

iSeries

Usługi zdalnego dostępu: połączenia PPP

IBM Confidential





@server

iSeries

Usługi zdalnego dostępu: połączenia PPP

IBM Confidential

Spis treści

Część 1. Usługi zdalnego dostępu: połączenia PPP	1
Rozdział 1. Co nowego w wersji V5R2.	3
Rozdział 2. Drukowanie tego dokumentu	5
Rozdział 3. Scenariusze PPP	7
Scenariusz: łączenie serwera iSeries z koncentratorom dostępu PPPoE	8
Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym	9
Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu	11
Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu	14
Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS	17
Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP	18
Rozdział 4. Pojęcia dotyczące protokołu PPP	23
Co to jest protokół PPP	23
Profile połączeń	23
Obsługa strategii dostępu do grupy	25
Rozdział 5. Planowanie protokołu PPP	27
Wymagania sprzętowe i programowe	27
Połączenia alternatywne	28
Analogowe linie telefoniczne	28
Usługi cyfrowe DDS	29
Linia Switched-56	30
ISDN	30
Linie T1/E1 i linia częściowa T1	31
Frame Relay	31
Obsługa połączeń PPP przez protokół L2TP (tunelowanie)	32
Tunel dobrowolny	32
Tunel wymuszony - połączenia przychodzące	32
Tunel wymuszony - połączenia zdalne	32
Połączenie wieloprzeskokowe L2TP	32
Obsługa PPPoE (DSL) dla połączeń PPP	32
Urządzenia łączące	33
Modemy	33
Urządzenia CSU/DSU	33
Adaptory terminali ISDN	33
Zalecane adaptory terminali ISDN	34
Ograniczenia adaptera terminalu ISDN	34
Obsługa adresów IP	35
Filtrowanie pakietów IP	37
Uwierzytelnianie systemu	38
Protokół CHAP-MD5	38
Protokół EAP	38
Protokół PAP	39
Protokół RADIUS	39
Lista weryfikacji	39
Uwagi dotyczące przepustowości - Multilink	40
Rozdział 6. Konfigurowanie protokołu PPP	41
Tworzenie profilu połączenia	41

Typ protokołu: PPP lub SLIP	42
Wybór trybu	42
Linia komutowana	42
Linia dzierżawiona	43
Protokół L2TP (linia wirtualna)	43
Protokół L2TP (Layer 2 Tunneling Protocol)	44
Linia PPPoE	44
Konfigurowanie połączenia	45
Pojedyncza linia	45
Pula linii	45
Obsługa profili połączeń wielokrotnych	46
Pule zdalnych adresów IP	47
ISDN	48
Konfigurowanie modemu dla połączeń PPP	48
Konfigurowanie nowego modemu.	48
Ustawianie łańcuchów komend modemu	49
Przykład: konfigurowanie adaptera terminalu ISDN	49
Przypisanie modemu do opisu linii	50
Konfigurowanie zdalnego komputera PC	51
Konfigurowanie zdalnego połączenia z Internetem poprzez AT&T Global Network	51
Kreatory połączeń	52
Konfigurowanie strategii dostępu do grupy	52
Przypisywanie reguł filtrowania pakietów IP do połączeń PPP	54
Udostępnianie usług RADIUS i DHCP profilom połączeń	54
Rozdział 7. Zarządzanie PPP	55
Ustawianie właściwości dla profili połączeń PPP	55
Monitorowanie aktywności połączeń PPP	55
Rozdział 8. Rozwiązywanie problemów związanych z protokołem PPP	59
Rozdział 9. Inne informacje o protokole PPP.	61

Część 1. Usługi zdalnego dostępu: połączenia PPP

Protokół Point-to-Point (PPP) jest internetowym standardem służącym do przesyłania danych przy pomocy łączy szeregowych. Jest też najczęściej używanym przez dostawców usług internetowych protokołem połączeniowym. Protokół PPP pozwala indywidualnym komputerom na dostęp do sieci, umożliwiając połączenie z Internetem. Serwer 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. Przy pomocy 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 V5R2 opisuje uaktualnienia dla Usług zdalnego dostępu
- Drukowanie tego dokumentu opisuje, w jaki sposób pobrać i wydrukować ten dokument w wersji PDF.

Zrozumienie Usług zdalnego dostępu: połączenia PPP

Sekcje te opisują w skrócie usługi zdalnego dostępu na serwerze iSeries 400. Pomagają w planowaniu środowiska protokołu PPP dla sieci.

- **Scenariusze dla protokołu PPP** są przykładami różnych implementacji połączeń przy pomocy tego protokołu. Każdy z nich zawiera instrukcje i określa przykładowe wartości potrzebne do skonfigurowania połączenia PPP.
- **Pojęcia dotyczące protokołu PPP** zawiera informacje na temat terminów związanych z protokołem PPP oraz z wymaganiami serwera iSeries 400 dla połączeń PPP.
- **Planowanie protokołu PPP** zawiera informacje na temat terminów związanych z protokołem PPP oraz z wymaganiami serwera iSeries 400 dla połączeń PPP.

Korzystanie z Usług zdalnego dostępu: połączenia PPP

Sekcje te opisują konfigurację i zarządzanie połączeniami PPP na serwerze iSeries 400.

- **Konfigurowanie protokołu PPP** opisuje podstawowe kroki podczas konfigurowania połączenia PPP.
- **Zarządzanie protokołem PPP** zawiera informacje, które pomogą zarządzać połączeniami PPP.
- **Rozwiązywanie problemów związanych z protokołem PPP** opisuje podstawowe błędy połączenia PPP i wskazuje, gdzie znajdują się informacje umożliwiające ich usunięcie.

Również ta sekcja zawiera dodatkowe informacje o protokole PPP. Na tej stronie znajdują się odsyłacze do przydatnych i pokrewnych informacji dotyczących serwera iSeries.

Rozdział 1. Co nowego w wersji V5R2

W wersji V5R2, program iSeries Navigator umożliwia inicjowanie z serwera iSeries połączeń PPP przez sieć Ethernet (PPPoE). Do nawiązania połączenia PPP przy użyciu adaptera Ethernet LAN, przyłączonego do modemu DSL, na linii Ethernet tworzony jest nowy, wirtualny rodzaj linii PPPoE. Po nawiązaniu połączenia pomiędzy serwerem iSeries i dostawcą ISP, użytkownicy sieci LAN mają dostęp do dostawcy ISP przez połączenie iSeries PPPoE. Nowa funkcja jest dostępna z okna dialogowego Profil połączenia nadawcy lub Uniwersalny kreator połączenia.

Więcej informacji zawiera sekcja Łączenie serwera iSeries z koncentratorom dostępu PPPoE.


Poniżej wymienionych zostało kilka dodatków do programu iSeries Navigator, usprawniających konfigurowanie i zarządzanie połączeniami PPP:

- Okno dialogowe konfiguracji DHCP-WAN automatycznie kontaktuje się z serwerem DHCP i z interfejsem klienta w celu określenia adresu IP dla interfejsu DHCP-WAN klienta. Aby skorzystać z tego okna dialogowego:
 - rozwiń **Sieć > Usługi zdalnego dostępu**,
 - kliknij prawym przyciskiem myszy **Usługi zdalnego dostępu**,
 - wybierz **Usługi**,
 - wybierz zakładkę **klient WAN DHCP**.
- Ulepszone okno dialogowe statusu połączenia przedstawia szczegóły dotyczące połączeń L2TP, wieloprzeskokowych L2TP, typu multilink i PPP przez sieć Ethernet, ułatwiając zarządzanie połączeniami PPP.
- Do programu Task Pad dodano możliwości tworzenia profilu połączenia nadawcy, odbiorcy i strategii dostępu do grupy.
- Zmieniono nazwy kreatorów. Kreator nowego połączenia telefonicznego i Kreator połączenia uniwersalnego obecnie noszą nazwę: New Internet Dial Connection lub ISP Dial Connection (Nowe połączenie z Internetem lub Nowe połączenie telefoniczne z ISP) i New IBM Universal Connection (Nowe połączenie uniwersalne IBM).
- Profil połączenia nadawcy może "pożyczyć" 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 dialogowego konfiguracji linii PPP. Linie PPP można konfigurować z zakładki Połączenie profilu połączenia nadawcy lub profilu połączenia odbiorcy.
- Nie można zmieniać właściwości puli linii będących już w użyciu; zapobiega to wystąpieniu potencjalnych problemów z pulą linii.
- Z profilu połączenia nadawcy dla połączeń L2TP usunięto obsługę trybów pracy Inicjator na żądanie i Zdalne wybieranie na żądanie.

Rozdział 2. Drukowanie tego dokumentu

W celu przeglądania i drukowania tego dokumentu można pobrać jego wersję PDF. Pliki PDF można przeglądać za pomocą programu Adobe® Acrobat® Reader. Jego kopię można pobrać ze strony Adobe



Aby przejrzeć lub pobrać wersję PDF, należy wybrać Usługi zdalnego dostępu połączenia PPP  (277 kB lub około 58 stron).

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

1. Otwórz PDF w swojej przeglądarce (kliknij powyższy odsyłacz).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako...**
4. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Rozdział 3. Scenariusze PPP

Poniższe scenariusze 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.

Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE

Wielu dostawców ISP proponuje szybki dostęp do Internetu przez DSL z wykorzystaniem protokołu 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

Zdalni użytkownicy, tacy jak tele-użytkownicy lub klienci wykorzystujący komputery przenośne, wymagają częstego dostępu do sieci LAN. Mogą oni uzyskać dostęp do serwera iSeries za pomocą protokołu PPP.

Scenariusz: łączenie sieci LAN z Internetem za pomocą modemu

Najczęściej administratorzy konfiguruje sieć LAN w taki sposób, aby pracownicy mieli dostęp do Internetu. Do połączenia serwera iSeries z dostawcą usług internetowych (ISP) mogą oni 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 za pomocą 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 pomiędzy serwerem iSeries znajdującym się w centrali i serwerem będącym w oddziale.

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 i portami dla użytkownika.

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 niektórych 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.

Scenariusz: protokoły PPP i DHCP działające na jednym serwerze iSeries

Klienci z połączeniem komutowanym lub użytkownicy zdalni mogą uzyskać dostęp do serwera iSeries, wykorzystując protokół PPP. Klient DHCP WAN na tym samym serwerze iSeries umożliwia użytkownikom zdalnym otrzymanie dynamicznie przydzielonego adresu IP przy użyciu tych samych usług, z których korzystają użytkownicy lokalni.

Scenariusz: profile DHCP i PPP działające na różnych serwerach iSeries

Względy ochrony lub fizyczna warstwa sieci powodują, że większość przedsiębiorstw rozdziela usługi sieciowe i umieszcza je na różnych serwerach. Scenariusz ten opisuje złożone zagadnienie posiadania

osobnego serwera PPP i DHCP. Tak jak w poprzednim scenariuszu, konfiguracja ta pozwala zdalnym użytkownikom na połączenie telefoniczne i dostęp do sieci LAN.

Scenariusz: protokół PPP i sieć VPN: tunel dobrowolny protokołu L2TP zabezpieczony przez sieć VPN

Oddział może zostać połączony z centralą przedsiębiorstwa przy pomocy protokołu tunelującego warstwy 2 (L2TP). Protokół ten ustanawia wirtualne połączenie PPP. W efekcie protokół L2TP rozszerza sieć powodując, że oddziały stają się częścią sieci LAN. Sieć VPN zabezpiecza ruch danych w tunelu protokołu L2TP.

Scenariusz: łączenie serwera iSeries z koncentratorem dostępu PPPoE

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 1. 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, skonfigurowanej do korzystania z adaptera Ethernet 2838. 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 i 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.

Przykładowa konfiguracja:

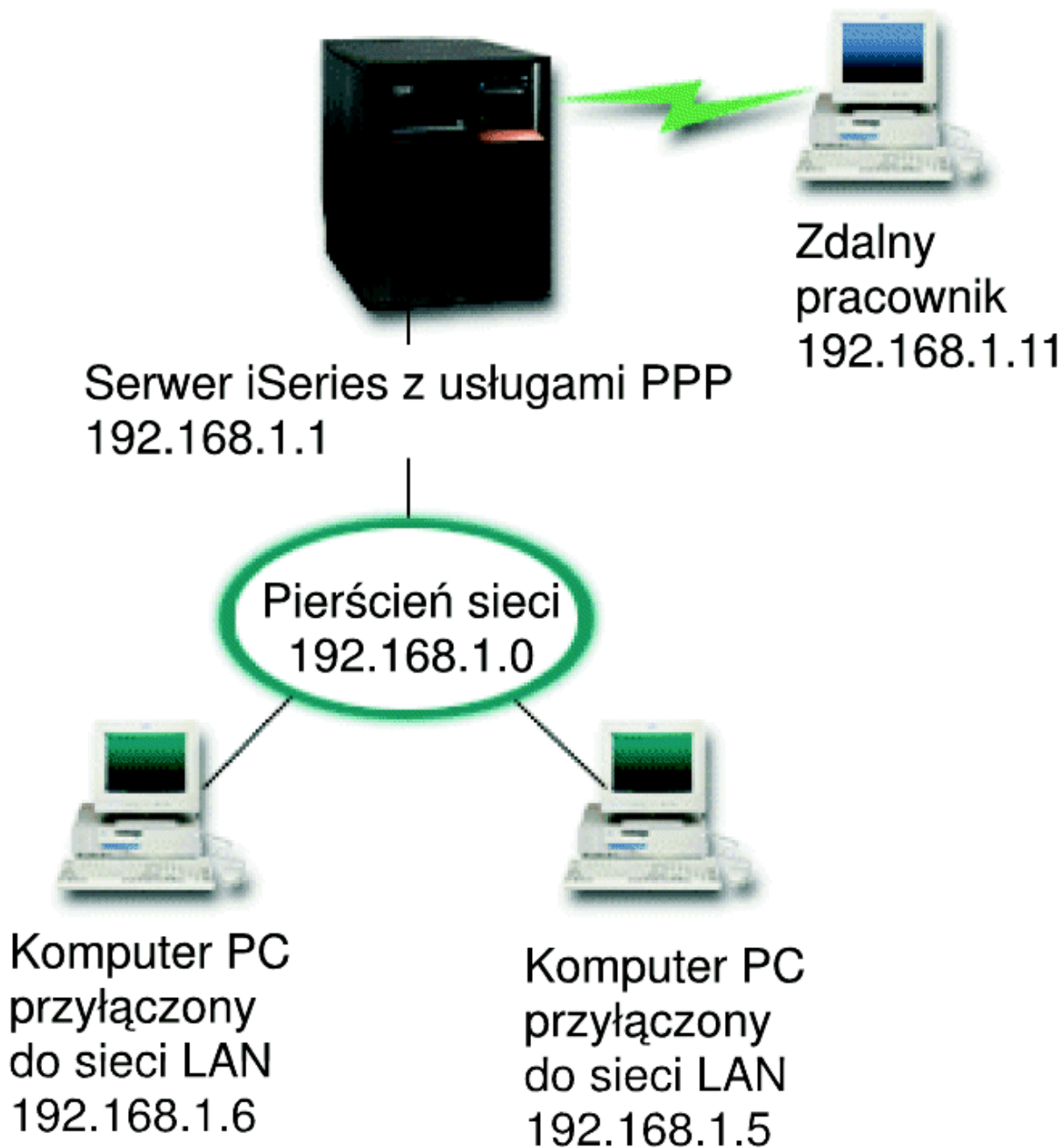
1. Skonfiguruj połączenie z dostawcą ISP.

2. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries.
Upewnij się, że wprowadziłeś poniższe informacje:
 - **Typ protokołu:** PPP
 - **Typ połączenia:** Protokół PPP przez sieć Ethernet
 - **Tryb pracy:** Inicjator
 - **Konfiguracja linii:** Linia pojedyncza
3. Na stronie **Ogólne** we Właściwościach nowego profilu połączenia punkt z punktem, wprowadź nazwę i opis profilu nadawcy. Nazwa ta będzie się odnosić zarówno do profilu połączenia, jak i do linii wirtualnej PPPoE.
4. Kliknij 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 rzeczowy opis linii wirtualnej PPPoE.
 - b. Kliknij stronę **Łącza**. 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 2838.
 - 1) Na stronie **Ogólne** wprowadź rzeczowy opis linii Ethernet i sprawdź, czy w definicji linii podano odpowiednie zasoby sprzętowe.
 - 2) Kliknij stronę **Łącza**. Wprowadź właściwości fizycznej linii Ethernet. Więcej informacji na ten temat znajduje się w dokumentacji karty Ethernet i w pomocy elektronicznej.
 - 3) Kliknij stronę **Inne**. Określ poziom dostępu i uprawnienia użytkowników tej linii.
 - 4) Kliknij **OK**, aby powrócić do strony właściwości linii wirtualnej PPPoE.
 - c. Kliknij **Ograniczenia**, aby zdefiniować właściwości uwierzytelniania LCP lub kliknij **OK**, aby wrócić do strony **Połączenie** nowego profilu połączenia punkt z punktem.
5. Jeśli dostawca ISP wymaga, aby serwer iSeries uwierzytelił się lub jeśli chcesz, aby serwer iSeries uwierzytelił zdalny serwer, kliknij stronę **Uwierzytelnianie**. Więcej informacji na ten temat można znaleźć w sekcji Uwierzytelnianie systemu.
6. Kliknij stronę **Ustawienia TCP/IP** i określ parametry obsługi adresów IP dla tego profilu połączenia. Aby użytkownicy sieci lokalnej mogli łączyć się z Internetem korzystając z adresu IP przydzielonego do serwera iSeries, wybierz **Ukrywanie adresów (pełne maskowanie)**.
7. Kliknij 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 stronę **Inne**.
9. Kliknij **OK**, aby zakończyć.

Więcej informacji o ograniczaniu użytkownikom dostępu do zewnętrznych adresów IP lub zasobów serwera iSeries można znaleźć w sekcjach Filtrowanie IP i Strategie dostępu do grupy.

Scenariusz: łączenie zdalnych klientów z serwerem iSeries połączeniem komutowanym

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 np. 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 jedyny modem, który można wykorzystać do nawiązania połączenia to modem 7852-400 ECS.



Rysunek 2. 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 się 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.

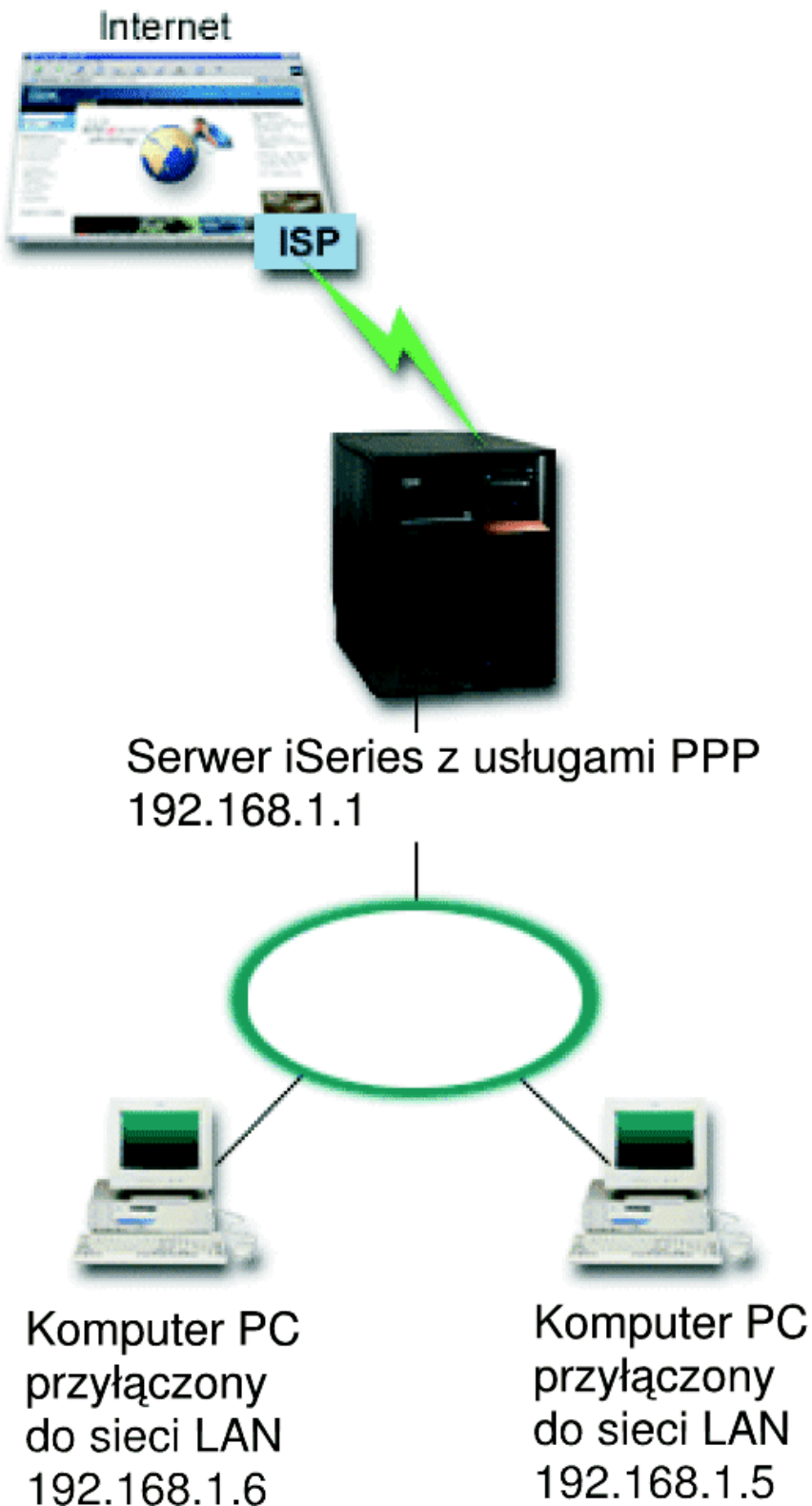
Na powyższym rysunku znajduje się tylko jeden klient połączenia modemowego, ponieważ modem ECS może nawiązać tylko jedno połączenie w określonym czasie. Informacje dotyczące jednoczesnej obsługi wielu klientów połączeń modemowych znajdują się w sekcji planowania opisującej zagadnienie zarówno od strony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

Przykładowa konfiguracja:

1. Skonfiguruj Dial-up Networking i utwórz połączenie modemowe na zdalnym komputerze PC.
2. Skonfiguruj Profil połączenia odbiorcy na serwerze iSeries.
Upewnij się, że wprowadziłeś 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 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 stronę **Modem**. Z listy wyboru nazw wybierz modem **IBM 2772**.
 - c. Kliknij **OK**, aby powrócić do strony Właściwości nowego profilu połączenia punkt z punktem.
5. Kliknij stronę **Uwierzytelnianie**.
 - a. Zaznacz **Wymagane przez serwer iSeries do weryfikacji 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 stronę **Ustawienia protokołu TCP/IP**.
 - a. Zaznacz lokalny adres IP 192.168.1.1.
 - b. Dla zdalnego adresu zaznacz **Stały adres IP (Fixed IP address)** z początkowym adresem 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.

Scenariusz: łączenie sieci LAN z Internetem przy pomocy modemu

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 3. Łączenie sieci LAN z Internetem przy pomocy modemu

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

Po ustanowieniu połączenia, 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 zarezerwowane adresy IP, komunikację z Internetem.

Po połączeniu serwera i sieci z Internetem, należy uświadomić sobie, że występuje związane z tym ryzyko 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.

Jeśli przy tego typu połączeniu PPP wykorzystywany jest modem ECS, należy go skonfigurować do pracy w trybie asynchronicznym. 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.

Przykładowa konfiguracja:

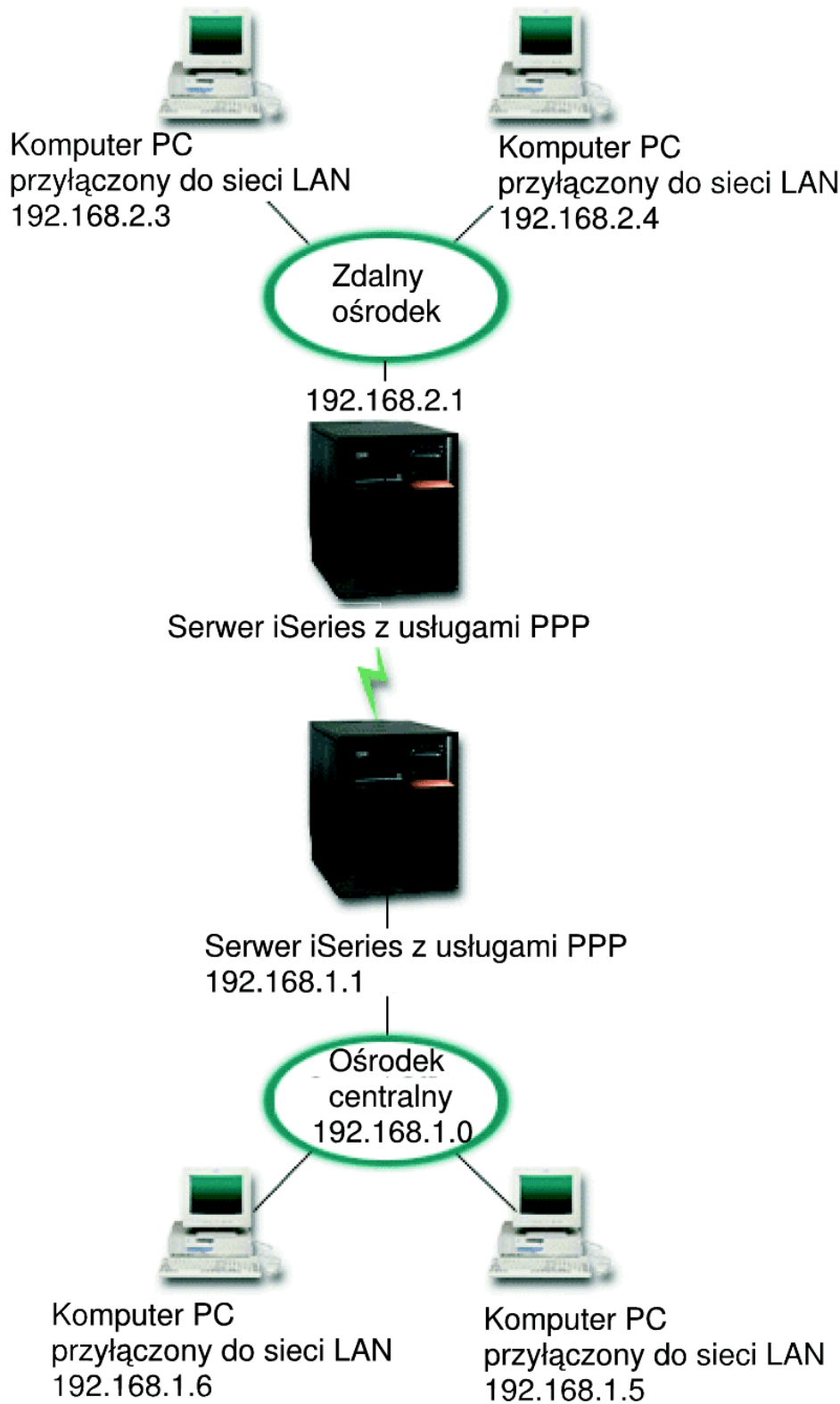
1. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries.
Upewnij się, że wybrałeś poniższe informacje:
 - **Typ protokołu:** PPP
 - **Typ połączenia:** Linia komutowana
 - **Tryb pracy:** Wybieranie
 - **Konfiguracja linii:** Może to być w zależności od środowiska linia pojedyncza lub pula linii.
2. Na stronie **Ogólne** we Właściwościach nowego profilu połączenia punkt z punktem, wprowadź nazwę i opis profilu nadawcy.
3. Kliknij 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 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 dostawcy ISP. Upewnij się, że uwzględniłeś wszystkie wymagane przedrostki.
5. Kliknij stronę **Uwierzytelnianie**, wybierz **Zezwalaj zdalnemu systemowi na weryfikację tożsamości tego serwera iSeries**. Wybierz protokół uwierzytelniający i wprowadź informacje dotyczące nazwy użytkownika i hasła.
6. Kliknij Ustawienia 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 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: Musisz upewnić się również, 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 do serwera iSeries.

Scenariusz: łączenie sieci LAN z sieciami zdalnymi za pomocą modemu

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 4. Łączenie sieci LAN z sieciami zdalnymi za pomocą modemu

Rozwiązanie: Za pomocą protokołu PPP można połączyć dwie sieci LAN ustanawiając połączenie pomiędzy 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 pomiędzy sieciami LAN. Przy rozstrzyganiu nazw hostów pomiędzy sieciami LAN należy wziąć pod uwagę serwer DNS i względy bezpieczeństwa.

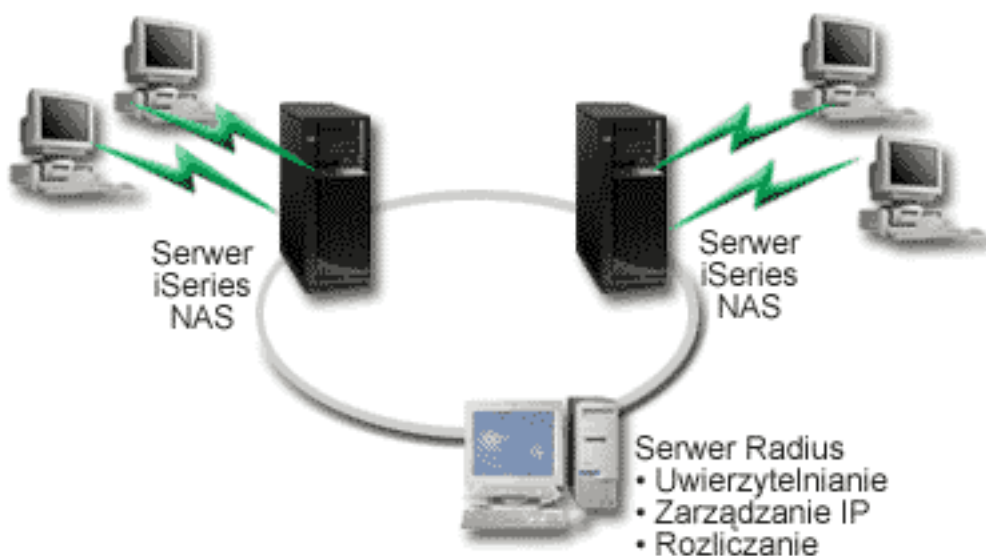
Przykładowa konfiguracja:

1. Skonfiguruj Profil połączenia nadawcy na serwerze iSeries znajdującym się w oddziale.
Upewnij się, że wybrałeś poniższe 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 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 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. Upewnij się, że uwzględniłeś wszystkie wymagane przedrostki.
5. Kliknij stronę **Uwierzytelnianie** i wybierz **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 stronę **Ustawienia protokołu 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.
Upewnij się, że wybrałeś 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.
8. Na stronie **Ogólne** we Właściwościach nowego profilu połączenia punkt z punktem wprowadź nazwę i opis profilu odbiorcy.
9. Kliknij 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 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 stronę **Uwierzytelnianie**.
- a. Sprawdź **Wymagane przez serwer iSeries do weryfikacji tożsamości systemu zdalnego**.
 - b. Dodaj nowego użytkownika do listy weryfikacji.
 - c. Sprawdź uwierzytelnianie przy pomocy algorytmu CHAP-MD5.
11. Kliknij stronę **Ustawienia protokołu 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**. Pojawi się okno dialogowe Adresy IP zdefiniowane dla nazwy użytkownika. Kliknij **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 serwerów iSeries jako bramy.
12. Kliknij **OK**, aby zakończyć.

Scenariusz: uwierzytelnianie połączeń modemowych za pomocą RADIUS NAS

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 obsługiwaniu żądań sprawdzenia ID użytkowników i ich haseł, a także określanie przysługujących im adresów IP.



Rysunek 5. 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.

Przykładowa konfiguracja:

1. W programie iSeries Navigator rozwiń **Sieć**, kliknij prawym klawiszem myszy **Usługi zdalnego dostępu** i wybierz **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 Authentication Server (i opcjonalnie Accounting Server) kliknij **Dodaj** i wprowadź następujące dane:
 - a. W oknie **Lokalny adres IP** wprowadź adres IP dla interfejsu serwera iSeries używanego do połączenia z serwerem RADIUS.
 - b. W oknie **Adres IP serwera** wprowadź adres IP serwera RADIUS.
 - c. W oknie **Hasło** wprowadź hasło używane do identyfikacji serwera iSeries na serwerze RADIUS.
 - d. W oknie **Port** wprowadź numer portu serwera iSeries używanego do komunikacji z serwerem RADIUS. Dla serwera uwierzytelniającego wprowadź port 1812, a dla serwera rozliczającego port 1813.
6. Kliknij **OK**.
7. W programie iSeries Navigator rozwiń **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 **Wymagane przez serwer iSeries do weryfikacji tożsamości systemu zdalnego**.
10. Wybierz **Uwierzytelnianie zdalne przy użyciu serwera RADIUS**.
11. Wybierz protokół uwierzytelniania (EAP, PAP lub CHAP-MD5). Protokół ten musi być także używany przez serwer RADIUS. Więcej informacji na ten temat zawiera sekcja Uwierzytelnianie systemu.
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.

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

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, partner w interesach potrzebuje połączenia modemowego i dostępu do usług takich jak HTTP, FTP czy Telnet, ale ze względów bezpieczeństwa nie powinien 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 6. 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 strategię dostępu do grup i reguły filtrowania IP. Strategię 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". 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 strategię dostępu do grupy (po jednej dla każdej grupy). Strategię 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.

Przykładowa konfiguracja:

1. Utwórz identyfikator filtra PPP i filtry reguł pakietów IP, które określą uprawnienia i ograniczenia dla tej strategii dostępu do grupy. Więcej informacji na temat filtrowania IP zawiera sekcja Reguły pakietów IP (filtrowanie i NAT) .
 - a. W programie iSeries Navigator rozwiń **Sieć -> Usługi zdalnego dostępu**.
 - b. Kliknij **Profil połączenia odbiorcy**, kliknij prawym klawiszem myszy profil połączenia dla tego połączenia i wybierz opcję **Właściwości**.
 - c. Wybierz zakładkę **Ustawienia TCP/IP** i kliknij **Zaawansowane**.
 - d. 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.
 - e. 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 niejawną, domyślną instrukcję odmowy, ograniczającą 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
```

```
FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = * SRCADDR = %
* DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * 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 = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT %
= * FRAGMENTS = NONE JRN = OFF
```

```
FILTER SET reguly_uslug ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR %
= 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT %
= 23 FRAGMENTS = NONE JRN = OFF
```

- f. Otwórz menu **Insert** i wybierz opcję **Filter Interface**. Przy użyciu interfejsu filtra utwórz identyfikator filtra i dołącz zdefiniowane zestawy filtrów.

- 1) W zakładce **Ogólne** wpisz

```
dozwolone_uslugi
```

jako identyfikator filtra PPP.

- 2) W zakładce **Filter sets** wybierz **reguly_uslug** i kliknij **Add**.

- 3) Kliknij OK. Do pliku reguł zostanie dodany następujący wiersz:

```
###Następujące instrukcje przypisują (wiążą) zestaw filtrów "reguly_uslug" z
identyfikatorem filtra PPP "dozwolone_uslugi".
```

Identyfikator filtra może zostać zastosowany na fizycznym interfejsie powiązany z profilem połączenia PPP lub strategią dostępu do grup.

```
FILTER_INTERFACE PPP_FILTER_ID = dozwolone_uslugi SET = reguly_uslug
```

- g. Składaj zmiany i wyjdź. Jeśli zaistnieje potrzeba cofnięcia tych zmian, w interfejsie znakowym wprowadź komendę:

```
RMVTCPTBL
```

Usuń ją z serwera wszystkie reguły filtrowania i NAT.

- h. W oknie dialogowym **Advanced TCP/IP settings** zostaw puste okno **PPP filter identifier** i kliknij **OK**, aby wyjść. Następnie zastosuj utworzony identyfikator filtra do strategii dostępu do grupy, nie do profilu połączenia.
2. Zdefiniuj nową strategię dostępu do grupy dla tej grupy użytkowników. Dokładniejszy opis opcji strategii dostępu do grup zawiera sekcja Konfigurowanie strategii dostępu do grupy.
 - a. W programie iSeries Navigator rozwiń **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 filtra PPP **dozwolone_usługi**.
 - 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 **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.

Więcej informacji o uwierzytelnianiu użytkowników przez połączenie PPP zawiera sekcja Uwierzytelnianie systemu.

Rozdział 4. 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. Więcej informacji zawierają następujące sekcje.

Co to jest protokół PPP

Protokół Point-to-Point Protocol (PPP) jest to protokół TCP/IP używany do połączenia dwóch systemów komputerowych. Sekcja zawiera dokładniejszą definicję tego protokołu.

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 dodzwania (rozpoczynania) lub nasłuchiwania (odbioru) połączeń PPP.

Strategie dostępu do grup

Strategie te definiują zestawy atrybutów połączenia i ochrony dla grupy użytkowników. W sekcji tej przedstawione są informacje dotyczące definiowania ich w systemie.

Co to jest protokół PPP

Komputery wykorzystują protokół **PPP**, lub inaczej **protokół typu punkt z punktem (Point-to-Point)**, do łączenia się z Internetem przy pomocy linii telefonicznych. 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 pomiędzy 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 na temat tych standardów można znaleźć na stronie <http://www.rfc-editor.org>.

- RFC1661 Protokół Point-to-Point
- RFC1662 Protokół PPP on HDLC-like framing
- RFC1994 Protokół PPP CHAP

Profile połączeń

Wersja V5R2 korzysta z dwóch rodzajów 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 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 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 pomiędzy 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 **wybijanie**, czy **odpowiadanie** (odpowiednio: nadawca lub 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. Więcej informacji można znaleźć w poniższych tabelach.

Więcej informacji o profilu połączenia odbiorcy można znaleźć w tabeli.

Tabela 1. Tryby pracy dostępne dla profilu połączenia odbiorcy

Typ połączenia	Dostępne tryby pracy
Linia komutowana	<ul style="list-style-type: none"> – Połączenie – Połączenie zamawiane (tylko inicjowanie) – Połączenie zamawiane (możliwa odpowiedź dedykowanych węzłów sieci) – Połączenie zamawiane (zdalne węzły włączone)
Linia dzierżawiona	Inicjator
L2TP	<ul style="list-style-type: none"> – Inicjator – Inicjator wieloprzeskokowy – Zdalne inicjowanie
Protokół PPP przez sieć Ethernet	Inicjator

Więcej informacji o profilu połączenia nadawcy można znaleźć w tabeli:

Tabela 2. Tryby pracy dostępne dla profilu połączenia nadawcy.

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:

- linię pojedynczą,
- pulę linii,
- zintegrowaną linię ISDN.

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

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. Chodzi tu o to, że 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.

Przykład można znaleźć w sekcji Scenariusz: zarządzanie dostępem użytkowników do zasobów za pomocą strategii dostępu do grup i filtrowania adresów IP.

Rozdział 5. Planowanie protokołu PPP

Tworzenie i administrowanie połączeniami PPP wymaga znajomości zarówno obsługi protokołu PPP, jak i alternatywnych połączeń serwera iSeries, a także wielu wykorzystywanych w przedsiębiorstwie planów sieci i ochrony. Zadaniem poniższych sekcji jest przybliżenie użytkownikom dostępnych opcji i wymagań połączeń PPP serwera iSeries.

Wymagania sprzętowe i programowe

Połączenia PPP obsługuje program Operations Navigator w wersji V4R4 lub nowszej. Sekcja zawiera szczegółową listę wymagań.

Połączenia alternatywne

Serwer iSeries obsługuje połączenia PPP przez różne nośniki, od analogowych lub cyfrowych linii telefonicznych, do dedykowanych lub częściowych linii T1. Sekcja zawiera opis obsługiwanych opcji połączeń.

Urządzenia łączące

Serwer iSeries do obsługi połączeń PPP korzysta z modemów, adapterów terminali ISDN, adapterów Token Ring, adapterów Ethernet lub urządzeń CSU/DSU. Sekcja zawiera informacje o obsługiwanych sprzęcie.

Obsługa adresów IP

Połączenia PPP mają kilka opcji służących do przypisania adresu IP i do filtrowania pakietów IP w trakcie połączenia. Opis tych opcji znajduje się w sekcji.

Uwierzytelnianie systemu

Serwer iSeries może uwierzytelniać połączenia modemowe za pomocą listy weryfikacji lub wymiany haseł serwera RADIUS. Dostarcza także informacji o uwierzytelnianiu systemom, z którymi jest połączony. W sekcji zawarty jest opis opcji uwierzytelniania.

Uwagi na temat przepustowości

Serwer iSeries obsługuje protokół multilink do połączeń PPP. Dzięki temu można korzystać z wielu analogowych linii telefonicznych w pojedynczym połączeniu, zwiększając w ten sposób pasmo. Sekcja zawiera opis tych czynności.

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, muszą być spełnione poniższe wstępne wymagania.

- **Program iSeries Navigator** wydanie 4 wersja 4 (V4R4) lub nowsza z obsługą protokołu 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 (95/98/NT/Millennium/2000/XP)** i programem iSeries Navigator.
- Zainstalowany adapter

Istnieje możliwość wyboru jednego z poniższych adapterów:

 - 2699*: Adapter 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)
 - 2750: Adapter I/O PCI ISDN V.90 Basic Rate Interface U (interfejs dwuprzewodowy)
 - 2751: Adapter I/O PCI ISDN V.90 Basic Rate Interface U (interfejs czteroprzewodowy)
 - 2761: Adapter I/O dla ośmioportowego modemu analogowego

- 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
- 2838: 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 RS232 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.

Połączenia alternatywne

Protokół PPP może przysyłać datagramy poprzez szeregowe łącza typu punkt z punktem. Protokół ten umożliwia współdzielenie sprzętu pochodzącego od różnych dostawców oraz wielu protokołów poprzez ujednoczenie komunikacji typu punkt z punktem. Warstwa łącza danych PPP wykorzystuje HDLC-like framing do obudowania datagramów przesyłanych zarówno przez synchroniczne, jak i asynchroniczne łącza telekomunikacyjne PPP.

Protokół PPP obsługuje wiele typów linii, natomiast protokół SLIP 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 pomiędzy klientem a centralą.

Przy pomocy protokołu PPP można ustanowić fizyczne połączenie pomiędzy lokalnym i 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,
- cyfrowe usługi i DDS,
- linia Switched-56,
- linia ISDN,
- linie T1/E1 i częściowa linia T1,
- frame relay,
- obsługa protokołu L2TP (tunelowanie) dla połączeń PPP,
- obsługa PPPoE (DSL) dla połączeń PPP.

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 pomiędzy 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 (bps) zwiększana jest najczęściej 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 RS232 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 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 10 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.

Linia Switched-56

Kiedy nie musimy korzystać z łącza stałego, możemy zmniejszyć koszty używając cyfrowej usługi komutowanej, która ogólnie nazywana jest 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.

ISDN

Podobnie jak usługa Switched-56, 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 6 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 RS232 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 pomiędzy 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 zwykle 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 RS232 i protokołu asynchronicznego z szybkością dochodzącą do 230,4 kb/s. Jednak maksymalna szybkość transmisji serwera dla połączenia asynchronicznego przez interfejs RS232 wynosi 115,2 kb/s. Ogranicza to niestety maksymalną szybkość do 11,5kb/s, podczas gdy adapter terminalu z połączeniem wielokrotnym jest zdolny do nieskompresowanego przesyłania rzędu 14/16k. Niektóre adaptery terminali obsługują połączenia synchroniczne przez RS232 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 RS232 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.

Linie T1/E1 i linia częściowa T1

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 przepustowości 2,048 Mb/s. Multipleksowanie czasowe TDM pozwala wielu użytkownikom na współużytkowanie cyfrowego nośnika przesyłania dzięki wykorzystaniu przydzielanych wcześniej odstępów czasowych. Wiele central cyfrowych 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 działała 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 pomiędzy 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 adresowym (identyfikator połączeniowy łącza) w ramce i umożliwiającym zarządzanie trasą lub połączeniem wirtualnym.

Sieci Frame relay na terenie Stanów Zjednoczonych przesyłają dane z szybkościami T-1 (1.544 Mb/s) i T-3 (45 Mb/s). Są sposobem na wykorzystanie istniejących już linii T-1 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 ATM.)

Obsługa połączeń PPP przez protokół L2TP (tunelowanie)

Protokół L2TP jest protokołem tunelowym rozszerzającym protokół PPP o obsługę w warstwie łącza tuneli tworzonych pomiędzy zgłaszającym klientem L2TP (koncentrator dostępu L2TP lub LAC) a serwerem końcowym L2TP (Serwer sieciowy L2TP lub LNS). Wykorzystanie tuneli L2TP pozwala oddzielić miejsce, w którym kończy się protokół połączenia telefonicznego, a zaczyna się dostęp do sieci. Dlatego też protokół L2TP nazywany jest również Wirtualnym połączeniem PPP. Protokół L2TP jest opisany jako standard RFC2661. Więcej informacji o RFC można znaleźć pod adresem <http://www.rfc-editor.org>. Tunel może obejmować całą sesję PPP lub tylko jeden segment sesji dwusegmentowej. Można wyróżnić cztery modele tunelowania:

- Tunel dobrowolny
- Tunel wymuszony - połączenia przychodzące
- Tunel wymuszony - połączenia zdalne
- Połączenie wieloprzeskokowe L2TP

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 (Internet Service Provider), 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 - połączenia 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 pomiędzy dostawcą ISP a serwerem LNS.

Tunel wymuszony - połączenia 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 pomiędzy serwerem LNS a dostawcą ISP.

Połączenie wieloprzeskokowe 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. Tunel jest ustanawiany pomiędzy klientem LAC a bramą wieloprzeskokową L2TP oraz pomiędzy bramą a docelowym serwerem LNS. 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 pomiędzy klientem a dostawcą ISP. Umożliwia ona symultaniczne przekazywanie głosu i szybkie przesyłanie danych przez pojedynczą parę miedzianego okablowania telefonicznego. Szybkości osiągnięte przez modemy zostały stopniowo zwiększone dzięki użyciu kompresji i innych technik, jednak najszybsze obecnie modemy (56 kbit/s) osiągnęły teoretyczny limit

dla tej technologii. Technologia DSL umożliwiła zwiększenie szybkości na liniach typu skrętka, od głównego biura do domu, szkoły czy przedsiębiorstwa. Osiągane szybkości rzędu 2 megabitów na sekundę są ponad 30-krotnie większe niż w dzisiejszych najszybszych modemach. 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). Technologia DSL jest uważana za następną generację technologii modemowej. Wprawdzie modemy DSL przypominają modemy konwencjonalne, ale znacznie zwiększają przepustowość.

Urządzenia łączące

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

- modemy,
- urządzenia CSU/DSU,
- adaptory terminali ISDN,
- adaptory Ethernet 2838 (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 przy pomocy 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, jako modem ECS mogą zostać użyte wewnętrzne modemy 2771 lub 2772.

Urządzenia 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.

Adaptory terminali ISDN

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

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

- aby określić najlepszy rodzaj adaptera terminalu, należy zapoznać się z zaleceniami wyboru adaptera terminalu ISDN,
- informacje na temat różnych adapterów terminali ISDN przetestowanych z serwerem iSeries oraz ich oceny można znaleźć pod hasłem Ograniczenia adaptera terminalu ISDN.

W celu skonfigurowania adaptera terminalu wykonaj następujące kroki:

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. 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.

Przykładowe procedury z użyciem programu Operations Navigator opisano pod hasłem Konfigurowanie adaptera terminalu ISDN.

Zalecane adaptery terminali ISDN

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 systemem AS/400. 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 system 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. Wciąż zalecana jest wersja RS-232, mimo że mniejsza ona wydajność serwera iSeries z powodu ograniczenia połączenia do 115.2 Kb.

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 i zalecane są 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 115200 b/s.
- Adapter terminalu nie obsługuje automatycznie protokołu CHAP. Jednakże ustawienie S84=0 umożliwi 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 115200 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, co umożliwia zarządzanie adresami IP dla połączenia PPP bez powiązania z istniejącą architekturą sieci. Informacje dotyczące definiowania schematu adresów IP dla sieci można znaleźć w następujących artykułach:

- DHCP
Protokół DHCP umożliwia centralne zarządzanie przypisywaniem adresów IP w sieci. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami DHCP w sieci.
- DNS
System DNS pomaga w zarządzaniu nazwami hostów i przypisanymi im adresami IP. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami DNS w sieci.
- BOOTP
Protokół BOOTP służy do powiązania klienckich stacji roboczych z serwerem iSeries i przypisania im adresów IP. Artykuł zawiera informacje o tym, w jaki sposób konfigurować i zarządzać usługami BOOTP w sieci.
- Filtrowanie pakietów IP
Ograniczanie dostępu do określonych adresów IP użytkownikom i grupom dzięki utworzeniu pliku reguł filtrowania IP. Artykuł zawiera informacje na temat obsługi filtrowania IP i implementacji tej opcji w sieci.

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 wcześniej zdefiniowane. Zazwyczaj definiuje się adres lokalny jako stały adres IP, a adres zdalny jako przypisany do systemu zdalnego. System, z którym się łączymy, można zdefiniować w ten sam sposób. Gdy dwa systemy zostaną połączone, będą one wymieniać pomiędzy 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 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. Występują również dodatkowe elementy związane z routingiem dotyczące zarówno systemów znajdujących się w sieci LAN (aby upewnić się, że cały ruch internetowy jest przesyłany do serwera iSeries), jak również serwera iSeries, na którym należy włączyć opcję "dodaj system zdalny jako domyślną trasę".

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. Adres ten 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 virtualny 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 z zakresu systemów przyłączonych do sieci LAN i upewnić się, że zarówno dla profilu połączenia, jak i systemu iSeries zostało włączone przekazywanie IP.

Tabela 3. Opcje przypisania adresu IP dla profilu połączenia odbiorcy

Opcja	Opis
Staly 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 ze zdefiniowanego wcześniej zakresu. Adres ten jest adresem hosta (maska podsieci to 255.255.255.255) dostępnym jedynie dla profili odbiorcy połączeń wielokrotnych.

Tabela 3. Opcje przypisania adresu IP dla profilu połączenia odbiorcy (kontynuacja)

Opcja	Opis
RADIUS	Zdalny adres IP i związana z nim maska podsieci określane są przez serwer RADIUS. Jest to możliwe, gdy: <ul style="list-style-type: none"> 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 przebieżnik DHCP. Jest to możliwe jedynie wtedy, gdy obsługa DHCP jest włączona z poziomu konfiguracji usług Remote Access Server. 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 modemu różnych adresów IP (i skojarzonych z nimi masek podsieci). Umożliwia to również zdefiniowanie dodatkowych tras związanych z poszczególnymi identyfikatorami użytkowników. Dzięki temu można dostosować środowisko do konkretnego, zdalnego użytkownika. Aby funkcja ta działała prawidłowo, należy włączyć uwierzytelnianie.
Definiowanie dodatkowych adresów IP bazujących na identyfikatorze użytkownika zdalnego systemu	Opcja ta pozwala na zdefiniowanie adresów 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 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 ten, 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.
IP address routing	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.

Filtrowanie pakietów IP

Filtrowanie pakietów IP jest mechanizmem ograniczającym usługi dostępne dla indywidualnego użytkownika po zalogowaniu do sieci. Dzięki filtrowaniu pakietów można "Umożliwić" lub "Zabronić" dostępu na podstawie docelowego adresu IP lub portu. 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. Więcej informacji zawiera artykuł Reguły pakietów IP w Centrum informacyjnym.

Przy połączeniach L2TP do zabezpieczenia ruchu w sieci należy użyć sieci VPN z filtrowaniem IP SEC. Więcej informacji zawiera artykuł VPN w Centrum informacyjnym.

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. Ma także kilka opcji do szyfrowania informacji o identyfikatorze użytkownika i hasle, 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.

Więcej wiadomości o informacjach sprawdzających i uwierzytelniających zawierają sekcje:

- Usługa Remote Authentication Dial In User Service (RADIUS)
- Lista weryfikacji

Więcej informacji o obsługiwanych protokołach uwierzytelniania haseł zawierają sekcje:

- Protokół CHAP-MD5
- Protokół PAP
- Protokół EAP

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 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.

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 RAS za pomocą urządzeń zabezpieczających wyprodukowanych przez firmy zewnętrzne. Protokół ten chroni również bezpieczne sieci VPN przed atakami hakerów, którzy przy pomocy słowników próbują odgadnąć hasła. Zwiększa on funkcjonalność 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 obsługuje protokół EAP jedynie w wersji, która działa podobnie jak protokół CHAP-MD5. Istnieje jednak możliwość wykorzystania zdalnego uwierzytelniania przy pomocy serwera RADIUS, który obsługuje niektóre z dodatkowych schematów uwierzytelniających opisanych powyżej.

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.

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. Mogą to być pliki z hasłami systemu UNIX, protokół Kerberos, systemy zabezpieczające dostępne w sprzedaży lub nawet systemy projektowane na zamówienie. 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. Przykład konfiguracji serwera RADIUS znajduje się w Scenariuszu: uwierzytelnianie połączeń modemowych za pomocą serwera RADIUS.

Lista weryfikacji

Lista weryfikacji używana jest do przechowywania nazw i haseł zdalnych użytkowników. Istnieje możliwość wykorzystania istniejącej listy lub utworzenia nowej przy pomocy strony uwierzytelniania profilu połączenia odbiorcy. Pozycje na liście weryfikacji wymagają określenia typu protokołu uwierzytelniania skojarzonego z hasłem i identyfikatorem użytkownika. Może to być protokół **zaszyfrowany - CHAP-MD5/EAP** lub **niezaszyfrowany - PAP**.

Więcej informacji na ten temat znajduje się w pomocy online.

Uwagi dotyczące przepustowości - 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 pomiędzy 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 pod adresem <http://www.rfc-editor.org>.

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).

Rozdział 6. Konfigurowanie protokołu PPP

Przed przystąpieniem do konfigurowania połączenia PPP, należy skonfigurować środowisko dla tego protokołu. Informacje o konfigurowaniu środowiska PPP można znaleźć w następujących sekcjach:

- Tworzenie profilu połączenia
- Konfigurowanie modemu
- Konfigurowanie zdalnego komputera PC
- Konfigurowanie zdalnego połączenia z Internetem poprzez AT&T Global Network
- Kreatory połączeń
- Konfigurowanie strategii dostępu do grupy
- Przypisywanie reguł filtrowania pakietów IP do połączeń PPP
- Udostępnianie usług RADIUS oraz DHCP profilom odbierającym połączenie PPP

Tworzenie profilu połączenia

Pierwszym krokiem podczas konfigurowania połączenia PPP pomiędzy 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 **OK**.

Pojawi się strona **Właściwości nowego profilu punkt z punktem**, na której możesz ustawić pozostałe wartości specyficzne dla sieci. Informacje na ten temat można znaleźć w pomocy elektronicznej.

Typ protokołu: PPP lub 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 pomiędzy 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 iServer obsługuje go. Jednakże firma IBM zaleca 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 wykorzystuje się:

- modem (wewnętrzny lub zewnętrzny),
- wewnętrzny adapter ISDN,
- 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. W tym trybie możliwe jest także inicjowanie 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 pomiędzy 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 pomiędzy 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 pomiędzy 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.

Protokół L2TP (linia wirtualna)

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

Po ustanowieniu tunelu L2TP, pomiędzy 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**

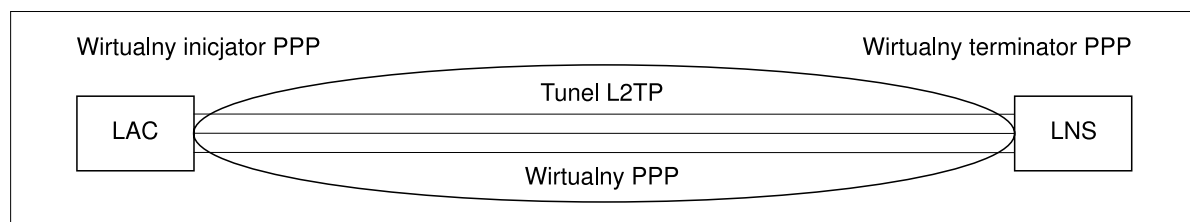
Wybór tego trybu umożliwia serwerowi iSeries ustanowienie połączenia wieloprzeskokowego.

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.

Protokół L2TP (Layer 2 Tunneling Protocol): Protokół L2TP jest protokołem rozszerzającym protokół PPP o obsługę tunelu warstwy połączenia pomiędzy zgłaszającym klientem L2TP a serwerem końcowym L2TP. Wykorzystanie tuneli L2TP pozwala oddzielić miejsce, w którym kończy się protokół połączenia telefonicznego, a zaczyna się dostęp do sieci.

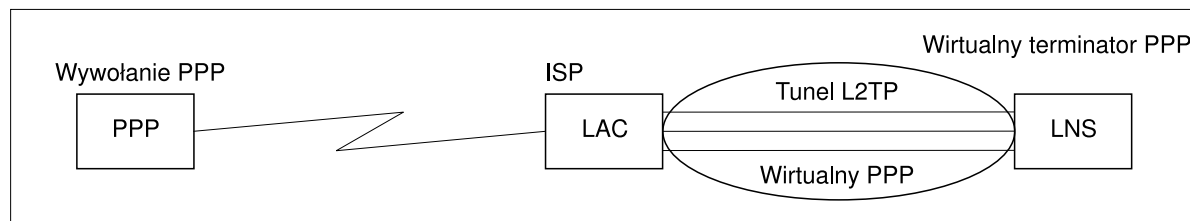
Dostawca usług internetowych korzysta z trybu linii wirtualnej do obsługi sieci VPN (Virtual Private Networks). Aby lepiej zrozumieć współdziałanie sieci VPN z protokołem L2TP, należy zapoznać się z dokumentem Konfigurowanie połączenia L2TP chronionego przez sieć VPN.

Poniżej pokazane są trzy różne implementacje tunelowania protokołu L2TP:



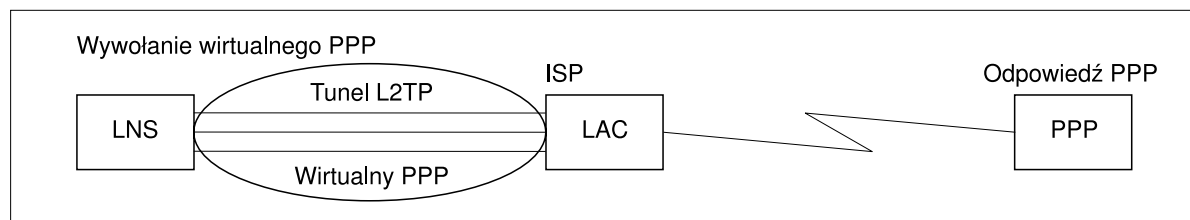
RBAEE563-0

Rysunek 7. Wirtualny inicjator PPP lub wirtualny terminator PPP



RBAEE561-0

Rysunek 8. Wybierający inicjator PPP lub wirtualny terminator PPP



RBAEE562-0

Rysunek 9. Wywołanie wirtualnego PPP lub odpowiedź wirtualnego PPP

Linia PPPoE

Połączenia PPPoE korzystają z linii wirtualnej do wysyłania danych PPP przez adapter Ethernet 2838 do modemu DSL, dostarczonego przez dostawcę ISP, który jest jednocześnie podłączony do sieci LAN. Dzięki temu użytkownicy sieci LAN mają szybki dostęp do Internetu przez sesje PPP poprzez serwer iSeries. Po nawiązaniu połączenia pomiędzy 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.

- Pojedyncza linia
- Pula linii
- Zintegrowana linia ISDN

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 wybranego, 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". Zostanie następnie 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 '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 pulę 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 obsługiwać.
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.
Tak więc, 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.

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 do obsługi czteroportowego zintegrowanego modemu 2805, który udostępnia cztery linie z jednego adaptera, a także w przypadku adapterów 2750 lub 2751 obsługujących osiem osobnych połączeń ISDN w kanale B.

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 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 nie chcemy, 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 innej sieci dołączonych do serwera iSeries.

W celu utworzenia wirtualnego adresu IP, wykonaj poniższe czynności:

1. W programie iSeries Navigator wybierz odpowiedni system, a następnie **Sieć** → **Konfiguracja TCP/IP** > **IPv4** > **Interfejsy**.
2. Kliknij prawym przyciskiem myszy **Interfejsy** i wybierz **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 po utworzeniu interfejsu, należy wybrać opcję uruchomienia adresu 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 puli 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, rodzimego protokołu ISDN 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 ten jest już używany, systemowi przypisywany jest następny adres z zakresu Liczba adresów. Zakładając na przykład, że początkowy adres IP to 10.1.1.1, a Liczba adresów wynosi 5, adresy w puli zdalnych adresów IP to 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 jednak wszystkie adresy w puli są używane, każde żądanie kolejnego połączenia będzie odrzucane, dopóki inne połączenie się nie zakończy i nie zwolni adresu.

- Aby przydzielić określone adresy niektórym zdalnym systemom, a innym systemom pozwolić na 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.

ISDN

Wybierz ten typ obsługi linii, aby zdefiniować linię PPP powiązaną z połączeniem sieciowym ISDN.

Zalety korzystania z ISDN:

- ISDN umożliwia lepszą komunikację przy większych szybkościach.
- ISDN dąży do zapewnienia uniwersalnego środka łączności za pomocą pojedynczego interfejsu i szybkich sieci cyfrowych do transmisji danych wszystkich typów.
- ISDN ma możliwość szybkiego zestawiania połączeń komutowanych. Zestawienie połączenia za pomocą modemu analogowego może zająć do 30 sekund lub więcej, podczas gdy zestawienie połączenia przez ISDN zajmuje tylko kilka sekund.

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.

Aby skonfigurować modem, należy wykonać następujące czynności:

- skonfigurować nowy modem,
- przypisać modem do opisu linii,
- ustawić łańcuchy komend modemu.

Konfigurowanie nowego modemu

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieci** → **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.

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

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieci** → **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 **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 musisz utworzyć opis modemu i dodać go do listy modemów.

Aby utworzyć opis modemu, wykonaj następujące kroki:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieci** → **Usługi zdalnego dostępu**.
2. Wybierz **Modemy**.
3. Na liście modemów kliknij prawym przyciskiem myszy **generic hayes** i wybierz **Nowy modem na podstawie**.
4. W oknie dialogowym **Nowy modem** zmień łańcuchy komend, aby dopasować dane do wymagań modemu.

Ustawianie łańcuchów komend modemu

Poniższa tabela zawiera minimalny zestaw komend używanych przez modemy zdefiniowane na serwerze iSeries. W podręczniku użytkownika modemu można znaleźć równoważne łańcuchy komend. W opisie modemu należy użyć ustawień zalecanych przez producenta.

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 dzwonekach	S0= n gdzie $n = 1$ lub 2
Rozłącz przy braku sygnału nośnego (połączenia) po m sekundach	S7= m
Tryb wybierania numeru	ATDT dla wybierania tonowego lub ATDP dla wybierania impulsowego

Przykład: konfigurowanie adaptera terminalu ISDN

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieci** → **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.

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 być dowolną cyfrą 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.

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 dialogowe Właściwości nowej linii.
4. W oknie dialogowym 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.

W wersji V5R2 można tak skonfigurować profil połączenia nadawcy, aby ten "pożyczył" 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 dialogowego konfiguracji linii PPP. Linie PPP można konfigurować z zakładki Połączenie profilu połączenia nadawcy lub profilu połączenia odbiorcy.

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 konfiguracji Dial-up Networking można znaleźć w dokumentacji firmy Microsoft dla systemu 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, dlatego należy go dodatkowo skonfigurować.
- W przypadku haseł niezaszyfrowanych (lub niezabezpieczonych) automatycznie używany jest protokół 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

Firma IBM umożliwia dostęp do Internetu poprzez swoją sieć AT&T Global Network. W celu skorzystania z tej usługi można użyć kreatora AT&T Global Network Dial Connection, który pomoże skonfigurować profil połączenia wybierającego PPP. 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 AT&T Global Network wymagają takiej samej obsługi, jak wszystkie inne profile połączeń PPP.

Aby użyć kreatora 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)
- 2761: Adapter I/O dla ośmioportowego modemu analogowego
- 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 kreator 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 AT&T Global Network account (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 kreator AT&T Global Network Dial Connection, wykonaj poniższe kroki:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć** → **Usługi zdalnego dostępu**.
2. Kliknij prawym przyciskiem myszy **Profile połączenia nadawcy** i wybierz **Nowe połączenie telefoniczne z siecią AT&T Global Network**.
3. Po uruchomieniu kreatora połączenia telefonicznego z AT&T Global Network kliknij **Pomoc** w celu uzyskania informacji niezbędnych do wypełnienia panelu.

Kreatory połączeń

Kreator nowego połączenia telefonicznego

Kreator pomagający krok po kroku skonfigurować profil połączenia modemowego z dostawcą ISP (Internet Service Provider) lub intranetem. Aby podać wszystkie dane wymagane przez kreatora, potrzebne są informacje od administratora sieci lub dostawcy ISP (Internet Service Provider). Więcej informacji na ten temat można znaleźć w pomocy elektronicznej.

Kreator połączenia uniwersalnego

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

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 Operations Navigator wybierz odpowiedni serwer i rozwiń gałąź **Sieć** → **Usługi zdalnego dostępu** → **Profile połączenia odbiorcy**.
2. Kliknij prawym przyciskiem myszy **Strategie dostępu do grupy** i wybierz **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 16 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 łączy.
5. Kliknij zakładkę **Ustawienia TCP/IP**, aby:
- Umożliwić zdalnym systemom dostęp do innych sieci (przekazywanie IP)
Ta opcja określa, czy przekazywanie IP jest pożądane. Jeśli zostanie ona wybrana, serwer iSeries będzie pracował jako router dla danego połączenia. Dzięki temu datagramy IP nie przeznaczone dla serwera iSeries będą przekazywane dalej. W przypadku niewybrania tej opcji datagramy IP pochodzące ze zdalnego systemu i nie przeznaczone dla żadnego lokalnego adresu serwera iSeries zostaną usunięte.
Ze względów bezpieczeństwa można wyłączyć przekazywanie IP. Dostawcy ISP (Internet Service Provider) zazwyczaj udostępniają przekazywanie IP. Należy zauważyć, że opcja ta jest brana pod uwagę, tylko jeśli uaktywnione jest przekazywanie datagramów IP dla całego systemu. W przeciwnym razie jest ona ignorowana, nawet jeśli zostanie wybrana. Ustawienie przekazywania datagramów IP dla całego systemu można sprawdzić w zakładce Ustawienia na stronie Właściwości TCP/IP.
 - Zażądać kompresji VJ nagłówka TCP/IP
Opcja ta określa, czy informacje znajdujące się w nagłówku mają być kompresowane przez protokół IP po nawiązaniu połączenia. Kompresja zazwyczaj zwiększa wydajność w przypadku interaktywnego ruchu w sieci lub wolnych linii szeregowych. 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 system po drugiej stronie nie obsługuje kompresji VJ, serwer iSeries nawiązuje połączenie, które nie wykorzystuje kompresji.
 - Użyć reguł dla pakietów IP w danym połączeniu
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.
Więcej informacji o regułach dla pakietów IP można znaleźć w Centrum informacyjnym w dokumencie Filtrowanie pakietów IP i translacja NAT.

Przykład można znaleźć w sekcji Zarządzanie dostępem użytkowników do zasobów za pomocą strategii dostępu do grupy i filtrowania IP.

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:

1. Kliknij **Uwierzytelnianie**.
2. Sprawdź **Wymagane przez serwer iSeries do weryfikacji tożsamości systemu zdalnego**.
3. Wybierz **Uwierzytelnianie lokalne za pomocą listy weryfikacji**.
4. Jeśli lista weryfikacji już istnieje, wybierz ją z rozwijanej listy i kliknij **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:
 - Wybierz protokół uwierzytelniania zdefiniowany dla nazwy użytkownika.
 - Wpisz nazwę użytkownika i hasło.

Uwaga: Ze względów bezpieczeństwa zaleca się nieużywanie tego samego hasła co w przypadku protokołu CHAP (Challenge Handshake Authentication Protocol22314), EAP (Extensible Authentication Protocol) oraz PAP (Password Authentication Protocol).

- Zaznacz **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. Kliknij **OK**, aby zakończyć konfigurację i powrócić do strony Właściwości PPP.

Przypisywanie reguł filtrowania pakietów IP do połączeń PPP

Sekcja Filtrowanie pakietów IP i reguły NAT w Centrum informacyjnym omawia sposób tworzenia reguł pakietów IP, które można zastosować do profili połączeń PPP. Dzięki zbiorowi reguł pakietów można ograniczyć dostęp grupy użytkowników do adresów IP w sieci. Przykład użycia reguł filtrowania w połączeniu PPP znajduje się w sekcji Scenariusz: zarządzanie dostępem użytkowników zdalnych do zasobów za pomocą strategii dostępu do grup i filtrowania IP.

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 **Dla tego połączenia użyj reguł pakietów IP** i wybierz z rozwijanej 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 **Dla tego połączenia użyj reguł pakietów IP** i wybierz z rozwijanej listy identyfikator filtru PPP.
 4. Kliknij **OK**, aby zatwierdzić filtr PPP.

Udostępnianie usług RADIUS i DHCP profilom połączeń

Aby udostępnić usługi RADIUS i DHCP profilom odbiorcy połączeń PPP:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieci** → **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 services, wybierz zakładkę **RADIUS**.
 - a. Zaznacz **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 OK, aby powrócić do programu iSeries Navigator.

Przykład konfiguracji serwera RADIUS znajduje się w Scenariuszu: uwierzytelnianie połączeń modemowych za pomocą serwera RADIUS.

Rozdział 7. Zarządzanie PPP

Zarządzanie połączeniami na serwerze iSeries obejmuje:

- Ustawianie właściwości dla profili połączeń
- Monitorowanie aktywności połączeń PPP

Ustawianie właściwości dla profili połączeń PPP

Podczas tworzenia profilu połączenia w oknie dialogowym Konfigurowanie profilu połączenia PPP, należy wybrać protokół, typ połączenia oraz tryb pracy nowego profilu połączenia. Po wprowadzeniu tych informacji pojawi się 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 dialogowym **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 pojawiające się w oknie dialogowym. Więcej informacji zawierają procedury i przykłady połączeń PPP.

Monitorowanie aktywności połączeń PPP

Poniżej wyjaśniono, jak korzystając z programu iSeries Navigator uzyskać podgląd profilu połączenia i protokołu sesji.

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.
- Zadania połączeń PPP są uruchamiane w profilu QTCP i wykorzystywane do obsługi indywidualnych połączeń PPP. Zadania te są domyślnie uruchamiane w podsystemie QUSRWRK, ale można je skonfigurować tak, aby uruchamiały się gdzie indziej. Istnieją dwie nazwy zadań połączeń PPP:
 - QTPPPSSN - Zadanie obsługujące wszystkie połączenia PPP nie wykorzystujące protokołu L2TP.
 - QTPPPL2SSN - Zadanie obsługujące dane wirtualne PPP po pomyślnym zakończeniu negocjacji połączenia L2TP przez zadanie QTPPPL2TP.
- 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. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Siec** → **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:
 - **Zadania** otwiera protokół zadania dla zadań QTPPxxx.

- **Połączenia** otwiera okno dialogowe z informacjami o wszystkich połączeniach przypisanych do tego profilu. W informacjach tych zawarte są dane o połączeniu bieżącym oraz połączeniach poprzednich. Dodatkowo można przejrzeć dane wyjściowe zadania zawierające szczegółowe informacje o każdym połączeniu.
- **Właściwości** otwiera stronę Właściwości w celu wyświetlenia bieżących właściwości połączenia.

Przeglądanie informacji o połączeniu:

1. W programie iSeries Navigator wybierz odpowiedni system i rozwiń gałąź **Sieć** → **Usługi zdalnego dostępu**. Wybierz **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, lokalny i zdalny adres IP oraz nazwa zadania PPP pojawiają się w zależności od statusu zadania PPP.
3. Aby przejrzeć dane wyjściowe zadania lub informacje szczegółowe o połączeniu, kliknij prawym przyciskiem myszy połączenie w celu uaktywnienia odpowiednich przycisków.
4. Aby przejrzeć dane wyjściowe zadania, kliknij **Zadania**. W protokole zadań kliknij prawym przyciskiem myszy nazwę zadania i wybierz **Wydruk**. Zostanie wyświetlona zawartość protokołu sesji połączenia oraz protokoły zadania (jeśli sesja została zakończona).
5. Aby przejrzeć informacje szczegółowe o połączeniu, kliknij **Szczegóły**. Informacje te mogą zostać wyświetlone tylko dla połączeń aktywnych. Pojawi się okno dialogowe z dodatkowymi informacjami o danym połączeniu.

Praca z danymi wyjściowymi PPP serwera iSeries:

Aby pracować z danymi wyjściowymi PPP, w wierszu komend serwera iSeries wpisz WRKTCPPPTP:

- 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. Skorzystaj z komendy WRKSPLF, aby przejrzeć 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 dialogowym Połączenia.

Podstawowy opis statusu	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
Terminator wieloprzeskokowy uruchamia inicjator wieloprzeskokowy	Trwa nawiązywanie połączenia wieloprzeskokowego
Połączenie wieloprzeskokowe jest aktywne	Połączenie wieloprzeskokowe zostało nawiązane pomyślnie

Dodatkowy opis statusu	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

Rozdział 8. Rozwiązywanie problemów związanych z protokołem PPP

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

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.

1. Wymagany materiał pomocniczy:

- typ zdalnego hosta, system operacyjny i poziom,
- poziom systemu operacyjnego hosta serwera iSeries,
- protokół zadania nieudanej sesji oraz plik dialogu połączenia,
W wersji V5R1 protokoły zadań oraz dane wyjściowe dialogu połączenia zapisywane są w kolejce OUTQ pod tą samą nazwą co profil.
- 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 WRKTCPTP.
- typ i model modemu,
- łańcuchy komend modemu,
- śledzenie komunikacji.

Dokumentacja techniczna ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)



wyczerpująco opisuje poniższe problemy związane z PPP oraz udostępnia szczegółowe informacje na temat rozwiązywania problemów.


Problem	Rozwiązanie
Konfiguracja sprzętowa modemu Błędna konfiguracja zworek i innych ustawień sprzętowych.	Upewnij się, czy modem został skonfigurowany dla odpowiedniego typu ramek. Dopuszczalne ustawienia to <i>Asynchroniczne</i> lub <i>Synchroniczne</i> . 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 pojawiają się błędy związane z nazwą użytkownika i hasłem.	<ul style="list-style-type: none"> • 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 węzle, jeśli na drugim węzle 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.

Problem	Rozwiązanie
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.

Rozdział 9. Inne informacje o protokole PPP

Inne źródła informacji o protokole PPP:

- Najnowsze poprawki PTF (program temporary fix) i najnowsze informacje o konfiguracji protokołów PPP i

L2TP dostępne są poprzez odsyłacz PPP na stronie głównej serwera iSeries TCP/IP  . Odsyłacz ten dostarcza najnowszych informacji, uzupełniając i zastępując te, które zawarte są w sekcji **Usługi zdalnego dostępu: połączenia PPP**.

- Dokumentacja techniczna ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)



wyczerpująco opisuje zagadnienia usług i aplikacji TCP/IP.



IBM Confidential