiorstwa, jak i klientów korzystających z połączeń komutowanych.

Aby profil PPP opóźniał rozprowadzanie IP przez DHCP, należy go odpowiednio skonfigurować. Należy zmienić wartość metody przypisywania zdalnego adresu IP ze ″Stały″ na ″DHCP″ w ustawieniach protokołu TCP/IP profilu połączenia odbiorcy. Aby umożliwić klientom z połączeniami komutowanymi komunikację z innymi klientami sieci, np. z drukarką sieciową, należy również umożliwić przekazywanie IP w ustawieniach protokołu TCP/IP profilu oraz

właściwościach (stosu) konfiguracji TCP/IP. Jeśli przekazywanie IP zostanie określone tylko w profilu PPP, serwer iSeries nie będzie przekazywać pakietów IP. Przekazywanie IP musi być skonfigurowane zarówno w profilu, jak i stosie.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP zgodnym z definicją podsieci na serwerze DHCP. W poniższym przykładzie powinien on wynosić 10.1.1.1. Należy go również wykluczyć z puli adresów serwera DHCP, tak aby uniemożliwić jego przypisanie klientowi DHCP.

Planowanie konfiguracji DHCP dla klientów w siedzibie przedsiębiorstwa i klientów wykorzystujących protokół PPP

Tabela 3. Globalne opcje konfiguracji (dotyczą wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracji	opcja 1: maska podsieci	255.255.255.0
	opcja 6: serwer nazw domen	10.1.1.1
	opcja 15: nazwa domeny	mojafirma.com
Czy serwer dokonuje aktualizacji usługi DNS?		Nie
Czy serwer obsługuje klientów protokołu BOOTP?		Nie

Tabela 4. Podsieć dla klientów w siedzibie przedsiębiorstwa i klientów z połączeniami komutowanymi

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 podsieci nie przypisane przez serwer		10.1.1.1 (interfejs lokalny określony w Ustawieniach TCP/IP właściwości Profilu połączenia odbiorcy programu iSeries Navigator)

Pozostałe opcje

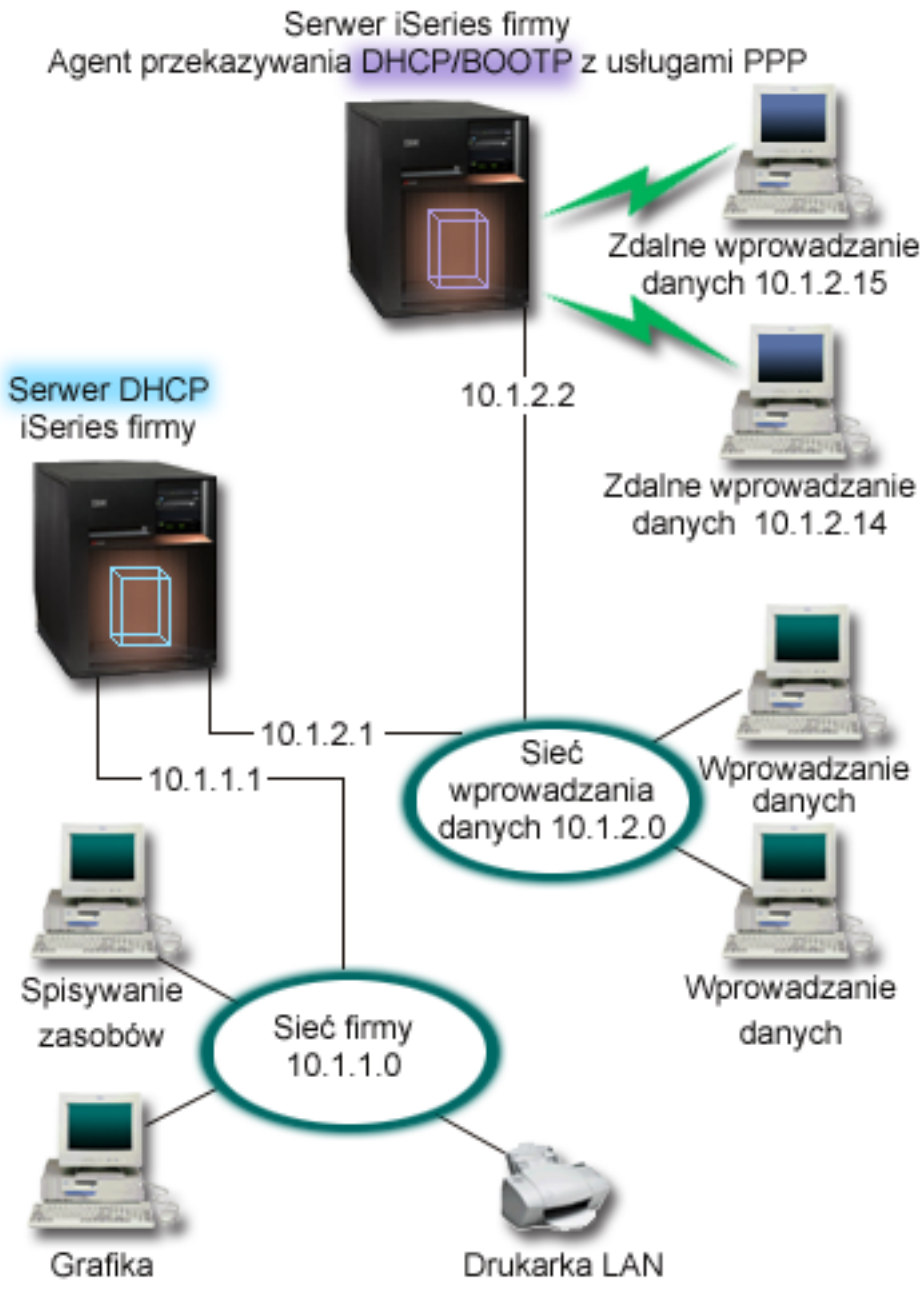
- Podaj DHCP jako metodę zdalnego adresu IP w profilu połączenia odbiorcy.
  1. Uaktywnij połączenie klienta sieci WAN używającego DHCP z serwerem DHCP lub przekazywanie połączeń za pomocą menu Usługi opcji Usługa Remote Access Service programu iSeries Navigator.
  2. Wybierz opcję Używaj DHCP dla metody przypisywania adresu IP we właściwościach Ustawień TCP/IP Profilu połączenia odbiorcy w programie iSeries Navigator.
- Udostępnij systemom zdalnym możliwość dostępu do innych sieci (przekazywanie IP) we właściwościach Ustawień TCP/IP Profilu połączenia odbiorcy w programie iSeries Navigator.
- Aktywuj przekazywanie datagramów IP we właściwościach Ustawień Konfiguracji TCP/IP w programie iSeries Navigator.

Przykład: profile DHCP i PPP działające na różnych serwerach iSeries

Informacje przedstawiające sposób konfiguracji dwóch serwerów iSeries jako sieciowego serwera DHCP oraz agenta przekazywania DHCP/BOOTP dla dwóch sieci lokalnych i klientów zdalnych z połączeniami komutowanymi.

W poprzednim przykładzie (Protokoły PPP i DHCP działające na jednym serwerze iSeries) przedstawiony został sposób umożliwienia zdalnym klientom z połączeniami komutowanymi dostępu do sieci za pomocą protokołów PPP i DHCP działających na jednym serwerze iSeries. Ze względu na fizyczny układ sieci lub kwestie bezpieczeństwa pożądane może być oddzielenie serwerów PPP i DHCP lub utworzenie dedykowanego serwera PPP bez usług DHCP.

Poniższa ilustracja przedstawia sieć, w której istnieją klienci z połączeniami komutowanymi, a strategie PPP i DHCP są zaimplementowane na różnych serwerach.



Rysunek 2. Usługa DHCP i profil PPP na różnych serwerach iSeries

Klienci usługi zdalnego wprowadzania danych (Remote Data Entry) łączą się połączeniem komutowanym z serwerem PPP iSeries. W profilu PPP na tym serwerze metoda zdalnego adresowania IP i właściwości przekazywania IP oraz stosu TCP/IP muszą być skonfigurowane tak, jak w poprzednim przykładzie. Ponadto, ponieważ serwer działa jako agent przekazywania DHCP, serwer TCP/IP agenta przekazywania DHCP musi być włączony. Umożliwia to serwerowi dostępu zdalnego iSeries przekazywanie pakietów DHCP DISCOVER do serwera DHCP. Serwer DHCP wyśle odpowiedź i rozprowadzi informacje TCP/IP między klientów z połączeniem komutowanym poprzez serwer PPP.

Serwer DHCP rozprowadza adresy IP do sieci 10.1.1.0 i 10.1.2.0. W sieci wprowadzania danych przypisze on klientom z połączeniem komutowanym i klientom podłączonym bezpośrednio adresy IP z zakresu 10.1.2.10 - 10.1.2.40. Dla

klienta wprowadzania danych należy ponadto określić adres routera (opcja 3) 10.1.2.1, aby umożliwić komunikację z siecią przedsiębiorstwa. Na serwerze DHCP iSeries włączona musi być opcja przekazywania IP.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP zgodnym z definicją podsieci na serwerze DHCP. W poniższym przykładzie powinien on wynosić 10.1.2.2. Należy go również wykluczyć z puli adresów serwera DHCP, tak aby uniemożliwić jego przypisanie klientowi DHCP.Adres IP interfejsu lokalnego musi być adresem, do którego serwer DHCP może wysyłać pakiety odpowiedzi.

Planowanie konfiguracji DHCP dla usługi DHCP z agentem przekazywania DHCP

Tabela 5. Globalne opcje konfiguracji (dotyczą wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracji	opcja 1: maska podsieci	255.255.255.0
	opcja 6: serwer nazw domen	10.1.1.1
	opcja 15: nazwa domeny	mojafirma.com
Czy serwer dokonuje aktualizacji usługi DNS?		Nie
Czy serwer obsługuje klientów protokołu BOOTP?		Nie

Tabela 6. Podsieć sieci firmy

Obiekt		**Wartość**
Nazwa podsieci		SiecFirmy
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 podsieci nie przypisane 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 podsieci nie przypisane przez serwer		10.1.2.1 (router) 10.1.2.15 (adres IP interfejsu lokalnego klienta usługi zdalnego wprowadzania danych) 10.1.2.14 (adres IP interfejsu lokalnego klienta usługi zdalnego wprowadzania danych)

Pozostałe opcje serwera iSeries, na którym działa protokół PPP

- Konfigurowanie agenta przekazywania protokołu BOOTP/DHCP serwera TCP/IP

Obiekt	**Wartość**
Adres interfejsu	10.1.2.2
Przekazuj pakiety do adresu IP serwera	10.1.2.1

- Podaj DHCP jako metodę zdalnego adresu IP w profilu połączenia odbiorcy.

1. Uaktywnij połączenie klienta sieci WAN używającego DHCP z serwerem DHCP lub przekazywanie połączeń za pomocą menu Usługi opcji Usługa Remote Access Service programu iSeries Navigator.
2. Wybierz opcję Używaj DHCP dla metody przypisywania adresu IP we właściwościach Ustawień TCP/IP Profilu połączenia odbiorcy w programie iSeries Navigator.

- Udostępnij systemom zdalnym możliwość dostępu do innych sieci (przekazywanie IP) we właściwościach Ustawień TCP/IP Profilu połączenia odbiorcy w programie iSeries Navigator (w celu umożliwienia klientom zdalnym komunikacji z siecią wprowadzania danych).
- Aktywuj przekazywanie datagramów IP we właściwościach Ustawień konfiguracji TCP/IP w programie iSeries Navigator (w celu umożliwienia klientom zdalnym komunikacji z siecią wprowadzania danych).

Scenariusz: ochrona dobrowolnego tunelu L2TP za pomocą IPSec

Poniższy scenariusz zawiera instrukcje konfigurowanie połączenia między komputerem w lokalnym oddziale firmy a komputerem w oddziale centralnym przy użyciu protokołu L2TP, chronionego przez IPSec. Oddział lokalny ma dynamicznie przypisany adres IP, a oddział centralny - statyczny, globalny adres IP.

Sytuacja

Firma ma niewielki oddział lokalny w innym stanie. Oddział może w dowolnej chwili zgłosić potrzebę dostępu do poufnych informacji o systemieiSeries w sieci wewnętrznej przedsiębiorstwa. Obecnie do zapewnienia dostępu używana jest kosztowna linia dzierżawiona. Firma pragnie zredukować koszty połączenia przy jednoczesnym zapewnieniu stałego dostępu do sieci intranet. Rozwiązaniem jest użycie dobrowolnego tunelu protokołu Layer 2 Tunnel Protocol (L2TP), który rozszerza sieć powodując, że oddziały stają się częścią sieci LAN. Sieć VPN zabezpiecza ruch danych w tunelu protokołu L2TP.

W przypadku dobrowolnego tunelu L2TP oddział lokalny ustanawia tunel bezpośrednio z serwerem sieciowym L2TP (LNS) sieci wewnętrznej przedsiębiorstwa. Koncentrator dostępu L2TP (LAC) znajduje się w oddziale klienckim. Tunel jest niewidoczny dla dostawcy ISP klienta, a więc dostawca ISP nie musi obsługiwać protokołu L2TP. Więcej informacji dotyczących protokołu L2TP można znaleźć w temacie Protokół Layer 2 Tunnel Protocol (L2TP).

Ważne: W poniższym scenariuszu przedstawione są bramy ochrony podłączone bezpośrednio do Internetu. Brak zapory firewall jest zamierzony celem uproszczenia scenariusza. Nie oznacza on, że zapora nie jest konieczna. Należy pamiętać o zagrożeniach występujących podczas pracy w Internecie.

Cele

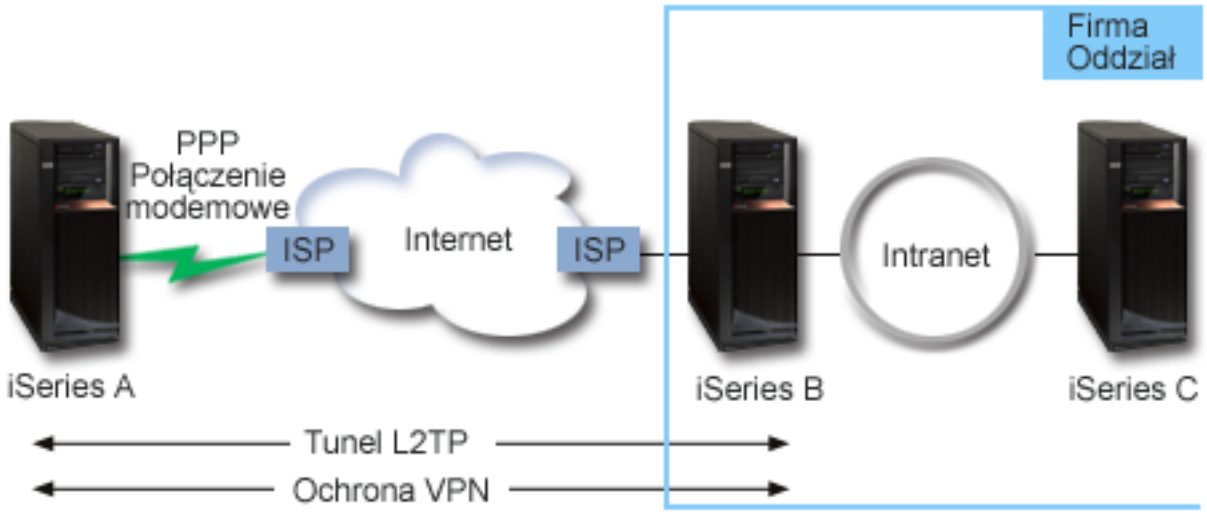
W poniższym scenariuszu system w oddziale lokalnym łączy się z siecią firmy poprzez system z bramą za pomocą tunelu L2TP chronionego przez VPN.

Główne cele scenariusza są następujące:

- System lokalny ma zawsze inicjować połączenie z siecią firmy.
- System lokalny ma być jedynym systemem w oddziale lokalnym wymagającym dostępu do sieci firmy. Innymi słowy, system ten pełni rolę hosta, a nie bramy.
- System w oddziale centralnym jest systemem hosta w sieci firmy.

Szczegóły

Poniższa ilustracja przedstawia charakterystykę sieci w tym scenariuszu:



iSeries-A

- Musi mieć dostęp do aplikacji TCP/IP na wszystkich serwerach wewnętrznej sieci firmy.
- Otrzymuje od dostawcy ISP dynamicznie przypisany adres IP.
- Musi obsługiwać protokół L2TP.

iSeries-B

- Musi mieć dostęp do aplikacji TCP/IP na serwerze iSeries-A.
- Jest w sieci o następujących parametrach: podsieć - 10.6.0.0, maska podsieci - 255.255.0.0. Podsieć odpowiada punktowi końcowemu danych tunelu VPN w oddziale centralnym.
- Łączy się z Internetem przy użyciu adresu IP 205.13.237.6. Jest to punkt końcowy połączenia. Oznacza to, że serwer iSeries-B wykonuje główne czynności zarządzania i stosuje technologię IPSec do przychodzących i wychodzących datagramów IP. Serwer iSeries-B łączy się z podsiecią przy użyciu adresu IP 10.6.11.1.

W terminologii L2TP serwer *iSeries-A* jest inicjatorem L2TP, a serwer *iSeries-B* jest terminatorem L2TP.

Zadania konfiguracyjne

Przy założeniu, że działająca konfiguracja TCP/IP istnieje, należy wykonać następujące zadania:

Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE

Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia 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 poprzez serwer iSeries.

Rysunek 3. Połączenie serwera iSeries do dostawcy ISP przy użyciu PPPoE

Rozwiązanie

Można obsługiwać połączenie PPPoE z dostawcą ISP poprzez serwer iSeries. Serwer iSeries umożliwia wykorzystanie nowego rodzaju linii wirtualnej PPPoE, która jest połączona z fizyczną linią Ethernet, używającą adaptera ethernet typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 lub 573A. Linia wirtualna obsługuje protokoły sesji PPP przez sieć LAN typu Ethernet połączoną z modemem DSL, który stanowi bramę do zdalnego dostawcy ISP. Umożliwia to użytkownikom sieci lokalnej szybki dostęp do Internetu przy użyciu połączenia PPPoE serwera iSeries. Po nawiązaniu połączenia pomiędzy serwerem iSeries a dostawcą ISP użytkownicy sieci LAN mają dostęp do dostawcy ISP przez połączenie PPPoE i korzystają z adresu IP przydzielonego do serwera iSeries. W celu zapewnienia dodatkowej ochrony, można zastosować dla linii wirtualnej PPPoE reguły filtrowania, które ograniczą pewną część ruchu przychodzącego.

Przykład konfiguracji

1. Skonfiguruj połączenie z dostawcą ISP.
2. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries.

   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 dokonaniu wyboru program iSeries Navigator wyświetli okno dialogowe **właściwości linii**.

   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 iSeries Navigator wyświetli okno dialogowe **Właściwości linii Ethernet**.

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

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 serwer iSeries uwierzytelnił się lub jeśli chcesz, aby serwer iSeriesuwierzytelnił zdalny serwer, kliknij przycisk **Uwierzytelnianie**, aby otworzyć stronę Uwierzytelnianie.
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 lokalnej łączenie się z Internetem przy użyciu adresu IP przydzielonego do serwera iSeries, wybierz opcję **Ukrywanie adresów (pełne maskowanie)**.
7. Kliknij przycisk **DNS**, aby otworzyć stronę DNS i wprowadź adres IP serwera DNS udostępnionego przez dostawcę ISP.
8. Jeśli chcesz określić podsystem, w którym ma być uruchamiane zadanie połączenia, kliknij przycisk **Inne**, aby otworzyć stronę Inne.
9. Kliknij **OK**, aby zakończyć.

Pojęcia pokrewne

“Obsługa strategii dostępu do grupy” na stronie 5
Obsługa strategii dostępu do grupy umożliwia administratorom sieci definiowanie użytkownika na podstawie strategii. Jest to pomocne przy zarządzaniu zasobami i umożliwia przypisywanie strategii sterowania dostępem indywidualnym użytkownikom podczas logowania do sieci poprzez sesje PPP lub L2TP.

Zadania pokrewne

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

Odsyłacze pokrewne

“Konfigurowanie połączenia” na stronie 51
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

“Uwierzytelnianie systemu” na stronie 44
Połączenia PPP serwera iSeries obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów dodzwaniających się do serwera iSeries, jak i połączeń do dostawcy ISP lub innego serwera, do którego dodzwania się serwer iSeries.

“Obsługa adresów IP” na stronie 42
Połączenia PPP pozwalają dowolnie zarządzać adresami IP w zależności od rodzaju profilu połączenia.

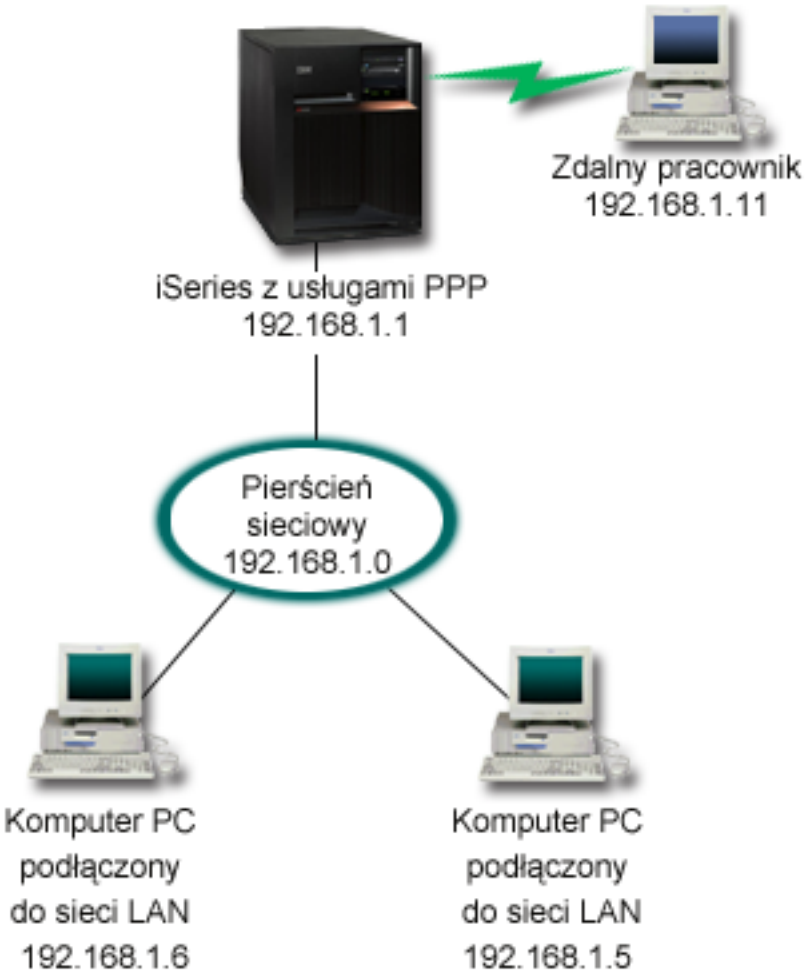
“Filtrowanie pakietów IP” na stronie 42
Filtrowanie pakietów IP jest ogranicza usługi dostępne dla indywidualnego użytkownika po zalogowaniu do sieci.

Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym

Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

Sytuacja

Administrator sieci LAN ma zapewnić poprawne działanie zarówno serwera iSeries, jak i klientów sieci. Zamiast przychodzić do pracy w celu zdiagnozowania i rozwiązania problemów może on wykonać te zadania zdalnie, na przykład z domu. Dopóki firma nie będzie miała ograniczeń dotyczących połączeń z Internetem, połączenie modemowe z serwerem iSeries można będzie nawiązać za pomocą protokołu PPP. Dodatkowo jedynym modemem, który można wykorzystać do nawiązania połączenia, jest modem 7852-400 elektronicznego wsparcia klienta (ECS).



Rysunek 4. Łączenie zdalnych klientów z serwerem iSeries

Rozwiązanie

Protokół PPP można wykorzystać do połączenia komputera PC z serwerem iSeries za pomocą modemu. Jeśli do tego typu połączeń wykorzystywany jest modem ECS, należy upewnić się, że jest on skonfigurowany do pracy zarówno w trybie synchronicznym, jak i niesynchronicznym. Powyższa ilustracja przedstawia serwer iSeries wykorzystujący

usługi PPP połączony z siecią LAN, w której znajdują się dwa komputery PC. Zdalny pracownik łączy się telefonicznie z serwerem iSeries, autoryzuje się i staje się częścią sieci LAN (192.168.1.0). W tym przypadku klientowi łączącemu się telefonicznie łatwiej jest przydzielić statyczny adres IP.

Do uwierzytelnienia na serwerze iSeries zdalny pracownik używa algorytmu CHAP-MD5. Ponieważ serwer iSeries nie obsługuje algorytmu MS_CHAP, należy upewnić się, że klient PPP wykorzystuje algorytm 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.

Na powyższym rysunku znajduje się tylko jeden klient połączenia modemowego, ponieważ modem ECS może nawiązać tylko jedno połączenie w określonym czasie. Informacje dotyczące jednoczesnej obsługi wielu klientów połączeń modemowych znajdują się w sekcji planowania opisującej zagadnienie zarówno od strony oprogramowania, jak i sprzętu.

Przykład konfiguracji

1. Skonfiguruj Dial-up Networking i utwórz połączenie modemowe na zdalnym komputerze PC.
2. Skonfiguruj Profil połączenia odbiorcy na serwerze iSeries.

   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 32
Poniższy temat zawiera informacje dotyczące tworzenia i administrowania połączeniami PPP.

Zadania pokrewne

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

Odsyłacze pokrewne

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

“Konfigurowanie połączenia” na stronie 51
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

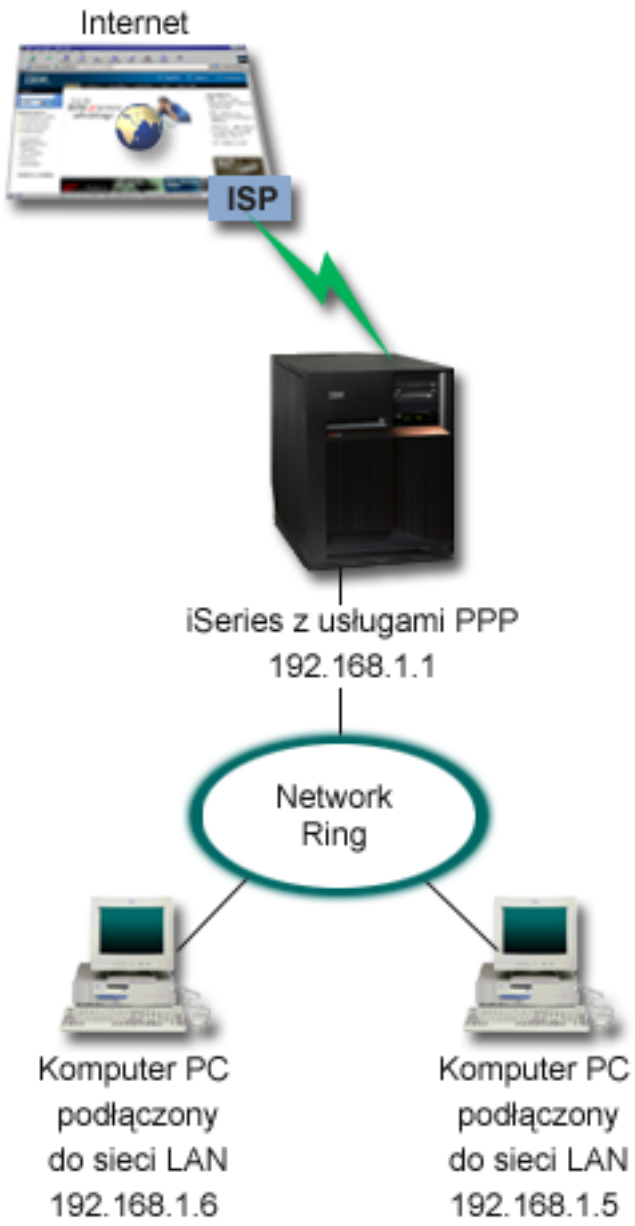
“Pula linii” na stronie 52
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP wykorzystujące linię z puli linii. Podczas uruchamiania połączenia PPP serwer iSeries wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie serwer nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu

Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą ISP mogą wykorzystać modem. Klienci PC przyłączeni do sieci LAN mogą łączyć się z Internetem, wykorzystując serwer iSeries jako bramę.

Sytuacja

Aplikacje wykorzystywane przez firmę wymagają, aby użytkownicy mieli dostęp do Internetu. Jeśli aplikacje te nie wymagają wymiany zbyt dużej ilości danych, istnieje możliwość wykorzystania modemu do połączenia z Internetem serwera iSeries oraz klientów sieci LAN. Poniższa ilustracja przedstawia przykład takiej sytuacji.



Rysunek 5. Łączenie sieci LAN z Internetem przy pomocy modemu

Rozwiązanie

Do połączenia serwera iSeries z dostawcą ISP można wykorzystać modem zintegrowany (lub inny kompatybilny). Aby ustanowić połączenie PPP z dostawcą ISP, należy utworzyć na serwerze profil nadawcy PPP.

Po ustanowieniu połączenia między serwerem iSeries a dostawcą ISP komputery PC w sieci LAN mogą komunikować się z Internetem, wykorzystując serwer iSeries jako bramę. W profilu nadawcy należy upewnić się, czy opcja Ukrywaj adresy jest włączona. Umożliwia ona klientom sieci LAN, którzy mają wewnętrzne adresy IP, komunikację z Internetem.

Po połączeniu serwera iSeries i sieci z Internetem, należy uświadomić sobie, że występuje związany z tym problem ochrony. Współpraca z dostawcą ISP pomoże zapoznać się z jego strategią ochrony. Dzięki temu stanie się możliwe podjęcie działań mających na celu zabezpieczenie sieci i serwera.

W zależności od tego, do czego wykorzystywany jest Internet, problemem może okazać się przepustowość. Więcej informacji na temat zwiększenia przepustowości połączenia znajduje się w sekcji o planowaniu.

Przykład konfiguracji

1. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries.

   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 wykorzystać profil połączenia do łączenia się z Internetem, kliknij go prawym przyciskiem myszy w programie iSeries Navigator i zaznacz **Start**. Jeśli status został zmieniony na **Aktywny**, połączenie powiodło się. Odśwież widok ekranu.

Uwaga: Należy się również upewnić, że inne systemy znajdujące się w sieci mają zdefiniowany prawidłowy routing, tak aby ruch na łączu TCP/IP na granicy z Internetem, pochodzący z tych systemów, był przekazywany przez serwer iSeries.

Pojęcia pokrewne

“Planowanie protokołu PPP” na stronie 32
Poniższy temat zawiera informacje dotyczące tworzenia i administrowania połączeniami PPP.

Zadania pokrewne

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

Odsyłacze pokrewne

“Pula linii” na stronie 52
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP wykorzystujące linię z puli linii. Podczas uruchamiania połączenia PPP serwer iSeries wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie serwer nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

“Konfigurowanie połączenia” na stronie 51
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

Scenariusz: łączenie sieci LAN z sieciami zdalnymi przy pomocy modemu

Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Za pomocą protokołu PPP można połączyć ze sobą dwie sieci LAN, ustanawiając połączenie między serwerem iSeries znajdującym się w centrali a serwerem iSeries będącym 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 LAN z sieciami zdalnymi za pomocą modemu

Rozwiązanie

Za pomocą protokołu PPP można połączyć dwie sieci LAN, ustanawiając połączenie między serwerami iSeries tak, jak pokazano to na powyższej ilustracji. W takim przypadku zakładamy, że oddział inicjuje połączenie z centralą. Należy skonfigurować profil nadawcy na zdalnym serwerze iSeries oraz profil odbiorcy na serwerze w centrali.

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

1. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries.

   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 **Dodaj** i wpisz numer telefoniczny, aby połączyć się z serwerem iSeries znajdującym się w centrali. Należy uwzględnić 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 **Wymagane zaszyfrowane hasło (CHAP-MD5)** i wprowadź wymagane informacje dotyczące 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** na serwerze iSeries znajdującym się 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. Z pola wyboru wybierz dla lokalnego adresu IP adres interfejsu LAN 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**, aby umożliwić innym systemom w sieci wykorzystanie serwera iSeries 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 na serwerze iSeries profilu połączenia.

Odsyłacze pokrewne

"Konfigurowanie połączenia" na stronie 51
Konfiguracja połączenia definiuje typ obsługi linii używany przez profil połączenia PPP do nawiązania połączenia.

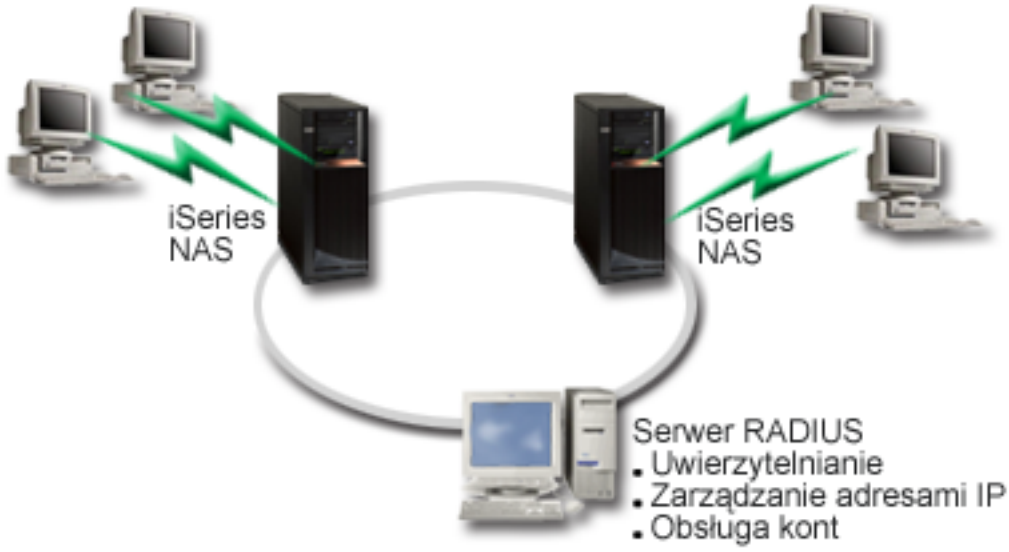
"Pula linii" na stronie 52
Ten typ obsługi należy wybrać, aby skonfigurować połączenie PPP wykorzystujące linię z puli linii. Podczas uruchamiania połączenia PPP serwer iSeries wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie serwer nie wybiera linii, dopóki nie wykryje na łączu TCP/IP ruchu skierowanego do zdalnego systemu.

Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS

Serwer dostępu do sieci działający na serwerze iSeries może kierować żądania uwierzytelnienia od klientów z połączeniem komutowanym do odrębnego serwera RADIUS. Po uwierzytelnieniu serwer RADIUS może także sterować adresami IP dla użytkownika.

Sytuacja

W sieci firmowej pracują zdalni użytkownicy dodzwaniający się do dwóch serwerów iSeries z sieci rozproszonej z połączeniem modemowym. Potrzebna jest metoda scentralizowania uwierzytelniania, usług i rozliczania, umożliwiająca jednemu serwerowi obsługiwanie żądań sprawdzenia ID użytkowników i ich haseł, a także określanie przypisanych im adresów IP.



Rysunek 7. Uwierzytelnianie połączeń modemowych za pomocą serwera RADIUS

Rozwiązanie

Podczas próby nawiązania połączenia, działający na serwerze iSeries serwer NAS 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. Aby obsługiwać serwer RADIUS, na serwerze iSeries musi być zdefiniowany serwer RADIUS NAS.

Przykład konfiguracji

1. W programie iSeries Navigator rozwiń opcję **Sieć**, kliknij prawym przyciskiem myszy opcję **Usługi zdalnego dostępu** i wybierz opcję **Usługi**.
2. W zakładce RADIUS wybierz **Włącz połączenie RADIUS Network Access Server** i **Włącz RADIUS dla uwierzytelniania**. 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 wprowadź adres IP interfejsu serwera iSeries używanego do połączenia z serwerem RADIUS.
   b. W polu Adres IP serwera wprowadź adres IP serwera RADIUS.
   c. W polu Hasło wprowadź hasło używane do identyfikacji serwera iSeries na serwerze RADIUS.
   d. W polu Port wprowadź numer portu serwera iSeries używanego do komunikacji z serwerem RADIUS. Wartością domyślną dla serwera uwierzytelniającego jest port 1812, a dla serwera rozliczającego port 1813.
6. Kliknij przycisk **OK**.
7. W programie iSeries Navigator rozwiń opcję **Sieć → Usługi zdalnego dostępu**.
8. Wybierz profil połączenia, który będzie korzystał z serwera RADIUS do uwierzytelniania. Usługi RADIUS dostępne są 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, serwer iSeries przekazuje dane dotyczące uwierzytelniania do określonego serwera RADIUS. Po pomyślnym sprawdzeniu użytkownika zostanie zestawione połączenie z zastosowaniem ograniczeń określonych w danych użytkownika na serwerze RADIUS.

Zadania pokrewne

“Udostępnianie usług RADIUS i DHCP profilom połączeń” na stronie 61
Aby udostępnić usługi RADIUS lub DHCP profilom odbiorcy połączeń PPP, należy wykonać następujące czynności:

Odsyłacze pokrewne

“Uwierzytelnianie systemu” na stronie 44
Połączenia PPP serwera iSeries obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów dodzwaniających się do serwera iSeries, jak i połączeń do dostawcy ISP lub innego serwera, do którego dodzwania się serwer iSeries.

“Protokół RADIUS” na stronie 46
Protokół 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 do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie 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 baz danych i innych aplikacji, podczas gdy użytkownicy z innych firm potrzebują połączenia modemowego i dostępu do usług takich jak HTTP, FTP czy Telnet, ale ze względów bezpieczeństwa nie powinni mieć dostępu do innych usług TCP/IP czy ruchu w sieci. Zdefiniowanie szczegółowych atrybutów połączenia i uprawnień dla każdego użytkownika wymaga dodatkowej pracy, a udostępnienie ograniczeń sieciowych wszystkim użytkownikom tego profilu użytkownika nie zapewni wystarczającej kontroli. Istnieje potrzeba zdefiniowania ustawień połączenia i uprawnień dla kilku odrębnych grup użytkowników stale łączących się z serwerem połączeniem modemowym.

Rysunek 8. Zastosowanie ustawień połączenia do połączeń modemowych z wykorzystaniem ustawień 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. Prezentowany przykład wykorzystuje filtr PPP zawierający reguły filtrowania IP dla strategii dostępu do grupy ″Partner w interesach IBM″. Reguły te zezwalają na usługi HTTP, FTP i Telnet, ale ograniczają dostęp przez serwer iSeries do innego ruchu TCP/IP i pozostałych 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). Strategie dostępu do grupy umożliwiają zdefiniowanie wspólnych atrybutów połączenia dla grupy użytkowników. Dodając Strategię dostępu do grupy do Listy weryfikacji serwera iSeries, można zastosować te ustawienia połączenia podczas procesu uwierzytelniania. Strategia dostępu do grupy określa kilka ustawień dla sesji użytkownika, włącznie z możliwością zastosowania reguł filtrowania IP, ograniczających adresy IP i usługi TCP/IP dostępne użytkownikowi w czasie trwania sesji.

Przykład konfiguracji

1. Utwórz identyfikator filtru PPP i filtry reguł pakietów IP, które określą uprawnienia i ograniczenia dla tej strategii dostępu do grupy.
   a. W programie iSeries Navigator rozwiń opcję **Sieć → Usługi zdalnego dostępu**.
   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 grup, kliknij prawym przyciskiem myszy Strategie dostępu dla grup i wybierz opcję **Nowa strategia dostępu dla grup**. Wpisz odpowiednie informacje w zakładce Ogólne. Następnie kliknij zakładkę Ustawienia TCP/IP i przejdź do kroku e poniżej.
   d. Wybierz zakładkę Ustawienia TCP/IP i kliknij **Zaawansowane**.
   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. W zakładce Ogólne zdefiniuj zestawy filtrów, a w zakładce Usługi dozwolone usługi, takie jak 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) W zakładce Ogólne wpisz dozwolone_uslugi jako identyfikator filtru PPP.
2) W zakładce Zestawy filtrów wybierz opcję **reguly_uslug** i kliknij przycisk **Dodaj**.
3) Kliknij 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 zaistnieje potrzeba cofnięcia tych zmian, w interfejsie znakowym wprowadź komendę: RMVRCPTBL *ALL

i. W oknie dialogowym **Zaawansowane ustawienia TCP/IP** pozostaw puste pole identyfikatora filtru PPP i kliknij przycisk **OK**, aby wyjść. Następnie zastosuj utworzony identyfikator filtru do strategii dostępu do grupy, nie do profilu połączenia.

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

a. W programie iSeries Navigator rozwiń opcję **Sieć → Usługi zdalnego dostępu → Profil połączenia odbiorcy**.

b. Kliknij prawym przyciskiem myszy ikonę Strategia dostępu do grupy i wybierz Nowa strategia dostępu do grupy. Program iSeries Navigator wyświetli okno dialogowe definicji nowej strategii dostępu do grupy.
c. Na stronie Ogólne wprowadź nazwę i opis strategii dostępu do 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 składować strategię dostępu do grupy.

3. Zastosuj strategię dostępu do grupy użytkowników powiązanych z tą grupą.
   a. Otwórz Profil połączenia odbiorcy sterujący tymi połączeniami modemowymi.
   b. Na stronie Uwierzytelnianie Profilu połączenia odbiorcy wybierz listę sprawdzania, która zawiera informacje uwierzytelniające użytkowników i kliknij przycisk **Otwórz**.
   c. Z grupy Sprzedaż wybierz użytkownika, dla którego chcesz zastosować strategię dostępu do grupy, i kliknij **Otwórz**.
   d. Kliknij **Przypisanie użytkownikowi strategii dostępu dla grupy** i wybierz strategię dostępu do grupy zdefiniowaną w kroku 2.
   e. Powtórz czynności dla każdego użytkownika grupy Sprzedaż.

Pojęcia pokrewne

"Konfigurowanie strategii dostępu do 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 do grupy" na stronie 5
Obsługa strategii dostępu do grupy umożliwia administratorom sieci definiowanie użytkownika na podstawie strategii. Jest to pomocne przy zarządzaniu zasobami i umożliwia przypisywanie strategii sterowania dostępem indywidualnym użytkownikom podczas logowania do sieci poprzez sesje PPP lub L2TP.

Zadania pokrewne

"Tworzenie profilu połączenia" na stronie 47
Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie na serwerze iSeries 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 44
Połączenia PPP serwera iSeries obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów dodzwaniających się do serwera iSeries, jak i połączeń do dostawcy ISP lub innego serwera, do którego dodzwania się serwer iSeries.

Informacje pokrewne

Reguły pakietów IP (filtrowanie i translacja NAT)

Scenariusz: współużytkowanie modemu między partycjami logicznymi za pomocą protokołu L2TP

Między czterema partycjami logicznymi skonfigurowana jest wirtualna sieć Ethernet. Realizacja tego scenariusza umożliwi współużytkowanie modemu przez wybrane partycje logiczne. Będą one używały tego modemu w celu uzyskiwania dostępu do zewnętrznej sieci LAN.

Sytuacja

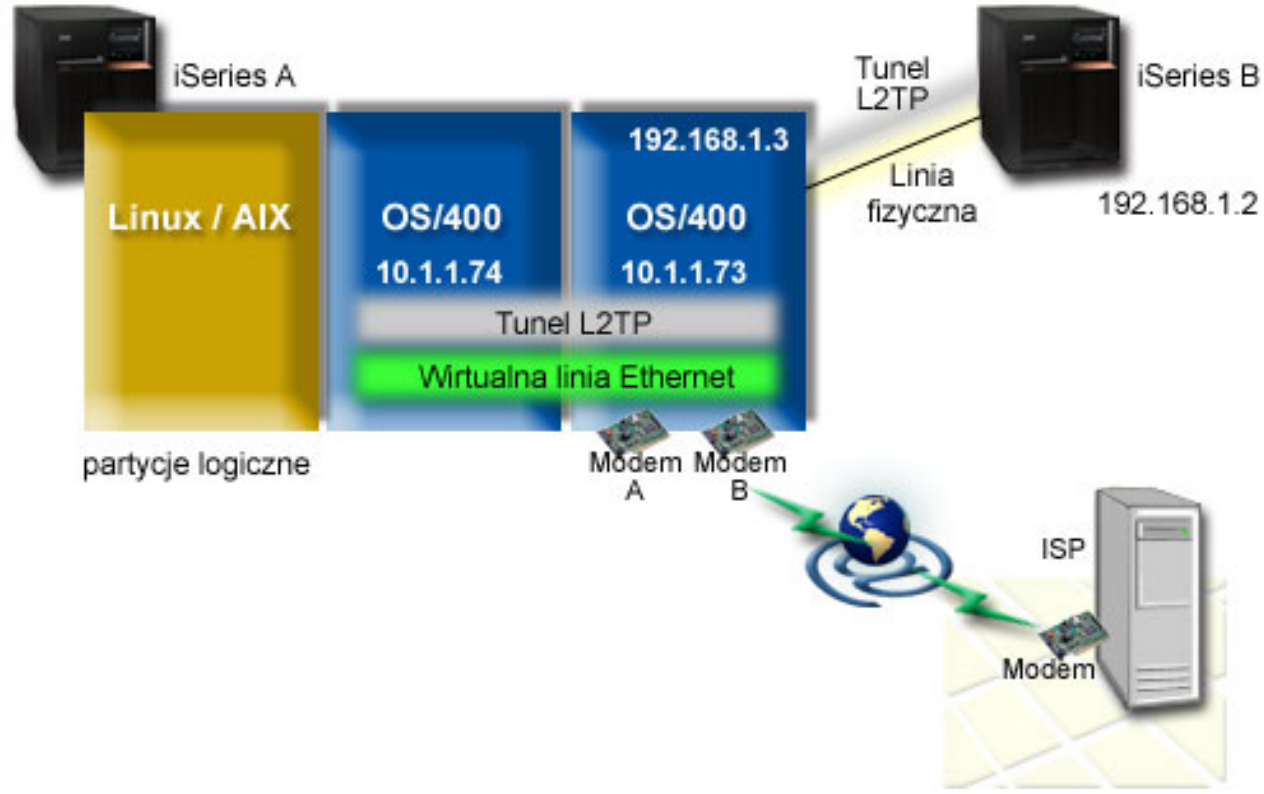
Użytkownik jest administratorem systemu w przedsiębiorstwie średniej wielkości. Czas na modernizację sprzętu, ale przy okazji chciałby on zrobić trochę więcej: usprawnić jego działanie. Proces ten rozpocznie się od konsolidacji pracy trzech starych serwerów w ramach jednego serwera iSeries. Na tym serwerze iSeries utworzone zostaną trzy partycje logiczne. Nowy serwer iSeries jest wyposażony w modem wewnętrzny 2793. W tym egzemplarzu serwera jest to jedyny procesor wejścia/wyjścia (IOP), który obsługuje protokół PPP. Użyty zostanie także stary modem elektronicznego wsparcia klienta (ECS) 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 dzięki tunelom i profilom L2TP, które zezwalają na połączenia wychodzące. W omawianej sieci tunele będą tworzone na bazie wirtualnej sieci Ethernet i sieci fizycznej. Linia fizyczna będzie połączona z innym serwerem w sieci, który także współużytkuje modemy.

Szczegóły

Poniższa ilustracja przedstawia charakterystykę sieci w tym scenariuszu:



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

Wymagania wstępne i założenia

Wymagania konfiguracyjne dla systemu iSeries A są następujące:

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

- Programy iSeries Access for Windows oraz iSeries Navigator (komponent Konfiguracja i serwis aplikacji iSeries Navigator), wersja 5 wydanie 3 lub nowsze.
- Na serwerze utworzono co najmniej dwie partycje logiczne (LPAR). Na partycji, do której należy modem, musi być zainstalowany system i5/OS wersja 5 wydanie 3. Na innych partycjach mogą być zainstalowane systemy OS/400 w wersji V5R2 lub V5R3, Linux bądź AIX. W tym scenariuszu na partycjach zainstalowane są systemy operacyjne i5/OS lub Linux.
- Do obsługi komunikacji między partycjami utworzono wirtualną sieć Ethernet. Patrz następujący scenariusz: Tworzenie wirtualnej sieci Ethernet do komunikacji między partycjami.

Wymagania konfiguracyjne dla systemu iSeries B są następujące:

- Programy iSeries Access for Windows oraz iSeries Navigator (komponent Konfiguracja i serwis aplikacji iSeries Navigator), wersja 5 wydanie 2 lub nowsze.

Informacje pokrewne

Partycje logiczne

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

Po spełnieniu wymagań wstępnych można zacząć konfigurowanie profili L2TP.

Etap 1: Konfigurowanie profilu terminatora L2TP dla każdego interfejsu na partycji, do której należą modemy:

Aby utworzyć profil terminatora dla każdego interfejsu:

1. W programie iSeries Navigator rozwiń opcję *używany serwer* → **Sieć** → **Usługi zdalnego dostępu** .
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 w zakładce **Nowy profil - ogólne**:
   - **Nazwa**: toExternal
   - **Opis**: Połączenie odbiornika dla połączeń wychodzących
   - Wybierz opcję **Uruchom profil z TCP**.
5. Wypełnij poniższe pola w zakładce **Nowy profil - połączenie**.
   - **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. Zostanie wyświetlone okno Właściwości linii L2TP. Kliknij zakładkę **Uwierzytelnianie** i wprowadź nazwę hosta swojego serwera. Kliknij przycisk **OK**, aby powrócić do zakładki Połączenie w oknie Właściwości nowego profilu PPP.
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 nowe okno Właściwości linii.

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**, aby dodać modem ECS 7852-400. Zostanie wyświetlone nowe okno Właściwości linii.
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 ECS 7852-400).
   - **Zasoby sprzętu**: cmn04 (port V.24).
   - **Ramki**: Asynchroniczne
14. Wybierz w zakładce **Właściwości nowej linii - modem** 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 podano konkretny numer telefonu, to zostanie on użyty.
17. W zakładce **Ustawienia TCP/IP** wybierz następujące wartości:
   - **Lokalny adres IP**: Brak
   - **Zdalny adres IP**: Brak

    Uwaga: Jeśli profil używany jest także do kończenia sesji L2TP, należy wybrać lokalny adres IP przypisany do serwera iSeries. W przypadku zdalnego adresu IP można wybrać pulę adresów, które znajdują się w tej samej podsieci, co serwer. Wszystkie sesje L2TP będą pobierały adresy IP z tej puli. Pozostałe informacje na ten temat znajdują się w sekcji Obsługa profilu wielu połączeń.
18. W zakładce **Uwierzytelnianie** zatwierdź wszystkie wartości domyślne.

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

Etap 2: konfigurowanie profilu inicjatora L2TP dla adresu 10.1.1.74:

Aby utworzyć profil inicjatora L2TP, wykonaj następujące kroki:

1. Rozwiń w programie iSeries Navigator opcję **10.1.1.74 → Sieć → Usługi zdalnego dostępu**.
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. W zakładce **Ogólne** wypełnij następujące pola:
   - **Nazwa**: toModem
   - **Opis**: połączenie inicjatora kierowane do partycji z modemem.
5. W zakładce **Połączenie** wypełnij następujące pola:

   Nazwa linii wirtualnej: z linią toModemThis nie jest powiązany żaden interfejs fizyczny. Linia wirtualna opisuje różne cechy tego profilu PPP. Zostanie wyświetlone okno Właściwości linii L2TP.
6. W zakładce **Ogólne** wprowadź opis linii wirtualnej.
7. W zakładce **Uwierzytelnianie** 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. W zakładce **Uwierzytelnianie** wybierz **Zezwalaj zdalnemu systemowi na weryfikację tożsamości tego serwera iSeries**.
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 wybierany serwer.
12. Wpisz nazwę użytkownika i hasło.

    Uwaga: Nazwa użytkownika i hasło powinny być zgodne z dowolną poprawną nazwą użytkownika i hasłem na serwerze, 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 **OK**, aby zapisać profil PPP.

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

Powtórz czynność 2, zmieniając adres zdalnego punktu końcowego tunelu na 192.168.1.3 (interfejs fizyczny, z którym łączy się system iSeries B).

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

Etap 4: testowanie połączenia:

Po skonfigurowaniu obu serwerów należy przetestować połączenia, aby upewnić się, że systemy współużytkują modemy, aby łączyć się z zewnętrznymi sieciami. W tym celu wykonaj poniższe czynności:

1. Upewnij się, że profil terminatora L2TP jest aktywny.
   a. Rozwiń w programie iSeries Navigator opcję **10.1.1.73 → Sieć → Usługi zdalnego dostępu → Profil połączenia odbiorcy**.
   b. W prawym panelu znajdź żądany profil (toExternal) i sprawdź, czy w polu **Status** wyświetlona jest wartość *Aktywny*. Jeśli nie, kliknij go prawym przyciskiem myszy i wybierz opcję **Start**.
2. Uruchom profil zdalnego wybierania w systemie 10.1.1.74.
   a. Rozwiń w programie iSeries Navigator opcję **10.1.1.74 → Sieć → Usługi zdalnego dostępu → Profil połączenia nadawcy**.

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

3. Uruchom profil zdalnego wybierania serwera iSeries B.
   a. Rozwiń w programie iSeries Navigator opcję **192.168.1.2 → Sieć → Usługi zdalnego dostępu → Profil połączenia nadawcy**.
   b. W prawym panelu znajdź utworzony profil i sprawdź, czy w polu **Status** wyświetlona jest wartość *Aktywny*. Jeśli nie, kliknij go prawym przyciskiem myszy i wybierz opcję **Start**.
4. W miarę możliwości uruchom komendę ping z adresem dostawcy ISP lub innego punktu docelowego, aby sprawdzić, czy połączenie powiodło się i czy oba profile są aktywne. Należy spróbować uruchomić komendę ping z obu adresów: 10.1.1.74 i 192.168.1.2.
5. Zamiennie, można sprawdzić Status połączenia.
   a. Rozwiń w programie iSeries Navigator *żądany serwer (np. 10.1.1.73)* **→ Sieć → Usługi zdalnego dostępu → Profil połączenia nadawcy**.
   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

Poniższy temat zawiera informacje dotyczące tworzenia i administrowania połączeniami PPP.

Odsyłacze pokrewne

"Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym" na stronie 14
Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

"Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu" na stronie 16
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą ISP mogą wykorzystać modem. Klienci PC przyłączeni do sieci LAN mogą łączyć się z Internetem, wykorzystując serwer iSeries jako bramę.

"Informacje pokrewne dotyczące protokołu PPP" na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Wymagania sprzętowe i programowe

Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących protokół PPP. Jeden z tych komputerów, serwer iSeries, może być zarówno inicjatorem, jak i odbiorcą.

Aby systemy zdalne mogły się połączyć z serwerem iSeries, muszą być spełnione poniższe wstępne wymagania.

- Program iSeries Navigator z obsługą TCP/IP.
- Jeden z dwóch profili połączeń:
  - Profil połączenia inicjatora do obsługi wychodzących połączeń PPP
  - Profil połączenia odbiorcy do obsługi przychodzących połączeń PPP
- Konsola stacji roboczej PC z zainstalowanym programem iSeries Access for Windows(95) i programem iSeries Navigator.
- Zainstalowany adapter

  Istnieje możliwość wyboru jednego z poniższych adapterów:
  - 2699*: adapter wejścia/wyjścia (IOA) Two-line WAN
  - 2720*: adapter IOA PCI PCI WAN/Twinaxial
  - 2721*: adapter IOA PCI Two-line WAN
  - 2745*: adapter IOA PCI Two-line WAN IOA (zastępuje IOA 2721)
  - 2742*: adapter Two-line IOA (zastępuje 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: adapter ethernet do połączeń PPPoE
– 2793*: dwuportowy adapter WAN IOA ze zintegrowanym modemem V.92 na porcie 1 i standardowym interfejsem komunikacyjnym na porcie 2. Aby wykorzystać port 2 adaptera 2793, wymagany jest modem zewnętrzny lub adapter terminalu ISDN z odpowiednim kablem (zastępuje adapter IOA 2771)
– 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 3
Profile połączeń punkt z punktem definiują zestaw parametrów i zasobów dla określonych połączeń PPP. Profile, które wykorzystują takie ustawienia parametrów, można uruchomić podczas dodzwaniania (rozpoczynania) lub nasłuchiwania (odbioru) połączeń PPP.

“Modemy” na stronie 39
Do połączeń PPP mogą być wykorzystane zarówno modemy wewnętrzne, jak i zewnętrzne.

“CSU/DSU” na stronie 40
Urządzenia Channel Service Unit (CSU) łączą terminal z linią cyfrową. Urządzenia Data Service Unit (DSU) pełnią funkcje zabezpieczające i diagnostyczne dla linii telekomunikacyjnych. Najczęściej te dwa urządzenia występują jako jedno: CSU/DSU.

“Adaptery terminali ISDN” na stronie 40
Sieć ISDN umożliwia połączenie cyfrowe, które pozwala na wymianę głosu, danych i obrazów wideo między różnymi aplikacjami multimedialnymi.

Połączenia alternatywne

Protokół PPP może przesyłać datagramy poprzez 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 wykorzystują istniejące urządzenia sieciowe 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. Przesyłanie danych jest metodą asymetryczną, tzn. transmisja w kierunku przeciwnym (głównie 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 umożliwiając zwiększenie szybkości zwrotnej do 48 kb/s. Ponadto czas połączenia zostaje zredukowany dzięki ulepszeniom w procesie nawiązywania połączenia, a modemy obsługujące opcję ″hold″ mogą zostać połączone w czasie, gdy linia telefoniczna akceptuje połączenia przychodzące lub oczekuje na połączenie.

Usługi cyfrowe i DDS

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 zwanego *Channel Service Unit/Data Service Unit (CSU/DSU)*, które jest odpowiednikiem modemu przy połączeniach analogowych. Usługi DDS mają ograniczenia związane z odległością urządzeń CSU/DSU od centrali firmy 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. Dla większych odległości, połączenia, które obejmują różne centrale, 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 wykorzystując protokół synchroniczny o szybkości dochodzącej do 56 kb/s.

Odsyłacze pokrewne

"CSU/DSU" na stronie 40
Urządzenia Channel Service Unit (CSU) łączą terminal z linią cyfrową. Urządzenia Data Service Unit (DSU) pełnią 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 urządzenie CSU/DSU. Urządzenia CSU/DSU dla SW56 posiadają klawiaturę, z której wprowadza się numer telefonu zdalnego hosta. Usługa SW56 umożliwia cyfrowe połączenie telefoniczne z innym użytkownikiem SW56 znajdującym się w kraju lub poza jego granicami. 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 przy pomocy V.35 lub interfejsu szeregowego RS 449 wykorzystując protokół synchroniczny o szybkości 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

"Usługi cyfrowe i DDS" na stronie 34
Z protokołem PPP można używać usług cyfrowych i usług DDS.

"Sieć cyfrowa z integracją usług"
Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W odróżnieniu od innych usług, ISDN może przesyłać zarówno głos, jak i dane wykorzystując to samo połączenie.

Sieć cyfrowa z integracją usług

Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W odróżnieniu od innych usług, ISDN może przesyłać zarówno głos, jak i dane wykorzystując to samo połączenie.

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 jednoczesnemu przesyłaniu danych i głosu użytkownicy z pojedynczą linią ISDN mogą obsługiwać zarówno ISDN, jak i zwykłe połączenia analogowe. Nowa technologia umożliwia również adapterowi terminalu działanie jako cyfrowy serwer dla klientów 56K(X2/56Flex).

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 serwera iSeries dla połączenia asynchronicznego przez interfejs RS-232 wynosi 115,2 kb/s. Ogranicza to niestety maksymalną szybkość do 11,5 kb/s, podczas gdy adapter terminalu z połączeniem wielokrotnym jest zdolny do nieskompresowanego przesyłania rzędu 14/16 k. Niektóre adaptery terminali obsługują połączenia synchroniczne przez RS-232 z szybkością 128 kb/s, jednak dla tego typu połączeń maksymalna szybkość transmisji dla serwera iSeries wynosi 64 kb/s.

Serwer iSeries obsługuje połączenie asynchroniczne za pomocą V.35 z szybkością dochodzącą do 230,4 kb/s. Jednak producenci adapterów terminali w większości przypadków nie oferują takiej możliwości. Konwerter interfejsu z RS-232 do V.35 mógłby stanowić rozwiązanie tego problemu. Jednak metoda taka nie została uwzględniona w serwerze iSeries. Kolejną możliwością jest wykorzystanie adaptera terminalu z interfejsem V.35 obsługującym protokół synchroniczny z szybkością 128 kb/s. Chociaż tego typu adaptery terminali są produkowane, nie wydaje się, aby zbyt wiele z nich oferowało synchroniczne połączenia PPP typu multilink.

Odsyłacze pokrewne

“Linia Switched-56” na stronie 35
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 40
Sieć ISDN umożliwia połączenie cyfrowe, które pozwala na wymianę głosu, danych i obrazów wideo między różnymi aplikacjami multimedialnymi.

Linie T1/E1 i linia częściowa T1

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

Linia T1/E1

Połączenie T1 scala ze sobą dwadzieścia cztery kanały multipleksowe z podziałem czasu (TDM) o przepustowości 64 kb/s. Jest to fizycznie 4-żyłowy kabel miedziany. Jego całkowita przepustowość wynosi 1.544 Mb/s. Linia E1 w Europie i innych częściach świata łączy ze sobą trzydzieści dwa kanały o szybkości 64 kb/s o łącznej przepustowści 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 np. do 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 przy pomocy 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 64 kb/s kanałów 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 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 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 wykorzystującym połączenia o szybkości od 56 kb/s do T-1. (W Europie szybkość frame relay zmienia się od 64 kb/s do 2 Mb/s. W Stanach Zjednoczonych usługa ta jest dość popularna ponieważ jest tania. Jednak na niektórych obszarach została ona zastąpiona szybszą technologią, taką jak asynchroniczny tryb przesyłania (ATM).

Konfigurowanie opisów linii L2TP dla połączeń PPP (tunelowanie)

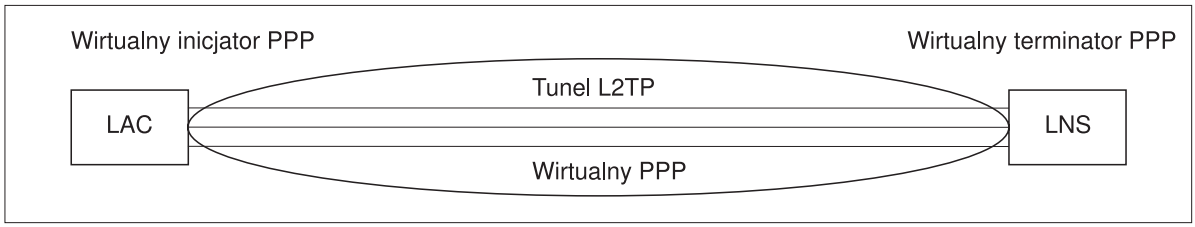
Protokół L2TP jest protokołem tunelowym rozszerzającym protokół PPP o obsługę w warstwie łącza tuneli tworzonych między zgłaszającym klientem L2TP (koncentrator dostępu L2TP lub LAC) a serwerem końcowym L2TP (Serwer sieciowy L2TP lub LNS).

Protokół L2TP (Layer 2 Tunneling Protocol)

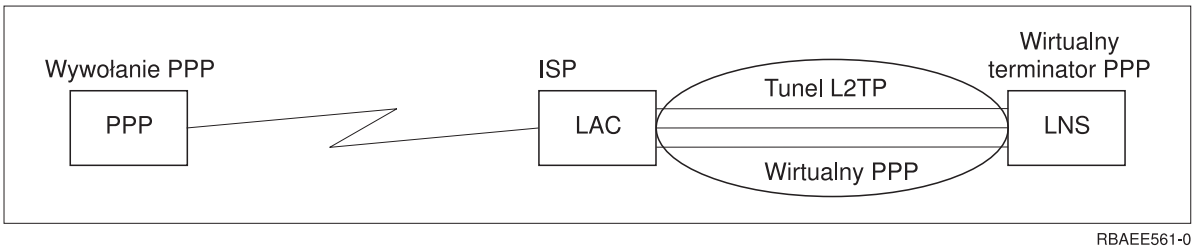
Wykorzystanie tuneli L2TP pozwala oddzielić miejsce, w którym kończy się protokół połączenia telefonicznego, a zaczyna się dostęp do sieci. Z tego względu protokół L2TP jest nazywany również *wirtualnym PPP*.

Dostawca usług internetowych korzysta z trybu linii wirtualnej do obsługi sieci VPN (virtual private networks). Więcej informacji dotyczących współdziałania protokołu IPSec z protokołem L2TP można znaleźć w temacie Konfigurowanie połączenia L2TP chronionego przez sieć VPN.

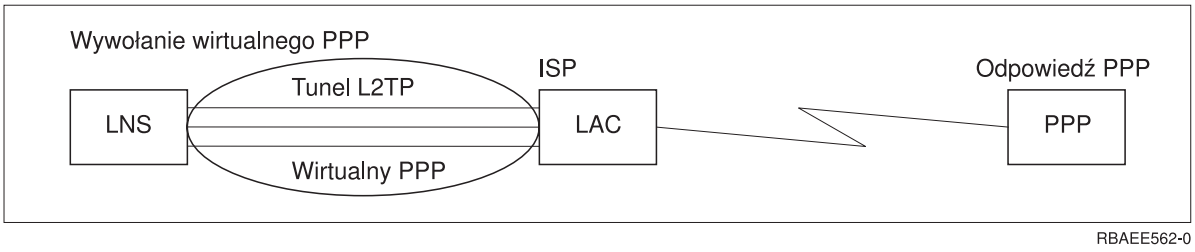
Poniżej znajdują się ilustracje obrazujące trzy różne implementacje tunelowania protokołu L2TP.



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 L2TP jest opisany jako standard RFC2661. Więcej informacji o RFC można znaleźć na stronie WWW RFC Editor. Tunel L2TP może obejmować całą sesję PPP lub tylko jeden segment dwusegmentowej sesji. Można wyróżnić cztery modele tunelowania:

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 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 rezultacie użytkownik wysyła pakiety PPP do dostawcy ISP (LAC), który przesyła je tunelem w ramach protokołu L2TP do serwera LNS. W przypadku tunelowania wymuszonego dostawca ISP musi obsługiwać protokół L2TP. W modelu tym tunel biegnie jedynie w segmencie sesji PPP między dostawcą ISP a serwerem LNS.

Tunel wymuszony - połączenie zdalne:

W tym modelu lokalna brama (serwer LNS) 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 jest sposobem na przekierowywanie ruchu L2TP w imieniu klientów LAC i LNS.

Połączenie to jest ustanawiane za pomocą 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

DSL oznacza klasę technologii stosowaną do uzyskania większego pasma przy wykorzystaniu istniejącego miedzianego 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 teoretyczny limit dla tej technologii. Technologia DSL umożliwia zwiększenie szybkości na liniach typu skrętka, od głównego biura do domu, szkoły czy przedsiębiorstwa. W niektórych obszarach osiągane są szybkości rzędu 2 megabitów na sekundę. Skrót PPPoE oznacza Point to Point Protocol over Ethernet (protokół PPP przez sieć Ethernet). 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 z uwagi na dodane opcje logowania się i ochrony. Co to jest modem DSL? ″Modem″ DSL to urządzenie umieszczone na jednym końcu miedzianej linii telefonicznej umożliwiające komputerowi (lub sieci lokalnej) połączenie 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 modemy konwencjonalne, ale znacznie zwiększają przepustowość.

Urządzenia łączące

Serwer iSeries do obsługi połączeń PPP korzysta z modemów, adapterów terminali ISDN, adapterów token-ring, adapterów Ethernet lub urządzeń CSU/DSU.

Istnieje kilka rodzajów urządzeń łączących, które można wykorzystać w środowisku PPP. Są to:

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

Modemy

Do połączeń PPP mogą być wykorzystane zarówno modemy wewnętrzne, jak i zewnętrzne.

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. Jeśli jest to modem wewnętrzny, to łańcuch ten jest już zdefiniowany.

Serwer iSeries posiada wiele predefiniowanych modeli modemów. Natomiast nowe modele mogą zostać zdefiniowane za pomocą programu iSeries Navigator. 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. Dostarczona i określona wcześniej definicja nie może być zmieniana. Jednak do istniejących komend inicjujących lub sekwencji wybierania można dodawać dodatkowe komendy.

Aby ustanowić połączenie PPP, można wykorzystać modem elektronicznego wsparcia klienta (ECS) dostarczony wraz z serwerem iSeries. W starszych systemach modem ECS był zewnętrznym modemem IBM 7852-400. 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 32
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących protokół PPP. Jeden z tych komputerów, serwer iSeries, może być zarówno inicjatorem, jak i odbiorcą.

CSU/DSU

Urządzenia Channel Service Unit (CSU) łączą terminal z linią cyfrową. Urządzenia Data Service Unit (DSU) pełnią 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 32
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących protokół PPP. Jeden z tych komputerów, serwer iSeries, może być zarówno inicjatorem, jak i odbiorcą.

“Usługi cyfrowe i DDS” na stronie 34
Z protokołem PPP można używać usług cyfrowych i usług DDS.

Adaptery terminali ISDN

Sieć ISDN umożliwia połączenie cyfrowe, które pozwala na wymianę głosu, danych i obrazów wideo między różnymi aplikacjami multimedialnymi.

Należy sprawdzić, czy adapter terminalu został przygotowany do użycia z serwerem iSeries.

W celu skonfigurowania adaptera terminalu wykonaj następujące kroki:

1. W programie iSeries Navigator wybierz odpowiedni serwer i rozwiń gałąź **Sieć → > Usługi zdalnego dostępu**.
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. W oknie dialogowym **Właściwości nowego modemu** w zakładce Ogólne wpisz we wszystkie pola poprawne wartości. 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 57

Odsyłacze pokrewne

“Wymagania sprzętowe i programowe” na stronie 32
Środowisko PPP wymaga dwóch lub więcej komputerów obsługujących protokół PPP. Jeden z tych komputerów, serwer iSeries, może być zarówno inicjatorem, jak i odbiorcą.

“Sieć cyfrowa z integracją usług” na stronie 35
Sieć cyfrowa z integracją usług (ISDN) udostępnia stałe, komutowane połączenie cyfrowe. W odróżnieniu od innych usług, ISDN może przesyłać zarówno głos, jak i dane wykorzystując to samo połączenie.

Zalecane adaptery terminali ISDN:

Istnieje kilka różnych adapterów terminali.

Zalecany zewnętrzny adapter terminalu ISDN (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 odbierającym połączenie w systemie serwera iSeries. 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 serwera iSeries.** Na wezwania protokołu CHAP pochodzące ze strony odbierającej adapter terminalu Courier I odpowiada podczas negocjacji uwierzytelniania protokołu PAP z serwerem iSeries. Odpowiedzi protokołu PAP nie są widoczne w połączeniu ISDN.
- **Połączenia odbierane przez serwer iSeries.** Adapter Courier I wymaga uwierzytelniania protokołu CHAP przez stronę wywołującą, jeśli konfiguracja odpowiedzi serwera iSeries powoduje, że serwer iSeries otwiera uwierzytelnianie wezwaniem protokołu CHAP. Gdy serwer iSeries otwiera uwierzytelnianie według protokołu PAP, adapter terminalu Courier I przeprowadza uwierzytelnianie zgodnie z tym protokołem.

Jeśli używany jest modem Courier I wyprodukowany przed rokiem 1999, w celu uzyskania najlepszej wydajności połączenia ISDN należy sprawdzić, czy jest on podłączony do serwera iSeries poprzez kabel 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 firmy 3Com/US Robotics wersje V.35 adaptera terminalu nie są już dostępne, jednak można je znaleźć u użytkowników. Nadal zalecana jest wersja RS-232, mimo że zmniejsza ona wydajność serwera iSeries z powodu ograniczenia połączenia do 115,2 kb/s.

Adapter z V.35 na RS-232 można także otrzymać z Black Box Corporation. Część ta ma numer FA-058.

Należy upewnić się, że szybkość linii V.35 w systemie serwera iSeries ustawiona jest na 230,4 kb/s.

Ograniczenia adaptera terminalu ISDN:

Przedstawione poniżej adaptery terminali zostały przetestowane. Są zalecane jedynie do inicjowania zdalnych połączeń ISDN pochodzących z serwera iSeries.

3Com Impact IQ ISDN:

Nie poleca się tego adaptera terminalu dla serwera iSeries 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 serwerem iSeries z szybkością większą niż 115 200 b/s.
- Adapter terminalu nie obsługuje automatycznie protokołu CHAP. Jednakże opcja S84=0 umożliwia serwerowi iSeries wykonanie uwierzytelniania CHAP.
- Serwer iSeries nie potrafi określić zakończenia połączenia na podstawie monitorowania sygnału DSR (Data Set Ready) z adaptera terminalu. Może to prowadzić do potencjalnego osłabienia bezpieczeństwa systemu.

Motorola BitSurfr Pro ISDN:

Nie poleca się tego adaptera terminalu dla serwera iSeries 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 serwerem iSeries z szybkością większą niż 115 200 b/s.
- Adapter terminalu nie obsługuje automatycznie protokołu CHAP. Jednakże ustawienie parametru @M2=C umożliwia wykonanie uwierzytelnienia CHAP przez serwer iSeries.
- 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.
- Mechanizm sterowania przepływem serwera iSeries nie współpracuje dobrze z tym adapterem terminalu, co powoduje spadek wydajności przy wysyłaniu przez serwer iSeries danych w połączeniu PPP multilink.

Obsługa adresów IP

Połączenia PPP pozwalają dowolnie zarządzać adresami IP w zależności od rodzaju profilu połączenia.

Odsyłacze pokrewne

“Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE” na stronie 11
Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

Filtrowanie pakietów IP

Filtrowanie pakietów IP jest ogranicza usługi dostępne dla indywidualnego użytkownika po zalogowaniu do sieci.

Filtrowanie pakietów umożliwia przyznawanie lub odmawianie dostępu w zależności od docelowego adresu IP i/lub portów. Poprzez definiowanie wielu zestawów reguł filtrowania pakietów, z których każdy ma własny, unikalny identyfikator filtrowania PPP tworzy się różne strategie. Reguły filtrowania pakietów mogą być przypisywane do poszczególnych profili połączeń odbiorcy lub za pomocą strategii dostępu do grup do kategorii użytkowników. Reguły filtrowania pakietów nie są definiowane w protokole PPP, ale w opcji Reguły pakietów IP w programie iSeries Navigator.

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

Odsyłacze pokrewne

“Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE” na stronie 11
Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

Informacje pokrewne

Reguły pakietów IP

sieć VPN

Strategia zarządzania adresami IP

Przed rozpoczęciem konfigurowania profilu połączenia PPP należy zapoznać się ze strategią zarządzania adresami IP w sieci. Strategia ta ma wpływ na wiele decyzji podczas całego procesu konfiguracji, włącznie ze strategią uwierzytelniania, założeniami dotyczącymi ochrony i ustawieniami TCP/IP.

Profile połączenia nadawcy:

Lokalne i zdalne adresy IP określone dla profilu nadawcy będą najczęściej zdefiniowane jako *Przypisane do systemu zdalnego*. Pozwala to administratorom systemów zdalnych na kontrolę 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 stały adres dla lokalnego albo zdalnego adresu IP zostanie zdefiniowany, należy upewnić się, że system zdalny akceptuje adresy IP wcześniej zdefiniowane. 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 uaktywnienie maskowania adresów IP. Przykładowo, jeśli serwer iSeries jest połączony z Internetem za pomocą dostawcy ISP, wówczas sieć przyłączona poprzez serwer iSeries również może mieć dostęp do Internetu. Z reguły serwer iSeries będzie ″ukrywał″ adresy IP systemów znajdujących się w sieci za lokalnym adresem przypisanym przez dostawcę ISP, w taki sposób, że będzie wyglądało iż cały ruch sieciowy IP pochodzi z serwera iSeries. Należy wziąć pod uwagę także dodatkowe kwestie dotyczące routingu w odniesieniu do obu systemów w sieci LAN (aby zapewnić przekazywanie ruchu internetowego do serwera iSeries), a także w odniesieniu do serwera iSeries, dla którego należy zaznaczyć pole wyboru ’Dodaj system zdalny jako trasę domyślną’.

Profile połączenia odbiorcy:

Profile połączenia odbiorcy posiadają 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 istnieje możliwość zdefiniowania unikalnego adresu IP lub wykorzystania istniejącego adresu, znajdującego się na serwerze iSeries. Ten adres IP będzie identyfikował koniec połączenia PPP, w którym znajduje się serwer iSeries. Dla profili odbiorcy, zdefiniowanych do obsługi wielu połączeń jednocześnie, należy użyć istniejącego adresu IP. Jeśli nie ma żadnych istniejących lokalnych adresów IP, można do tego 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 systemu iSeries.

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.

Tabela 8. Opcje przypisania adresu IP dla profilu połączenia odbiorcy (kontynuacja)

Opcja	Opis
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. Kiedy z serwerem iSeries połączy się zdalny użytkownik, nastąpi próba określenia, czy zdalny adres IP dla tego użytkownika jest ściśle określony. Jeśli tak, adres IP, maska oraz zestaw możliwych tras będą przydzielone dla tego połączenia. W przeciwnym razie będzie on domyślnie zdefiniowany jako Stały adres IP lub jako następny wolny z Puli adresów IP.
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 za pomocą jednej 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 komutowanym ma mieć dostęp do dowolnego adresu IP w sieci lokalnej (w tym do serwera iSeries), to zarówno klient, jak i serwer iSeries muszą mieć odpowiednio skonfigurowany routing adresów IP.

Uwierzytelnianie systemu

Połączenia PPP serwera iSeries obsługują kilka opcji uwierzytelniania zarówno zdalnych klientów dodzwaniających się do serwera iSeries, jak i połączeń do dostawcy ISP lub innego serwera, do którego dodzwania się serwer iSeries.

Serwer iSeries zapewnia kilka metod obsługi informacji uwierzytelniających, od prostych list sprawdzania w serwerze iSeries , które zawierają spis uprawnionych użytkowników i powiązane z nimi hasła, do serwera RADIUS, który obsługuje szczegółowe informacje uwierzytelniające dla użytkowników sieciowych. Serwer iSeries ma także kilka opcji do szyfrowania informacji o identyfikatorze użytkownika i haśle, od prostej wymiany haseł, do obsługi niszczenia z CHAP-MD5. Preferencje dotyczące uwierzytelniania w systemie, włącznie z identyfikatorem użytkownika i hasłem używanym do sprawdzania poprawności serwera iSeries przy połączeniu telefonicznym można określić na zakładce **Uwierzytelnianie** profilu połączenia w programie iSeries Navigator.

Odsyłacze pokrewne

“Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE” na stronie 11
Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

“Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS” na stronie 22
Serwer dostępu do sieci działający na serwerze iSeries może kierować żądania uwierzytelnienia od klientów z połączeniem komutowanym do odrębnego serwera RADIUS. Po uwierzytelnieniu serwer RADIUS może także sterować adresami IP dla użytkownika.

“Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP” na stronie 24
Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

Protokół CHAP-MD5

Protokół **Challenge Handshake Authentication Protocol (CHAP-MD5)** wykorzystuje algorytm (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 z serwerem iSeries połączeniem komutowanym" na stronie 14
Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

"Protokół PAP"
Protokół *Password Authentication Protocol (PAP)* używa dwukierunkowego uzgadniania. Dzięki czemu staje się możliwe ustalenie tożsamości przez system równorzędny.

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

Protokół EAP

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 serwerom na negocjację wymaganego uwierzytelnienia przed odebraniem lub wysłaniem jakichkolwiek danych.

Serwer iSeries nie obsługuje bezpośrednio protokołu EAP. Istnieje jednak możliwość wykorzystania zdalnego uwierzytelniania przy pomocy serwera RADIUS, który obsługuje niektóre z dodatkowych schematów uwierzytelniających opisanych powyżej.

Odsyłacze pokrewne

"Protokół PAP"
Protokół *Password Authentication Protocol (PAP)* używa dwukierunkowego uzgadniania. Dzięki czemu staje się możliwe ustalenie tożsamości przez system równorzędny.

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

Protokół PAP

Protokół *Password Authentication Protocol (PAP)* używa dwukierunkowego uzgadniania. Dzięki czemu staje się możliwe ustalenie tożsamości przez system równorzędny.

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. Ponieważ elementy te nigdy nie są zaszyfrowane, istnieje możliwość przechwycenia ich. Z tego powodu, o ile to możliwe, należy korzystać z protokołu CHAP.

Odsyłacze pokrewne

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

"Protokół EAP" na stronie 45
Protokół *Extensible Authentication Protocol (EAP)* umożliwia zewnętrznym modułom uwierzytelniającym współdziałanie z protokołem PPP.

Protokół RADIUS

Protokół 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. Serwer iSeries pracując jako serwer NAS, wysyła informacje dotyczące użytkownika i połączenia do wyznaczonego serwera RADIUS, wykorzystując standard protokołu RADIUS zdefiniowany w dokumencie RFC 2865.

Serwery RADIUS działają na podstawie przyjętych zgłoszeń o połączeniu użytkownika, uwierzytelniając go. Następnie zwracają wszystkie niezbędne informacje dotyczące konfiguracji do serwera NAS (serwera iSeries), tak aby połączeni użytkownicy mogli korzystać z autoryzowanych usług.

Jeśli serwer RADIUS nie jest dostępny, serwer iSeries może przesłać zgłoszenia dotyczące uwierzytelniania do serwera zastępczego. Umożliwia to międzynarodowym przedsiębiorstwom obsługę połączeń modemowych. Przydzielają one swoim użytkownikom unikalny identyfikator użytkownika potrzebny do zalogowania się bez względu na to, z którego miejsca nawiązano połączenie.

Kiedy zgłoszenie dotyczące uwierzytelniania odebrane jest przez serwer RADIUS, sprawdzana jest jego poprawność, a następnie serwer ten 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 serwera iSeries dowolne 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 22
Serwer dostępu do sieci działający na serwerze iSeries może kierować żądania uwierzytelnienia od klientów z połączeniem komutowanym do odrębnego serwera RADIUS. Po uwierzytelnieniu serwer RADIUS może także sterować adresami IP dla użytkownika.

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 **zaszyfrowany - CHAP-MD5/EAP** lub **niezaszyfrowany - PAP**.

Więcej informacji na ten temat znajduje się w pomocy online.

Odsyłacze pokrewne

"Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP" na stronie 24

Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

Uwagi dotyczące zakresu pasma - Multilink

Aby wykonać niektóre czynności, często wymagana jest dodatkowa przepustowość.

W takich przypadkach 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 Multilink. Protokół Multilink jest udokumentowany jako standard RFC1990. Więcej informacji o RFC można znaleźć na stronie WWW RFC Editor.

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 wykorzystać zalety ″Przepustowości na żądanie″, przynajmniej jeden węzeł musi 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 RFC2125 opisuje zarówno protokół BAP (PPP Bandwidth Allocation Protocol), jak i BACP (Bandwidth Allocation Control Protocol).

Konfigurowanie protokołu PPP

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

Odsyłacze pokrewne

“Informacje pokrewne dotyczące protokołu PPP” na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Tworzenie profilu połączenia

Pierwszym krokiem podczas konfigurowania połączenia PPP między systemami jest utworzenie na serwerze iSeries 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** - obiekt reprezentuje wychodzące połączenia PPP zainicjowane na serwerze iSeries (system lokalny). Połączenia te są odbierane przez system zdalny.
- **Profile połączenia odbiorcy** - obiekt reprezentuje połączenia PPP zainicjowane przez system zdalny. Połączenia te są odbierane przez serwer iSeries (system lokalny).
- **Modemy**.

W celu utworzenia profilu połączenia wykonaj następujące kroki:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń **Sieć → Usługi zdalnego dostępu**.
2. Wybierz jedną z poniższych opcji:
   - Kliknij prawym przyciskiem myszy **Profile połączenia nadawcy**, aby ustawić serwer iSeries jako serwer rozpoczynający połączenia.
   - Kliknij prawym przyciskiem myszy **Profile połączenia odbiorcy**, aby ustawić serwer iSeries jako odbiorcę połączeń ze zdalnych systemów i 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. Informacje na ten temat można znaleźć w pomocy elektronicznej.

   Zadania pokrewne

   “Przypisanie modemu do opisu linii” na stronie 57

   Odsyłacze pokrewne

   “Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE” na stronie 11
   Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

   “Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym” na stronie 14
   Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

   “Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu” na stronie 16
   Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą ISP mogą wykorzystać modem. Klienci PC przyłączeni do sieci LAN mogą łączyć się z Internetem, wykorzystując serwer iSeries jako bramę.

   “Scenariusz: łączenie sieci LAN z sieciami zdalnymi przy pomocy modemu” na stronie 19
   Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Za pomocą protokołu PPP można połączyć ze sobą dwie sieci LAN, ustanawiając połączenie między serwerem iSeries znajdującym się w centrali a serwerem iSeries będącym w oddziale.

   “Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP” na stronie 24
   Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

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

Jaki protokół należy wybrać dla połączeń PPP?

Protokół PPP jest standardem w Internecie. Umożliwia on współdziałanie programów zdalnego dostępu pochodzących od różnych producentów. Dodatkowo pozwala on wielu protokołom komunikacyjnym na wykorzystywanie tej samej fizycznej linii komunikacyjnej.

W połączeniach PPP protokół SLIP został zastąpiony przez PPP, jako że 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 wykorzystywany i w związku z tym serwer iSeries obsługuje go. Jednakże firma IBMzaleca korzystanie z protokołu PPP podczas konfigurowania połączeń PPP. Protokół SLIP nie obsługuje połączeń typu 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 wykorzystania przez serwer nowego połączenia PPP.

W celu wybrania trybu wykonaj następujące kroki:

1. Wybierz jeden z poniższych typów połączenia:
   - Linia komutowana
   - Linia dzierżawiona
   - L2TP (linia wirtualna)
   - Linia 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:

Ten typ połączenia należy wybrać, gdy do połączenia poprzez linię telefoniczną wykorzystywane jest połączenie modemowe (wewnętrzne lub zewnętrzne) albo zewnętrzny adapter terminalu ISDN.

Połączenie na liniach komutowanych może pracować w następujących trybach:

Odpowiedź

Wybór tego trybu pracy umożliwia zdalnym systemom inicjowanie połączenia z serwerem iSeries.

Połączenie

Wybór tego trybu pracy umożliwia serwerowi iSeries inicjowanie połączenia ze zdalnym systemem.

Połączenie na żądanie (tylko inicjowanie)

Wybór tego trybu pracy umożliwia serwerowi iSeries automatyczne inicjowanie połączenia ze zdalnym systemem wtedy, gdy w sieci zostanie wykryty ruch na łączu TCP/IP. 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)

Wybór tego trybu pracy umożliwia serwerowi iSeries odpowiadanie na próbę nawiązania połączenia ze strony dedykowanego systemu zdalnego. Tryb ten pozwala także serwerowi iSeries inicjować połączenia z systemem zdalnym, gdy zostanie wykryty ruch na łączu TCP/IP skierowany do systemu zdalnego. Jeśli zarówno system zdalny, jak i system lokalny są serwerami iSeries, przepływ danych TCP/IP między nimi może się odbywać na żądanie, bez konieczności 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. W celu obsługi połączeń przychodzących, 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:

Ten typ połączenia należy wybrać, gdy korzysta się z dedykowanej linii między lokalnym serwerem iSeries a systemem zdalnym. 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 dostęp do serwera iSeries poprzez linię dedykowaną. Ten tryb pracy odpowiada profilowi odbiorcy linii dzierżawionej.

Inicjator

Wybór tego trybu pracy umożliwia serwerowi iSeries dostęp do systemu zdalnego poprzez linię dedykowaną. Ten tryb pracy odpowiada profilowi nadawcy połączeń linii dzierżawionej.

L2TP (linia wirtualna):

Ten typ połączenia należy wybrać przy połączeniu między systemami wykorzystującymi protokół L2TP.

Po ustanowieniu tunelu L2TP między serwerem iSeries a systemem zdalnym nawiązywane jest połączenie 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 połączenie z serwerem iSeries poprzez tunel L2TP.

Inicjator

Wybór tego trybu pracy umożliwia serwerowi iSeries połączenie ze zdalnym systemem poprzez tunel L2TP.

Zdalne inicjowanie

Wybór tego trybu pracy umożliwia serwerowi iSeries połączenie z dostawcą ISP poprzez tunel L2TP i bezpośrednie zainicjowanie z poziomu ISP połączenia ze zdalnym klientem PPP.

Inicjator wieloprzeskokowy

Wybór tego trybu umożliwia serwerowi iSeries ustanowienie połączenia wieloprzeskokowego.

Uwaga: Profil terminatora L2TP przypisanego do inicjatora wieloprzeskokowego musi mieć ustawione pole ″Pozwolenie na połączenia wieloprzeskokowe″ oraz pozycję na liście zgodności 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 dostarczonego przez dostawcę ISP modemu DSL. Jest on podłączony do sieci lokalnej opartej na adapterze ethernet.

Dzięki temu użytkownicy sieci LAN mają szybki dostęp do Internetu przez sesje PPP poprzez serwer iSeries. Po nawiązaniu połączenia między serwerem iSeries i dostawcą ISP użytkownicy sieci LAN mogą rozpoczynać indywidualne sesje do dostawcy ISP poprzez PPPoE.

Połączenia PPPoE są używane tylko przez profile połączeń nadawcy i implikują tryb pracy inicjatora oraz wykorzystanie tylko linii pojedynczej.

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 serwera iSeries z koncentratorem dostępu PPPoE" na stronie 11
Wielu dostawców ISP oferuje szybki dostęp do sieci Internetu przy użyciu połączeń protokołu PPP przez sieć Ethernet (PPPoE). Serwer iSeries może łączyć się z takimi dostawcami usług, dzięki czemu uzyskuje większą szybkość przy zachowaniu zalet połączenia PPP.

"Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym" na stronie 14
Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

"Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu" na stronie 16
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą ISP mogą wykorzystać modem. Klienci PC przyłączeni do sieci LAN mogą łączyć się z Internetem, wykorzystując serwer iSeries jako bramę.

"Scenariusz: łączenie sieci LAN z sieciami zdalnymi przy pomocy modemu" na stronie 19
Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Za pomocą protokołu PPP można połączyć ze sobą dwie sieci LAN, ustanawiając połączenie między serwerem iSeries znajdującym się w centrali a serwerem iSeries będącym w oddziale.

Pojedyncza linia:

Ten typ obsługi linii należy wybrać, aby zdefiniować linię PPP skojarzoną z modemem analogowym. Opcja ta jest również używana dla linii dzierżawionych, w których modem nie jest potrzebny. Profil połączenia PPP zawsze wykorzystuje ten sam zasób portu komunikacyjnego serwera iSeries.

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**.

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 wykorzystujące linię z puli linii. Podczas uruchamiania połączenia PPP serwer iSeries wybiera nieużywaną linię z puli. Dla profilu połączenia na żądanie serwer 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 w zakładce Połączenia okna dialogowego **Właściwości nowego profilu punkt z punktem**. 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.

  Serwer iSeries 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 iSeries Navigator wybierz odpowiedni system i rozwiń opcję **Sieć → Usługi zdalnego dostępu**.
2. Utwórz profil połączenia służący do nawiązywania lub odbierania połączeń. Wybierz jedną z poniższych opcji:

- Kliknij prawym przyciskiem myszy **Profile połączenia nadawcy**, aby ustawić serwer iSeries jako serwer rozpoczynający połączenia.
- Kliknij prawym przyciskiem myszy **Profile połączenia odbiorcy**, aby ustawić serwer iSeries jako odbiorcę połączeń ze zdalnych systemów i 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 iSeries Navigator wyświetli okno właściwości tego profilu połączenia.

   Uwaga: Tworząc profile połączenia odbiornika również można wybrać pulę linii. Opcja Pula linii może być wyświetlona lub nie, w zależności od wartości 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 będzie po kolei sprawdzał listę dostępnych linii (w puli), aż znajdzie zasób, który jest dostępny i użyje tej linii do obsługi połączenia. Dalsze informacje zawiera pomoc elektroniczna do programu iSeries Navigator.

Odsyłacze pokrewne

“Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym” na stronie 14
Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP.

“Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu” na stronie 16
Najczęściej administratorzy konfigurują sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą ISP mogą wykorzystać modem. Klienci PC przyłączeni do sieci LAN mogą łączyć się z Internetem, wykorzystując serwer iSeries jako bramę.

“Scenariusz: łączenie sieci LAN z sieciami zdalnymi przy pomocy modemu” na stronie 19
Modem umożliwia wymianę danych między dwoma zdalnymi miejscami (np. centrala i oddział). Za pomocą protokołu PPP można połączyć ze sobą dwie sieci LAN, ustanawiając połączenie między serwerem iSeries znajdującym się w centrali a serwerem iSeries będącym w oddziale.

Obsługa profili połączeń wielokrotnych:

Profile połączeń PPP, które obsługują połączenia wielokrotne, pozwalają przy pomocy jednego profilu połączenia obsłużyć wiele połączeń cyfrowych, analogowych oraz L2TP.

Jest to przydatne, gdy wielu użytkowników potrzebuje połączyć się z serwerem iSeries . 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. W zasadzie dla każdej linii zdefiniowanej w puli uruchamiane jest osobne zadanie profilu połączenia. Wszystkie zadania 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 na serwerze iSeries. W celu wybrania istniejącego adresu IP można posłużyć się rozwijaną listą lokalnych adresów IP. Zdalni użytkownicy będą mieli dostęp do zasobów sieci lokalnej, jeśli jako lokalny adres IP profilu PPP wybrany zostanie adres IP lokalnego serwera iSeries. Trzeba ponadto zdefiniować adresy IP ze zdalnej puli adresów IP, tak aby były w tej samej sieci co adresy lokalne IP.

Jeśli na serwerze iSeries nie ma lokalnych adresów IP lub użytkownik nie chce, aby zdalni użytkownicy mieli dostęp do sieci lokalnej, należy zdefiniować wirtualne adresy IP na serwerze iSeries. Wirtualne adresy IP zwane są również interfejsem bezobwodowym. Profile połączeń PPP mogą używać takich adresów jako swoich lokalnych adresów IP. Ponieważ adresy takie nie są związane z fizyczną siecią, nie będą one automatycznie przekazywały danych do innych sieci dołączonych do serwera iSeries.

W celu utworzenia wirtualnego adresu IP, wykonaj poniższe czynności:

1. W programie iSeries Navigator wybierz odpowiedni system, a następnie wybierz opcję **Sieć → Konfiguracja TCP/IP → IPv4 → Interfejsy**.
2. Kliknij prawym przyciskiem myszy opcję **Interfejsy** i wybierz opcję **Nowy interfejs → Wirtualny adres IP**.
3. Aby utworzyć nowy interfejs dla wirtualnego adresu IP, wykonuj instrukcje kreatora interfejsu. Po utworzeniu wirtualnego adresu IP, profil połączenia PPP będzie mógł go używać. Możesz użyć listy rozwijanej z pola Lokalny adres IP na stronie Ustawienia TCP/IP.

   Uwaga: Wirtualne adresy IP muszą być aktywne 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.

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 pozwala systemowi przypisać unikalny zdalny adres IP każdemu połączeniu przychodzącemu.

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**.

  Kiedy zdalny użytkownik połączy się, serwer iSeries sprawdzi, czy dla tego użytkownika został 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 dla połączeń PPP

Na potrzeby analogowych połączeń PPP można użyć modemu zewnętrznego, modemu wewnętrznego albo adaptera terminalu ISDN. Modem umożliwia połączenie analogowe (na liniach dzierżawionych i komutowanych). Dla najbardziej popularnych typów modemów na serwerze iSeries zdefiniowano opisy modemów.

Odsyłacze pokrewne

“Rozwiązywanie problemów związanych z protokołem PPP” na stronie 64
Jeśli wystąpią problemy z połączeniem PPP, można wykorzystać listę kontrolną w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy identyfikacji objawu błędu oraz rozwiązywaniu problemów z połączeniem PPP.

Konfigurowanie nowego modemu

Poniższy temat zawiera opis konfigurowania nowego modemu.

Aby skonfigurować nowy modem, wykonaj poniższe czynności.

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. Na zakładce Ogólne wpisz poprawne wartości we wszystkie pola.
4. Opcjonalnie: Kliknij zakładkę **Parametry dodatkowe** i dodaj wszystkie konieczne komendy inicjowania modemu.
5. Kliknij **OK**, aby zapisać wprowadzone dane, i zamknij stronę Właściwości nowego modemu.

Użyj istniejącego opisu modemu

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

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
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 poprzedni opis modemu

Aby utworzyć opis modemu w oparciu od poprzedni opis modemu, wykonaj następujące kroki:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
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

   “Ustawianie łańcuchów komend modemu”

   “Rozwiązywanie problemów związanych z protokołem PPP” na stronie 64
   Jeśli wystąpią problemy z połączeniem PPP, można wykorzystać listę kontrolną w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy identyfikacji 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 na serwerze iSeries oraz 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

Pojęcia pokrewne

“Konfigurowanie nowego modemu” na stronie 55
Poniższy temat zawiera opis konfigurowania nowego modemu.

Przykład: konfigurowanie adaptera terminalu ISDN

Poniższy przykład przedstawia konfigurację terminalu adaptera ISDN.

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
2. Kliknij prawym przyciskiem **Modemy** i wybierz **Nowy modem**.
3. Na zakładce Ogólne wpisz poprawne wartości we wszystkie pola.
4. **Opcjonalne:** Kliknij zakładkę Parametry dodatkowe i dodaj 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 działań związanych z naprawą błędów wykonywaną przez serwer iSeries

   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 serwerowi iSeries 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. Kiedy 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 40
Sieć ISDN umożliwia połączenie cyfrowe, które pozwala na wymianę głosu, danych i obrazów wideo między różnymi aplikacjami multimedialnymi.

Przypisanie modemu do opisu linii

1. W programie iSeries Navigator wybierz odpowiedni serwer i rozwiń gałąź **Sieć → Usługi zdalnego dostępu → Profile połączenia nadawcy lub Profile połączenia odbiorcy**.
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 odpowiednie definicje. Więcej informacji na ten temat można znaleźć w pomocy elektronicznej.

Można tak skonfigurować profil połączenia nadawcy, aby ten ″pożyczał″ linię PPP i modem przypisane do profilu połączenia odbiorcy, oczekującego na połączenia przychodzące. Następnie, po zakończeniu połączenia, linia PPP i modem są ″oddawane″ profilowi połączenia odbiorcy. Aby włączyć nową funkcję, wybierz opcję **Włącz dynamiczne**

współużytkowanie zasobów z zakładki Modem okna konfiguracji linii PPP. Linie PPP można konfigurować z zakładki Połączenie profilu połączenia nadawcy lub profilu połączenia odbiorcy.

Zadania pokrewne

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

Konfigurowanie zdalnego komputera PC

Aby podłączyć do serwera iSeries komputer PC z 32-bitowym systemem operacyjnym Windows należy sprawdzić, czy zainstalowany modem został poprawnie skonfigurowany oraz czy zainstalowano protokół TCP/IP oraz Dial-Up Networking.

Informacje na temat konfigurowania Dial-up Networking można znaleźć w dokumentacji systemu Microsoft Windows. Upewnij się, czy zostały wprowadzone następujące informacje:

- Typ połączenia modemowego powinien być ustawiony na **PPP**.
- Do szyfrowania haseł powinien być używany protokół MD-5 CHAP (MS-CHAP nie jest obsługiwany przez serwer iSeries). 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). Żaden inny protokół nie jest obsługiwany przez serwer iSeries.
- Zazwyczaj adresowanie IP jest definiowane przez system zdalny, czyli w rozważanym przypadku serwer iSeries. W przypadku użycia alternatywnej metody adresowania IP (jak na przykład zdefiniowanie własnych adresów IP), należy się upewnić, czy serwer iSeries został skonfigurowany do akceptacji tej metody.
- Adres IP serwera DNS, jeśli istnieje.

Konfigurowanie zdalnego połączenia z Internetem 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 dwa typy aplikacji:

- **Mail Exchange**: umożliwia okresowe pobieranie poczty z pojedynczego konta AT&T Global Network i wysyłanie jej do serwera iSeries w celu dostarczenia jej użytkownikom Lotus Mail lub użytkownikom 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: 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. Wybierz w programie iSeries Navigator odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
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 pomaga skonfigurować profil połączenia modemowego. Pozwala to uzyskać dostęp 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 ten temat można znaleźć w pomocy elektronicznej.

Kreator połączenia uniwersalnego IBM

Kreator pomagający krok po kroku skonfigurować profil, który może zostać użyty przez oprogramowanie elektronicznego wsparcia klienta do połączenia z firmą IBM. Obsługa usług elektronicznych monitoruje środowisko systemowe serwera iSeries w celu wskazania indywidualnych poprawek dla systemu i sytuacji.

Informacje pokrewne

Konfigurowanie połączenia uniwersalnego

Konfigurowanie strategii dostępu do 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.

W celu skonfigurowania nowej strategii dostępu do grupy:

1. W programie iSeries Navigator wybierz odpowiedni serwer i rozwiń gałąź **Sieć → Usługi zdalnego dostępu → Profile połączenia odbiorcy**.
2. Kliknij prawym przyciskiem myszy opcję **Strategie dostępu do grupy** i wybierz opcję **Nowa strategia dostępu do grupy**.
3. W zakładce **Ogólne** 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. Jeśli zostanie wybrana, serwer iSeries będzie pracował jako router dla danego połączenia. Dzięki temu datagramy IP nieprzeznaczone dla serwera iSeries będą przekazywane dalej. Jeśli opcja ta nie została wybrana, to protokół IP będzie odrzucał te datagramy z systemu zdalnego, których punktem docelowym nie jest adres lokalny w danym systemie iSeries.

   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 wypadku, nawet pomimo zaznaczenia tej opcji, funkcja będzie ignorowana. Ustawienie przekazywania datagramów IP dla całego systemu można sprawdzić w zakładce **Ogólne** na stronie Właściwości IPv4.

   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 serwer iSeries ustanawia połączenie, które nie wykorzystuje kompresji.

   Dla tego połączenia użyj reguł pakietów IP. Opcja ta określa, czy w przypadku danej strategii dostępu do grupy zastosować reguły filtrowania. Reguły filtrowania umożliwiają sterowanie ruchem IP w sieci. Dzięki temu można chronić system lokalny poprzez 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 24
Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

Informacje pokrewne

Filtrowanie IP i translacja adresu sieciowego (NAT)

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 reguły NAT Centrum informacyjnego omówiony jest sposób tworzenia reguł pakietów IP, które można zastosować do profili połączeń PPP.

Istniejące reguły filtrowania pakietów IP można zastosować 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 do 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 24
Strategia dostępu do grupy rozpoznaje odrębne grupy użytkowników połączenia i umożliwia zastosowanie wspólnych atrybutów połączenia i ustawień ochrony dla całej grupy. W połączeniu z filtrowaniem IP, strategia umożliwia dopuszczenie lub ograniczenie dostępu do określonych adresów IP w sieci.

Udostępnianie usług RADIUS i DHCP profilom połączeń

Aby udostępnić usługi RADIUS lub DHCP profilom odbiorcy połączeń PPP, należy wykonać następujące czynności:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**.
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 wybrać rozliczanie RADIUS i konfigurację adresu TCP/IP.

5. Kliknij przycisk **Ustawienia NAS RADIUS**, aby skonfigurować połączenie z serwerem RADIUS.
6. Kliknij przycisk **OK**, aby powrócić do programu iSeries Navigator.

Odsyłacze pokrewne

"Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS" na stronie 22
Serwer dostępu do sieci działający na serwerze iSeries może kierować żądania uwierzytelnienia od klientów z połączeniem komutowanym do odrębnego serwera RADIUS. Po uwierzytelnieniu serwer RADIUS może także sterować adresami IP dla użytkownika.

Zarządzanie PPP

Informacje dotyczące zadań związanych z zarządzaniem protokołem PPP dostępnych na serwerach the iSeries.

Odsyłacze pokrewne

"Informacje pokrewne dotyczące protokołu PPP" na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF 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.

Poniższe wskazówki można wykorzystać 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 online do programu iSeries Navigator opisano wszystkie opcje dostępne w oknie. Więcej informacji zawierają procedury i przykłady połączeń PPP.

Monitorowanie aktywności połączeń PPP

Podgląd profilu połączenia i protokołu sesji można uzyskać za pomocą programu iSeries Navigator.

Zadania połączeń PPP:

- Są dwa zadania sterujące połączeniami PPP wykorzystywane do zarządzania indywidualnymi zadaniami połączeń PPP. Zadania te są uruchamiane w podsystemie QSYSWRK:
  - QTPPPCTL - Główne zadanie sterujące połączeniem PPP. Zadanie zarządzające każdym zadaniem połączenia 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*nn* to zadania połączeń przychodzących, gdzie *nn* jest dowolną liczbą od 1 do 99.

Praca z profilami połączeń:

1. Wybierz w programie iSeries Navigator odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**. 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. Wybierz w programie iSeries Navigator odpowiedni system i rozwiń gałąź **Sieć → Usługi zdalnego dostępu**. 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 **Zdania**. 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 **Szczegóły**. 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 serwera iSeries:

Aby pracować z danymi wyjściowymi PPP, w wierszu komend serwera iSeries wpisz 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** po wybraniu profili 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	Serwer 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

Tabela 10. Opis statusu podstawowego (kontynuacja)

Opis statusu podstawowego	Objaśnienie
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 związanych z protokołem PPP

Jeśli wystąpią problemy z połączeniem PPP, można wykorzystać listę kontrolną w celu zebrania informacji o błędzie. Lista kontrolna jest pomocna przy identyfikacji objawu błędu oraz rozwiązywaniu problemów z połączeniem PPP.

Bieżące oraz pokrewne informacje dotyczące poprawek PTF oraz rozwiązywania problemów są dostępne na stronie iSeries server TCP/IP home page  . Odsyłacz udostępnia dane, które uzupełniają lub zastępują informacje zawarte w tym artykule.

1. Wymagany materiał pomocniczy:
   - Typ zdalnego hosta, system operacyjny i poziom.
   - Poziom systemu operacyjnego hosta serwera iSeries
   - Wszystkie zbiory wyjściowe zapisywane w kolejce wyjściowej pod tą samą nazwą, co profil.
   - Protokoły zadań podsystemów QTPPPCTL i QTPPPL2TP (dla profili L2TP).
   - Skrypt połączenia, jeśli był używany w 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 (redbook) ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  zawiera informacje o poniższych problemów z protokołem PPP. Zawiera również szczegółowe informacje na temat rozwiązywania problemów.

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 iSeries 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 dolnych poziomów protokołu PPP. Jeśli protokół PPP oraz protokół zadania PPP nie wykazują żadnych problemów, można wykorzystać funkcję śledzenia.

Pojęcia pokrewne

“Konfigurowanie modemu dla połączeń PPP” na stronie 55
Na potrzeby analogowych połączeń PPP można użyć modemu zewnętrznego, modemu wewnętrznego albo adaptera terminalu ISDN. Modem umożliwia połączenie analogowe (na liniach dzierżawionych i komutowanych). Dla najbardziej popularnych typów modemów na serwerze iSeries zdefiniowano opisy modemów.

“Konfigurowanie nowego modemu” na stronie 55
Poniższy temat zawiera opis konfigurowania nowego modemu.

Odsyłacze pokrewne

“Informacje pokrewne dotyczące protokołu PPP” na stronie 66
Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Informacje pokrewne dotyczące protokołu PPP

Poniższy temat zawiera listę dokumentacji technicznej IBM Redbooks (w formacie PDF) i serwisów WWW związanych z usługą PPP. Każdy z plików PSF można wyświetlić lub wydrukować.

Dokumentacja techniczna IBM Redbooks

- TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)
- iSeries IP Networks: Dynamic! (SG24-6718)

Serwisy WWW

Najnowsze poprawki PTF i najnowsze informacje o konfiguracji protokołów PPP i L2TP dostępne są poprzez odsyłacz PPP na stronie iSeries™ server TCP/IP home page. Odsyłacz do danych, które uzupełniają lub zastępują informacje zawarte w tej kolekcji tematów.

Zapisywanie plików PDF

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

1. W oknie przeglądarki kliknij prawym przyciskiem myszy wybrany dokument (jeden z powyższych odsyłaczy).
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w ma zostać zapisany plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do wyświetlenia lub wydrukowania zawartości plików PDF niezbędny jest program Adobe Reader. Jego kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Dodatek. Uwagi

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

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

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
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 ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

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

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

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

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

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

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program 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 innych podmiotów uzyskano od dostawców tych produktów, z opublikowanych 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 innych podmiotów 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 są fikcyjne i jakiekolwiek ich podobieństwo do nazwisk, nazw i adresów używanych w rzeczywistych przedsiębiorstwach jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

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

Interfejs programistyczny - informacje

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
| i5/OS
| IBM
| iSeries
| Lotus
| OS/400
| Redbooks

Linux jest 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 i logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

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

Warunki

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

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

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

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

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

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

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.