



iSeries

Služby RAS (Remote Access Services): PPP

IBM Confidential





@server

iSeries

Služby RAS (Remote Access Services): PPP

IBM Confidential

Obsah

Část 1. Služby RAS (Remote Access Services): PPP.	1
Kapitola 1. Co je nového ve V5R2	3
Kapitola 2. Tisk tohoto tématu	5
Kapitola 3. Scénáře PPP	7
Scénář: Připojení serveru ke koncentrátoru přístupu PPPoE	8
Scénář: Připojení vzdálených volajících klientů k serveru iSeries.	9
Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu	11
Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu	13
Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS	16
Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí metod skupin a filtrování IP	18
Kapitola 4. Koncepce protokolu PPP	21
Co je PPP?	21
Profily připojení	21
Podpora metod skupiny	23
Kapitola 5. Plánování PPP	25
Softwarové a hardwarové požadavky	25
Alternativy připojení.	26
Analogové telefonní linky.	26
Digitální služby a DDS.	27
Komutovaná linka 56	27
ISDN	28
T1/E1 a částečná T1	28
Přenos rámce	29
Podpora L2TP (tunel) pro připojení PPP	29
Nepovinný tunel	29
Model povinného tunelu - příchozí volání	30
Model povinného tunelu - vzdálené vytáčení	30
Připojení L2TP s více přechody	30
Podpora PPPoE (DSL) pro připojení PPP	30
Vybavení pro připojení.	30
Modemy	31
CSU/DSU	31
Adaptéry terminálu ISDN	31
Doporučení adaptéru terminálu ISDN	31
Omezení adaptérů terminálu ISDN	32
Jak pracovat s IP adresou	33
Filtrování IP paketů	35
Autentizace systému	35
CHAP-MD5.	35
EAP	36
PAP	36
Přehled služby RADIUS	36
Ověřovací seznam	37
Pokyny ohledně šířky pásma - vícenásobné připojení	37
Kapitola 6. Konfigurace PPP	39
Vytvoření profilu připojení	39
Typ protokolu: PPP nebo SLIP	40

Výběry režimu	40
Komutovaná linka	40
Pronajatá linka	41
L2TP (virtuální linka)	41
Protokol L2TP (Layer 2 Tunneling Protocol)	42
Linka PPPoE	42
Konfigurace linky	43
Jediná linka	43
Společná oblast linek	43
Podpora profilu více připojení	44
Společná oblast IP adres vzdáleného systému	45
ISDN	46
Konfigurace modemu pro PPP	46
Konfigurace nového modemu	46
Nastavení příkazového řetězce modemu	47
Příklad: Konfigurace adaptéru terminálu ISDN	47
Přiřazení modemu k popisu linky	48
Konfigurace vzdáleného PC	48
Konfigurace přístupu k Internetu přes AT&T Global Network	49
Průvodci připojením	50
Konfigurace metody přístupu skupiny	50
Použití pravidel filtrování IP na připojení PPP	52
Povolení serverů RADIUS a DHCP pro profily připojení	52
Kapitola 7. Správa PPP	53
Nastavení vlastností profilů připojení PPP	53
Monitorování aktivity PPP	53
Kapitola 8. Odstraňování problémů s PPP	57
Kapitola 9. Další informace o PPP	59

Část 1. Služby RAS (Remote Access Services): PPP

Protokol PPP (point-to-point) je internetový standard pro datové přenosy po sériových linkách. Mezi poskytovateli služeb sítě Internet (ISP) je to nejpoužívanější protokol. Protokol PPP umožňuje jednotlivým počítačům přistupovat k sítím, které poskytují přístup k Internetu. Server iSeries podporuje TCP/IP PPP jako součást své připojitelnosti k síti WAN (dálková síť).

Když připojíte vzdálený počítač ke svému serveru iSeries pomocí PPP, můžete si vyměňovat data mezi jednotlivými místy. Prostřednictvím PPP mohou vzdálené počítače, které jsou připojeny k serveru iSeries, přistupovat k prostředkům nebo jiným počítačům, jež patří do stejné sítě jako váš server. Svůj server iSeries můžete také konfigurovat tak, aby se připojoval k Internetu pomocí PPP. Průvodce vytáčeným připojením v produktu iSeries Navigator vás provede připojením serveru iSeries k Internetu nebo k interní síti.

- Kapitola Co je nového ve V5R2? popisuje služby RAS v tomto vydání.
- Kapitola Tisk tohoto tématu vám umožňuje stáhnout nebo tisknout tyto informace ve formátu PDF.

Vysvětlení služeb RAS: PPP

Tyto části vás rychle uvedou do služeb vzdáleného přístupu, které jsou na vašem serveru iSeries 400. Níže uvedené části vám pomohou s plánováním prostředí PPP ve vaší síti.

- **Scénáře PPP** jsou příklady různých praktických implementací PPP. V každém příkladu jsou pokyny a ukázkové hodnoty pro konfiguraci připojení PPP.
- **Koncepce PPP** poskytují informace o koncepcích PPP a požadavcích na server iSeries 400 ohledně připojení PPP.
- **Plánování PPP** obsahuje informace o plánování PPP a požadavcích na server iSeries 400 ohledně připojení PPP.

Používání služeb RAS: PPP

Následující části vám mohou pomoci s konfigurací a správou připojení PPP na serveru iSeries 400.

- **Konfigurace PPP** uvádí základní kroky při konfiguraci připojení PPP.
- **Správa PPP** poskytuje informace, které můžete použít jako vodítko při správě připojení PPP.
- **Odstraňování problémů s PPP** popisuje základní chyby připojení PPP a poukazuje na informace, které jsou podstatné pro odstranění daného problému.

Zde si můžete také vyhledat další informace o PPP. Tato stránka obsahuje odkazy na užitečné a související informace o serveru iSeries.

Kapitola 1. Co je nového ve V5R2


Produkt iSeries Navigator ve verzi V5R2 umožňuje PPP přes připojení Ethernet (PPPoE) iniciované ze strany serveru iSeries. Tato podpora zajišťuje nový typ virtuální linky PPPoE, která je vázaná k fyzické lince Ethernet a slouží k ustanovení připojení PPP pomocí adaptéru Ethernet LAN připojeného k modemu DSL. Jakmile je připojení iSeries a ISP spuštěno, jednotliví uživatelé v síti LAN mohou přistupovat k ISP prostřednictvím připojení iSeries PPPoE. K této nové funkci můžete přistoupit z dialogu profilu připojení odesílatele nebo z průvodce univerzálním připojením.


Další informace naleznete v části Připojení serveru ke koncentrátoru přístupu PPPoE.

Několik níže popsaných přidanych funkcí produktu iSeries Navigator nyní usnadňuje konfiguraci a správu připojení PPP:

- Dialog konfigurace DHCP-WAN nyní automaticky kontaktuje server DHCP a klientské rozhraní, aby zjistil IP adresu pro klientské rozhraní DHCP-WAN. Do dialogu můžete přistoupit takto:
 - Rozbalte **Síť > RAS (Remote Access Services)**.
 - Klepněte pravým tlačítkem myši na **RAS (Remote Access Services)**.
 - Vyberte **Služby**.
 - Vyberte ouško **DHCP-WAN**.
- Vylepšený dialog stavu připojení nyní zobrazuje podrobnosti o připojení L2TP, L2TP s více přechody, vícenásobného připojení a PPP přes Ethernet, čímž vám usnadňuje správu připojení PPP.
- Do bloku úloh byla přidána možnost vytvoření profilu připojení odesílatele, profilu připojení příjemce a metody přístupu skupiny.
- Průvodce novým telefonickým připojením a Průvodce univerzálním připojením byli přejmenováni - nyní se jim říká **Nové internetové nebo telefonické připojení k ISP** a **Nové univerzální připojení IBM**.
- Profily připojení odesílatelů si nyní mohou "půjčovat" linku PPP a modem přiřazený k profilu připojení příjemce čekajícímu na příchozí volání. Jakmile se připojení ukončí, připojení odesílatele "vrátí" linku PPP a modem profilu připojení příjemce. Chcete-li tuto novou funkci povolit, vyberte volbu **Povolit dynamické sdílení prostředků** na oušku modemu v dialogu konfigurace linky PPP. Linky PPP můžete konfigurovat na oušku Připojení u Profilu připojení příjemce a Profilu připojení odesílatele.
- Vlastnosti společné oblasti linek již nelze modifikovat, když se používají, čímž se vlastně předchází potenciálním problémům se společnou oblastí linek.
- Podpora provozních režimů 'Iniciátor na vyžádání' a vzdálené 'Vytáčení na vyžádání' byla u profilů připojení odesílatelů využívajících připojení L2TP zrušena.

Kapitola 2. Tisk tohoto tématu

Tento dokument si můžete prohlížet nebo stáhnout pro prohlížení či tisk ve formátu PDF. K prohlížení souborů PDF potřebujete Adobe® Acrobat® Reader. Můžete si jej stáhnout od společnosti Adobe .

Chcete-li si prohlédnout nebo stáhnout verzi PDF, vyberte RAS (Remote Access Services): PPP  (277 KB, asi 58 stran).

Následovně uložte soubor PDF na své pracovní stanici, abyste jej mohli prohlížet a tisknout:

1. Otevřete soubor PDF ve svém prohlížeči (klepněte na výše uvedený odkaz).
2. V menu svého prohlížeče klepněte na **File (Soubor)**.
3. Klepněte na **Save As (Uložit jako)**.
4. Vyhledejte adresář, do kterého chcete soubor PDF uložit.
5. Klepněte na **Save (Uložit)**.

Kapitola 3. Scénáře PPP

Následující scénáře vám objasní, jak protokol PPP funguje a jak můžete implementovat prostředí PPP ve své síti. Než přistoupíte k plánování a konfiguraci, seznamte se základními koncepcemi PPP pomocí těchto scénářů, které jsou přínosné pro začínající i zkušené uživatele.

Scénář: Připojení serveru ke koncentrátoru přístupu PPPoE

Mnozí poskytovatelé služeb sítě Internet (ISP) nabízejí vysokorychlostní přístup k Internetu pomocí DSL s PPPoE. Server iSeries se může připojit k těmto poskytovatelům služeb tak, aby nabízel připojení s velkou šířkou pásma a se zachováním výhod PPP.

Scénář: Připojení vzdálených vytáčených klientů k serveru iSeries

Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Pomocí PPP mohou tyto vytáčení klienti získat přístup k serveru iSeries.

Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu

Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. Mohou používat modem pro připojení serveru iSeries k určitému poskytovateli služeb sítě Internet (ISP). PC klienti připojení k síti LAN mohou komunikovat s Internetem tak, že používají server iSeries jako bránu.

Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu

Modem vám umožňuje, aby si dvě vzdálená pracoviště (například ústředí a pobočka) vzájemně vyměňovala data. Pomocí PPP lze k sobě připojit obě sítě LAN tím, že se vytvoří spojení mezi serverem iSeries v ústředí a jiným serverem iSeries v pobočce.

Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS

NAS (Network Access Server) spuštěný na serveru iSeries může směřovat požadavky na ověření autentizaci klientů na samostatný server RADIUS. Jestliže dojde k autentizaci, může server RADIUS také řídit IP adresy a porty pro uživatele.

Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí metod skupin a filtrování IP

Metody přístupu skupin vymezují skupiny uživatelů pro určité připojení a umožňují vám použít některé běžné atributy připojení a bezpečnostního nastavení na celou skupinu. V kombinaci s filtrováním IP tak můžete povolovat a zamezovat přístup ke konkrétním IP adresám ve vaší síti.

Scénář: PPP a DHCP na jediném serveru iSeries

Volající klienti nebo vzdálení uživatelé mohou pomocí PPP získat přístup k serveru iSeries, který je v síti určité společnosti. Klient DHCP sítě WAN na stejném serveru iSeries umožňuje vzdáleným uživatelům získat dynamicky přidělenou IP adresu pomocí stejných služeb jako uživatelé připojení k LAN.

Scénář: DHCP a profil PPP na odlišných serverech iSeries

Z důvodu zabezpečení dat nebo fyzického uspořádání sítě odděluje většina společností síťové služby a distribuuje je na odlišné servery. Tento scénář se zabývá problémy, které vznikají, když máte oddělený server PPP a server DHCP. Stejně jako předchozí scénář i toto nastavení umožňuje vzdáleným uživatelům použít telefonické připojení (vytáčené připojení) a získat přístup do sítě společnosti.

Scénář: PPP a VPN: L2TP nepovinný tunel chráněný pomocí VPN

Pobočka se může připojovat do ústředí podniku pomocí protokolu L2TP (Layer 2 Tunnel Protocol). Nepovinný tunel L2TP vytvoří virtuální propojení PPP. Vlastně to funguje tak, že L2TP rozšíří podnikovou síť, takže pobočka se jeví jako součást podsítě podniku. Datové přenosy v tunelu L2TP jsou chráněny pomocí VPN.

Scénář: Připojení serveru ke koncentrátoru přístupu PPPoE

Situace: Váš podnik vyžaduje rychlejší připojení k Internetu, a proto se zajímáte o službu DSL u místního ISP. Po počátečním průzkumu zjistíte, že váš ISP používá pro připojování svých klientů protokol PPPoE. Chcete použít toto připojení PPPoE pro zajišťování širokopásmových připojení k Internetu prostřednictvím svého serveru iSeries.



Obrázek 1. Připojení serveru iSeries k ISP s PPPoE

Řešení: Na svém serveru iSeries můžete podporovat připojení PPPoE k ISP. Server iSeries používá nový typ virtuální linky PPPoE, která je vázána k fyzické lince Ethernet konfigurované pro použití adaptéru Ethernet typ 2838. Tato virtuální linka podporuje protokoly relace PPP přes síť Ethernet LAN připojenou k DSL modemu, jež zajišťuje bránu ke vzdálenému ISP. To umožňuje uživatelům připojeným k LAN, aby měli vysokorychlostní přístup k Internetu prostřednictvím serverů iSeries s připojením PPPoE. Jakmile je připojení iSeries a ISP spuštěno, jednotliví uživatelé v síti LAN mohou přistupovat k ISP prostřednictvím PPPoE, přičemž používají IP adresu přiřazenou serveru iSeries. Chcete-li zajistit dodatečné zabezpečení, můžete použít filtrační pravidla pro virtuální linku PPPoE, kterými se omezí určité příchozí internetové přenosy.

Ukázková konfigurace:

1. Konfigurujte připojovací zařízení, které se bude používat pro vašeho ISP.
2. Nakonfigurujte profil odesílatele připojení na svém serveru iSeries.

Dbejte na to, abyste zadali následující informace:

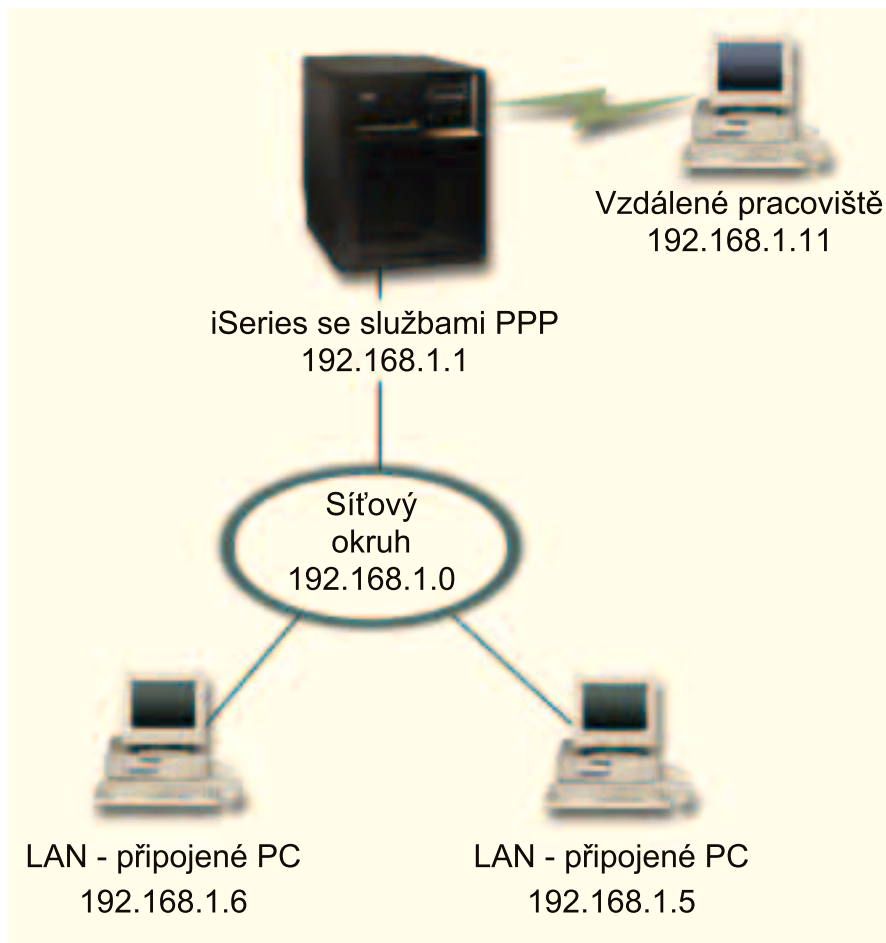
- **Typ protokolu:** PPP.
- **Typ připojení:** PPP přes Ethernet.
- **Provozní režim:** Iniciátor.

- **Konfigurace linky:** Jediná linka.
3. Na stránce **Obecné** ve vlastnostech nového profilu PPP zadejte jméno a popis profilu odesílatele. Toto jméno bude označovat profil připojení i virtuální linku PPPoE.
 4. Klepněte na stránku **Připojení**. Vyberte **PPPoE jméno virtuální linky**, které odpovídá jménu pro tento profil připojení. Jakmile vyberete linku, iSeries Navigator zobrazí dialog vlastností linky.
 - a. Na stránce **Obecné** zadejte smysluplný popis virtuální linky PPPoE.
 - b. Klepněte na stránku **Připojení**. Z výběrového seznamu jmen fyzické linky vyberte linku Ethernet, která bude toto připojení používat, a klepněte na **Otevřít**. Pokud však potřebujete definovat novou linku Ethernet, napište jméno linky a klepněte na **Nová**. iSeries Navigator zobrazí dialog vlastností linky Ethernet. **Poznámka:** PPPoE vyžaduje adaptéry Ethernet typu 2838.
 - 1) Na stránce **Obecné** zadejte smysluplný popis linky Ethernet a ověřte, že definice linky používá požadované hardwarové prostředky.
 - 2) Klepněte na stránku **Připojení**. Zadejte vlastnosti fyzické linky Ethernet. Další informace naleznete v dokumentaci ke své kartě Ethernet a v online nápovědě.
 - 3) Klepněte na stránku **Jiné**. Zadejte úroveň přístupu a oprávnění, jaké mohou mít ostatní uživatelé k této lince.
 - 4) Klepnutím na **OK** se vrátíte na stránku vlastností virtuální linky PPPoE.
 - c. Klepněte na **Limity**, abyste mohli definovat vlastnosti pro autentizaci LCP, nebo klepněte na **OK**, chcete-li se vrátit na stránku **Připojení** nového profilu PPP.
 5. Jestliže váš poskytovatel ISP požaduje, aby server iSeries prokazoval svou totožnost, nebo jestliže si přejete, aby iSeries autentizoval vzdálený server (ověřoval jeho totožnost), klepněte na stránku **Autentizace**. Další informace naleznete v části Autentizace systému.
 6. Klepněte na stránku **Nastavení TCP/IP** a uveďte parametry zacházení s IP adresami pro tento profil připojení. Chcete-li umožnit uživatelům připojeným k LAN, aby se připojovali k ISP pomocí IP adres alokovaných na server iSeries, vyberte **Skrýt adresy (zcela zamaskovat)**.
 7. Klepněte na stránku **DNS** a zadejte IP adresu serveru DNS, kterou vám poskytl ISP.
 8. Jestliže chcete zadat podsystém, který má spouštět úlohu připojení, klepněte na stránku **Jiné**.
 9. Klepnutím na **OK** profil dokončíte.

Informace o omezování přístupu uživatelů k externím IP adresám nebo prostředkům iSeries naleznete v části Filtrování IP a Metody přístupu skupin.

Scénář: Připojení vzdálených volajících klientů k serveru iSeries

Situace: Jste administrátor sítě vaší firmy a musíte udržovat server iSeries a síťové klienty. Místo toho, abyste chodili do práce řešit a odstraňovat problémy, jistě byste ocenili možnost pracovat z nějakého vzdáleného místa, například ze svého domova. Jelikož vaše společnost nemá vázané síťové připojení k Internetu, můžete se k firemnímu serveru iSeries připojit pomocí připojení PPP. Kromě toho máte v současné době pouze modem 7852-400 ECS a chcete jej využít pro toto připojení.



Obrázek 2. Připojení vzdálených klientů k serveru iSeries

Řešení: Pro připojení domácího PC se serverem iSeries pomocí modemu můžete použít PPP. Jelikož pro tento typ připojení PPP použijete modem ECS, musíte se ujistit, že modem je konfigurovaný pro synchronní i asynchronní režim. Na obrázku výše je znázorněný server iSeries se službami PPP, který je připojený k LAN se dvěma PC. Vzdálený pracovník se pak připojí k serveru iSeries a jakmile prokáže svou totožnost, stane se součástí sítě (192.168.1.0). V tomto případě je snazší volajícím klientovi přiřadit statickou IP adresu.

Vzdálený pracovník prokáže serveru iSeries svou totožnost pomocí CHAP-MD5. Server iSeries nedokáže používat MS_CHAP, a proto se musíte ujistit, že je váš PPP klient nastavený na používání CHAP-MD5.

Pokud chcete, aby vaši vzdálení pracovníci měli výše uvedený přístup k firemní síti, je nutné v balíku TCP/IP stejně jako v profilu příjemce PPP umožnit směrování pomocí IP, přičemž směrování IP musí být správně konfigurováno. Jestliže chcete omezit nebo zabezpečit akce, které může vzdálený klient podnikat ve vaší síti, můžete použít filtrační pravidla, jež se budou uplatňovat na IP pakety takového klienta.

Na výše uvedeném obrázku je pouze jeden volající klient, protože modem ECS může obsluhovat v daném okamžiku pouze jedno připojení. Pokud potřebujete více simultánních volajících klientů, prohlédněte si pokyny ohledně hardwaru a softwaru uvedené v části týkající se plánování.

Ukázková konfigurace:

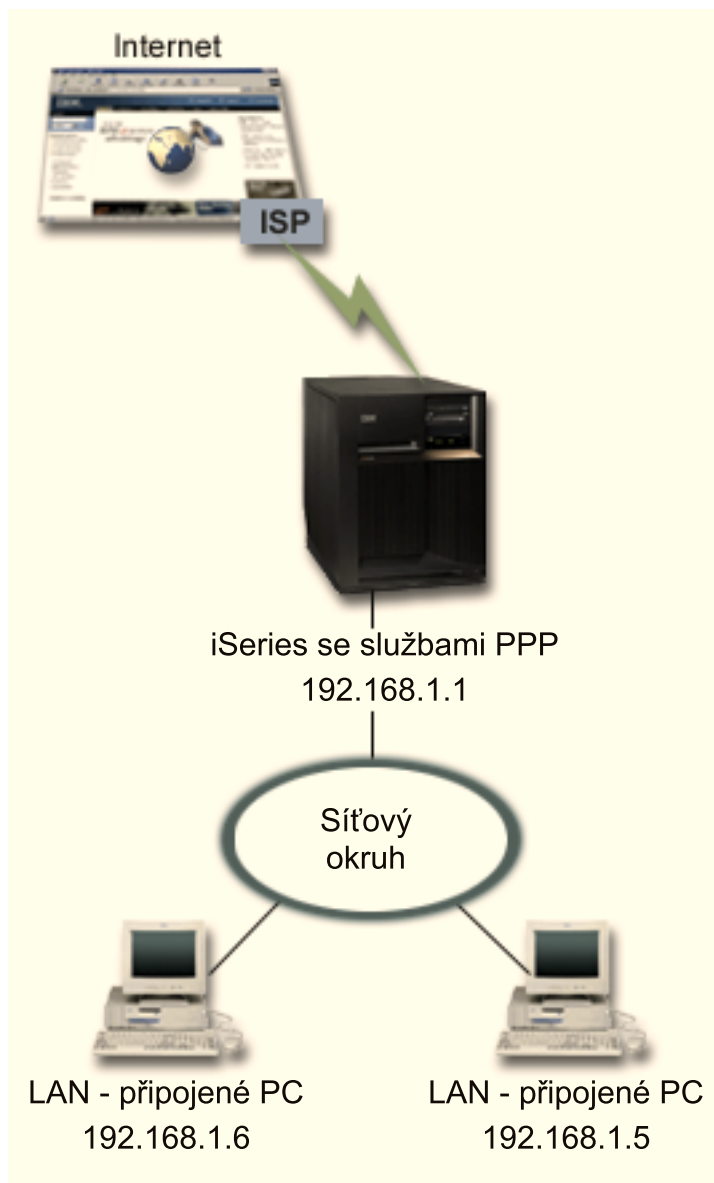
1. Nakonfigurujte vytáčené připojení do sítě a vytvořte vytáčené připojení ke vzdálenému PC.
2. Nakonfigurujte profil odesílatele připojení na svém serveru iSeries.

Dbejte na to, abyste zadali následující informace:

- **Typ protokolu:** PPP.
 - **Typ připojení:** Komutovaná linka.
 - **Provozní režim:** Odpověď.
 - **Konfigurace linky:** Může to být jediná linka nebo společná oblast linek, což závisí na vašem prostředí.
3. Na stránce **Obecné** ve vlastnostech nového profilu PPP zadejte jméno a popis profilu příjemce.
 4. Klepněte na stránku **Připojení**. Vyberte si příslušné **Jméno linky** nebo vytvořte novou linku tak, že napíšete nové jméno a klepnete na **Nová**.
 - a. Na stránce **Obecné** zvýrazněte existující hardwarový prostředek a nastavte rámcování na **Asynchronní**.
 - b. Klepněte na stránku **Modem**. Z výběrového seznamu Jméno vyberte modem **IBM 2772**.
 - c. Klepnutím na **OK** se vrátíte na stránku vlastností nového profilu PPP.
 5. Klepněte na stránku **Autentizace**.
 - a. Vyberte **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
 - b. Vyberte **Lokální autentizace pomocí ověřovacího seznamu** a přidejte nového vzdáleného uživatele do ověřovacího seznamu.
 - c. Vyberte **Povolit šifrované heslo (CHAP-MD5)**.
 6. Klepněte na stránku **Nastavení TCP/IP**.
 - a. Vyberte lokální IP adresu 192.168.1.1.
 - b. Pro vzdálenou adresu vyberte volbu **Pevná IP adresa** s počáteční adresou 192.168.1.11.
 - c. Vyberte **Povolit vzdálenému systému přístup k ostatním sítím**.
 7. Klepnutím na **OK** profil dokončíte.

Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu

Situace: Podniková aplikace, kterou vaše společnost nyní používá, vyžaduje, aby uživatelé měli přístup k Internetu. Jelikož aplikace nevyžaduje velké přenosy dat, možná budete chtít k připojení serveru iSeries a PC klientů v síti LAN k Internetu použít modem. Tuto situaci znázorňuje následující obrázek.



Obrázek 3. Připojení podnikové sítě LAN k Internetu pomocí modemů

Řešení: Pro připojení svého serveru iSeries k ISP (poskytovatel služeb sítě Internet) můžete použít modem ECS (nebo jiný kompatibilní modem). Musíte vytvořit profil odesílatele, pomocí něhož se bude ustanovovat PPP připojení k ISP.

Jakmile vytvoříte připojení mezi serverem iSeries a ISP, vaše počítače připojené k síti LAN budou moci komunikovat s Internetem, přičemž budou používat server iSeries jako bránu. Ujistěte se, že v profilu průvodce je zapnutá volba *Skrýt adresy*, aby klienti LAN, kteří mají vyhrazené IP adresy, mohli komunikovat po Internetu.

Když jsou nyní váš server iSeries a síť připojeny k Internetu, musíte porozumět riziku pro zabezpečení dat. Spolupracujte se svým ISP, abyste pochopili jeho strategii zabezpečení ochrany dat, a podnikněte další akce pro ochranu svého serveru a sítě.

Jestliže používáte modem ECS pro tento typ připojení PPP, nakonfigurujte svůj modem pro asynchronní komunikaci. Podle toho, jak využíváte Internet, byste se měli zajímat o šířku pásma. Chcete-li se dozvědět více o tom, jak zvýšit šířku pásma svého připojení, prostudujte si část týkající se plánování.

Ukázková konfigurace:

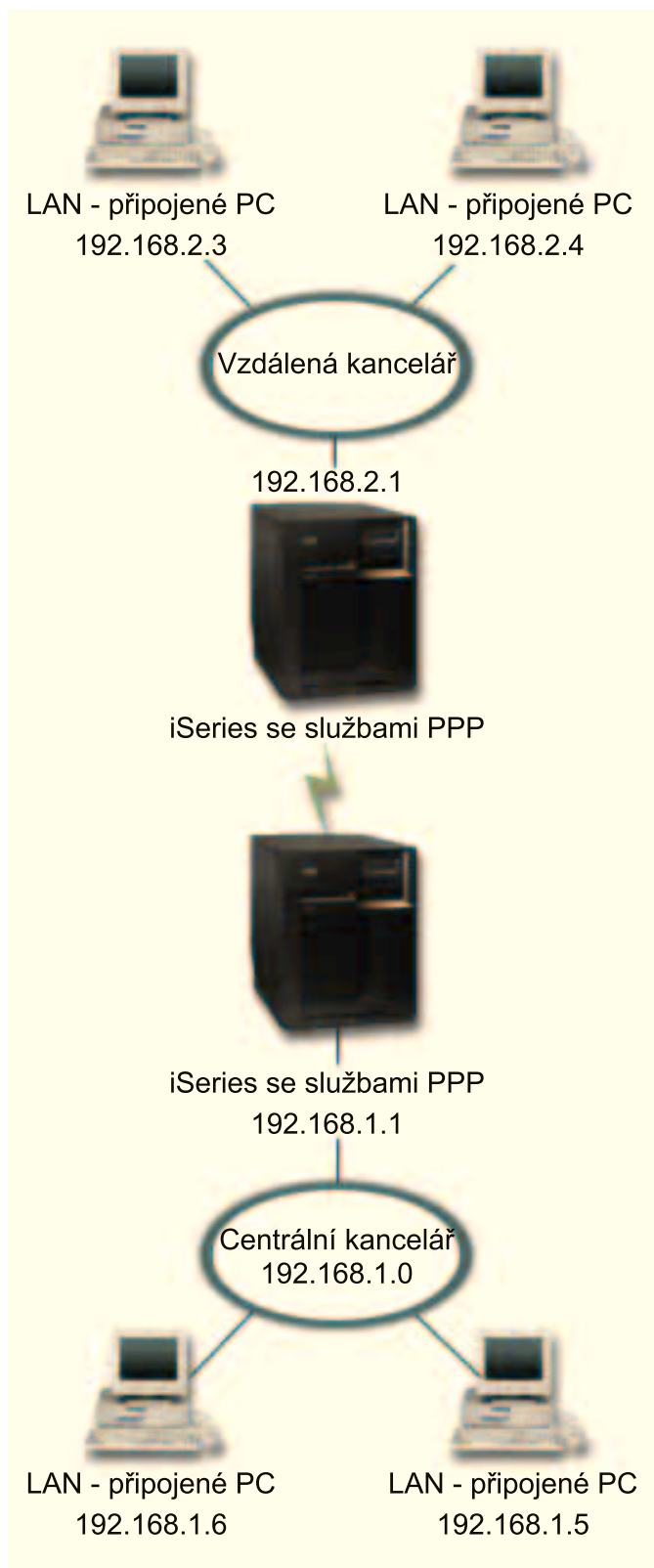
1. Nakonfigurujte profil odesílatele připojení na svém serveru iSeries.
Dbejte na to, abyste vybrali následující informace:
 - **Typ protokolu:** PPP.
 - **Typ připojení:** Komutovaná linka.
 - **Provozní režim:** Vytáčení.
 - **Konfigurace linky:** Může to být jediná linka nebo společná oblast linek, což závisí na vašem prostředí.
2. Na stránce **Obecné** ve vlastnostech nového profilu PPP zadejte jméno a popis profilu odesílatele.
3. Klepněte na stránku **Připojení**. Vyberte si příslušné Jméno linky nebo vytvořte novou linku tak, že napíšete nové jméno a klepnete na **Nová**.
 - a. Na stránce **Obecné** ve vlastnostech nové linky zvýrazněte existující hardwarový prostředek a nastavte rámcování na **Asynchronní**.
 - b. Klepněte na stránku **Modem**. Z výběrového seznamu Jméno vyberte modem, který používáte.
 - c. Klepnutím na **OK** se vrátíte na stránku vlastností nového profilu PPP.
4. Klepněte na **Přidat** a napište telefonní číslo, které se má vytáčet pro dosažení serveru ISP. Dbejte na to, abyste zahrnuli případně požadovanou předponu.
5. Klepněte na stránku **Autentizace** a vyberte volbu **Povolit vzdálenému systému ověřit identitu tohoto serveru iSeries**. Vyberte si autentizační protokol a zadejte požadované uživatelské jméno nebo heslo.
6. Klepněte na stránku Nastavení TCP/IP.
 - a. Vyberte volbu **Přiřazená vzdáleným systémem** pro IP adresy lokálních i vzdálených systémů.
 - b. Vyberte volbu **Přidat vzdálený systém jako předvolenou předepsanou cestu**.
 - c. Zaškrtněte volbu **Skrýt adresy**, aby vaše interní IP adresy nemohly být směrovány do Internetu.
7. Klepněte na stránku **DNS** a zadejte IP adresu serveru DNS, kterou vám poskytl ISP.
8. Klepnutím na **OK** profil dokončíte.

Chcete-li používat profil připojení pro připojení k Internetu, klepněte pravým tlačítkem myši na profil připojení z prostředí produktu iSeries Navigator a vyberte **Spustit**. Připojení je úspěšné, když se stav změní na **Aktivní**. Zobrazení aktualizujete pomocí tlačítka Obnovit.

Poznámka: Musíte zajistit, aby jiné systémy ve vaší síti měly definováno správné směrování, aby se přenosy TCP/IP směrované do Internetu z těchto systémů odesílaly do serveru iSeries.

Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu

Situace: Předpokládejme, že na dvou pracovištích máte dvě různé sítě - v pobočce a v ústředí podniku. Každý den se pobočka potřebuje spojit s ústředím firmy a vyměnit si databázové informace pro aplikace k zadávání dat. Množství vyměněných dat není důvodem pro koupi fyzického síťového připojení, takže se pro propojení těchto dvou sítí rozhodnete používat modemy.



Obrázek 4. Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu

Řešení: Pomocí PPP lze vzájemně propojit dvě sítě LAN tak, že se vytvoří spojení mezi servery iSeries, jak znázorňuje obrázek. V tomto případě předpokládejme, že vzdálená kancelář iniciuje připojení s ústředím firmy. Budete konfigurovat profil odesílatele na vzdáleném serveru iSeries a profil příjemce na serveru v ústředí společnosti.

Jestliže počítače ve vzdálené kanceláři potřebují přístup do podnikové sítě LAN (192.168.1.0), bude nutné, aby v profilu příjemce v kanceláři ústředí bylo zapnuto zasílání IP a aby pro tyto počítače bylo povoleno směrování IP adres (v tomto příkladu 192.168.2, 192.168.3, 192.168.1.6 a 192.168.1.5). Musí být také aktivováno zasílání IP adres pro balík TCP/IP. Tato konfigurace umožňuje základní komunikaci TCP/IP mezi sítěmi LAN. Měli byste zvážit činitele zabezpečení dat a DNS pro rozlišování hostitelských jmen mezi sítěmi LAN.

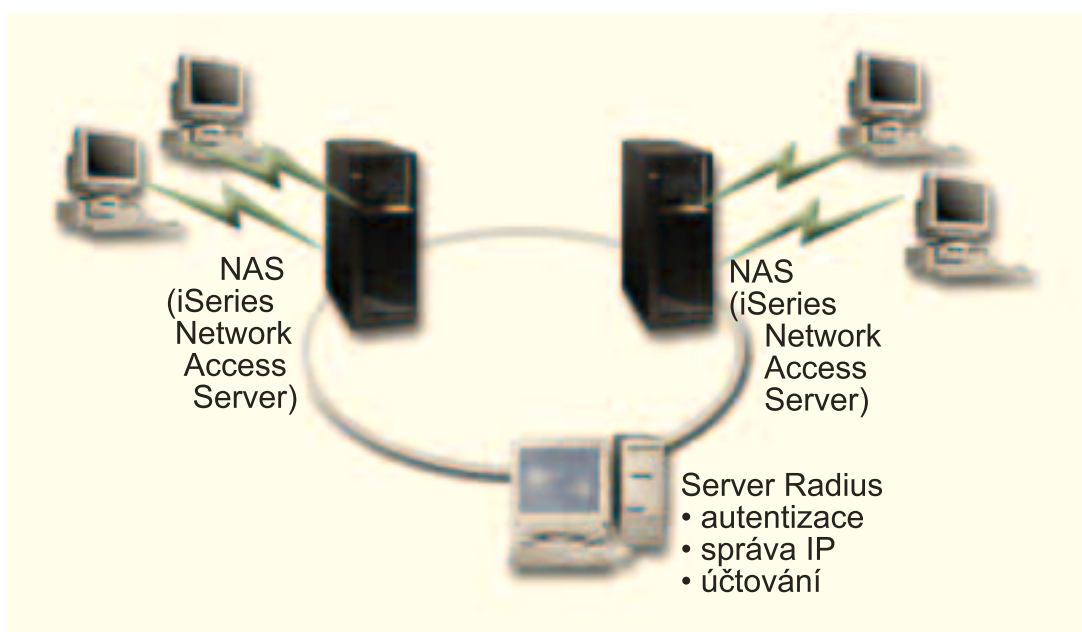
Ukázková konfigurace:

1. Nakonfigurujte profil odesílatele připojení na serveru iSeries ve vzdálené kanceláři.
Dbejte na to, abyste vybrali následující informace:
 - **Typ protokolu:** PPP.
 - **Typ připojení:** Komutovaná linka.
 - **Provozní režim:** Vytáčení.
 - **Konfigurace linky:** Může to být jediná linka nebo společná oblast linek, což závisí na vašem prostředí.
2. Na stránce **Obecné** ve vlastnostech nového profilu PPP zadejte jméno a popis profilu odesílatele.
3. Klepněte na stránku **Připojení**. Vyberte si příslušné Jméno linky nebo vytvořte novou linku tak, že napíšete nové jméno a klepnete na **Nová**.
 - a. Na stránce **Obecné** ve vlastnostech nové linky zvýrazněte existující hardwarový prostředek a nastavte rámcování na **Asynchronní**.
 - b. Klepněte na stránku **Modem**. Z výběrového seznamu Jméno vyberte modem, který používáte.
 - c. Klepnutím na **OK** se vrátíte na stránku vlastností nového profilu PPP.
4. Klepněte na **Přidat** a napište telefonní číslo, které se má vytáčet pro dosažení serveru iSeries v kanceláři ústředí. Dbejte na to, abyste zahrnuli případně požadovanou předponu.
5. Klepněte na stránku **Autentizace** a vyberte volbu **Povolit vzdálenému systému ověřit identitu tohoto serveru iSeries**. Vyberte volbu **Požadovat šifrované heslo (CHAP-MD5)** a zadejte požadované uživatelské jméno nebo heslo.
6. Klepněte na stránku **Nastavení TCP/IP**.
 - a. Jako lokální IP adresu vyberte IP adresu rozhraní LAN vzdálené kanceláře (192.168.2.1) z výběrového rámečku **Použít pevnou IP adresu**.
 - b. Jako IP adresu vzdáleného systému vyberte volbu **Přiřazená vzdáleným systémem**.
 - c. V části týkající se směrování vyberte volbu **Přidat vzdálený systém jako předvolenou předepsanou cestu**.
 - d. Klepněte na **OK**, čímž dokončíte profil odesílatele.
7. Nakonfigurujte **Profil příjemce připojení** na serveru iSeries v kanceláři ústředí.
Dbejte na to, abyste vybrali následující informace:
 - **Typ protokolu:** PPP.
 - **Typ připojení:** Komutovaná linka.
 - **Provozní režim:** Odpověď.
 - **Konfigurace linky:** Může to být jediná linka nebo společná oblast linek, což závisí na vašem prostředí.
8. Na stránce **Obecné** ve vlastnostech nového profilu PPP zadejte jméno a popis profilu příjemce.
9. Klepněte na stránku **Připojení**. Vyberte si příslušné jméno linky nebo vytvořte novou linku tak, že napíšete nové jméno a klepnete na **Nová**.

- a. Na stránce **Obecné** zvýrazněte existující hardwarový prostředek a nastavte rámcování na **Asynchronní**.
 - b. Klepněte na stránku **Modem**. Z výběrového seznamu Jméno vyberte modem, který používáte.
 - c. Klepnutím na **OK** se vrátíte na stránku vlastností nového profilu PPP.
10. Klepněte na stránku **Autentizace**.
- a. Zaškrtněte volbu **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
 - b. Přidejte nového vzdáleného uživatele do ověřovacího seznamu.
 - c. Zaškrtněte autentizaci CHAP-MD5.
11. Klepněte na stránku **Nastavení TCP/IP**.
- a. Jako lokální IP adresu vyberte z výběrového rámečku IP adresu rozhraní systému ústředí (192.168.1.1).
 - b. Jako IP adresu vzdáleného systému vyberte volbu **Na základě ID uživatele vzdáleného systému**. Objeví se dialog IP adresy definované jménem uživatele. Klepněte na tlačítko **Přidat**. Vyplňte pole pro jméno volajícího uživatele, IP adresu a masku podsítě. V našem scénáři jsou správné následující hodnoty:
 - Jméno volajícího uživatele: Remote_site
 - IP adresa: 192.168.2.1
 - Masky podsítě: 255.255.255.0Klepněte na **OK** a znovu klepněte na **OK**, čímž se vrátíte na stránku nastavení TCP/IP.
 - c. Vyberte volbu **Směrování pomocí IP**, čímž umožníte jiným systémům ve vaší síti, aby používaly tento server iSeries jako bránu.
12. Klepněte na **OK**, čímž dokončíte profil příjemce.

Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS

Situace: Do sítě vašeho podniku se telefonicky připojují vzdálení uživatelé ke dvěma serverům iSeries. Uvítali byste způsob, jak centralizovat autentizaci, služby a účtování, aby jeden server mohl vyřizovat požadavky na ověřování ID a hesel uživatelů a určovat, které IP adresy směřují na tyto servery.



Obrázek 5. Autentizace vytáčených připojení pomocí serveru RADIUS

Řešení: Když se uživatelé pokusí o připojení, server NAS (Network Access Server) spuštěný na serverech iSeries odešle autentizační informace do serveru RADIUS v síti. Server RADIUS, který ukládá všechny autentizační informace vaší sítě, zpracuje požadavky na autentizaci a odpoví. Server RADIUS lze také konfigurovat tak, aby po ověření uživatele přiřazoval peerům IP adresy a aktivoval účtování za účelem sledování aktivity uživatele a využití. Chcete-li podporovat server RADIUS, musíte na serveru iSeries definovat server RADIUS NAS.

Ukázková konfigurace:

1. V prostředí produktu iSeries Navigator rozbalte **Síť**, klepněte pravým tlačítkem myši na **RAS (Remote Access Services)** a vyberte volbu **Služby**.
2. Na oušku **RADIUS** vyberte volbu **Povolit připojení k serveru RADIUS pro přístup do sítě** a volbu **Povolit RADIUS pro autentizaci**. Podle vašeho řešení pomocí serveru RADIUS si můžete také zvolit, aby server RADIUS vyřizoval účtování připojení a konfiguraci adres TCP/IP.
3. Klepněte na tlačítko **Nastavení RADIUS NAS**.
4. Na stránce **Obecné** zadejte popis tohoto serveru.
5. Na stránce Autentizační server (a volitelně také na stránce Účtovací server) klepněte na **Přidat** a zadejte následující informace:
 - a. Do rámečku **IP adresa lokálního systému** zadejte IP adresu rozhraní serveru iSeries použitého pro připojení k serveru RADIUS.
 - b. Do rámečku **IP adresa serveru** zadejte IP adresu pro server RADIUS.
 - c. Do rámečku **Heslo** zadejte heslo použité pro identifikaci serveru iSeries na serveru RADIUS.
 - d. Do rámečku **Port** zadejte port serveru iSeries, který se používá pro komunikaci se serverem RADIUS. Zadejte port 1812 pro autentizační server nebo 1813 pro účtovací server.
6. Klepněte na **OK**.
7. V prostředí produktu iSeries Navigator rozbalte **Síť > RAS (Remote Access Services)**.
8. Vyberte profil připojení, který bude server RADIUS používat pro autentizaci. Pro profil připojení příjemce lze použít pouze služby RADIUS.
9. Na stránce Autentizace vyberte **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
10. Vyberte **Vzdálená autentizace pomocí serveru RADIUS**.

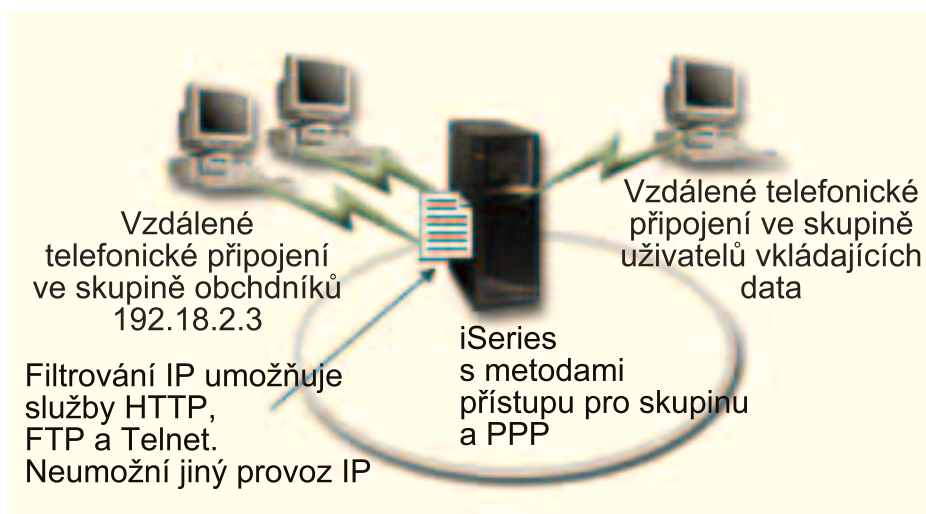
11. Vyberte autentizační protokol (EAP, PAP nebo CHAP-MD5). Tento protokol musí používat také server RADIUS. Další informace naleznete v části Autentizace systému.
12. Vyberte volbu **Povolit RADIUS pro editování a účtování připojení**.
13. Klepnutím na **OK** uložíte změny profilu připojení.

Musíte také nastavit server RADIUS včetně podpory autentizačního protokolu, uživatelských dat a informací o účtování. Další informace vám poskytne prodejce serveru RADIUS.

Když se uživatelé připojují po telefonní lince pomocí tohoto profilu připojení, server iSeries odešle autentizační informace uvedenému serveru RADIUS. Pokud je ověřena totožnost uživatele, připojení se aktivuje (umožní) a uplatní se všechna omezení připojení uvedená v informacích o uživateli na serveru RADIUS.

Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí metod skupin a filtrování IP

Situace: Vaše síť má několik skupin distribuovaných uživatelů, z nichž každý potřebuje přístup k různým prostředkům podnikové sítě LAN. Skupina uživatelů vkládajících data potřebuje přístup k databázi a několika jiným aplikacím. Obchodní partner zase potřebuje vytáčený přístup ke službám HTTP, FTP a Telnet, ale z důvodů zabezpečení dat nesmí mít možnost přistupovat k jiným TCP/IP službám nebo přenosům. Kdybyste podrobně definovali atributy a povolení připojení pro každého uživatele, bylo by to pracnější a omezení sítě pro všechny uživatele tohoto profilu připojení by nezaručovalo dostatečnou kontrolu. Potřebujete nějak definovat nastavení a možnosti připojení pro několik odlišných skupin uživatelů, kteří se běžně připojují k tomuto serveru přes telefonní linku.



Obrázek 6. Nastavení vytáčených připojení s uplatněním metody skupinového nastavení

Řešení: Potřebujete použít jedinečná filtrovací omezení IP na dvě různé skupiny uživatelů. Toho dosáhnete tak, že vytvoříte metody přístupu skupin a filtrovací pravidla IP. Metody přístupu skupin se odkazují na filtrovací pravidla IP, takže nejprve musíte vytvořit filtrovací pravidla. V tomto příkladu musíte vytvořit filtr PPP, který má zahrnovat filtrovací pravidla IP pro metodu přístupu skupiny "Obchodní partner". Tato filtrovací pravidla umožní služby HTTP, FTP a Telnet, ale zamezí přístupu ke všem jiným přenosům a službám TCP/IP na serveru iSeries. Tento scénář pouze zobrazuje filtrovací pravidla potřebná pro skupinu prodejce; podobné filtry si však můžete také nastavit pro skupinu "Vkládání dat".

Nakonec si musíte vytvořit metody přístupu skupiny (vždy jednu pro jednu skupinu), čímž svou skupinu definujete. Metoda přístupu skupiny vám umožňuje definovat běžné atributy připojení pro uživatele ve

skupině. Když přidáte metodu přístupu skupin do ověřovacího seznamu na serveru iSeries, můžete toto nastavení připojení použít při procesu autentizace. Metoda přístupu skupiny definuje několik nastavení pro relaci uživatele včetně možnosti uplatnit IP filtrovací pravidla, která omezí IP adresy a služby TCP/IP, které jsou uživateli v dané relaci dostupné.

Ukázková konfigurace:

1. Vytvořte identifikátor filtru PPP a filtry pro pravidla paketu IP, které specifikují povolení a omezení pro tuto metodu přístupu skupiny. Další informace o filtrování IP najdete v části Pravidla paketu IP (filtrování a NAT).
 - a. V prostředí produktu iSeries Navigator rozbalte **Síť > RAS (Remote Access Services)**.
 - b. Klepněte na volbu **Profily připojení příjemce**, pak klepněte pravým tlačítkem na profil tohoto připojení a vyberte **Vlastnosti**.
 - c. Vyberte oúško **Nastavení TCP/IP** a klepněte na volbu **Rozšířené**.
 - d. Vyberte volbu **Použit pro toto připojení pravidla paketu IP**. Pak klepněte na **Editovat soubor pravidel**. Tak spustíte editor pravidel paketu IP a otevřete soubor PPP filtrovacích pravidel paketu.
 - e. Otevřete menu **Vložit** a vyberte volbu **Filtry**, abyste mohli přidat sady filtrů. Na oúšku **Obecné** definujte sady filtrů a na oúšku **Služby** definujte službu, kterou povolujete, například HTTP. Následující sada filtrů, "services_rules," umožní služby HTTP, FTP a Telnet. Filtrovací pravidla obsahují implicitně omezovací příkazy, které zamezují všem službám TCP/IP nebo přenosům IP, jež nejsou výslovně povoleny.

Poznámka: IP adresy v následujícím příkladu jsou globálně směrovatelné a slouží pouze jako příklad.

Následující 2 filtry umožní HTTP (prohlížeč Web) přenosy do systému a z něj.

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

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

```
FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR = %
* DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS = %
NONE JRN = OFF
```

Následující 4 filtry umožní přenosy FTP do systému a z něj.

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

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

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

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

Následující 2 filtry umožní přenosy telnet do systému a z něj.

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

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

- f. Otevřete menu **Vložit** a vyberte **Filtrovací rozhraní**. Pomocí filtrovacího rozhraní můžete vytvořit identifikátor filtru PPP a zahrnout sady filtrů, které jste definovali.

- 1) Na oušku **Obecné** zadejte

```
permitted_services
```

jako identifikátor filtru PPP.

- 2) Na oušku **Sady filtrů** vyberte sadu filtrů **services_rules** a klepněte na **Přidat**.

- 3) Klepněte na **OK**. Do souboru pravidel se přidá následující řádek:

```
### Následující příkaz váže (přiřazuje) sadu filtrů 'services_rules' k
ID PPP filtru "permitted_services." Toto ID PPP filtru
lze pak použít na fyzické rozhraní přiřazené k profilu připojení PPP
nebo metodu přístupu skupiny.
```

```
FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

- g. Změny uložte a ukončete práci. Pokud budete později potřebovat tyto změny anulovat, zadejte do znakově orientovaného rozhraní příkaz:

```
RMVTCPTBL
```

Tak odstraní všechna filtrovací pravidla a NAT na serveru.

- h. V dialogu **Rozšířená nastavení TCP/IP** ponechejte okénko **Identifikátor filtru PPP** prázdné a klepněte na **OK**, čímž práci ukončíte. Později byste měli použít identifikátor filtru, který jste právě vytvořili, na metodu přístupu skupiny, nikoliv na tento profil připojení.
2. Definujte novou metodu přístupu skupiny pro tuto skupinu uživatelů. Podrobný popis voleb pro metody přístupu skupiny naleznete v části Konfigurace metody přístupu skupiny.
- V prostředí produktu iSeries Navigator rozbalte **Síť > RAS (Remote Access Services) > Profily příjemce připojení**.
 - Klepněte pravým tlačítkem na ikonu metody přístupu skupiny a vyberte volbu **Nová metoda přístupu skupiny**. Produkt iSeries Navigator zobrazí dialog definice nové metody přístupu skupiny.
 - Na stránce **Obecné** zadejte jméno a popis metody přístupu skupiny.
 - Na stránce **Nastavení TCP/IP**:
 - Vyberte volbu **Použít pro toto připojení pravidla paketu IP** a zvolte identifikátor filtru PPP **permitted_services**.
 - Vyberte **OK**, čímž uložíte metodu přístupu skupiny.
3. Použijte metodu přístupu skupiny na uživatele, kteří jsou přidružení k této skupině.
- Otevřete profil příjemce připojení, kterým se řídí tato vytáčená připojení.
 - Na stránce **Autentizace** u profilu příjemce připojení vyberte ověřovací seznam, který obsahuje autentizační informace o uživateli, a klepněte na **Otevřít**.
 - Vyberte uživatele ze skupiny prodeje, na kterého chcete uplatnit metodu přístupu skupiny, a klepněte na **Otevřít**.
 - Klepněte na tlačítko **Použít pro uživatele metodu skupiny** a vyberte metodu přístupu skupiny definovanou v kroku 2.
 - Kroky zopakujte pro všechny uživatele ve skupině prodeje.

Další informace o autentizaci uživatelů na připojení PPP naleznete v části Autentizace systému.

Kapitola 4. Koncepce protokolu PPP

PPP můžete používat pro připojení serveru iSeries ke vzdáleným sítím, ke klientským PC, k jiným serverům iSeries nebo k poskytovateli služeb sítě Internet (ISP). Chcete-li tento protokol plně využívat, musíte rozumět tomu, co server iSeries může pro tento protokol zajistit a jak jej může podporovat. Další informace naleznete v následujících částech.

Co je PPP?

Protokol PPP (point-to-point) je protokol TCP/IP, který se používá pro připojení jednoho počítačového systému k jinému. Podrobnější definici naleznete v této části.

Profily připojení

Profily připojení PPP definují sadu parametrů a prostředků pro určitá připojení PPP. Můžete spustit profily, které tato nastavení parametrů používají pro vytáčení (vytvoření) NEBO naslouchání (příjem) připojení PPP.

Metody přístupu skupiny

Tyto metody definují sadu připojovacích a zabezpečovacích atributů pro skupinu uživatelů. Informace o tom, jak je můžete definovat ve svém systému, naleznete v této části.

Co je PPP?

Počítače používají **protokol PPP** čili **Point-to-Point Protocol** ke komunikaci po Internetu prostřednictvím telefonních linek. Připojení PPP existuje tehdy, když se dva systémy fyzicky připojí pomocí telefonní linky. Protokol PPP tedy můžete používat pro připojování jednoho systému k druhému. Například vytvořené připojení PPP mezi pobočkou a ústředím firmy umožňuje oběma systémům přenášet po síti data do druhého systému.

Protokol PPP je internetovým standardem. Mezi poskytovateli služeb sítě Internet (ISP) je to nejpoužívanější protokol. Protokol PPP můžete použít k připojení ke svému ISP, ten vám pak umožní připojení k Internetu.

Protokol PPP umožňuje spolupráci systémů mezi softwarovými produkty pro vzdálený přístup od různých výrobců. Rovněž umožňuje, aby více síťových komunikačních protokolů používalo stejnou fyzickou komunikační linku.

Níže uvedené normy RFC (Request For Comment) popisují protokol PPP. Další informace o RFC naleznete na adrese <http://www.rfc-editor.org>.

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

Profily připojení

V5R2 používá dva typy profilů a tím vám umožňuje definovat sadu charakteristik pro připojení PPP nebo sadu připojení.

- **Profily připojení odesílatele** jsou připojení PPP, která pocházejí z lokálního serveru iSeries a vzdálený systém je přijme. Pomocí tohoto objektu můžete konfigurovat odchozí připojení.
- **Profily připojení původce** jsou připojení PPP, která pocházejí ze vzdáleného systému a lokální server iSeries je přijme. Pomocí tohoto objektu můžete konfigurovat příchozí připojení.

Profil připojení uvádí, jak by připojení PPP mělo fungovat. Informace v profilu připojení obsahují odpovědi na tyto otázky:

- Jaký typ protokolu připojení budete používat? (PPP nebo SLIP)
- Kontaktuje váš server iSeries jiný počítač tím, že navazuje telefonické připojení (odesílatel)? Čeká váš server iSeries na volání od jiného systému (příjemce)?

- Jakou komunikační linku bude připojení používat?
- Měl by váš server iSeries určovat, jaká IP adresa se má použít?
- Jak by měl váš server iSeries autentizovat jiný systém (ověřovat jeho totožnost)? Kam by měl server iSeries ukládat autentizační informace?

Profil připojení je logické znázornění následujících atributů připojení:

- linka a typ profilu
- nastavení s více linkami
- vzdálená telefonní čísla a volby vytáčení
- autentizace
- nastavení TCP/IP: IP adresy, směrování a IP filtrování
- řízení práce a přizpůsobení komunikace
- servery jmen domény

Server iSeries ukládá tyto informace o konfiguraci do profilu připojení. Tyto informace poskytují nutný kontext pro server iSeries, aby mohl ustanovit připojení PPP k jinému počítačovému systému. Profil připojení obsahuje následující informace:

- **Typ protokolu.** Můžete si vybrat mezi PPP a SLIP. IBM doporučuje, abyste používali PPP, kdykoli je to možné.
- **Výběr režimu.** Typ připojení a provozní režim tohoto profilu připojení.

Typ připojení uvádí typ linky, na které dochází k připojení, a to, zda tato připojení jsou, nebo nejsou, **vytáčená** nebo **přijímaná** (odesílatel nebo příjemce). Můžete si vybrat mezi těmito typy připojení:

- komutovaná linka
- pronajatá (vyhrazená) linka
- L2TP (virtuální linka)
- PPPoE (virtuální linka)

PPPoE je jediný podporovaný protokol pro profily odesílatele připojení.

- **Provozní režim.** Dostupný provozní režim závisí na typu připojení. Viz níže uvedená tabulka: Profily připojení odesílatele naleznete v níže uvedené tabulce:

Tabulka 1. Dostupné provozní režimy pro profily připojení odesílatele.

Typ připojení	Dostupné provozní režimy
komutovaná linka	<ul style="list-style-type: none"> – vytáčení – vytáčení na požádání (pouze vytáčení) – vytáčení na požádání (vyhrazený peer s možností odpovídat) – vytáčení na požádání (umožněný vzdálený peer)
pronajatá linka	iniciátor
L2TP	<ul style="list-style-type: none"> – iniciátor – iniciátor pro více přechodů – vzdálené vytáčení
PPP přes Ethernet	iniciátor

Profily připojení příjemce naleznete v následující tabulce:

Tabulka 2. Dostupné provozní režimy pro profily připojení příjemce.

Typ připojení	Dostupné provozní režimy
komutovaná linka	odpověď
pronajatá linka	terminátor
L2TP	terminátor (síťový server)

- **Konfigurace linky.** Uvádí typ služby linky, kterou toto připojení používá.

Tyto volby závisí na typu voleného režimu, který vyberete. Pro komutovanou linku a pronajatou linku si můžete vybrat z následujících možností:

- jediná linka
- společná oblast linek
- integrovaná linka ISDN

Pro všechny jiné typy připojení (pronajatá linka, L2TP, PPPoE) je jako služba linky možná pouze jediná linka.

Podpora metod skupiny

Podpora metod skupiny umožňuje síťovým administrátorům definovat metody skupin uživatelů pro snazší správu prostředků, zajišťuje přiřazování metod řízení přístupu jednotlivým uživatelům, když se přihlašují do sítě v relaci PPP nebo L2TP. Celá koncepce spočívá v tom, že uživatele lze identifikovat jako patřícího do určité třídy uživatelů, přičemž každá třída má svou vlastní jedinečnou metodu. Každá jedinečná metoda skupiny umožňuje definovat omezení prostředků, jako je třeba počet linek přípustných ve svazku vícenásobného připojení, atributy, jako třeba odeslání IP, a identifikaci toho, jaká filtrovací pravidla paketu IP se použijí. Pomocí podpory metody skupiny mohou správci sítě definovat například skupinu pracující_doma, což této třídě uživatelů poskytne plný přístup k síti, kdežto skupina prodejci_pracovníci může mít přístup pouze k omezenější sadě služeb.

Příklad naleznete ve scénáři Správa přístupu uživatelů k prostředkům pomocí metod přístupu skupiny a filtrování IP adres.

Kapitola 5. Plánování PPP

Vytvoření a správa připojení PPP vyžaduje dobrou znalost podpory PPP a alternativ připojení na serverech iSeries a také mnoha dalších plánů uspořádání sítě a zabezpečení dat, které váš podnik používá.

Následující části vám mohou pomoci seznámit se s dostupnými volbami a požadavky pro připojení PPP na serveru iSeries.

Softwarové a hardwarové požadavky

Produkt iSeries Navigator V4R4 a vyšší verze podporují připojení PPP. V této části naleznete seznam dalších požadavků.

Alternativy připojení

Server iSeries podporuje připojení PPP na různých médiích, počínaje analogovými či digitálními telefonními linkami, až po vyhrazená nebo částečná připojení T1. V této části naleznete popis podporovaných voleb připojení.

Příslušenství pro připojení

Servery iSeries používají pro obsluhování připojení PPP modemy, adaptéry terminálu ISDN, adaptéry Token-ring, adaptéry typu Ethernet nebo zařízení CSU/DSU. V této části naleznete informace o podporovaném hardwaru.

Zacházení s IP adresou

Připojení PPP mají několik voleb pro přiřazování IP adres a filtraci IP paketů při připojení. Pod tímto námětem naleznete popisy těchto voleb.

Autentizace systému

Server iSeries může autentizovat vytáčená připojení pomocí ověřovacího seznamu a výměny hesel nebo pomocí serveru RADIUS. Rovněž poskytuje autentizační informace systémům, k nimž se připojuje. V této části naleznete popis voleb autentizace.

Pokyny ohledně šířky pásma

Server iSeries podporuje protokol vícenásobných připojení pro připojení PPP. To vám umožňuje použít více analogových telefonních linek pro jedno připojení, čímž zvýšíte šířku pásma. V této části naleznete přehled této podpory.

Softwarové a hardwarové požadavky

Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, server iSeries, může být buď odesílatel, nebo příjemce. Tento server iSeries musí splňovat následující nezbytné požadavky, aby k němu vzdálené systémy mohly přistupovat.

- Produkt **iSeries Navigator** V4R4 nebo vyšší verze podporující protokol TCP/IP.
- Jeden z těchto dvou profilů připojení:
 - Profil připojení odesílatele pro práci s odchozím připojením PPP.
 - Profil připojení příjemce pro práci s příchozím připojením PPP.
- Konzole na pracovní stanici PC instalovaná s nainstalovaným produktem **iSeries Access for Windows (95/98/NT/Millennium/2000/XP)** a produktem iSeries Navigator.
- Instalovaný adaptér.

Můžete si vybrat některý z následujících adaptérů:

- 2699*: dvoulinkový WAN IOA.
- 2720*: PCI WAN/Twinaxial IOA.
- 2721*: PCI dvoulinkový WAN IOA.
- 2745*: PCI dvoulinkový WAN IOA (nahrazuje IOA 2721).
- 2742*: dvoulinkový IOA (nahrazuje IOA 2745).
- 2750: PCI ISDN V.90 Basic Rate Interface U IOA (2vodičové rozhraní).
- 2751: PCI ISDN V.90 Basic Rate Interface U IOA (4vodičové rozhraní).
- 2761: osmiportový analogový modem IOA.

- 2771: dvouportový WAN IOA modem s V.90 integrovaným na portu 1 a standardním komunikačním rozhraním na portu 2. Chcete-li používat port 2 adaptéru 2771, je nutný externí modem nebo adaptér terminálu ISDN s příslušným kabelem.
- 2772: dvouportový modem WAN IOA s integrovaným V.90.
- 2838: adaptér Ethernet pro připojení PPPoE.
- 2793*: dvouportový WAN IOA modem s V.92 integrovaným na portu 1 a standardním komunikačním rozhraním na portu 2. Chcete-li používat port 2 adaptéru 2793, je nutný externí modem nebo adaptér terminálu ISDN s příslušným kabelem. Nahrazuje IOA model 2771.
- 2805 čtyřportový WAN IOA s integrovaným analogovým modemem s integrovaným V.92. Nahrazuje modely 2761 a 2772.

* Tyto adaptéry vyžadují externí modem V.90 (nebo novější) nebo adaptér terminálu ISDN a kabel RS232 nebo kompatibilní.

- Jednu z následujících komponent - závisí na typu připojení a lince:
 - externí nebo interní modem nebo jednotka služby kanálu (CSU)/jednotka datové služby (DSU)
 - adaptér terminálu ISDN
- Jestliže plánujete, že se budete připojovat k Internetu, potřebujete si zajistit účet u ISP (poskytovatel služeb sítě Internet) pro vytáčené připojení. Váš ISP by vám měl poskytnout nutná telefonní čísla a informace o připojení k Internetu.

Alternativy připojení

PPP může přenášet datagramy po sériových linkách PPP. Protokol PPP umožňuje vzájemně propojit více vybavení od různých dodavatelů a více protokolů tím, že udává standard komunikace PPP. Vrstva datového spoje PPP používá rámcování podobné HDLC pro zapouzdření datagramů přenášených na asynchronních i synchronních telekomunikačních linkách.

Zatímco PPP podporuje širokou škálu typů linek, SLIP podporuje pouze asynchronní typy linek. SLIP se obvykle používá pouze pro analogové linky. Lokální telefonní společnosti nabízejí tradiční telefonní služby, kdy s rostoucími možnostmi roste i cena. Tyto služby využívají stávající síť telefonní společnosti mezi zákazníkem a telefonní ústřednou.

Linky PPP ustanovují fyzické propojení mezi lokálním a vzdáleným hostitelem. Propojené linky poskytují vyhrazenou šířku pásma. Nabízejí se také s nejrůznějšími přenosovými rychlostmi a protokoly. S linkou PPP si můžete vybírat z následujících alternativ připojení:

- analogové telefonní linky
- digitální služby a DDS
- komutovaná linka 56
- ISDN
- T1/E1 a částečná T1
- přenos rámce
- podpora L2TP (tunel) pro připojení PPP
- podpora PPPoE (DSL) pro připojení PPP

Analogové telefonní linky

Analogové připojení, které používá modemy pro přenos dat přes pronajatou nebo komutovanou telefonní linku, je nejnižší z možností využití PPP. Pronajaté linky představují trvalá propojení mezi dvěma zadanými místy, kdežto komutované linky jsou běžné telefonní linky. Nejrychlejší modemy nyní pracují s přenosovou rychlostí 56 Kbps u nekomprimovaných dat. Avšak kvůli poměru signál/šum na neupravených hlasových telefonních okruzích je tato rychlost často nedosažitelná.

Tvrzení výrobců o vyšších přenosových rychlostech v bitech za sekundu (bps) se obvykle zakládají na algoritmu komprese dat (CCITT V.42bis), který jejich modemy používají. Ačkoli V.42bis má potenciální možnost dosahovat až čtyřnásobného snížení objemu dat, komprese závisí na samotných datech a zřídka dosahuje 50%. Objem dat, která jsou již komprimována nebo zakódována, se při použití V.42bis může dokonce zvětšit. X2 nebo 56Flex rozšiřuje přenosovou rychlost analogových telefonních linek až na 56 Kbps. Jedná se o hybridní technologii, která vyžaduje, aby jeden konec linky PPP byl digitální a druhý analogový. Kromě toho, rychlost 56 Kbps se používá pouze tehdy, když přenášíte data z digitálního konce do analogového konce připojení. Tato technologie je velmi vhodná pro připojení k ISP, kteří mají na svém pracovišti digitální konec propojení a hardware. Obvykle se můžete připojovat k analogovému modemu V.24 přes sériové rozhraní RS232 s asynchronním protokolem při rychlostech až do 115,2 Kbps.

Standard V.90 ukončil otázku kompatibility K56flex/x2. Standard V.90 je výsledkem kompromisu mezi tábory x2 a K56flex na poli výroby modemů. Díky tomu, že veřejná komutovaná síť je považována za digitální síť, může technologie V.90 přenášet data z Internetu do počítače rychlostí, která může dosáhnout 56 Kbps. Technologie V.90 se liší od jiných standardů, protože data digitálně kóduje místo toho, že by je modulovala jako analogové modemy. Přenos dat je asymetrická metoda, takže přenosy v protisměru (většinou pokyny klávesnice a myši počítače určené pro centrální systém - přenosy, pro které postačuje nižší šířka pásma) nadále probíhají rychlostí 33,6 Kbps. Data odeslaná z modemu se odesílají jako analogové přenosy, které představují standard V.34. Pouze u datových přenosů po směru se uplatňují výhody vysokých rychlostí V.90.

Standard V.92 je vylepšením standardu V.90 v tom smyslu, že umožňuje dosahovat v protisměru až rychlosti 48 Kbps. Kromě toho je možné časy připojení snížit díky vylepšenému procesu navazování spojení a rovněž tomu, že modemy podporující funkci "zadržení" mohou nyní zůstat připojeni, když telefonní linka přijímá příchozí hovor nebo čeká na volání.

Digitální služby a DDS

Digitální služba

Digitální služba znamená, že data se po celé trase, tzn. od počítače odesílatele do ústředny telefonní společnosti, k poskytovateli dálkových přenosů, do telefonní ústředny a dále do počítače příjemce přenášejí v digitální podobě. Přenos digitálního signálu nabízí větší šířku pásma a vyšší spolehlivost než přenos analogového signálu. Systém digitálního přenosu signálu eliminuje mnohé problémy, s nimiž se musí analogové modemy vypořádávat, například šum, nestálá kvalita linky a zeslabení signálu.

DDS

Digitální datové služby (DDS) jsou úplným základem datových služeb. Linky DDS jsou pronajata trvalá připojení, která komunikují pevnou rychlostí až 56 Kbps. Tato služba se také běžně označuje jako DS0.

K lince DDS se můžete připojit pomocí speciálního zařízení nazvaného jednotka služby kanálu/jednotka datové služby (CSU/DSU), které slouží místo modemu v analogovém uspořádání. DDS má fyzická omezení, která souvisejí hlavně se vzdáleností mezi CSU/DSU a ústřednou telefonní společností. DDS pracuje nejlépe, když je vzdálenost menší než 9 kilometrů. Telefonní společnosti mohou obsluhovat delší vzdálenosti pomocí zesilovačů signálu, ale tato služba je nákladnější. DDS se nejvíce hodí pro připojení dvou míst, která mají tutéž telefonní ústřednu. U dálkových propojení přes několik telefonních ústředn mohou poplatky za meziměstské spojení narůst tak, že je služba DDS nepraktická. V těchto případech může být lepším řešením komutovaná linka 56. Obvykle se můžete připojit k DDS CSU/DSU přes sériové rozhraní V.35, RS449 nebo X.21 se synchronním protokolem při rychlostech až do 56 Kbps.

Komutovaná linka 56

Jestliže nepotřebujete trvalé připojení, můžete ušetřit peníze tak, že použijete komutovanou digitální službu, které se běžně říká komutovaná linka 56 (SW56). Linka SW56 se podobá službě DDS v tom, že DTE se připojuje k digitální službě prostřednictvím CSU/DSU. Linka SW56 CSU/DSU však zahrnuje číselník, na kterém zadáváte telefonní číslo vzdáleného hostitele. Linka SW56 vám umožní vytvářet digitální připojení k libovolnému účastníkovi služby SW56, který je kdekoli ve vaší zemi nebo i za hranicemi. Volání SW56 se

přenáší na dlouhou vzdálenost po digitální síti, jako by to bylo digitální hlasové volání. Služba SW56 využívá stejná telefonní čísla jako lokální telefonní systém a poplatky za používání jsou stejné jako poplatky za komerční telefonické hovory. Služba SW56 se používá jedině v sítích v severní Americe a je omezena pouze na jediný kanál, kterým lze pouze přenášet data. Služba SW56 je alternativou v těch místech, kde není k dispozici služba ISDN. Obvykle se můžete připojit k SW56 CSU/DSU přes sériové rozhraní V.35 nebo RS 449 se synchronním protokolem při rychlostech až do 56 Kbps. S volací/přijímací jednotkou V.25bis se data a volání přenášejí po jediném sériovém rozhraní.

ISDN

Podobně jako komutovaná linka 56 i ISDN poskytuje digitální připojení dvou koncových bodů po komutované lince. Avšak na rozdíl od jiných služeb, ISDN může přenášet hlas i data na stejném připojení. Existují různé druhy ISDN služeb, přičemž nejběžnější je BRI (rozhraní se základní přenosovou rychlostí). BRI se skládá ze dvou 64Kbps kanálů B pro přenášení dat zákazníka a jednoho kanálu D pro přenos signalizačních dat. Dva kanály B mohou být spojeny tak, aby dohromady poskytovaly rychlost 128 Kbps. V některých oblastech může telefonní společnost omezit každý kanál B na rychlost 56 Kbps neboli dohromady 112 Kbps. Existují zde také fyzická omezení v tom smyslu, že zákazník musí být vzdálen do 5,5 kilometru od hlavní telefonní ústředny. Tuto vzdálenost lze rozšířit pomocí opakovačů. K ISDN se můžete připojit pomocí zařízení, kterému se říká adaptér terminálu. Většina adaptérů terminálu má integrovanou jednotku ukončení sítě (NT1), která umožňuje přímé zapojení do telefonní zástrčky. Adaptéry terminálu se obvykle připojují k vašemu počítači přes asynchronní linku RS232 a pro nastavení a ovládání používají příkazy AT stejně jako konvenční analogové modemy. Každá značka adaptéru má své vlastní rozšíření příkazů AT pro nastavení parametrů, jež jsou pro ISDN jedinečné. Dříve se vyskytovalo mnoho problémů ohledně schopnosti spolupráce adaptérů terminálu ISDN různých značek. Tyto problémy byly většinou zapříčiněny různorodostí protokolů přizpůsobení rychlosti ve V.110 a V.120 stejně jako schémata vázání pro dva kanály B.

V tomto odvětví se nyní přešlo na synchronní protokol PPP s více kanály PPP pro napojování obou kanálů B. Výrobci některých adaptérů terminálu integrují do svých adaptérů terminálu schopnost V.34 (analogový modem). To umožňuje zákazníkům, kteří mají jednu linku ISDN, pracovat s ISDN i konvenčními analogovými voláními, přičemž mohou využívat toho, že služba ISDN umožňuje simultánně přenášet hlas a data. Nová technologie také umožňuje, aby adaptér terminálu fungoval jako digitální serverová strana pro klienty 56K(X2/56Flex).

Obvykle se budete chtít připojit k adaptéru terminálu ISDN přes sériové rozhraní RS232 pomocí asynchronního protokolu při rychlostech až do 230,4 Kbps. Avšak maximální rychlost přenosu serveru iSeries vyjádřená v baudech pro asynchronní přenos přes RS232 je 115,2 Kbps. To nás bohužel omezuje na maximální přenosovou rychlost 11,5 kilobajtů/s, kdežto adaptér terminálu s více linkami může přenášet za sekundu až 14/16 kilobajtů nekomprimovaných dat. Některé adaptéry terminálu podporují synchronní přenosy přes RS232 při rychlostech 128 Kbps, ale maximální rychlost synchronního přenosu přes RS232 na serveru iSeries je 64 Kbp.

Server iSeries je schopen spouštět asynchronní přenosy přes V.35 při rychlostech až do 230,4 Kbps, ale výrobci adaptérů terminálu obvykle takovou konfiguraci nenabízejí. Konvertory rozhraní, které konvertují RS232 na rozhraní V.35, by snad byly přiměřeným řešením problému, ale tento přístup nebyl vyhodnocen pro server iSeries. Další možností je používat adaptéry terminálu se synchronním protokolem rozhraní V.35 při rychlosti 128 Kbps. Třebaže tato třída adaptérů terminálu existuje, zdá se, že jen málo z nich nabízí synchronní PPP vícenásobných připojení.

T1/E1 a částečná T1

T1/E1

Připojení T1 spojuje celkem dvacet čtyři kanálů 64 Kbps (DS0) TDM (time division multiplexed) přes 4žilový měděný obvod. Tak vzniká celková šířka pásma 1,544 Mbps. Obvod E1 používaný v Evropě a jiných částech světa spojuje třicet šest kanálů 64 Kbps, čímž se dosahuje kapacity 2,048 Mbps. TDM umožňuje více uživatelům, aby sdíleli prostředek digitálních přenosů tak, že používají předem alokované časové sloty. Mnoho digitálních PBX využívá službu T1 pro import více volacích obvodů přes jednu linku T1, místo aby

měli 24 dvoulinek mezi PBX a telefonní společností. Je důležité uvést, že T1 lze sdílet mezi hlasovými a datovými přenosy. Telefonní služba může být zajišťována určitou částí z těchto 24 kanálů v lince T1, přičemž zbývající kanály lze používat pro připojení k Internetu. Pro správu 24 DS0 kanálů je nutné zařízení T1 multiplexer, když více služeb sdílí svazek T1. Pro jediné výhradně datové připojení může obvod pracovat bez stanovených kanálů (na signálu se neprovádí žádné TDM). V důsledku toho lze použít jednodušší zařízení CSU/DSU. Obvykle se můžete připojit k T1/E1 CSU/DSU nebo zařízení multiplexer přes sériové rozhraní V.35 nebo RS 449 se synchronním protokolem s rychlostí, která je násobkem hodnoty 64 Kbps, až do 1,544 Mbps nebo 2,048 Mbps. Zařízení CSU/DSU nebo multiplexer poskytuje měření času v síti.

Částečná služba T1

S částečnou službou T1 (FT1) si zákazník pronajímá přenosovou kapacitu, která je násobkem 64 Kbps a využívá linky T1. FT1 je užitečná tam, kde by náklady na jednouživatelskou linku T1 zákazníkům neumožňovaly skutečné používání šířky pásma. S FT1 si můžete zaplatit pouze to, co potřebujete. Služba FT1 má navíc následující funkci, která není k dispozici v úplném obvodu T1: Multiplexing kanálů DS0 v ústředně telefonní společnosti. Vzdálený konec obvodu FT1 je na přepínači Digital Access Cross-Connect Switch, který udržuje telefonní společnost. Systémy, které sdílejí stejný digitální přepínač, mohou přepínat mezi kanály DS0. Toto schéma je oblíbené u ISP, kteří používají jediný svazek T1 ze svého pracoviště k digitálnímu spínači telefonní společnosti. V těchto případech může být více klientů obslouženo službou FT1. Obvykle se můžete připojit k T1/E1 CSU/DSU nebo zařízení multiplexer přes sériové rozhraní V.35 nebo RS 449 se synchronním protokolem rychlostí, která je násobkem hodnoty 64 Kbps. S FT1 máte předem vyhrazenou určitou část z 24 kanálů. T1 multiplexer musí být konfigurovaný tak, aby plnil pouze ty časové sloty, které jsou přiřazeny vaší službě.

Přenos rámce

Přenos rámce je protokol pro směrování rámců pomocí sítě na základě pole adresy (identifikátor připojení datového spoje) v rámci a pro správu přenosové cesty nebo virtuálního připojení.

Sítě s přenosem rámce v USA podporují pro přenos dat rychlosti T-1 (1,544 Mbps) a T-3 (45 Mbps). O přenosu rámce můžete přemýšlet jako o způsobu využití stávajících linek T-1 a T-3, které vlastní poskytovatel služeb. Většina telefonních společností nyní poskytuje službu přenosu rámce těm zákazníkům, kteří chtějí připojení s rychlostí od 56 Kbps do T-1. (V Evropě se rychlosti přenosu rámce různí v rozsahu od 64 Kbps do 2 Mbps. V USA je přenos rámce velmi populární, protože je relativně laciný. V některých oblastech se však nahrazuje rychlejšími technologiemi, například ATM.)

Podpora L2TP (tunel) pro připojení PPP

Protokol L2TP (Layer 2 Tunneling Protocol) je protokol tunelu, který rozšiřuje PPP tak, aby podporoval tunel na vrstvě linky mezi požadujícím klientem L2TP (koncentrátor přístupu L2TP nebo LAC) a cílovým koncovým serverem L2TP (síťový server L2TP nebo LNS). Pomocí tunelů L2TP je možné oddělit pracoviště, na kterém končí komutovaný protokol a kde je zajištěný přístup do sítě - proto se L2TP označuje také jako virtuální PPP. Protokol L2TP je zdokumentován jako norma RFC2661 (Request For Comment). Další informace o RFC najdete na adrese <http://www.rfc-editor.org>. Tunel L2TP se může rozšířit na celou relaci PPP nebo pouze na jeden segment relace složené ze dvou segmentů. To může představovat čtyři odlišné modely tunelu:

- nepovinný tunel
- povinný tunel - příchozí volání
- povinný tunel - vzdálené vytáčení
- připojení L2TP s více přechody

Nepovinný tunel

V nepovinném tunelu si tunel vytváří uživatel, obvykle pomocí klienta, který má povolený L2TP. Probíhá to tak, že uživatel odesílá pakety L2TP poskytovateli služeb sítě Internet (ISP), který je odesílá do LNS. Při

používání nepovinného tunelu nepotřebuje ISP podporu L2TP a indikátor tunelu L2TP vlastně zůstává na stejném systému jako vzdálený klient. V tomto modelu se tunel rozkládá na celé relaci PPP od klienta L2TP až po LNS.

Model povinného tunelu - příchozí volání

V modelu povinného tunelu - příchozí volání se tunel vytváří, aniž by uživatel podnikl nějakou akci a aniž by měl nějakou volbu. Probíhá to tak, že uživatel odešle pakety PPP do ISP (LAC), který je zapouzdří do L2TP a odešle je tunelem do LNS. Při povinném tunelu musí mít ISP povolený L2TP. V tomto modelu se tunel rozkládá pouze přes segment relace PPP mezi ISP a LNS.

Model povinného tunelu - vzdálené vytáčení

V modemu povinného tunelu - vzdálené vytáčení domovská brána (LNS) iniciuje tunel k ISP (LAC) a dá pokyny ISP, aby lokální volání umístil do odpovídajícího klienta PPP. Tento model je určený pro ty případy, kdy má vzdálený odpovědní klient PPP trvale zavedené telefonní číslo u ISP. Tento model se má používat, když společnost se zavedenou přítomností na Internetu potřebuje ustanovovat připojení se vzdálenou kancelář, která potřebuje vytáčenou linku. V tomto modelu se tunel rozkládá pouze přes segment relace PPP mezi LNS a ISP.

Připojení L2TP s více přechody

Připojení L2TP s více přechody je způsob přeměrování přenosů L2TP ve prospěch klientských LAC a LNS. Připojení s více přechody se ustanovuje pomocí brány L2TP pro více přechodů (systém, který spojuje profil terminátoru L2TP a profil iniciátoru L2TP). Chcete-li ustanovit připojení s více přechody, brána L2TP pro více přechodů bude působit jako LNS pro skupinu LAC a zároveň jako LAC pro daný LNS. Tunel se ustanovuje z klienta LAC na bránu pro více přechodů L2TP, a pak se ustanovuje jiný tunel mezi bránou L2TP pro více přechodů a cílovým LNS. Přenosy L2TP z klientského LAC se pak přeměrují bránou L2TP pro více přechodů do cílového LNS a přenosy z cílového LNS se přeměrují do klientského LAC.

Podpora PPPoE (DSL) pro připojení PPP

DSL označuje třídu technologie, která se používá pro získání větší šířky pásma na stávajících měděných telefonních kabelech, které jsou položeny mezi budovou zákazníka a poskytovatelem služeb sítě Internet (ISP). Umožňuje simultánní hlasové a vysokorychlostní datové služby na jediném páru měděných telefonních kabelů. Rychlosti modemů se postupně zvyšovaly pomocí různých způsobů komprese a jiných technologií, ale dnešní maximální rychlost (56 kbit/s) dosahuje teoretické mezní hodnoty této technologie. Technologie DSL umožňuje dosahovat na linkách s kroucenou dvojlínkou mnohem vyšší rychlosti z telefonní ústředny do vlastního domu, do školy nebo do zaměstnání. V některých oblastech jsou dosažitelné rychlosti až do 2 megabitů za sekundu, což je třicetkrát či ještě vícekrát rychlejší než dnešní nejrychlejší modemy. Zkratka PPPoE znamená protokol PPP přes Ethernet. PPP se obvykle používá pro sériovou komunikaci jako například pro vytáčená modemová připojení. Mnozí poskytovatelé internetové služby DSL nyní používají PPP přes Ethernet, protože má rozšířené funkce pro přihlašování a zabezpečení dat. Co je modem DSL? "Modem" DSL je zařízení, které je umístěno na obou koncích měděné telefonní linky, aby umožnilo počítači (nebo LAN) připojení k Internetu pomocí připojení DSL. Na rozdíl od vytáčeného připojení není obvykle nutné mít jedinouživatelskou telefonní linku (POTS rozdělovač kanálů umožňuje simultánní sdílení linky). Služba DSL se považuje za následující generaci modemové technologie. Ačkoli DSL modemy vypadají podobně jako konvenční analogové modemy, poskytují mnohem větší propustnost.

Vybavení pro připojení

Toto jsou tři typy komunikačních zařízení, která můžete ve svém prostředí PPP používat.

- modemy
- CSU/DSU
- adaptéry terminálu ISDN
- adaptéry Ethernet typ 2838 (pro připojení PPPoE)
-

Modemy

Pro připojení PPP lze používat externí i interní modemy. Příkazová sada používaná v modemu je obvykle popsána v dokumentaci k modemu. Příkazy se používají pro nulování a inicializaci modemu i pro vytočení telefonního čísla vzdáleného systému. Každý model modemu se musí nejprve definovat, a teprve pak je možné jej použít s profilem připojení PPP, protože odlišné modely modemů mají odlišné inicializační příkazové řetězce. Pokud se jedná o interní modem, řetězce modemu jsou již pro jeho používání definovány.

Server iSeries má předdefinováno mnoho modelů modemů a nové modely lze definovat prostřednictvím produktu iSeries Navigator. Existující definici můžete použít jako základ pro nový typ, který chcete definovat. Pokud si nejste jisti tím, jaké příkazy váš modem používá, nebo pokud nemáte přístup k dokumentaci modemu, začněte s definicí modemu Generic Hayes. Předdefinované definice nelze měnit. Do existujícího inicializačního řetězce příkazů nebo vytáčení lze však přidávat další příkazy.

Pro ustanovení připojení PPP můžete použít modem ESC, který se dodává se serverem iSeries. Na starších systémech byl modem ECS externí modem IBM 7852-400. Na novějších systémech lze jako modemy ECS použít interní modemy 2771 nebo 2772.

CSU/DSU

CSU (jednotka služby kanálu) je zařízení, které připojuje terminál k digitální lince. Jednotka datové služby (DSU) je zařízení, které provádí ochranné a diagnostické funkce pro telefonní linku. Tato dvě zařízení se obvykle dodávají jako jedna jednotka CSU/DSU.

Jednotku CSU/DSU si můžete představit jako velmi výkonný a nákladný modem. Toto zařízení je zapotřebí umístit na oba konce připojení T-1 nebo T-3; jednotky na obou koncích musejí být od stejného výrobce.

Adaptéry terminálu ISDN

ISDN vám poskytuje digitální připojení, které vám umožní komunikovat pomocí libovolné kombinace hlasu, dat, videa a dalších multimediálních aplikací.

Ověřte, zda je váš adaptér terminálu schválený pro použití na serveru iSeries:

- Část Doporučení adaptéru terminálu ISDN uvádí, jaký adaptér terminálu se doporučuje použít.
- Část Omezení adaptéru terminálu ISDN obsahuje informace o nejrůznějších adaptérech terminálu, které byly testovány se serverem iSeries, a jejich stručné hodnocení.

Při konfiguraci adaptéru terminálu proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Klepněte pravým tlačítkem myši na **Modemy** a vyberte **Nový modem**.
3. Do dialogového okna Vlastnosti nového modemu zadejte správné hodnoty do všech okének na oušku Obecné. Neopomeňte jako komunikační zařízení uvést adaptér terminálu ISDN.
4. Vyberte ouško **Parametry ISDN**.
5. Přidejte nebo změňte vlastnosti ISDN na oušku **Parametry ISDN** tak, aby vyhovovaly vlastnostem, které vyžaduje váš adaptér terminálu.

Na příkladu konfigurace adaptéru terminálu ISDN si můžete prohlédnout vzorové procedury, které používají produkt iSeries Navigator.

Doporučení adaptéru terminálu ISDN

Doporučený externí adaptér terminálu ISDN, neboli ISDN modem, je **3Com/U.S. Robotics Courier I ISDN V.cokoli**. Podporuje analogová modemová připojení V.34, připojení V.90 (X2), V.92 a PPP vícenásobných připojení na lince ISDN v režimu odesílatele i režimu odpovědi na serveru iSeries. Rovněž automaticky

podporuje protokol CHAP (Challenge Handshake Authentication) na připojení ISDN PPP. K dispozici jsou také následující adaptéry terminálu ISDN: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA a ADtran ISU 2x64 Dual Port.

- **Připojení iniciovaná ze serveru iSeries.** Na výzvy CHAP pocházejí ze strany příjemce odpovídá adaptér terminálu Courier I, zatímco probíhá vyjednávání autentizace PAP (Password Authentication Protocol) se serverem iSeries. Odpovědi PAP se na připojení ISDN neobjevují.
- **Připojení, na která server iSeries odpovídá.** Courier I vyžaduje autentizaci CHAP volající stranou, jestliže se na základě konfigurace odpovědi serveru iSeries otevře autentizace po výzvě CHAP. Pokud server iSeries zahájí autentizaci pomocí PAP, adaptér terminálu Courier I se pomocí PAP ověří.

Jestliže používáte modem Courier I, který je starší než verze 1999, ověřte, zda je modem Courier I připojený na serveru iSeries pomocí kabelu V.35, abyste zajistili co nejvyšší výkon připojení ISDN. S modemem Courier I se dodává kabel RS-232 na V.35; starší verze tohoto kabelu však mají nesprávný konektor V.35. Kabel vám vymění středisko zákaznické podpory 3Com/US Robotics.

Poznámka: Podle společnosti 3Com/US Robotics se verze V.35 tohoto adaptéru terminálu již neprodává, ale některé mohou být ještě u dodavatelů, tzv. třetích stran. Verze RS-232 se stále doporučuje i přes trochu omezený výkon na serveru iSeries, neboť připojení RS-232 jsou omezena na 115,2 Kb.

Adaptér V.35 na RS-232 obdržíte od společnosti Black Box Corporation. Číslo dílu je FA-058.

Neopomeňte nastavit rychlost linky V.35 serveru iSeries na 230,4 Kbps.

Omezení adaptérů terminálu ISDN

Byly hodnoceny níže uvedené adaptéry terminálu. Doporučují se pouze pro iniciaci vzdálených připojení ISDN ze serveru iSeries.

3Com Impact IQ ISDN:

Tento adaptér terminálu se pro server iSeries nedoporučuje z následujících důvodů:

- Adaptér terminálu nepodporuje analogová modemová připojení V.34. Může však podporovat analogová modemová připojení V.34, pokud se používá připojení RJ-11.
- Adaptér terminálu v současné době nepodporuje připojení V.90.
- Adaptér terminálu se nemůže připojovat k serveru iSeries větší rychlostí než 115200 bps.
- Adaptér terminálu nepodporuje automaticky protokol CHAP (Challenge Handshake Authentication). Avšak nastavení S84=0 umožňuje serveru iSeries provádět autentizaci CHAP.
- Server iSeries není schopen určit, kdy připojení skončilo, jestliže monitoruje signál DSR (data set ready) od adaptéru terminálu. To představuje pro systém potenciální riziko zabezpečení.

Motorola BitSurfr Pro ISDN:

Tento adaptér terminálu se pro server iSeries nedoporučuje z následujících důvodů:

- Adaptér terminálu nepodporuje analogová modemová připojení V.34. Může však podporovat analogová modemová připojení V.34, pokud se používá připojení RJ-11.
- Adaptér terminálu v současné době nepodporuje připojení V.90.
- Adaptér terminálu se nemůže připojovat k serveru iSeries větší rychlostí než 115200 bps.
- Adaptér terminálu nepodporuje automaticky autentizaci CHAP. Avšak nastavení @M2=C umožňuje serveru iSeries provádět autentizaci CHAP.
- Adaptér terminálu neumožňuje automatické odpovídání na jednorázová volání PPP ani PPP s vícenásobným připojením. Vzdálený iniciační adaptér terminálu musí být nastavený na stejný protokol (jedna linka nebo vícenásobné připojení) jako odpovídající adaptér terminálu.

- Hardwarový mechanismus řízení toku na serveru iSeries nepracuje s tímto adaptérem terminálu správně. To vede ke snížení výkonu, když server iSeries zasílá data na vícenásobné připojení PPP.

Jak pracovat s IP adresou

Připojení PPP umožňuje několik různých množin voleb pro správu IP adres v závislosti na typu profilu připojení, což umožňuje, aby správa IP adres pro připojení PPP fungovala v rámci vaší síťové architektury hladce a bez problémů. Informace o definování schématu IP adres na své síti získáte v následujících částech:

- DHCP
DHCP může centrálně spravovat přiřazování IP adres ve vaší síti. Dozvíte se, jak na síti nastavit a spravovat služby DHCP.
- DNS
DNS vám může pomoci spravovat hostitelská jména a jejich přidružené IP adresy. Dozvíte se, jak v síti nastavit a spravovat služby DNS.
- BOOTP
BOOTP se používá pro přiřazení klientských pracovních stanic k serveru iSeries a k přiřazování IP adres těmto stanicím. Dozvíte se, jak v síti nastavit a spravovat služby BOOTP.
- Filtrování IP paketů
Omezte uživatelům a skupinám přístup ke konkrétním IP adresám tak, že vytvoříte soubor filtrovacích pravidel IP. Dozvíte se o podpoře filtrování IP a o tom, jak filtrování implementovat na své síti.

Než začnete konfigurovat profil připojení PPP, měli byste dobře znát strategii správy IP adres ve své síti. Tato strategie má vliv na mnohá rozhodnutí při procesu konfigurace, která se mimo jiné týkají i strategie autentizace, otázek zabezpečení a nastavení TCP/IP.

Profily připojení odesílatele:

Lokální a vzdálené IP adresy definované pro profil odesílatele se obvykle budou definovat jako **přiřazené vzdáleným systémem**. To umožňuje administrátorům na vzdáleném systému ovládat IP adresy, které se použijí pro připojení. Téměř všechna připojení k poskytovatelům služeb sítě Internet (ISP) budou definována tímto způsobem, třebaže mnozí ISP mohou za příplatek nabídnout fixní IP adresy.

Jestliže definujete fixní IP adresy pro lokální nebo vzdálenou IP adresu, pak se musíte ujistit, že vzdálený systém je definován na přijímání adres, které nastavíte vy. Obvyklým způsobem je definovat svou lokální adresu jako fixní IP adresu a vzdálenou nechat přiřazovat vzdáleným systémem. Systém, k němuž se připojujete, lze definovat stejným způsobem, takže jakmile se připojíte, oba systémy zjistí adresu vzdáleného systému tak, že si vzájemně vymění adresy. To může být užitečné, když jedna kancelář volá do druhé kanceláře pro dočasné připojení.

Další otázkou je, zda chcete povolit skrývání IP adres. Například, když se server iSeries připojuje k Internetu prostřednictvím ISP, pak by skrývání adres mohlo připojené síti za serverem iSeries také umožňovat přístup k Internetu. Server iSeries bude vlastně "skrývat" IP adresy systémů v síti za lokální IP adresu přiřazenou od ISP, jakoby veškeré přenosy pocházely ze serveru iSeries. Pro oba systémy v síti LAN je nutné ještě zvážit otázky dodatečného směrování (aby jejich internetové přenosy byly posílány do serveru iSeries) a také server iSeries, na kterém budete muset zaškrtnout okénko Přidat vzdálený systém jako předvolenou předepsanou cestu.

Profily připojení příjemce:

U profilů připojení příjemce je nutné zvážit více otázek a voleb ohledně IP adres než u profilu připojení odesílatele. To, jak budete konfigurovat IP adresy, závisí na plánu správy IP adres ve vaší síti, na vašich konkrétních požadavcích na výkon a funkci tohoto připojení a na plánu pro zabezpečení ochrany dat.

Lokální IP adresy

Pro jediný profil příjemce můžete na serveru iSeries definovat jedinečnou IP adresu nebo používat existující IP adresu. To bude adresa, která bude označovat stranu serveru iSeries v daném připojení PPP. Pro profily příjemců definovaných pro podporu souběžných vícenásobných připojení musíte použít existující lokální IP adresu. Pokud nejsou k dispozici žádné dříve existující lokální IP adresy, můžete za tímto účelem vytvořit virtuální IP adresu.

IP adresy vzdáleného systému

Existuje mnoho voleb pro přiřazování IP adres vzdáleného systému klientům PPP. Následující volby lze uvést na stránce **TCP/IP** u profilu připojení příjemce.

Poznámka: Jestliže chcete, aby vzdálený systém byl považován za součást sítě LAN, musíte konfigurovat směrování IP adres, zadat IP adresu z rozsahu IP adres systémů připojených k síti LAN a ověřit, že směrování pomocí IP je povoleno pro oba tyto profily připojení a pro systém iSeries.

Tabulka 3. Volby přiřazení IP adresy v profilu připojení příjemce

Volba	Popis
fixní IP adresa	Definujete jedinou IP adresu, která se má předat vzdáleným uživatelům, když se připojí. Jedná se o výhradně hostitelskou IP adresu (maska podsítě je 255.255.255.255) a slouží pouze pro profily příjemců jediného připojení.
společná oblast adres	Můžete definovat počáteční IP adresu a pak rozsah udávající, kolik dalších dodatečných IP adres se má definovat. Každý uživatel, který se připojí, pak dostane jedinečnou adresu z definovaného rozmezí. Jedná se o výhradně hostitelskou IP adresu (maska podsítě je 255.255.255.255) a slouží pouze pro profily příjemců více připojení.
RADIUS	Vzdálenou IP adresu a její masku podsítě určí server Radius. To je možné pouze tehdy, pokud je definováno následující: <ul style="list-style-type: none"> Podpora serveru Radius v oblasti autentizace a IP adresování je povolena v konfiguraci služeb serveru vzdáleného přístupu. Autentizace je povolena pro profil připojení příjemce a je definováno, že autentizace se provádí na dálku serverem Radius.
DHCP	Vzdálenou IP adresu určuje přímo nebo nepřímo server DHCP pomocí předávání DHCP. To je možné jen tehdy, pokud byla povolena podpora DHCP v konfiguraci služeb serveru vzdáleného přístupu. Jedná se o výhradně hostitelskou IP adresu (maska podsítě je 255.255.255.255).
na základě ID uživatele vzdáleného systému	Vzdálená IP adresa se určuje podle uživatelského ID definovaného pro vzdálený systém, když se provádí jeho autentizace. To umožňuje administrátorovi přiřadit různé vzdálené IP adresy (a jejich přiřazené masky podsítě) uživateli, který se připojí. To rovněž umožňuje definovat dodatečné přenosové cesty pro každé z těchto uživatelských ID, takže pro známého vzdáleného uživatele můžete prostředí přesně upravit. Má-li tato funkce řádně fungovat, musí být povolena autentizace.
definování dodatečných IP adres na základě uživatelského ID vzdáleného systému	Tato volba vám umožňuje definovat adresy založené na uživatelském ID vzdáleného systému. Tato volba se automaticky volí (a musí se použít), jestliže je metoda přiřazování vzdálených IP adres definována jako Na základě ID uživatele vzdáleného systému . Tato volba je také povolena pro tyto metody přiřazování adres: fixní IP adresa a společná oblast adres. Když se vzdálený uživatel připojí k serveru iSeries, provede se vyhledávání, aby se zjistilo, zda je nějaká vzdálená IP adresa definována konkrétně pro tohoto uživatele. Pokud je definována, použije se pro připojení tato adresa, maska a sada možných přenosových cest. Jestliže uživatel není definován, pak adresa nabývá předem stanovené hodnoty definované fixní IP adresy nebo další adresy ze společné oblasti IP adres.

Tabulka 3. Volby přiřazení IP adresy v profilu připojení příjemce (pokračování)

Volba	Popis
povolení vzdálenému systému definovat svou vlastní IP adresu	Tato volba umožňuje vzdálenému uživateli definovat své vlastní IP adresy, pokud o to požádají. Pokud nepožadují použití své vlastní adresy, vzdálená IP adresa se určí definovanou metodou přiřazování IP adres vzdáleného systému. Tato volba je zpočátku zablokována a měli byste ji použít po pečlivém uvážení.
směrování IP adres	Volající klient a server iSeries musí mít správně konfigurováno směrování IP adres, jestliže klient potřebuje přístup k nějakým IP adresám v síti LAN, ke které server iSeries patří.

Filtrování IP paketů

Filtrování IP paketů je mechanismus, který může omezit služby pro jednotlivého uživatele, když se přihlašuje do sítě. Filtrování paketů může "povolit" nebo "zamítnout" přístup na základě IP adres míst určení a/nebo na základě portů. Uplatňují se různé metody tak, že se definuje více sad pravidel filtrování paketů, z nichž má každá jedinečný identifikátor filtru PPP. Pravidla filtrování paketů lze přiřadit jednotlivému profilu připojení příjemce nebo je lze přiřadit pomocí skupinové strategie, která použije filtrovací pravidla na určitou kategorii uživatelů. Pravidla filtrování paketů nejsou sama o sobě definována v PPP, ale jsou definována pod pravidly IP paketů v rámci produktu iSeries Navigator. Další informace najdete pod tématem Pravidla IP paketu v rámci aplikace Information Center.

Pro připojení L2TP musí být použito VPN s filtrováním IP SEc, aby byl chráněn provoz v síti. Další informace naleznete pod tématem VPN v aplikaci Information Center.

Autentizace systému

Spojení PPP se serverem iSeries podporuje několik voleb pro autentizaci vzdálených klientů volajících do serveru iSeries i připojení k ISP nebo k jinému serveru, kterému server iSeries volá. Server iSeries podporuje několik metod pro uchovávání autentizačních informací: od jednoduchého ověřovacího seznamu na serveru iSeries, který uvádí oprávněné uživatele a příslušná hesla, až po podporu serverů RADIUS, které uchovávají podrobné autentizační informace o uživateli sítě. Server iSeries také podporuje několik voleb pro šifrování ID a hesla uživatele počínaje prostou výměnou hesel až po podporu macerace pomocí CHAP-MD5. Můžete uvést své preference pro autentizaci systému včetně ID a hesla uživatele, které se používají pro ověřování serveru iSeries při odchozím volání, a to na oušku **Autentizace** v profilu připojení v prostředí produktu iSeries Navigator.

Další informace o uchovávání ověřovacích a autentizačních informací naleznete v těchto částech:

- RADIUS (Remote Authentication Dial In User Service).
- Ověřovací seznam.

Další informace o podporovaných protokolech pro autentizaci hesel najdete v těchto částech:

- CHAP-MD5 (Challenge Handshake Authentication Protocol).
- PAP (Password Authentication Protocol).
- EAP (Extensible Authentication Protocol).

CHAP-MD5

Protokol CHAP-MD5 (Challenge Handshake Authentication Protocol) používá algoritmus (MD-5) pro výpočet hodnoty, která je známa pouze systému, který provádí autentizaci, a vzdálenému zařízení. Při použití CHAP se ID uživatele a heslo vždy šifrují, a proto je to bezpečnější protokol než PAP. Tento protokol je účinný proti pokusům o získání přístupu metodou opakování nebo metodou pokusu a omylu. Autentizace CHAP může při připojení proběhnout více než jednou.

System, který provádí autentizaci, vyšle výzvu do vzdáleného zařízení, které se pokouší o připojení do sítě. Vzdálené zařízení odpoví hodnotou, která se vypočítá podle známého algoritmu (MD-5), který používají obě zařízení. System, který provádí autentizaci, zkontroluje odpověď na základě výpočtu, který sám provedl. Autentizace je úspěšná, pokud se hodnoty shodují; v opačném případě se připojení ukončí.

EAP

EAP (Extensible Authentication Protocol) umožňuje autentizačním modulům třetí strany spolupracovat s implementovaným PPP. Protokol EAP rozšiřuje PPP tím, že poskytuje standardní podpůrný mechanismus pro autentizační schémata, jako jsou například karty token (smart), Kerberos, veřejný klíč a S/klíč. Protokol EAP je reakcí na stále větší poptávku po rozšíření autentizaci RAS o zařízení ochrany dat třetí strany. Protokol EAP chrání zabezpečené VPN před hackery (počítačovými piráty), kteří při napadání systémů používají zjišťování hesla pomocí slovníků a hádání. Protokol EAP zdokonaluje protokoly PAP a CHAP.

Při použití EAP nejsou autentizační informace zahrnuty do informací, ale spíše k informacím. To umožňuje vzdáleným serverům vyjednat nutnou autentizaci ještě předtím, než přijmou nebo předají jakékoli informace.

Server iSeries v současné době podporuje pouze tu verzi EAP, která je v zásadě ekvivalentem CHAP-MD5. Můžete však používat vzdálenou autentizaci pomocí serveru RADIUS, který může podporovat některá přídatná autentizační schémata popsaná výše.

PAP

Protokol PAP (Password Authentication Protocol) používá dvoucestné navazování spojení, aby poskytl peer systému snadnou metodu pro prokázání své totožnosti. Navazování spojení se provádí při vytváření spojení. Jakmile se spojení ustanoví, vzdálené zařízení odešle ID a heslo uživatele do autentizačního systému. Podle toho, zda je dvojice ID uživatele a heslo, autentizační systém v připojení pokračuje, nebo je ukončí.

Autentizace PAP vyžaduje, aby se jméno uživatele a heslo odesílalo na vzdálený systém v čistě textové podobě. Při použití PAP se ID a heslo uživatele nikdy nešifrují - proto je možné je zachytit a hacker může systém snadno napadnout. Z tohoto důvodu byste měli používat CHAP všude, kde je to možné.

Přehled služby RADIUS

RADIUS (Remote Authentication Dial in User Service) je standardní internetový protokol, který poskytuje služby centralizované autentizace, účtování a správy IP uživatelům vzdáleného přístupu na distribuované vytáčené síti.

V modelu klient-server RADIUS funguje NAS (Network Access Server) jako klient serveru RADIUS. Server iSeries, který funguje jako NAS, odesílá informace o uživateli a připojení do určeného serveru RADIUS pomocí standardního protokolu RADIUS, který je definovaný v RFC 2865.

Servery RADIUS reagují na přijaté požadavky uživatelů o připojení tím, že uživatele autentizují, a pak vracejí všechny nutné konfigurační informace serveru NAS, aby NAS (server iSeries) mohl poskytnout oprávněné služby uživateli, který se připojil.

Pokud nelze server RADIUS dosáhnout, server iSeries může směřovat požadavky na autentizaci do alternativního serveru. Tak je možné, aby podniky umožňovaly svým uživatelům vytáčenou službu s jedinečným přihlašovacím ID uživatele v celopodnikovém rozsahu, přičemž nerozhoduje, jaký přístupový bod se použije.

Když server RADIUS přijme autentizační protokol a požadavek se ověří, server RADIUS dešifruje datový paket pro přístup ke jménu a heslu uživatele. Tyto informace se předají příslušnému systému zabezpečení ochrany dat, který je podporován. Může se jednat o soubory hesel UNIX, Kerberos, komerční systémy zabezpečení dat nebo dokonce o systém zabezpečení dat vyvinutý zákazníkem. Server RADIUS odešle zpět serveru iSeries informaci o všech službách, které smí autentizovaný uživatel používat, například IP

adresu. Podobně se vyřizují si účtovací požadavky na server RADIUS. Účtovací informace o vzdáleném uživateli lze zasílat do označeného účtovacího serveru RADIUS. Standardní účtovací protokol RADIUS je definovaný v RFC 2866. Účtovací server RADIUS reaguje na přijaté účtovací požadavky tím, že protokoluje informace z účtovacího požadavku na RADIUS. Příklad konfigurace serveru RADIUS naleznete ve scénáři Autentizace vytáčených připojení pomocí RADIUS NAS.

Ověřovací seznam

Ověřovací seznam se používá pro ukládání ID a hesel vzdálených uživatelů. Můžete použít existující ověřovací seznamy, nebo můžete vytvořit svůj vlastní ověřovací seznam na stránce autentizace v Profilu příjemce připojení. Položky v ověřovacím seznamu také vyžadují, abyste označili typ autentizačního protokolu, který se má přiřadit k ID a heslu uživatele. Může se jednat o **šifrovaný - CHAP-MD5/EAP** nebo **nešifrovaný - PAP**.

Další informace naleznete v online nápovědě.

Pokyny ohledně šířky pásma - vícenásobné připojení

Pro provádění určitých úkolů je často zapotřebí větší šířka pásma, která však není nutná stále. V těchto případech to možná není důvod pro nákup specializovaného hardwaru a nákladných komunikačních linek. Protokol PPP MP (protokol vícenásobného připojení) spojuje více linek PPP tak, aby vznikla jediná virtuální linka neboli "svazek". Spojení více linek zvyšuje celkovou efektivní šířku pásma mezi dvěma systémy při použití standardních modemů nebo telefonních linek. V jednom MP svazku může být až šest linek. Chcete-li ustanovit vícenásobné připojení, oba konce připojení PPP musí podporovat protokol vícenásobných připojení. Protokol vícenásobných připojení je dokumentovaný jako norma RFC1990 (Request For Comment). Další informace o RFC naleznete na stránkách <http://www.rfc-editor.org>.

Šířka pásma na vyžádání:

Schopnost dynamicky přidávat a odebírat fyzické linky umožňuje konfigurovat systém tak, aby zajišťoval šířku pásma pouze tehdy, když je to zapotřebí. Tento přístup, kterému se obvykle říká "šířka pásma na požádání", vám umožňuje platit za zvýšenou šířku pásma pouze tehdy, když ji skutečně využíváte. K tomu, abyste mohli využívat výhody "šířky pásma na požádání", musí být alespoň jeden peer schopen monitorovat využití celkové šířky pásma, kterou v daný okamžik zajišťuje svazek MP. Jednotlivé linky lze pak do svazku přidávat nebo z něj odstraňovat, když využití šířky pásma přesáhne hodnoty definované v konfiguraci. Protokol BAP (Bandwidth Allocation Protocol) umožňuje peerům vyjednávat přidávání nebo odstraňování linek ve svazku MP. RFC2125 dokumentuje oba protokoly PPP: BAP (Bandwidth Allocation Protocol) a BACP (Bandwidth Allocation Control Protocol).

Kapitola 6. Konfigurace PPP

Než budete moci používat PPP pro nastavení připojení PPP, musíte konfigurovat své prostředí PPP. Následující části poskytují informace o konfiguraci prostředí PPP:

- Vytvoření profilu připojení
- Konfigurace modemu
- Konfigurace vzdáleného PC
- Konfigurace přístupu k Internetu pomocí AT&T
- Průvodci připojením
- Konfigurace metody přístupu skupiny
- Použití pravidel filtrování IP na připojení PPP
- Povolení služby RADIUS a DHCP pro profily příjemců připojení PPP

Vytvoření profilu připojení

Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na serveru iSeries. Profil připojení je logické znázornění následujících atributů připojení:

- linka a typ profilu
- nastavení s více linkami
- vzdálená telefonní čísla a volby vytáčení
- autentizace
- nastavení TCP/IP: IP adresy a směrování
- řízení práce a přizpůsobení komunikace
- servery jmen domény

Služby RAS (Remote Access Services), v adresáři Síť, obsahují následující objekty:

- **Profily připojení odesílatele** jsou odchozí připojení PPP, která jsou iniciována ze serveru iSeries (lokální systém). Jedná se o připojení PPP, která přijímá vzdálený systém.
- **Profily připojení příjemce** jsou příchozí připojení PPP, která jsou iniciována ze vzdáleného systému. Jedná se o připojení PPP, která přijímá server iSeries (lokální systém).
- **Modemy**

Při vytváření profilu připojení proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj systém a rozbalte **Síť → RAS (Remote Access Services)**.
2. Vyberte jednu z následujících voleb:
 - Klepněte pravým tlačítkem myši na **Profily připojení odesílatele**, abyste mohli nastavit server iSeries jako server, který iniciuje připojení.
 - Klepněte pravým tlačítkem myši na **Profily připojení příjemce**, abyste mohli nastavit server iSeries jako server, který umožňuje příchozí připojení od vzdálených systémů a uživatelů.
3. Vyberte **Nový profil**.
4. Na stránce **Nastavení nového profilu dvoubodového spojení** vyberte typ protokolu.
5. Zadejte výběry režimu.
6. Vyberte konfigurace linky.
7. Klepněte na **OK**.

Zobrazí se stránka **Vlastnosti nového profilu dvoubodového spojení**. Můžete nastavit zbývající hodnoty, které jsou specifické pro vaši síť. Konkrétní náповědu získáte v online náповědě.

Typ protokolu: PPP nebo SLIP

Jaký protokol byste měli vybrat pro vytváření dvoubodového připojení?

Protokol PPP je standardní internetový připojovací protokol. Protokol PPP umožňuje schopnost spolupráce systémů mezi softwarovými produkty vzdáleného přístupu od různých výrobců. Protokol PPP rovněž umožňuje, aby více síťových komunikačních protokolů používalo stejnou fyzickou komunikační linku.

Protokol PPP nahrazuje protokol SLIP, který lze také volit pro dvoubodová připojení. Protokol SLIP definovaný v RFC (Request for Comment) se na Internetu nikdy nestal standardem kvůli následujícím nedostatkům:

- SLIP nemá žádný standardní způsob, jak definovat IP adresování mezi dvěma hostiteli. To znamená, že nelze použít nečíslovanou síť.
- SLIP nemá žádnou podporu pro detekci nebo potlačení chyb. V PPP jsou detekce i potlačení chyb implementovány.
- SLIP nepodporuje autentizaci systému. PPP naopak podporuje obousměrnou autentizaci.

SLIP se v současnosti stále používá a server iSeries jej nadále podporuje. Společnost IBM však doporučuje, abyste při nastavování dvoubodového připojení používali PPP. Protokol SLIP nepodporuje vícenásobná připojení. Oproti protokolu SLIP má protokol PPP lepší autentizaci. PPP má větší výkon díky své schopnosti komprimace.

Poznámka: Profily připojení SLIP, které jsou definovány u asynchronních typů linek (ASYNC), již nejsou v tomto vydání podporovány. Jestliže máte takové profily připojení, musíte je migrovat buď na profil SLIP, nebo na profil PPP, který používá typ linky PPP.

Výběry režimu

Výběry režimu pro profil připojení PPP zahrnují výběry pro **typ připojení** a **provozní režim**. Výběry režimu uvádějí, jak server používá nové připojení PPP.

Chcete-li zadat výběry režimu, proveďte následující kroky:

1. Vyberte jeden z následujících typů připojení:
 - komutovaná linka
 - pronajatá linka
 - L2TP (virtuální linka)
 - linka PPPoE
2. Vyberte provozní režim, který odpovídá novému připojení PPP.
3. Poznamenejte si typ připojení a provozní režim, které jste vybrali. Tyto informace budete potřebovat, až začnete konfigurovat svá připojení PPP.

Komutovaná linka

Tento typ připojení vyberte, jestliže používáte některé z níže uvedených zařízení pro připojení přes telefonní linky:

- modem (interní nebo externí)
- interní adaptér ISDN (basic rate interface)
- externí adaptér terminálu ISDN

Připojení typu komutované linky má následující provozní režimy:

- **Odpověď**
Tento provozní režim vyberte tehdy, pokud chcete povolit vzdálenému systému, aby se připojoval k serveru iSeries.
- **Vytáčení**

Tento provozní režim vyberte tehdy, pokud chcete povolit serveru iSeries iniciovat připojení ke vzdálenému systému.

- **Vytáčení na požádání (pouze vytáčení)**

Tento provozní režim vyberte tehdy, chcete-li serveru iSeries umožnit, aby se automaticky připojoval ke vzdálenému systému, když se v systému detekuje provoz TCP/IP. Připojení se ukončí, když se dokončí datový přenos a po určité době se nevyskytne provoz TCP/IP.

- **Vytáčení na požádání (vyhrazený peer s možností odpovídat)**

Tento provozní režim zvolte tehdy, chcete-li serveru iSeries povolit příjem volání od vyhrazeného vzdáleného systému. Tento provozní režim serveru iSeries rovněž umožňuje iniciovat připojení ke vzdálenému systému, jakmile se objeví provoz TCP/IP určený pro vzdálený systém. Jestliže oba systémy jsou servery iSeries a jestliže oba používají tento provozní režim, k provozu TCP/IP dochází mezi těmito dvěma systémy na vyžádání, aniž by bylo nutné nějaké trvalé fyzické připojení. K tomuto provoznímu režimu je nutný vyhrazený prostředek. Má-li tento provozní režim řádně fungovat, musí se vzdálený peer připojovat.

- **Vytáčení na požádání (umožněný vzdálený peer)**

Tento provozní režim vyberte, chcete-li povolit vytáčení vzdáleného systému nebo příjem volání ze vzdáleného systému. K tomu, abyste mohli zpracovávat příchozí volání, musíte vytvořit odkaz na existující profil příjmu z profilu připojení PPP, který uvádí tento provozní režim. Tak je možné, aby jeden profil příjmu obsluhoval veškerá volání přicházející od jednoho nebo více vzdálených peerů, kdežto jiný profil vytáčení na vyžádání může vyřizovat každé odchozí volání. Tento provozní režim nevyžaduje vyhrazený prostředek, který by vyřizoval volání přicházející od vzdálených peerů.

Pronajatá linka

Tento typ připojení si vyberte tehdy, jestliže máte vyhrazený spoj mezi lokálním serverem iSeries a vzdáleným systémem. Pokud máte pronajatou linku, nepotřebujete pro propojení těchto dvou systémů modem ani adaptér terminálu ISDN.

Připojení pronajatou linkou mezi dvěma systémy se považuje za trvalý neboli vyhrazený spoj. Je stále otevřený. Jeden konec pronajaté linky je konfigurovaný jako iniciátor, druhý jako terminátor.

Typ připojení pronajatou linkou umožňuje následující provozní režimy:

- **Terminátor**

Tento provozní režim si vyberte, chcete-li vzdálenému systému povolit přístup do serveru iSeries přes vyhrazený spoj. Tento provozní režim se odkazuje na profil odpovědi použitý pro pronajatou linku.

- **Iniciátor**

Tento provozní režim vyberte, chcete-li serveru iSeries umožnit přístup do vzdáleného systému přes vyhrazený spoj. Tento provozní režim se odkazuje na profil vytáčení použitý pro pronajatou linku.

L2TP (virtuální linka)

Tento typ připojení vyberte, chcete-li zajistit připojení mezi systémy, které používají protokol L2TP (Layer Two Tunneling Protocol).

Jakmile se zavede tunel L2TP, vytvoří se virtuální připojení PPP mezi serverem iSeries a vzdáleným systémem. Když budete používat L2TP tunel ve spojení se zabezpečením IP (IP-SEC), můžete po Internetu odesílat, směrovat a přijímat zabezpečená data.

Typ připojení L2TP (virtuální linka) umožňuje následující provozní režimy:

- **Terminátor**

Tento provozní režim si vyberte, chcete-li vzdálenému systému povolit, aby se připojoval k serveru iSeries tunelem L2TP.

- **Iniciátor**

Tento provozní režim vyberte tehdy, chcete-li serveru iSeries povolit, aby se připojoval ke vzdálenému systému tunelem L2TP.

- **Vzdálené vytáčení**

Tento provozní režim vyberte, chcete-li serveru iSeries povolit, aby se připojoval k ISP tunelem L2TP a nařizoval ISP vytáčení vzdáleného klienta PPP.

- **Iniciátor pro více přechodů**

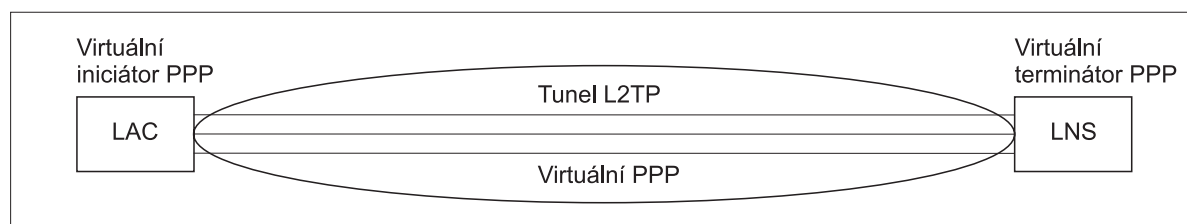
Tento provozní režim vyberte, chcete-li serveru iSeries povolit, aby ustanovoval připojení s více přechody.

Poznámka: Profil terminátoru L2TP, s nímž je tento iniciátor pro více přechodů asociovaný, musí mít zaškrtnuto políčko "Povolit připojení s více přechody" a musí mít v ověřovacím seznamu PPP záznam, který spojuje jméno uživatele PPP s profilem iniciátoru pro více přechodů.

Protokol L2TP (Layer 2 Tunneling Protocol): Protokol L2TP rozšiřuje protokol PPP tak, aby podporoval tunel na vrstvě linky mezi požadujícím klientem L2TP a cílovým koncovým serverem L2TP. Pomocí tunelů L2TP je možné oddělit místo, kde končí vytáčený protokol, od místa, kde se poskytuje přístup do sítě.

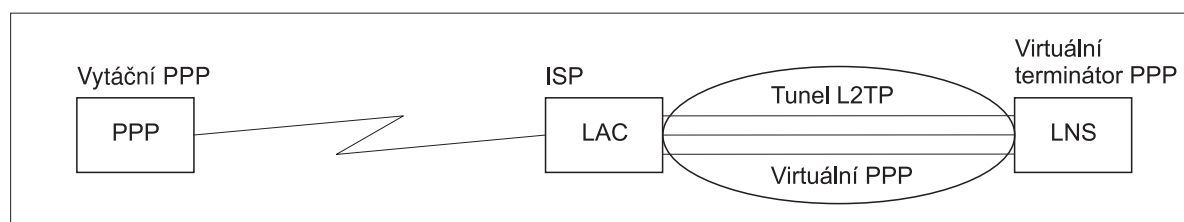
Poskytovatel služeb sítě Internet (ISP) používá režim virtuální linky pro provozování VPN (Virtual Private Network). Chcete-li lépe pochopit, jak VPN funguje s L2TP, prostudujte si část Konfigurace připojení L2TP chráněného pomocí VPN.

Toto jsou nákresy tří odlišných příkladů implementace tunelu L2TP:



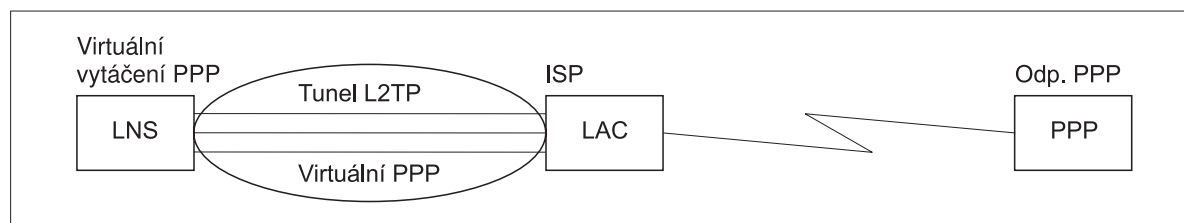
RBAEE563-0

Obrázek 7. PPP virtuální iniciátor nebo PPP virtuální terminátor



RBAEE561-0

Obrázek 8. PPP iniciátor vytáčení nebo PPP virtuální terminátor



RBAEE562-0

Obrázek 9. PPP virtuální vytáčení nebo PPP virtuální příjem

Linka PPPoE

Připojení PPPoE využívají virtuální linku pro zasílání dat PPP přes adaptér Ethernet, typ 2838, do modemu DSL vašeho ISP, který je také připojený do sítě LAN na bázi Ethernetu. To umožňuje uživatelům v síti LAN

vysoke rychlostní přístup k Internetu prostřednictvím relací PPP přes server iSeries. Jakmile se zahájí připojení mezi serverem iSeries a ISP, jednotliví uživatelé mohou v síti LAN spouštět jedinečné relace s ISP přes PPPoE.

Připojení PPPoE se používají pouze s profily připojení odesílatele, přičemž se předpokládá provozní režim iniciátoru a používá pouze jediná linka.

Konfigurace linky

V konfiguraci linky se definuje typ služby linky, kterou váš profil připojení PPP používá pro ustanovení připojení. Typy služby linky závisejí na typu připojení, který uvedete.

- jediná linka
- společná oblast linek
- integrovaná linka ISDN

Jediná linka

Tuto službu linky uveďte, chcete-li definovat linku PPP, která je asociovaná s analogovým modemem. Tato volba se také používá pro pronajaté linky, u kterých se modem nepožaduje. Profil připojení PPP vždy používá tentýž prostředek komunikačního portu serveru iSeries.

Pokud to budete požadovat, můžete jedinou analogovou linku konfigurovat jako "sdílenou" mezi profilem příjmu a profilem volání. Dynamické sdílení prostředků je nová funkce určená ke zlepšení využitelnosti prostředků. Až do vydání V5R2 byly prostředky modemu vázány, jakmile byl spuštěný profil, který je používal. Tak byl uživatel omezený na jeden prostředek na jednu relaci, a to i tehdy, když prostředek byl ve stavu pasivního čekání. Nyní se uplatňují nová pravidla sdílení, když se přistupuje ke konkrétnímu prostředku. Existují dva možné případy: Za prvé, profil vytáčení byl spuštěný před profilem odpovědi. Za druhé, profil odpovědi byl spuštěný před profilem vytáčení. Předpokladem je, že sdílení prostředku je povoleno. V prvním případě se spuštěný profil vytáčení úspěšně připojí. Profil odpovědi, který byl spuštěn jako druhý, bude čekat, až bude linka k dispozici. Jakmile připojení profilu vytáčení skončí, profil odpovědi si linku vyžádá a spustí se. V druhém případě spuštěný profil odpovědi čeká na příchozí připojení. Jestliže příchozí připojení není ustanoveno, profil vytáčení, který byl spuštěný jako druhý, si "půjčí" linku od profilu odpovědi, který linku "přenechá". Pak se ustanoví odchozí propojení. Jakmile se připojení ukončí, profil vytáčení vrátí linku profilu odpovědi, který znovu bude připravený na příjem příchozích připojení. Chcete-li povolit funkci sdílení, klepněte na ouško modemu, na popis komutované linky a vyberte volbu "Povolit dynamické sdílení prostředků".

Služba jediné linky se také používá pro typy připojení L2TP (virtuální linka) a PPPoE (virtuální linka). Pro typy připojení L2TP (virtuální linka) se s jedinou linkou nepoužívá žádný hardwarový komunikační port. Jediná linka použitá s připojením L2TP je totiž *virtuální* v tom, smyslu, že neexistuje žádný fyzický hardware PPP, který se požaduje pro ustanovení tunelu. Jediná linka použitá s připojením PPPoE je také virtuální v tom smyslu, že poskytuje mechanismus pro zacházení s fyzickou linkou Ethernet tak, jako kdyby to byla linka PPP podporující vzdálená připojení. Virtuální linka PPPoE je vázána k fyzické lince Ethernet a používá se pro podporu datových přenosů s protokolem PPP přes připojení LAN Ethernet do modemu DSL.

Společná oblast linek

Tuto službu linky vyberte, chcete-li nastavit, aby připojení PPP používalo linku ze společné oblasti linek. Když se spustí připojení PPP, server iSeries vybere nepoužitou linku ze společné oblasti linek. U profilů volání na vyžádání server vybírá linku až tehdy, když detekuje provoz TCP/IP pro vzdálený systém.

Můžete používat společnou oblast linek místo toho, že byste definovali příslušný popis linky pro nějaký profil připojení. Ve společné oblasti linek můžete uvést jeden nebo více popisů linek.

Společná oblast linek také umožňuje, aby jediný profil připojení obsluhoval buď větší počet příchozích analogových volání, nebo jediné odchozí analogové volání. Linka se vrací do společné oblasti linek, jakmile připojení PPP skončí.

Jestliže používáte společnou oblast linek pro simultánní práci s více příchozími analogovými voláními, musíte uvést maximální počet příchozích připojení. Ten můžete nastavit prostřednictvím oúška Připojení v dialogu **Vlastnosti nového profilu dvoubodového spojení**, když konfiguruje profil připojení. Pomocí nastavení vícenásobného připojení můžete společnou oblast linek používat pro jednotlivá připojení se zvýšenou šířkou pásma.

Výhody používání společné oblasti linek:

- Nevážete prostředek linky k připojení PPP do doby, než se spustí.

U připojení PPP, která používají konkrétní linku, se připojení ukončí, jestliže linka není dostupná, kromě případů, kdy se používá sdílení prostředku. U připojení, která používají společnou oblast linek, musí být alespoň jedna linka v oblasti linek volná, když se spouští profil.

Pokud jsou prostředky konfigurované jako sdílené (povolit dynamické sdílení prostředků), dosahuje se také vyšší dostupnosti, a to zvláště pro odchozí připojení.

- Profily vytáčení na požádání můžete používat se společnými oblastmi linek, čímž budete prostředky využívat efektivněji.

Server iSeries vybere linky ze společné oblasti linek pouze tehdy, když ji použije pro připojení vytáčení na požádání. Jindy mohou tuto linku používat jiná připojení.

- Můžete spouštět více připojení PPP s menším množstvím podporovaných prostředků.

Pokud vaše prostředí například potřebuje čtyři jedinečné typy připojení, ale vy kdykoli potřebujete najednou pouze dvě linky, můžete použít společnou oblast linek, aby toto prostředí fungovalo. Můžete vytvořit čtyři profily připojení vytáčení na požádání, přičemž každý z těchto profilů se bude odvolávat na společnou oblast linek, která obsahuje dva popisy linek. Každá linka bude určena pro použití všemi čtyřmi profily připojení, takže v jakýkoliv okamžik budou moci být aktivní dvě připojení. Když použijete společnou oblast linek, nemusíte mít čtyři oddělené linky.

Pokud vaše prostředí je kombinací mezi klientem PPP a serverem PPP, linky lze sdílet (povolit dynamické sdílení prostředků), ať už se používají jako "jediné linky" nebo jsou součástí "společné oblasti linek".

Profil, který se spustil jako první, nebude vázat prostředek, pokud připojení není aktivní. Když se například server PPP spustí a naslouchá příchozím připojením, "přenechá" linku, kterou používá, klientovi PPP, který se spustí a "půjčí" si sdílenou linku od serveru PPP.

Podpora profilu více připojení

Profily dvoubodových připojení, které podporují více připojení, vám umožňují mít jeden profil připojení, který obsluhuje mnoho digitálních, analogových nebo L2TP volání. To je užitečné tehdy, když chcete, aby se více uživatelů připojovalo k serveru iSeries, ale nechcete uvést zvláštní profil dvoubodového připojení, který má každou linku PPP obsluhovat. Tato funkce je zvláště užitečná pro 4portový integrovaný modem 2805, u něhož čtyři linky používá jeden adaptér, nebo pro adaptéry 2750 a 2751, které podporují osm nezávislých připojení ISDN přes B-kanály.

Pro analogové linky s podporou profilu více připojení se používají všechny linky uvedené ve společné oblasti linek až do maximálního počtu připojení. Vlastně pro každou linku, která je definována ve společné oblasti linek, se spouští zvláštní úloha profilu připojení. Všechny úlohy profilu připojení čekají na příchozí volání na svých příslušných linkách.

IP adresa lokálního systému pro profily více připojení:

S profily více připojení můžete používat lokální IP adresu, ale musí to být existující IP adresa, která je definována na serveru iSeries. Pomocí rozbalovacího seznamu lokálních IP adres si můžete vybrat existující adresu. Vzdálení uživatelé mohou přistupovat k prostředkům, jež jsou na lokální síti, pokud jako lokální IP adresu pro protokol PPP zvolíte IP adresu lokálního serveru iSeries. Musíte také definovat IP adresy, které jsou ve společné oblasti IP adres, aby byly ve stejné síti jako lokální IP adresa lokálního systému.

Jestliže nemáte IP adresu lokálního serveru iSeries nebo nechcete, aby vzdálení uživatelé přistupovali k LAN, musíte pro svůj server iSeries definovat virtuální IP adresu. Virtuální IP adresa je také známá jako bezobvodové rozhraní. Vaše profily dvoubodového připojení mohou používat tuto IP adresu jako svou

lokální IP adresu. Jelikož tato adresa není vázána k nějaké fyzické síti, nebude automaticky předávat provoz jiným sítím, které jsou připojeny k vašemu serveru iSeries.

Chcete-li vytvořit virtuální IP adresu, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť** → **Konfigurace TCP/IP** > **IPV4** > **Rozhraní**.
2. Klepněte pravým tlačítkem myši na **Rozhraní** a vyberte **Nové rozhraní** → **Virtuální IP**.
3. Podle pokynů průvodce rozhraním vytvoříte virtuální IP rozhraní. Vaše profily dvoubodového připojení mohou používat virtuální IP adresu, jakmile ji vytvoříte. Pomocí rozbalovacího seznamu v poli Lokální IP adresa, které je na stránce Nastavení TCP/IP, vyberte adresu, kterou chcete použít se svým profilem.

Poznámka: Virtuální IP adresa musí být před spuštěním profilu pro více připojení aktivní; jinak se profil nespustí. Chcete-li po vytvoření rozhraní adresu aktivovat, vyberte v průvodci rozhraním volbu, že se má adresa spouštět.

Společná oblast IP adres vzdáleného systému pro profily více připojení:

Můžete rovněž používat společné oblasti IP adres vzdáleného systému s profily pro více připojení. Typický profil dvoubodového jediného spojení vám umožní uvést pouze jednu vzdálenou IP adresu, která se předává volajícimu systému, když se připojení vytváří. Jelikož nyní se může více volajících připojovat simultánně, rozsah IP adres vzdáleného systému se používá pro definování výchozí vzdálené IP adresy a také rozsahu dodatečných IP adres, které se předávají volajícimu systému.

Omezení společné oblasti linek:

Tato omezení platí tehdy, když používáte společné oblasti linek pro více připojení:

- V daném okamžiku může konkrétní linka existovat pouze v jedné společné oblasti linek. Když linku odejmete ze společné oblasti linek, můžete ji použít v jiné společné oblasti linek.
- Když spouštíte profil připojení, který používá společnou oblast linek, všechny linky ve společné oblasti linek se používají až do maximální počtu připojení zadaného v profilu. Pokud už nejsou volné žádné linky, všechna nová připojení selžou. Podobně pokud nejsou ve společné oblasti linek žádné linky, každý spouštěný profil se ihned ukončí.
- Když spustíte profil jediného připojení, který má společnou oblast linek, systém použije pouze jednu linku ze společné oblasti linek. Jestliže spustíte profil více připojení, který používá tutéž společnou oblast linek, všechny zbývající linky ve společné oblasti linek lze využít.

Společná oblast IP adres vzdáleného systému: Systém může používat společnou oblast IP adres vzdáleného systému pro příjem nebo ukončování profilu dvoubodového připojení, který se používá s více příchozími připojeními. To zahrnuje L2TP, nativní ISDN a společné oblasti linek s maximální počtem připojení větším než jedna. Tato funkce systému umožňuje přiřazovat jedinečnou vzdálenou IP adresu ke každému příchozímu připojení.

První systém pro připojení obdrží IP adresu definovanou v poli výchozí IP adresa. Pokud se tato adresa již používá, vydá se další adresa z daného rozsahu adres. Předpokládejme například, že výchozí IP adresa je 10.1.1.1 a počet adres je definovaný jako 5. Adresy v rámci společné oblasti IP adres vzdáleného systému budou 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 a 10.1.1.5. Maska podsítě definovaná pro společnou oblast IP adres vzdáleného systému bude pokaždé 255.255.255.255.

Tato omezení platí, když se používají společné oblasti vzdálených IP adres:

- Více než jeden profil připojení může uvádět stejnou společnou oblast adres. Pokud se však používají všechny adresy uvedené ve společné oblasti, každý další požadavek o připojení se odmítá do doby, než jiné připojení skončí a uvolní nějakou adresu.
- Chcete-li alokovat určité adresy pro některé vzdálené systémy, zatímco chcete jiným příchozím systémům povolit používání adresy ze společné oblasti, proveďte následující kroky:

1. Povolte ověřování vzdáleného systému na oúšku **Autentizace**, aby mohlo být zjištěno uživatelské jméno vzdáleného systému.
2. Definujte rozsah vzdálených IP adres pro všechny příchozí požadavky na připojení, které nevyžadují konkrétní IP adresu.
3. Definujte IP adresy pro konkrétní uživatele tak, že zaškrtnete volbu **Definovat přídavné IP adresy na základě ID uživatele vzdáleného systému**, a pak klepněte na volbu **IP adresa definovaná na základě jména uživatele**.

Když se vzdálený uživatel připojí, server iSeries určí, zda je pro tohoto uživatele definována určitá IP adresa. Pokud ano, předá se IP adresa vzdálenému systému; v opačném případě se vrátí adresa ze společné oblasti vzdálených IP adres.

ISDN

Tuto službu linky vyberte, chcete-li definovat PPP linku, která je asociována se síťovým připojením ISDN.

Výhody používání ISDN:

- ISDN poskytuje volnou komunikaci vyšší rychlostí.
- ISDN má za cíl poskytovat univerzální připojitelnost používáním jediného rozhraní a vysokorychlostní digitální sítě pro přenášení všech typů dat.
- ISDN má také schopnost dosahovat krátkých časů připojení na komutovaných spojeních. Ustanovení analogového modemového připojení může trvat až 30 sekund nebo více, kdežto připojení ISDN zabere pouze několik sekund.

Konfigurace modemu pro PPP

Pro svá analogová připojení PPP můžete používat externí modem, interní modem nebo adaptér terminálu ISDN. Modem vám poskytuje schopnosti analogového připojení (pronajatá linka a komutovaná linka). Pro server iSeries byly definovány popisy nejpobulárnějších modemů.

Můžete provést tyto úkoly konfigurace modemu:

- konfigurace nového modemu
- přiřazení modemu k popisu linky
- příkaz nastavení příkazového řetězce modemu

Konfigurace nového modemu

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Klepněte pravým tlačítkem myši na **Modemy** a vyberte **Nový modem**.
3. Na oúšku **Obecné** zadejte správné hodnoty do všech okének.
4. **Volitelné:** Pokud chcete přidat nějaké inicializační příkazy pro modem, klepněte na oúško **Přídavné parametry**.
5. Klepnutím na **OK** uložíte své záznamy a uzavřete stránku **Vlastnosti nového modemu**.

Chcete-li zjistit, zda můžete používat stávající popis modemu, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Vyberte **Modemy**.
3. Prohlédněte si seznam modemů a vyhledejte jméno výrobce, model a typ svého modemu.

Poznámka: Jestliže je váš modem zahrnutý v předvoleném seznamu, nemusíte provádět žádné další kroky.

4. Klepněte pravým tlačítkem myši na popis modemu, který co nejvíce odpovídá vašemu modemu a vyberte **Vlastnosti**, chcete-li si prohlédnout příkazové řetězce.
5. Konkrétní příkazové řetězce pro svůj modem naleznete v dokumentaci k modemu.
Použijte vlastnosti předvoleného modemu, jestliže se příkazové řetězce shodují s požadavky vašeho modemu. V opačném případě musíte pro svůj modem vytvořit popis modemu a přidat jej do seznamu modemů.

Chcete-li vytvořit popis modemu, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Vyberte **Modemy**.
3. V seznamu modemů klepněte pravým tlačítkem myši na **\$generic hayes** a vyberte **Nový modem podle...**
4. V dialogu **Nový modem** změňte příkazové řetězce tak, aby odpovídaly informacím, které požaduje váš modem.

Nastavení příkazového řetězce modemu

Níže uvedená tabulka uvádí minimální sadu příkazů, které se používají v modemech, jež jsou definovány na serveru iSeries. Můžete si vyhledat ekvivalentní příkazové řetězce v uživatelské příručce ke svému modemu. V popisu modemu použijte výrobcem doporučené nastavení.

Vlastnost modemu	Správný příkazový řetězec pro většinu modemů
vynulování modemu zpět na tovární nastavení	AT&F nebo AT&Z
Inicializace modemu:	
zobrazovat textové výsledkové kódy	Q0 a V1
normální režimy CD a DTR	&C1 a &D2
režim opakování vypnutý	E0
DSR (data set ready) následující po detekci nosného kmitočtu (carrier detect)	&S1
povolit hardwarové řízení toku (RTS/CTS)	
povolit korekci chyb a volitelně kompresi (V.42/V.42 bis)	
zajistit, že linka DTE-DCE je povolena pro pevnou rychlost 115,2 Kbps (nebo maximální rychlost umožněnou modemem)	
(volitelné) povolení doby nečinnosti, pokud tuto funkci modem podporuje	
Režim odpovědi modemu:	
odpovědět po n zvoněních	S0= n kde $n = 1$ nebo 2
odpojit, pokud není nosná frekvence (připojení) po m sekundách	S7= m
typ vytáčení modemu	ATDT pro tónovou volbu nebo ATDP pro pulzní volbu

Příklad: Konfigurace adaptéru terminálu ISDN

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Klepněte pravým tlačítkem myši na **Modemy** a vyberte **Nový modem**.
3. Na oušku Obecné zadejte správné hodnoty do všech okének.
4. **Volitelné:** Pokud chcete přidat nějaké inicializační příkazy pro modem, klepněte na ouško parametrů ISDN.

U adaptérů terminálu ISDN se příkazy a parametry v tomto seznamu odesílají do adaptéru terminálu pouze za následujících podmínek:

- Dojde-li je změně nebo přidání příkazů uvedených v seznamu.
- V důsledku určitých akcí pro zotavení z chyb, které server iSeries může podnikat.

Proto by tyto příkazy měly obsahovat a být omezeny na následující:

- Nastavení typu komutované ISDN a verze, kterou poskytuje lokální telefonní společnost.
 - Nastavení adresářových čísel a identifikátorů profilu služby (SPID), které poskytuje lokální telefonní společnost.
 - Nastavení identifikátorů TEI (terminal entry ID), které může poskytovat lokální telefonní společnost.
 - Nastavení protokolu B kanálu (asynchronní-na-synchronní PPP).
 - Jiná modemová nastavení, která mají proměnlivou délku parametrů, jež vyžadují návrat vozíku pro indikaci délky parametru.
 - Ukládání a aktivace nových nastavení, aby se obnovovala po vynulování nebo po vypnutí systému.
 - Testovací příkaz aktivního stavu rozhraní *U* (ATDx), který serveru iSeries umožňuje určit, kdy byla dosažena synchronizace s přepínačem ústředny ISDN. Číslo *x* mohou být libovolná čísla, která jsou přípustná pro telefonní číslo, včetně # a *.
5. Když klepnete na **Přidat**, budete moci přidat další příkazy pro modem. Mohou to být příkazy s přiřazeným parametrem nebo bez parametru a krátký popis určený pro seznam příkazů. Ke všem příkazům, které uvedete bez přiřazeného parametru, lze přiřadit parametr, když se modem asociuje s popisem linky.
 6. Klepnutím na **OK** uložíte své záznamy a uzavřete stránku Vlastnosti nového modemu.

Přiřazení modemu k popisu linky

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services) → Profily připojení odesílatele** nebo **Profily připojení příjemce**.
2. Vyberte jednu z následujících voleb:
 - Chcete-li pracovat s existujícím profilem připojení, klepněte pravým tlačítkem myši na profil připojení a vyberte **Vlastnosti**.
 - Chcete-li pracovat s novým profilem připojení, vytvořte nový.
3. Na stránce vlastností profilu dvoubodového spojení vyberte ouško **Připojení** a klepněte na **Nové**.
 - Zadejte jméno konfigurace linky.
 - Klepnutím na **Nová** otevřete dialogové okno Vlastnosti nové linky.
4. V dialogovém okně Vlastnosti nové linky klepněte na ouško **Modem** a vyberte modem ze seznamu. Vybraný modem se asociuje s tímto popisem linky. Pro interní modemy byste vždy měli vybrat odpovídající definici modemu. Další informace naleznete v online nápovědě.

Ve vydání V5R2 můžete konfigurovat profily připojení odesílatele tak, aby si "půjčovaly" linku PPP a modem přiřazený k profilu připojení příjemce, který čeká na příchozí volání. Jakmile se připojení ukončí, odesílatel připojení "vrátí" linku PPP a modem profilu připojení příjemce. Chcete-li tuto novou funkci povolit, vyberte volbu **Povolit dynamické sdílení prostředků** na oušku modemu v dialogu konfigurace linky PPP. Linky PPP můžete konfigurovat na oušku připojení u profilů připojení příjemce a odesílatele.

Konfigurace vzdáleného PC

Chcete-li se připojit k serveru iSeries z PC, který má některý 32bitový operační systém Windows, ověřte, že je modem instalovaný a řádně konfigurovaný, a nezapomeňte, že na osobním počítači musíte mít instalované TCP/IP a telefonické připojení k síti.

Informace o konfiguraci telefonického připojení k síti na PC naleznete v dokumentaci k operačnímu systému Microsoft Windows. Dbejte na to, abyste uvedli nebo vložili následující informace:

- Typ telefonického připojení by měl být **PPP**.

- Jestliže používáte šifrovaná hesla, pamatujte na to, že musíte používat MD-5 CHAP (MS-CHAP NENÍ na serveru iSeries podporovaný). Některé verze Windows nepodporují MD-5 CHAP přímo, ale lze je takto konfigurovat za asistence pracovníků společnosti Microsoft.
- Jestliže používáte nešifrovaná (nebo nezabezpečená) hesla, používá se automaticky PAP. Žádný jiný typ nezabezpečeného protokolu nebude server iSeries podporovat.
- IP adresování se obvykle definuje vzdáleným systémem, nebo - jako v tomto případě - serverem iSeries. Jestliže plánujete použít střídavé metody adresování IP (například definování svých vlastních IP adres), zajistěte, aby byl server iSeries konfigurovaný tak, aby přijímal vaši metodu adresování.
- Přidejte IP adresu DNS, pokud je to vhodné pro dané prostředí.

Konfigurace přístupu k Internetu přes AT&T Global Network

IBM poskytuje přístup k Internetu prostřednictvím své sítě AT&T Global Network. Chcete-li získat přístup k této službě, můžete použít průvodce telefonickým připojením do AT&T Global Network, který vám pomůže konfigurovat profil komutovaného připojení PPP pro vytáčení sítě AT&T Global Network. Průvodce vás provede asi osmi podokny a jeho dokončení trvá přibližně deset minut. Průvodce můžete kdykoli zrušit, přičemž se neuloží žádná vložená data.

Připojení do AT&T Global Network mohou využívat dva typy aplikací:

- **Výměna pošty:** Umožňuje vám pravidelně odebírat poštu z jednoho účtu AT&T Global Network a odesílat ji do serveru iSeries, který ji bude distribuovat uživatelům Lotus Mail nebo uživatelům protokolu SMTP (Simple Mail Transfer Protocol).
- **Telefonické připojení do sítě:** Používejte aplikace telefonického připojení do sítě AT&T Global Network, například standardní přístup k Internetu.

Profily připojení do AT&T Global Network si můžete uchovávat jako jakékoli jiné profily připojení PPP.

Chcete-li použít průvodce telefonickým připojením do sítě AT&T Global Network, potřebujete jeden z těchto adaptérů:

- 2699: dvoulinkový WAN IOA.
- 2720: PCI WAN/Twinaxial IOA.
- 2721: PCI dvoulinkový WAN IOA.
- 2745: PCI dvoulinkový WAN IOA (nahrazuje IOA 2721).
- 2761: osmiportový analogový modem IOA.
- 2771: dvouportový WAN IOA modem s V.90 integrovaným na portu 1 a standardním komunikačním rozhraním na portu 2. Chcete-li používat port 2 adaptéru 2771, je nutný externí modem nebo adaptér terminálu ISDN s příslušným kabelem.
- 2772: dvouportový modem WAN IOA s integrovaným V.90.
- 2793: dvouportový WAN IOA, s integrovaným modemem V.92 na portu 1 a standardním komunikačním rozhraním na portu 2. Nahrazuje model 2771.
- 2805: čtyřportový WAN IOA s integrovaným modemem s integrovaným V.92. Nahrazuje modely 2761 a 2772.

Než spustíte průvodce připojením k síti AT&T Global Network, musíte si o svém prostředí zjistit tyto informace:

- Účetní informace AT&T Global Network (číslo účtu, ID uživatele a heslo) pro aplikaci doručování pošty nebo aplikaci telefonického připojení do sítě.
- IP adresy poštovního serveru a serveru jmen domény pro aplikaci doručování pošty.
- Jméno modemu, který se používá pro připojení po jedné lince.

Chcete-li spustit průvodce telefonickým připojením k síti AT&T Global Network, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Klepněte pravým tlačítkem myši na **Profily připojení odesílatele** a vyberte **Nové telefonické připojení do AT&T Global Network**.
3. Poté, co se spustí průvodce připojením k síti AT&T Global Network, klepněte na volbu **Nápověda**, kde naleznete další informace týkající se vyplnění podokna.

Průvodci připojením

Průvodce novým telefonickým připojením

Tento průvodce vás provede konfigurací profilu telefonického připojení, abyste získali přístup ke svému poskytovateli služeb sítě Internet (ISP) nebo přístup do sítě typu intranet. Pravděpodobně budete muset u správce sítě nebo poskytovatele služeb sítě Internet (ISP) zjistit určité informace, abyste mohli tohoto průvodce dokončit. Další informace pro dokončení tohoto průvodce získáte v online nápovědě.

Průvodce univerzálním připojením

Tento průvodce vás provede konfigurací profilu, který může být použit softwarem elektronické podpory zákazníka (ECS) pro připojení k IBM. Podpora elektronické služby poskytuje monitorování vašeho jedinečného prostředí serveru iSeries, aby vám mohly být doporučeny úpravy určené konkrétně pro váš systém a situaci. Další informace pro dokončení tohoto průvodce získáte v online nápovědě.

Konfigurace metody přístupu skupiny

Pořadač **Metody přístupu ke skupině** pod volbou **Profily připojení příjemce** poskytuje volby konfiguračních parametrů pro dvoubodové připojení, které se používají pro skupiny vzdálených uživatelů. To se týká pouze těch dvoubodových připojení, která jsou iniciována ze vzdáleného systému a jsou přijata lokálním systémem.

Jak konfigurovat novou metodu přístupu skupiny:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services) → Profily připojení příjemce**.
2. Klepněte pravým tlačítkem myši na **Metody přístupu ke skupině** a vyberte **Nová metoda přístupu ke skupině**.
3. Na oúšku **Obecné** zadejte jméno a popis nové metody přístupu skupiny.
4. Klepněte na oúško **Vícenásobné připojení** a nastavte konfiguraci více linek.

Konfigurace více linek znamená, že chcete, aby se více fyzických linek spojovalo do svazku. Maximální počet linek ve svazku může být mezi 1 a 16. Jelikož neznáte typ nastavení linky, dokud se připojení neuskuteční, je předvolená hodnota vždy 1. Metodu skupiny lze použít pro rozšíření nebo omezení schopností protokolu vícenásobných připojení pro konkrétního uživatele.

- **Maximum linek ve svazku** uvádí maximální počet linek, které se mají stát jednou logickou linkou. Maximální počet linek nesmí být větší než počet volných linek, když se tato metoda skupiny uplatňuje na relaci pro profil PPP.
 - Zaškrtněte **Vyžadovat BACP**, jestliže chcete uvést, že připojení se ustanovuje pouze tehdy, pokud vzdálený systém podporuje protokol BACP (Bandwidth Allocation Protocol). Jestliže není možné vyjednat BACP, povolí se pouze jediná linka.
5. Klepnutím na oúško **Nastavení TCP/IP** povolíte libovolné z následujících možností:
 - Povolit vzdálenému systému přístup k ostatním sítím (směrování pomocí IP)
Tato volba uvádí, zda chcete směrování pomocí IP. Pokud tuto volbu vyberete, v podstatě povolujete, aby server pracoval pro toto připojení jako směrovač. Tak mohou datagramy protokolu Internetu (IP), které nejsou určeny pro tento server iSeries, projít systémem do jiné připojené sítě. Jestliže toto pole

ponecháte prázdné, protokol Internetu (IP) vyřadí ze vzdáleného systému ty datagramy, které nejsou určeny pro nějakou adresu, která je pro tento server iSeries lokální.

Kvůli zabezpečení dat možná směrování pomocí IP nepovolíte. Poskytovatelé služeb sítě Internet (ISP) naopak obvykle směrování pomocí IP poskytují. Pamatujte, že to bude fungovat pouze tehdy, když je povoleno postoupení datagramů pomocí IP v celém systému - jinak bude tato volba ignorována, i když bude označena. Postoupení datagramů pomocí IP v celém systému lze zobrazit prostřednictvím ouška Nastavení na stránce Vlastnosti TCP/IP.

- Požadovat komprimaci hlavičky TCP/IP (VJ)

Tato volba uvádí, zda chcete, aby protokol Internetu (IP) komprimoval informace v hlavičce poté, co ustanoví připojení. Komprimace obvykle zvýší výkon, zvláště při interaktivním provozu nebo na pomalých sériových linkách. Komprimace hlavičky se řídí metodou Van Jacobsona (VJ) definovanou v RFC 1332. Pro PPP se komprimace vyjednává, když se připojení ustanovuje. Pokud druhý konec připojení nepodporuje kompresi VJ, server iSeries ustanoví připojení, které kompresi nepoužívá.

- Použít pro toto připojení pravidla paketu IP

Tato volba uvádí, zda chcete na tuto metodu skupiny použít nějaké filtrovací pravidlo. Filtrovací pravidla vám umožňují řídit, jaké IP přenosy chcete ve své síti povolit. Tuto komponentu pro filtraci paketů můžete použít pro ochranu svého systému. Komponenta filtrování IP paketů chrání váš systém tím, že filtruje pakety podle pravidel, která zadáte. Tato pravidla se zakládají na informacích v záhlaví paketu.

Další informace o pravidlech IP paketů naleznete ve filtrování IP paketů a pod tématem NAT v aplikaci Information Center.

Příklad naleznete ve scénáři Správa přístupu uživatelů k prostředkům pomocí metody přístupu skupiny a filtrování IP.

Použití metod skupiny na uživatele se vzdáleným přístupem:

Metody skupiny můžete použít na uživatele se vzdáleným přístupem tehdy, když doplníte vlastnosti dvoubodového připojení pro nový **profil připojení příjemce**.

Použití metody skupiny na uživatele se vzdáleným přístupem:

1. Klepněte na stránku **Autentizace**.
2. Zaškrtněte volbu **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
3. Vyberte volbu **Lokální autentizace pomocí ověřovacího seznamu**.
4. Jestliže existuje ověřovací seznam, vyberte jej z rozbalovacího seznamu a klepněte na **Otevřít**. Pokud jej vytváříte poprvé, zadejte jméno nového ověřovacího seznamu a klepněte na **Nový**.
5. Klepněte na **Přidat**, chcete-li nového uživatele přidat do ověřovacího seznamu.
6. V dialogovém okně Přidat uživatele vyplňte následující:
 - Vyberte autentizační protokol, pro který je jméno uživatele definované.
 - Zadejte jméno uživatele a heslo.

Poznámka: Z důvodů zabezpečení se doporučuje, abyste nepoužívali stejné heslo pro uživatele definovaného pro protokol CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) a PAP (Password Authentication Protocol).

- Zaškrtněte volbu **Použít pro uživatele metodu skupiny**, vyberte metodu skupiny z rozbalovacího seznamu a klepněte na **Otevřít**.

Vlastnosti metody skupiny můžete upravit nebo můžete pracovat s existujícím nastavením. Klepnutím na **OK** dokončíte konfiguraci a vrátíte se na stránku vlastností dvoubodového připojení.

Použití pravidel filtrování IP na připojení PPP

Téma Filtrování paketu IP a pravidla NAT v aplikaci Information Center popisuje, jak vytvářet pravidla IP paketů, na která se můžete odkazovat v profilu připojení PPP. Soubor pravidel paketů můžete použít pro omezení přístupu uživatelům nebo skupinám k IP adresám ve vaší síti. Příklad používání filtračních pravidel s připojením PPP naleznete ve scénáři Správa přístupu vzdálených uživatelů k prostředkům pomocí metod skupin a filtrování IP.

Na existující filtrovací pravidla IP paketů se můžete odvolávat dvěma způsoby:

- Úroveň profilu připojení
 1. Když ukončíte **Vlastnosti dvoubodového spojení** pro určitý **profil připojení příjemce**, vyberte stránku Nastavení TCP/IP a klepněte na **Rozšířené**.
 2. Zaškrtněte volbu **Použít pro toto připojení pravidla paketu IP** a vyberte identifikátor filtru PPP z rozbalovacího seznamu.
 3. Klepněte na **OK**, chcete-li použít filtr PPP pro profil připojení.
- Uživatelská úroveň
 1. Otevřete existující metody přístupu skupiny nebo vytvořte novou metodu přístupu skupiny.
 2. Klepněte na stránku Nastavení TCP/IP.
 3. Zaškrtněte volbu **Použít pro toto připojení pravidla paketu IP** a vyberte identifikátor filtru PPP z rozbalovacího seznamu.
 4. Klepnutím na **OK** použijete filtr PPP.

Povolení serverů RADIUS a DHCP pro profily připojení

Povolení serverů RADIUS a DHCP pro profily příjemce připojení PPP:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**.
2. Klepněte pravým tlačítkem myši na **RAS (Remote Access Services)** a vyberte **Služby**.
3. Klepněte na ouško **DHCP-WAN**. Tím automaticky povolíte DHCP a detekuje se, který server DHCP a agenti přenosu (pokud vůbec nějakí) jsou spuštěny v systému.
4. Chcete-li aktivovat služby RADIUS, klepněte na ouško **RADIUS**.
 - a. Vyberte **Povolit připojení k serveru RADIUS pro přístup do sítě**.
 - b. Vyberte **Povolit RADIUS pro autentizaci**.
 - c. Jestliže je to vhodné pro vaše řešení RADIUS, můžete také povolit účtování RADIUS a konfiguraci adres TCP/IP.
5. Když klepnete na tlačítko **Nastavení RADIUS NAS**, můžete konfigurovat připojení k serveru RADIUS.
6. Klepnutím na OK se vrátíte do prostředí produktu iSeries Navigator.

Příklad konfigurace serveru RADIUS naleznete ve scénáři Autentizace vytáčených připojení pomocí RADIUS NAS.

Kapitola 7. Správa PPP

Toto jsou úkoly správy PPP, které můžete provádět na serveru iSeries:

- nastavení vlastností profilů připojení
- monitorování aktivity PPP

Nastavení vlastností profilů připojení PPP

Při vytváření profilu připojení obvykle v dialogovém okně Nastavení profilu dvoubodového spojení vyberete protokol, typ připojení a provozní režim nového profilu připojení. Jakmile zadáte své volby do tohoto dialogového okna, zobrazí se list vlastností profilu připojení. Výběr, který uvedete v dialogovém okně nastavení profilu dvoubodového spojení určuje obsah stránky a pořadí oušek na listu vlastností profilu připojení. List vlastností se liší pro profily připojení odesílatele a profily připojení příjemce.

Při vyplňování každé stránky nového dialogového okna **Vlastnosti nového profilu dvoubodového spojení** můžete použít toto vodítko. Nastavení, která vyberete na každé stránce, závisí na vašem prostředí a typu připojení, které konfiguruje. Online nápověda pro produkt iSeries Navigator popisuje každou volbu, která se objevuje v dialogovém okně. Další informace naleznete v příkladech a procedurách PPP.

Monitorování aktivity PPP

Tato stránka vysvětluje, jak zobrazit profil připojení a protokol relace pomocí produktu iSeries Navigator.

Něco o úlohách připojení PPP:

- Existují dvě řídicí úlohy PPP, které se používají pro správu jednotlivých úloh připojení PPP. Tyto úlohy se provádějí v podsystému QSYSWRK:
 - QTPPPCTL - Hlavní řídicí úloha PPP. Tato úloha spravuje všechny úlohy připojení PPP.
 - QTPPPL2TP - Server L2TP. Tato úloha spravuje ustanovení tunelu L2TP a spouští se pouze tehdy, když je v daný okamžik spuštěný profil L2TP.
- Úlohy připojení PPP se provádějí pod uživatelským profilem QTCP a používají se pro obsluhování všech jednotlivých připojení PPP. Tyto úlohy se standardně spouští v podsystému QUSRWRK, lze je však konfigurovat tak, aby se spouštěly v jiných podsystémech. Používají se dvě jména úloh připojení:
 - QTPPPSSN - Tato úloha se používá pro obsluhu všech připojení, která nejsou L2TP PPP.
 - QTPPPL2SSN - Tato úloha se používá pro obsluhu virtuálních dat PPP poté, co úloha QTPPPL2TP úspěšně vyjedná tunel L2TP.
- Úlohy připojení SLIP se spouštějí v podsystému QSYSWRK pod uživatelským jménem QTCP. Existují dva typy jmen úloh SLIP:
 - QTPPDIAL nn jsou úlohy odchozího připojení, kde nn je libovolné číslo od 1 do 99.
 - QTPPANS nn jsou úlohy příchozího připojení, kde nn je libovolné číslo od 1 do 99.

Práce s komunikačními profily:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**. Vyberte volbu **Profil připojení odesílatele** nebo volbu **Profil připojení příjemce**.
2. Ve sloupci Profil klepněte pravým tlačítkem myši na libovolné jméno profilu připojení a vyberte jednu z následujících voleb:
 - Volba **Úlohy** otevírá protokol úloh pro úlohy QTPP xxx.
 - Volba **Připojení** otevírá dialogové okno pro zobrazení informací o všech připojeních, která jsou asociována s profilem. Informace mohou zahrnovat připojovací data pro aktuální připojení, dřívější připojení, nebo obojí. K dispozici jsou volby pro zobrazení výstupu úlohy nebo podrobností o každém připojení.

- Volba **Vlastnosti** otevírají stránky vlastností, které zobrazují aktuální vlastnosti připojení.

Zobrazení informací o připojení:

1. V prostředí produktu iSeries Navigator vyberte svůj server a rozbalte **Síť → RAS (Remote Access Services)**. Vyberte volbu **Profil připojení odesílatele** nebo volbu **Profil připojení příjemce**.
2. Ve sloupci Profil klepněte pravým tlačítkem myši na libovolné jméno profilu připojení, které není v neaktivním stavu, a vyberte **Připojení**, čímž se zobrazí informace o připojení.
Zobrazí se každé připojení s tímto profilem (aktuální i dřívější). Pole stavu ukazuje aktuální stav připojení. Další informace, jako například ID připojeného uživatele, lokální a vzdálené IP adresy a jméno úlohy PPP, mohou být uvedeny v závislosti na stavu každé PPP úlohy.
3. Chcete-li zobrazit výstup úlohy nebo podrobnosti pro připojení, klepněte pravým tlačítkem na připojení a tlačítka se povolí.
4. Chcete-li zobrazit výstup, klepněte na **Úlohy**. V protokolu úloh klepněte na jméno úlohy a vyberte **Tiskový výstup**. Pak je možné zobrazit obsah protokolů relace připojení a protokolů úloh (ukončených relací).
5. Chcete-li zobrazit podrobnosti o připojení, klepněte na **Podrobnosti**. Podrobnosti lze zobrazovat pouze pro momentálně aktivní připojení. Dialog podrobností připojení vám umožňuje prohlédnout si další informace o tomto konkrétním připojení.

Práce s výstupem PPP ze serveru iSeries:

Chcete-li pracovat s výstupem PPP, napište na příkazovou řádku serveru iSeries příkaz WRKTCPTP:

- Chcete-li pracovat se VŠEMI aktivními PPP úlohami (včetně úloh QTPPPCTL a QTPPPL2TP), stiskněte **F14** (Pracovat s aktivními úlohami).
- Chcete-li pracovat se všemi výstupy profilu určitého připojení, vyberte u daného profilu **volbu 8** (Pracovat s výstupem).
- Chcete-li vytisknout konfiguraci profilu PPP, vyberte u daného profilu **volbu 6** (Tisk). Pro přístup k tiskovému výstupu použijte příkaz WRKSPLF.

Stav připojení:


Stav profilu připojení se zobrazuje v poli **Stav** u daného profilu v seznamu profilů připojení, pod **Síť > RAS (Remote Access Services)** poté, co vyberete profily odesílatele nebo příjemce. Stav jednotlivého připojení se zobrazuje pomocí dialogu Připojení.

Popis primárního stavu	Vysvětlení
Waiting for connection requests (Čekání na požadavky o připojení)	Profil příjemce je připravený k připojení.
Waiting for incoming call (Čekání na příchozí volání)	Server je připravený k připojení.
Connecting (Připojování)	Probíhá proces připojování k vzdálenému systému.
Active/Active connections (Aktivní/aktivní připojení)	Připojení bylo vytvořeno a úloha probíhá úspěšně.
Inactive (Neaktivní)	S tímto profilem připojení se v současné době neprovádějí žádné úlohy.
Ended (Ukončeno)	Informace jsou dostupné.
Multihop terminator is starting a multihop initiator (Terminátor pro více přechodů spouští iniciátor pro více přechodů)	Probíhá připojování s více přechody.
Multihop connection is active (Připojení s více přechody je aktivní)	Připojení s více přechody úspěšně navázáno.

Popis sekundárního stavu	Vysvětlení
--------------------------	------------

Initializing modem (Inicializace modemu)	Inicializace modemu při spouštění telefonického připojení.
Waiting for modem connection (Čekání na připojení modemu)	Server PPP ve stavu naslouchání.
DIALING xxx-xxxx (VYTÁČENÍ xxx-xxxx)	Číslo vytáčené telefonním klientem.
Incoming call detected (Detekováno příchozí volání)	Server PPP detekuje příchozí modemové volání.
Modem connected (Modem připojen)	Navázání spojení PPP úspěšně dokončeno.
Operational (V provozu)	Připojení PPP je aktivní.
Link terminated (Spojení ukončeno)	Připojení ukončil peer.
Stopped (Zastaveno)	Profil nebo úloha skončily.
Authentication failure (Autentizace selhala)	Připojení PPP nebylo vytvořeno, protože selhala autentizace.
Connection inactivity timeout (Časový limit nečinnosti připojení)	Připojení PPP nebylo vytvořeno z důvodu překročení časového limitu nečinnosti.
Negotiating IP addresses (Vyjednávání IP adres)	Připojení PPP skončilo kvůli problémům při vyjednávání IP.
Remote modem did not answer (Vzdálený modem neodpověděl)	Připojení PPP nebylo vytvořeno, protože z druhé strany nepřišla žádná odezva.
Protocol reject (Protokol zamítnut)	Připojení PPP nebylo vytvořeno kvůli selhání vyjednávání NCP.
Retry failure (Selhání opakovaného pokusu)	Připojení PPP nebylo vytvořeno, protože byl překročen počet opětovných pokusů.
Received PPPoE session confirmation from peer (Přijato potvrzení relace PPPoE od peera)	Vyjednávání PPPoE úspěšně dokončeno.
L2TP call established (L2TP volání vytvořeno)	Zpráva o vytvoření tunelu L2TP.

Kapitola 8. Odstraňování problémů s PPP

Aktuální a podstatné informace o PTF a odstraňování problémů najdete na domovské stránce TCP/IP serveru iSeries . Pod tímto odkazem jsou uvedeny nejnovější informace, které nahrazují informace obsažené v této části a převažují nad nimi.

Jestliže budete mít problémy s připojením PPP, můžete použít tento kontrolní seznam, abyste získali informace o chybě. Tento kontrolní seznam vám může pomoci odhalit symptomy chyb a řešit problémy s připojením PPP.


1. Požadované výchozí informace:

- typ vzdáleného hostitele, operační systém a úroveň
- úroveň operačního systému hostitelského serveru iSeries
- protokol úlohy selhávající relace a soubor spojovacího dialogu
Ve vydání V5R1 se protokoly úloh a výstup spojovacích dialogů ukládají do fronty OUTQ se stejným jménem jako profil.
- skript pro spojení, jestliže se ve vašem prostředí používá
- stav profilu připojení před selháním připojení a po selhání připojení

2. Doporučené výchozí informace:

- popis linky
- profil připojení
volba 6 z WRKTCPPPTP tiskne nastavení profilu.
- typ a model modemu
- příkazové řetězce modemu
- sledování komunikace

O následujících problémech s PPP rozsáhle pojednává červená kniha ITSO TCP/IP for iSeries server: More



Cool Things Than Ever (SG24-5190) . Tato publikace rovněž poskytuje podrobné informace o řešení problémů.

Problém	Řešení
Hardwarová konfigurace modemu Nesprávná konfigurace přepínačů typu dip a dalšího hardwaru.	Ujistěte se, že je modem konfigurovaný pro správný typ rámce. Může být buď <i>asynchronní</i> , nebo <i>synchronní</i> . Další informace naleznete v příručce k modemu.
AT příkazy modemu Modem, který se snažíte používat, není v seznamu modemů, který je předdefinovaný v produktu iSeries Navigator.	Vytvořit nový modem.
Uživatelé a hesla PPP Při pokusu o připojení PPP se objevují chyby jména uživatele a hesla.	<ul style="list-style-type: none"> • Zajistěte, aby ID uživatele a heslo byly zadány stejnou velikostí písma. • Zajistěte, aby autentizační protokol, který používají peerové, byl tentýž. • Nepoužívejte u jednoho peera PAP, zatímco druhý peer je konfigurovaný jako CHAP.
Linky PPP pro spuštění profilu připojení Označené linky PPP jsou používány stejným hardwarovým prostředkem.	Neopomeňte logicky vypnout jiné linky, které používají stejný hardwarový prostředek.

Problém	Řešení
Protokol PPP K chybám připojení může docházet kvůli vadné konfiguraci protokolu PPP.	Možná bude nutné důkladně prozkoumat protokol PPP v těch případech, kdy peerové nejsou schopni spolu vzájemně komunikovat kvůli chybě konfigurace. Pokud protokol PPP ani protokol úlohy neukazují žádný náznak problému, můžete problém prozkoumat pomocí funkce pro sledování komunikace.

Kapitola 9. Další informace o PPP

Další zdroje informací o PPP:

- Nejnovější PTF a nejnovější informace o konfiguraci PPP a L2TP najdete pod odkazem PPP na domovské stránce TCP/IP serveru iSeries  . Pod tímto odkazem jsou uvedeny nejnovější informace, které nahrazují informace obsažené v části **RAS (Remote Access Services): Připojení PPP**, a převažují nad nimi.
- O službách a aplikacích TCP/IP rozsáhle pojednává červená kniha ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  .



IBM Confidential
Vytisťeno v Dánsku společností IBM Danmark A/S.