System i

Vytváření sítí RAS (Služby vzdáleného přístupu): Připojení PPP

verze 6, vydání 1

System i

Vytváření sítí RAS (Služby vzdáleného přístupu): Připojení PPP

verze 6, vydání 1

Poznámka

Před použitím informací a produktu, ke kterému se vztahují, si přečtěte informace uvedené v části “Poznámky”, na stránce 63.

Toto vydání se týká verze 6, vydání 1, modifikace 0 operačního systému IBM i5/OS (číslo produktu 5761–SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tuto verzi není možné spouštět na všech modelech RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

Služby vzdáleného přístupu: Připojení PPP

Protokol PPP (point-to-point) je internetový standard pro datové přenosy po sériových linkách.

PPP je mezi poskytovateli služeb sítě Internet (ISP) nejpoužívanější protokol. Protokol PPP povoluje jednotlivým počítačům přístup do sítí. Sítě postupně poskytují přístup k Internetu. Systém System i zahrnuje podporu TCP/IP PPP jako část své připojitelnosti k dálkové síti (WAN).

Připojíte-li vzdálený počítač k platformě System i přes protokol PPP, budete si moci vyměňovat data mezi jednotlivými místy. Prostřednictvím PPP mohou vzdálené počítače, které jsou připojeny k systému, přistupovat k prostředkům nebo jiným počítačům, které patří do téže sítě jako váš systém. Systém také můžete nakonfigurovat tak, aby se přes protokol PPP připojoval k Internetu. Průvodce vytáčeným připojením v produktu System i Navigator vás provede připojením systému k Internetu nebo k interní síti.

Soubor PDF pro RAS (Služby vzdáleného přístupu)

Tyto informace můžete prohlížet a tisknout ve formátu PDF.

Chcete-li zobrazit nebo stáhnout verzi PDF tohoto dokumentu, vyberte odkaz RAS: Připojení PPP (zhruba 940 kB).

Ukládání souborů ve formátu PDF

Takto uložíte soubor ve formátu PDF na své pracovní stanici, abyste jej mohli prohlížet a tisknout:

1. Klepněte pravým tlačítkem myši na odkaz na PDF v prohlížeči.
2. Klepněte na volbu, která ukládá soubor PDF lokálně.
3. Vyhledejte adresář, do kterého chcete soubor PDF uložit.
4. Klepněte na **Save (Uložit)**.

Jak stáhnout produkt Adobe Reader

Chcete-li prohlížet a tisknout soubory PDF, musíte mít v systému nainstalovaný produkt Adobe Reader. Jeho kopii si můžete stáhnout z webových stránek Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Související odkazy

“Informace související s RAS (Služby vzdáleného přístupu)” na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Koncepce PPP

PPP můžete používat k připojení platformy System i ke vzdáleným sítím, klientským PC, jiným platformám System i nebo k poskytovateli služeb sítě Internet (ISP). Chcete-li tento protokol plně využívat, je třeba dobře rozumět jeho možnostem a vědět, jak jej systém i5/OS může podporovat.

Související odkazy

“Informace související s RAS (Služby vzdáleného přístupu)” na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Co je PPP

Protokol PPP (point-to-point) je protokol TCP/IP, který se používá pro připojení jednoho počítačového systému k jinému. Počítače používají protokol PPP, ke komunikaci po telefonní síti nebo po Internetu.

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 umožňuje schopnost spolupráce systémů mezi softwarovými produkty vzdáleného přístupu 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 webových stránkách produktu RFC Editor .

- RFC-1661 Point-to-Point Protocol
- RFC-1662 PPP on HDLC-like framing
- RFC-1994 PPP CHAP

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.

Můžete použít dva typy profilů, které vám umožňují definovat sadu charakteristik pro připojení PPP nebo sadu připojení:

- *Profily připojení odesílatele* jsou připojení PPP, která jsou iniciována lokálním systémem a přijata vzdáleným systémem. Pomocí tohoto objektu můžete konfigurovat odchozí připojení.
- *Profily připojení příjemce* jsou připojení PPP iniciovaná vzdáleným systémem a přijatá místním systémem. Pomocí tohoto objektu můžete konfigurovat příchozí připojení.

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

- Jaký typ protokolu připojení budete používat? (PPP nebo SLIP (Serial Line Internet Protocol))
- Kontaktuje váš systém jiný počítač tím, že navazuje telefonické připojení (odesílatel)? Čeká váš systém na přijetí volání od jiného systému (příjemce)?
- Jakou komunikační linku bude připojení používat?
- Jak by měl váš systém určovat, jakou adresu IP použít?
- Jak by měl váš systém autentizovat jiný systém? Kam by měl systém 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
- ověření
- nastavení TCP/IP: adresy IP, směrování a IP filtrování
- řízení práce a přizpůsobení komunikace
- servery jmen domény

Systém ukládá tyto informace o konfiguraci do profilu připojení. Tyto informace poskytují systému kontext nutný k vytvoření připojení PPP k jinému 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**. Výběr režimu uvádí typ připojení a provozní režim tohoto profilu připojení.

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

  – komutovaná linka

– pronajatá (vyhrazená) linka
– L2TP (Layer Two Tunneling Protocol) (virtuální linka)
– protokol PPP (Point-to-Point Protocol) over Ethernet (PPPoE) (virtuální linka)

PPPoE je jediný podporovaný protokol pro profily odesílatele připojení.

- **Provozní režim**. Dostupný provozní režim závisí na typu připojení.

Tabulka 1. Dostupné provozní režimy pro profily připojení odesílatele

Typ připojení	Dostupné provozní režimy
Komutovaná linka	• vytáčení • vytáčení na požádání (pouze vytáčení) • vytáčení na požádání (vyhrazený peer s možností odpovídat) • vytáčení na požádání (umožněný vzdálený peer)
Pronajatá linka	iniciátor
L2TP	• iniciátor • iniciátor pro více přechodů • vzdálené vytáčení
PPP přes Ethernet	iniciátor

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
  – oblast linek

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

  Související odkazy

  “Požadavky na software a hardware” na stránce 30
  Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, platforma System i, může být buď odesílatelem, nebo příjemcem.

Podpora zásad skupiny

S podporou zásad skupiny mohou správci sítě definovat zásady skupin podle uživatelů pro správu prostředků. K určitým uživatelům je možné přiřadit zásady pro řízení přístupu, když se přihlásí k relaci protokolu PPP (Point-to-Point Protocol) nebo L2TP (Layer Two Tunneling Protocol).

Uživatelé mohou být identifikováni jako ti, kteří náleží do určité třídy uživatelů. Každá třída má jedinečné zásady, které definují omezení prostředků (například linky povolené v balíku multilink), atributy (například přesměrování IP) a označení, která sada pravidel filtrování paketů IP bude použita. Například s podporou zásad skupiny mohou správci sítě definovat skupinu Work_at_Home, která bude umožňovat úplný přístup do sítě, nebo skupinu Vendor_Workers, která bude mít omezení pro množinu služeb.

Související odkazy

"Scénář: Připojení systému ke koncentrátoru přístupu PPPoE" na stránce 10
Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

"Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP" na stránce 22
Zásady 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 adresám IP ve vaší síti.

Scénáře: Vzdálený přístup s pomocí připojení PPP

Tyto scénáře popisují, jak funguje protokol PPP a jak naimplementovat prostředí PPP v síti. Než přistoupíte k plánování a konfiguraci, seznamte se základními koncepcemi PPP pomocí těchto scénářů, které jsou přínosné pro začínající i zkušené uživatele.

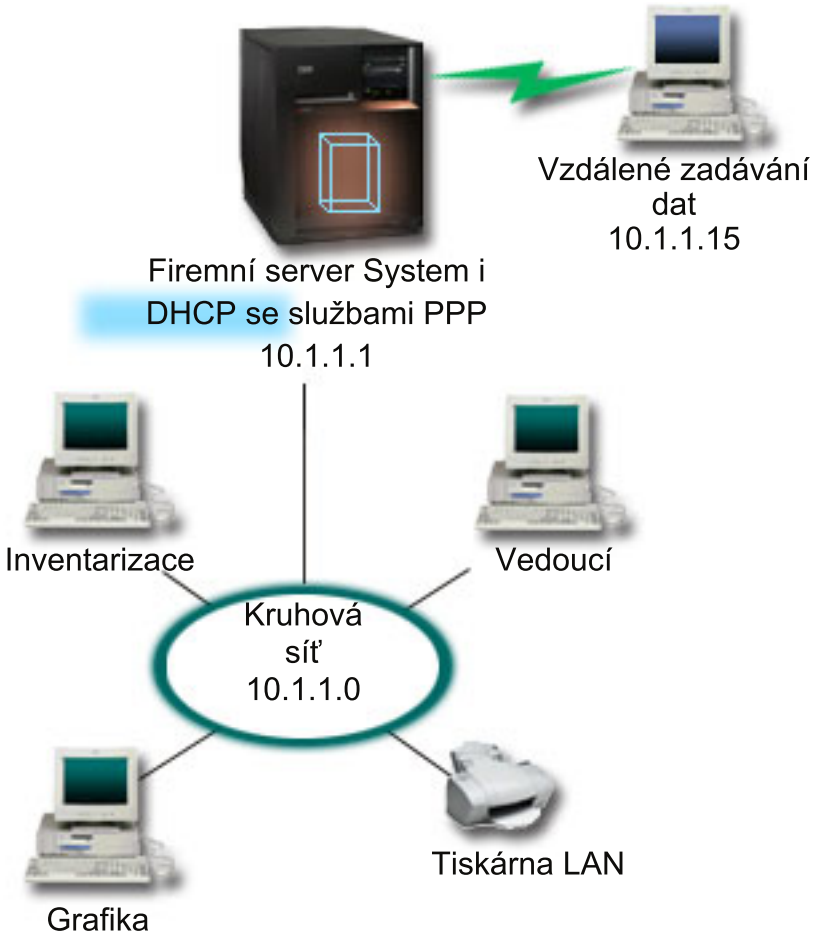
Související odkazy

"Informace související s RAS (Služby vzdáleného přístupu)" na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Příklad: PPP a DHCP na jediném systému System i

Tento příklad vysvětluje, jak nastavit model System i jako server DHCP (Dynamic Host Configuration Protocol) pro síť LAN a vzdálené volající klienty.

Vzdálení uživatelé, jako například volající klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup k modelu System i prostřednictvím protokolu PPP. Pro přístup k síti potřebuje volající klient IP informace, stejně jako jakýkoliv přímo připojený síťový klient. Server System i DHCP může volajícímu klientovi PPP informace o adrese IP distribuovat stejně jako v případě jakéhokoliv jiného přímo připojeného klienta. Následující obrázek zobrazuje vzdáleného klienta, který se musí telefonicky připojit do sítě společnosti, aby mohl vyřídit nějakou práci.



Obrázek 1. PPP a DHCP na jediném modelu System i

Aby se mohl vzdálený zaměstnanec úspěšně připojit k síti společnosti, musí model System i použít kombinaci služeb RAS (Služby vzdáleného přístupu) a DHCP. Funkce RAS (Služby vzdáleného přístupu) umožňuje modelu System i využívat funkce volání. Pokud je správně nastavena, sdělí server PPP serveru DHCP poté, co klient vytvoří připojení prostřednictvím telefonu, aby klientovi distribuoval informace TCP/IP.

V tomto příkladu jediná zásada podsítě DHCP ovlivňuje síťové klienty na místě i volající klienty.

Pokud chcete, aby profil PPP odložil distribuci adres IP serverem DHCP, musíte to provést v profilu PPP. V nastavení TCP/IP profilu příjemce připojení musíte nastavit metodu přiřazování vzdálených adres IP z ″Pevná″ na ″DHCP″. Chcete-li povolit volajícím klientům, aby komunikovali s ostatními síťovými klienty, jako například s tiskárnou sítě LAN, musíte také v nastavení TCP/IP tohoto profilu a vlastnostech konfigurace (zásobníku) TCP/IP povolit směrování pomocí IP. Pokud nastavíte směrování pomocí IP pouze v profilu PPP, nebude model System i IP pakety předávat. Směrování pomocí IP musíte nastavit pro profil i zásobník.

Kromě toho adresa IP lokálního rozhraní v profilu PPP musí být adresou IP, která spadá pod definici podsítě na serveru DHCP. V tomto příkladu profil PPP lokálního rozhraní musí být 10.1.1.1. Tato adresa také musí být vyloučena z oblasti adres serveru DHCP tak, že není přiřazena některému klientu DHCP.

Plánování nastavení DHCP pro klienty na místě a klienty PPP

Tabulka 3. Volby globální konfigurace (platí pro všechny klienty obsluhované serverem DHCP)

Objekt		**Hodnota**
Volby konfigurace	Volba 1: maska podsítě	255.255.255.0
	Volba 6: server DNS (domain name server)	10.1.1.1
	Volba 15: název domény	mycompany.com
Provádí systém aktualizace DNS?		Ne
Podporuje systém klienty BOOTP?		Ne

Tabulka 4. Podsíť pro klienty na místě a volající klienty

Objekt		**Hodnota**
Jméno podsítě		MainNetwork
Adresy ke spravování		10.1.1.3 - 10.1.1.150
Čas pronájmu		24 hodin (předvoleno)
Volby konfigurace	zděděné volby	Volby z globální konfigurace
Adresy podsítě, které nejsou přiřazené serverem		10.1.1.1 (adresa lokálního rozhraní zadaná v nastavení TCP/IP profilu příjemce připojení v prostředí produktu System i Navigator)

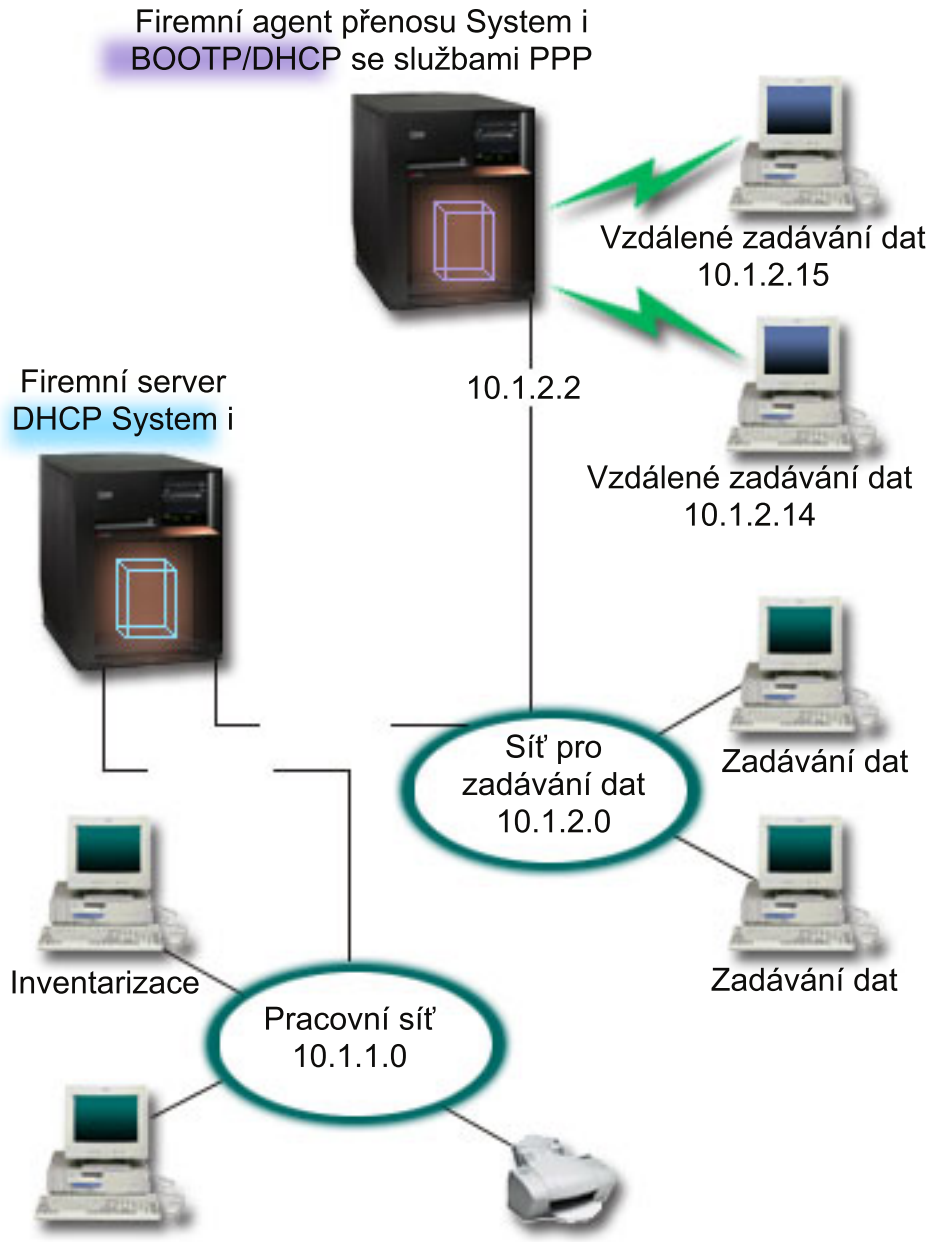
Ostatní nastavení

- Nastavte metodu vzdálených adres IP v profilu příjemce připojení PPP na DHCP.
  1. V prostředí produktu System i Navigator prostřednictvím položky nabídky **Služby** pro RAS (Služby vzdáleného přístupu) povolte připojení klienta DHCP WAN k serveru DHCP nebo připojení pro přenos.
  2. V prostředí produktu System i Navigator vyberte na stránce nastavení vlastností TCP/IP profilu připojení příjemce jako metodu přiřazení adres IP volbu Použít DHCP.
- V prostředí produktu System i Navigator v nastavení vlastností TCP/IP profilu příjemce připojení povolte vzdálenému systému přístup k ostatním sítím (směrování pomocí IP).
- V prostředí produktu System i Navigator na stránce nastavení vlastností konfigurace TCP/IP povolte Postoupení datagramu pomocí IP.

Příklad: Profil PPP a DHCP na různých modelech System i

Tento příklad vysvětluje, jak nastavit dva modely System i jako síťový server DHCP agenta přenosu BOOTP/DHCP pro dvě sítě LAN a vzdálené volající klienty.

Předchozí příklad, PPP a DHCP na jediném modelu System i popisuje, jak použít PPP a DHCP na jediném systému k tomu, aby byl volajícím klientům povolen přístup k síti. Ať již z důvodu fyzického rozvržení vaší sítě nebo potřeb zabezpečení dat může být vhodnější mít servery PPP a DHCP oddělené nebo mít vyhrazený server PPP bez služeb DHCP. Následující obrázek zobrazuje síť, která má volající klienty, ale zásady PPP a DHCP jsou na jiných serverech.



Obrázek 2. Profil PPP a DHCP na různých modelech System i

Vzdálení klienti pro zadávání dat volají server PPP System i. Profil PPP na tomto serveru musí mít stejně jako v příkladu použití PPP a DHCP v jednom modelu System i metodu vzdálených adres IP protokolu DHCP. Profil PPP a vlastnosti zásobníku TCP/IP na serveru PPP musí mít funkci přesměrování IP. Mimoto tento server funguje jako agent přenosu DHCP, musí být agent BOOTP/DHCP pro přenosy TCP/IP zapnutý. To umožňuje serveru vzdáleného přístupu System i předávat pakety DHCPDISCOVER DISCOVER serveru DHCP. Server DHCP bude poté odpovídat a distribuovat informace TCP/IP volajícím klientům prostřednictvím serveru PPP.

Server DHCP je zodpovědný za distribuci adres IP oběma sítím 10.1.1.0 a 10.1.2.0. V síti zadávání dat rozdá adresy IP v rozsahu od 10.1.2.10 do 10.1.2.40 buď volajícímu serveru, nebo přímo připojeným klientům. Klienti zadávání dat také potřebují adresu směrovače (volba 3) 10.1.2.1 ke komunikaci s pracovní stanicí a také server System i DHCP musí mít povoleno směrování pomocí adres IP.

Kromě toho adresa IP lokálního rozhraní v profilu PPP musí být adresou IP, která spadá pod definici podsítě na serveru DHCP. V tomto příkladu profil PPP lokálního rozhraní musí být 10.1.2.2. Tato adresa také musí být vyloučena z oblasti adres serveru DHCP tak, že není přiřazena některému klientu DHCP. Adresa IP lokálního rozhraní musí být adresa, na kterou server DHCP může zaslat pakety odpovědi.

Plánování nastavení DHCP pro DHCP s agentem přenosu DHCP

Tabulka 5. Volby globální konfigurace (platí pro všechny klienty obsluhované serverem DHCP)

Objekt		**Hodnota**
Volby konfigurace	Volba 1: maska podsítě	255.255.255.0
	Volba 6: server DNS (domain name server)	10.1.1.1
	Volba 15: název domény	mycompany.com
Provádí systém aktualizace DNS?		Ne
Podporuje systém klienty BOOTP?		Ne

Tabulka 6. Podsíť pracovní sítě

Objekt		**Hodnota**
Jméno podsítě		WorkNetwork
Adresy ke spravování		10.1.1.3 - 10.1.1.150
Čas pronájmu		24 hodin (předvoleno)
Volby konfigurace	zděděné volby	Volby z globální konfigurace
Adresy podsítě, které nejsou přiřazené serverem		žádné

Tabulka 7. Podsíť sítě pro zadávání dat

Objekt		**Hodnota**
Jméno podsítě		DataEntry
Adresy ke spravování		10.1.2.10 - 10.1.2.40
Čas pronájmu		24 hodin (předvoleno)
Volby konfigurace	Volba 3: směrovač	10.1.2.1
	zděděné volby	Volby z globální konfigurace
Adresy podsítě, které nejsou přiřazené serverem		10.1.2.1 (směrovač) 10.1.2.15 (adresa IP lokálního rozhraní klienta vzdáleného zadávání dat) 10.1.2.14 (adresa IP lokálního rozhraní klienta vzdáleného zadávání dat)

Jiné nastavení na platformě System i, na které jsou provozovány přenosy PPP

- Jak nastavit agenta přenosu BOOTP/DHCP serveru TCP/IP.

Objekt	**Hodnota**
Adresa rozhraní	10.1.2.2
Adresa IP serveru, na který jsou přenášeny pakety	10.1.2.1

- Nastavte metodu vzdálených adres IP v profilu příjemce připojení PPP na DHCP.
  1. V prostředí produktu System i Navigator prostřednictvím položky nabídky Služby pro RAS (Služby vzdáleného přístupu) povolte připojení klienta DHCP WAN k serveru DHCP nebo připojení pro přenos.

2. V prostředí produktu System i Navigator vyberte na stránce nastavení vlastností TCP/IP profilu připojení příjemce jako metodu přiřazení adres IP volbu Použít DHCP.

- V prostředí produktu System i Navigator ve vlastnostech nastavení TCP/IP pro profil připojení příjemce povolte vzdálenému systému přístup k ostatním sítím (směrování pomoci IP; abyste umožnili vzdáleným klientům komunikovat se sítí zadávání dat).
- V prostředí produktu System i Navigator na stránce nastavení vlastností konfigurace TCP/IP povolte Postoupení datagramu pomocí IP (aby mohli vzdálení klienti komunikovat se sítí zadávání dat).

Scénář: Ochrana nepovinného tunelu L2TP pomocí IPSec

V tomto scénáři se naučíte jak nastavit připojení mezi hostitelem pobočky firmy a ústředím firmy, které používá L2TP chráněný protokolem IPSec. Pobočka firmy má dynamicky přiřazenou adresu IP, zatímco ústředí firmy má statickou, globálně směrovatelnou adresu IP.

Situace

Předpokládejme, že má vaše společnost malou kancelář pobočky v jiném státě. V průběhu libovolného pracovního dne může pobočka vyžadovat přístup k důvěrným informacím o serveru System i, které jsou na společném intranetu. V současné době používá vaše společnost pro poskytnutí přístupu k firemní síti pobočce drahou pronajatou linku. Přestože chce vaše společnost i nadále poskytovat zabezpečený přístup k intranetu, chcete snížit náklady spojené s pronajatou linkou. To lze učinit vytvořením nepovinného tunelu L2TP (Layer 2 Tunnel Protocol), který rozšiřuje vaši firemní síť tak, že se bude kancelář pobočky zdát součástí firemní podsítě. Datové přenosy v tunelu L2TP jsou chráněny pomocí VPN.

S nepovinným tunelem L2TP ustanoví vzdálená kancelář pobočky tunel přímo k serveru LNS (L2TP network server) firemní sítě. Funkce L2TP Access Concentrator (LAC) jsou umístěny na klientovi. Tunel je transparentní pro ISP (Internet Service Provider) vzdáleného klienta, takže ISP nemusí podporovat L2TP. Pokud si chcete přečíst více o konceptech L2TP, přečtěte si informace uvedené v tématu L2TP (Layer 2 Tunnel Protocol).

Důležité: Tento scénář zobrazuje bezpečnostní přenosové brány připojené přímo k Internetu. Brána firewall je zde nepřítomna z důvodu zjednodušení scénáře. Z toho nevyplývá, že by použití brány firewall nebylo nutné. Rizika zabezpečení zvažte při každém připojení k Internetu.

Cíle

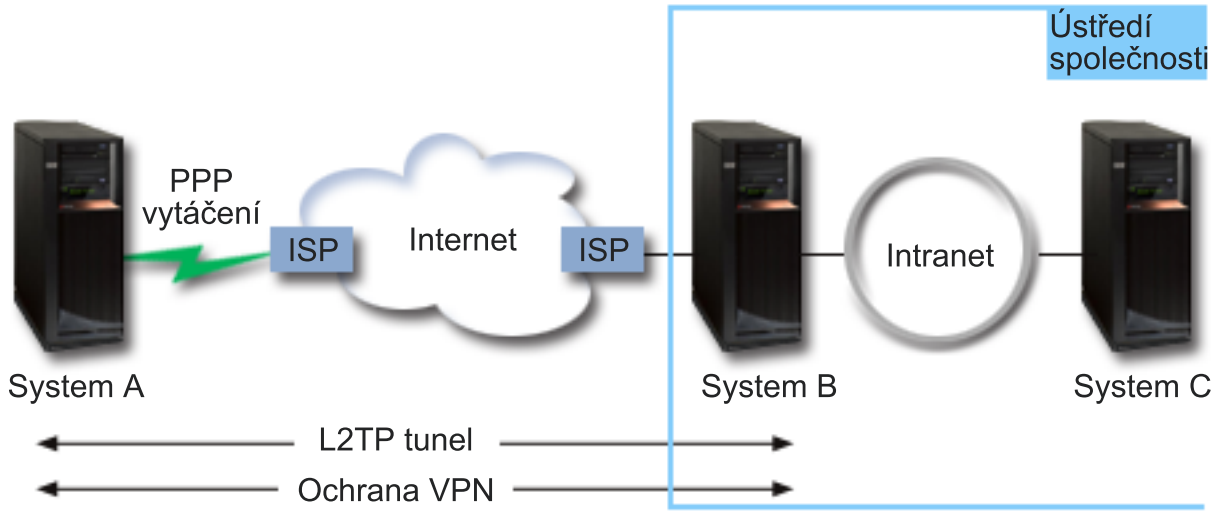
V tomto scénáři se systém kanceláře pobočky připojuje k firemní síti prostřednictvím systému brány s tunelem L2TP chráněným prostřednictvím VPN.

Hlavní cíle tohoto scénáře jsou :

- Systém kanceláře pobočky vždy iniciuje spojení s kanceláří ústředí.
- Systém kanceláře pobočky je jediným systémem v síti kanceláře pobočky, který potřebuje přístup do sítě ústředí. Jinými slovy jeho role v síti kanceláře pobočky je role hostitele, nikoliv brány.
- Korporační systém - hostitelský počítač v síti ústředí.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítě s tímto scénářem:



Systém A

- Musí mít přístup k aplikacím TCP/IP ve všech systémech ve firemní síti.
- Přijímá dynamicky přidělené adresy IP od svého ISP.
- Musí být konfigurován, aby poskytoval podporu L2TP.

Systém B

- Musí mít přístup k aplikacím TCP/IP na systému A.
- Podsíť je 10.6.0.0 s maskou 255.255.0.0. Tato podsíť představuje datový koncový bod tunelu VPN ve firemní síti.
- Připojuje se k Internetu s adresou IP 205.13.237.6. Toto je koncový bod připojení. Systém B tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy. Systém B se ke svým podsítím připojuje s adresou IP 10.6.11.1.

V podmínkách protokolu L2TP vystupuje *Systém A* jako iniciátor L2TP, zatímco *Systém B* vystupuje jako terminátor L2TP.

Úlohy konfigurace

Za předpokladu, že konfigurace TCP/IP je již vytvořena a funguje, musíte dokončit tyto úlohy:

Scénář: Připojení systému ke koncentrátoru přístupu PPPoE

Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

Situace

Váš podnik vyžaduje rychlejší připojení k Internetu, a proto se zajímáte o službu DSL (Digital Subscriber Line) u místního poskytovatele internetových služeb (ISP). Po počátečním průzkumu zjistíte, že váš ISP používá pro připojování svých klientů protokol PPPoE. Potřebujete toto připojení PPPoE využít k zajišťování širokopásmových připojení k Internetu prostřednictvím svého systému.

Obrázek 3. Připojení systému k ISP s využitím PPPoE

Řešení

Připojení k ISP přes PPPoE můžete podporovat prostřednictvím systému. Systém využívá nového typu virtuální linky, která je vázána na fyzickou linku sítě Ethernet konfigurovanou pro použití adaptéru Ethernet typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A nebo 576A. Tato virtuální linka podporuje protokoly relace PPP přes síť Ethernet LAN připojenou k DSL modemu, jež zajišťuje bránu ke vzdálenému ISP. Tato přenosová brána umožňuje uživatelům připojeným k síti LAN-connected vysokorychlostní přístup k Internetu prostřednictvím připojení PPPoE. Jakmile je připojení mezi systémem a ISP spuštěno, mohou jednotliví uživatelé v síti LAN přistupovat k ISP prostřednictvím PPPoE s použitím adresy IP přiřazené systému. Chcete-li zajistit dodatečné zabezpečení, můžete použít filtrační pravidla pro virtuální linku PPPoE, kterými se omezí určité příchozí internetové přenosy.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci PPP z produktu System i Navigator, postupujte takto:

1. Konfigurujte připojovací zařízení, které se bude používat pro váš ISP.
2. Nakonfigurujte profil připojení odesílatele na systému.

   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 označuje profil připojení i virtuální linku PPPoE.
4. Klepněte na **Připojení** a otevře se stránka Připojení. Vyberte **jméno virtuální linky PPPoE**, které odpovídá jménu pro tento profil připojení. Poté, co vyberete linku, produkt System i Navigator zobrazí dialog **vlastností linky**.

   a. Na stránce Obecné zadejte smysluplný popis virtuální linky PPPoE.

b. Klepněte na **Připojení** a otevře se stránka 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**. Produkt System i Navigator zobrazí dialog **Vlastnosti linky typu Ethernet**.

   Poznámka: PPPoE požaduje adaptér pro síť Ethernet typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A nebo 576A.

   1) Na stránce Obecné zadejte smysluplný popis linky Ethernet a ověřte, že definice linky používá požadované hardwarové prostředky.
   2) Klepněte na **Připojení** a otevře se stránka Připojení. Zadejte vlastnosti fyzické linky Ethernet. Další informace naleznete v dokumentaci ke svému adaptéru Ethernet a v online nápovědě.
   3) Klepněte na **Jiné** a otevře se stránka 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.

d. Když se vrátíte na stránku Připojení , určete adresování serveru PPPoE podle informací, které poskytuje váš ISP.

5. Pokud váš ISP požaduje, aby systém prokazoval svou totožnost, nebo chcete-li, aby systém autentizoval vzdálený systém, klepněte na **Autentizace**, čímž otevřete stránku Autenzizace, kde zadáte požadované informace.
6. Klepněte na **Nastavení TCP/IP**, čímž otevřete stránku Nastavení TCP/IP, a uveďte parametry zacházení s adresami IP pro tento profil připojení. Nastavení, které se má používat, by měl poskytnout váš ISP (poskytovatel služeb Internetu). Chcete-li umožnit uživatelům připojeným k LAN, aby se připojovali k ISP pomocí adres IP alokovaných na systému, vyberte volbu **Skrýt adresy (zcela zamaskovat)**.
7. Klepněte na **DNS** a otevře se stránka DNS, kde zadejte adresu IP serveru DNS, kterou vám poskytl ISP.
8. Klepnutím na tlačítko **OK** profil dokončete.

Související pojmy

“Podpora zásad skupiny” na stránce 3
S podporou zásad skupiny mohou správci sítě definovat zásady skupin podle uživatelů pro správu prostředků. K určitým uživatelům je možné přiřadit zásady pro řízení přístupu, když se přihlásí k relaci protokolu PPP (Point-to-Point Protocol) nebo L2TP (Layer Two Tunneling Protocol).

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Související odkazy

“Konfigurace linky” na stránce 48
V konfiguraci linky se definuje typ služby linky, kterou váš profil připojení PPP používá pro ustanovení připojení.

“Autentizace systému” na stránce 41
Na platformě System i podporují připojení PPP několik voleb pro autentizaci vzdálených klientů volajících na systém, a také připojení k ISP nebo k jinému systému, na který systém volá.

“Práce s adresou IP” na stránce 39
Připojení PPP umožňuje několik různých množin voleb pro správu adres IP v závislosti na typu profilu připojení.

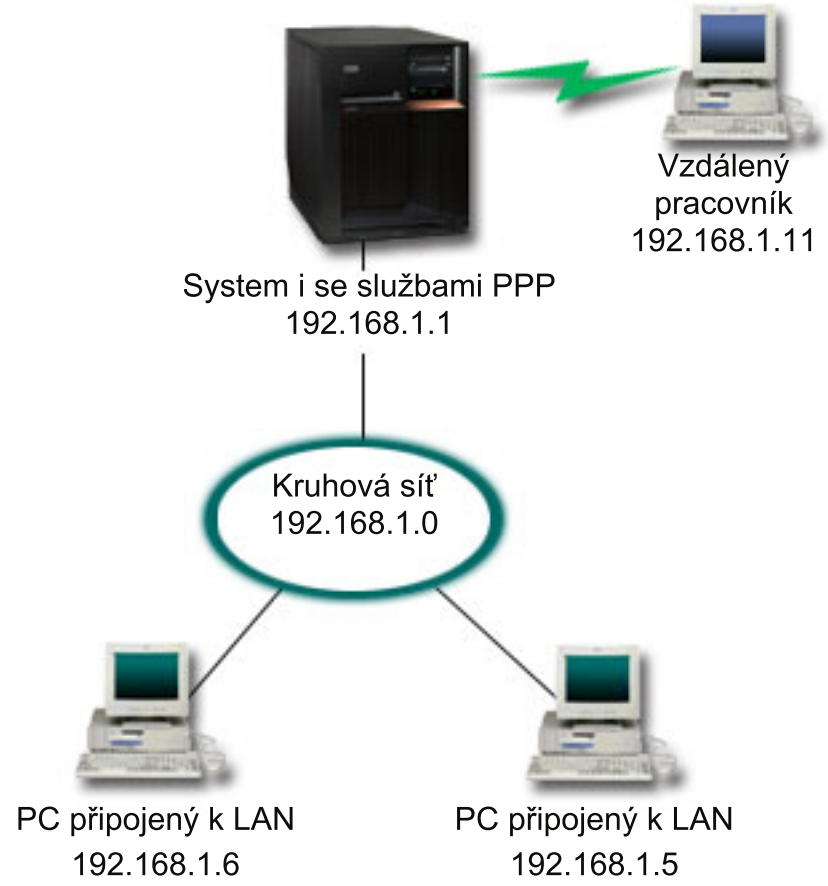
“Filtrování IP paketů” na stránce 39
Filtrování IP paketů omezuje služby pro jednotlivé uživatele, když se přihlašují do sítě.

Scénář: Připojení vzdálených volajících klientů k systému

Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

Situace

Jako administrátor sítě vaší firmy máte na starost údržbu systému i síťových klientů. Místo toho, abyste chodili do práce řešit a odstraňovat problémy, potřebujete možnost pracovat z nějakého vzdáleného místa, například ze svého domova. Jelikož vaše firma nemá vázané síťové připojení k Internetu, můžete se k firemnímu systému připojit prostřednictvím protokolu PPP. Kromě toho máte v současné době pouze modem 7852-400 ECS, který pro toto připojení musíte využít.



Obrázek 4. Připojení vzdálených klientů k systému

Řešení

Pro připojení domácího PC k systému 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 je znázorněn systém se službami PPP, který je připojen k síti LAN se dvěma PC. Vzdálený pracovník se pak spojí se systémem. Systém ověří svou totožnost a stane se součástí pracovní sítě (192.168.1.0). V tomto případě je snazší klientovi, který se připojuje pomocí vytáčeného připojení, přiřadit statickou adresu IP.

Vzdálený pracovník použije protokol CHAP-MD5 (Challenge Handshake Authentication) k autentizaci v systému. Systém nemůže používat MS-CHAP, proto se ujistěte, že je klient PPP nastaven 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 pravidla filtrování, jež se budou uplatňovat na IP pakety takového klienta.

Na výše uvedeném obrázku je pouze jeden volající klient, protože modem electronic může obsluhovat v daném okamžiku pouze jedno připojení.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci PPP z produktu System i Navigator, postupujte takto:

1. Nakonfigurujte vytáčené připojení do sítě a vytvořte vytáčené připojení ke vzdálenému PC.
2. Nakonfigurujte profil připojení příjemce na systému.

   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 oblast linek v závislosti na vašem prostředí.
3. Na stránce Obecné ve vlastnostech nového profilu PPP zadejte jméno a popis profilu příjemce.
4. Klepněte na **Připojení** a otevře se stránka 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, kde je připojen váš 7852–400 adaptér a nastavte Rámcování na **Asynchronní**.
   b. Klepněte na **Modem** a otevřete stránku Modem. Z výběrového seznamu Jméno vyberte modem **IBM 7852–400**.
   c. Klepnutím na **OK** se vrátíte na stránku vlastností nového profilu PPP.
5. Klepněte na **Autentizace** a otevře se stránka autentizace.
   a. Klepněte na **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 **Nastavení TCP/IP** a otevřete stránku TCP/IP.
   a. Vyberte lokální adresu IP 192.168.1.1.
   b. Pro vzdálenou adresu IP vyberte volbu **Pevná adresa IP** s počáteční adresou IP 192.168.1.11.
   c. Vyberte **Povolit vzdálenému systému přístup k ostatním sítím**.
7. Klepnutím na tlačítko **OK** profil dokončete.

Související pojmy

“Plánování PPP” na stránce 30
Plánování PPP (Point-to-Point Protocol) zahrnuje vytváření a správu připojení PPP.

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Související odkazy

“CHAP-MD5 (Challenge Handshake Authentication Protocol with MD5)” na stránce 42
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.

“Konfigurace linky” na stránce 48
V konfiguraci linky se definuje typ služby linky, kterou váš profil připojení PPP používá pro ustanovení připojení.

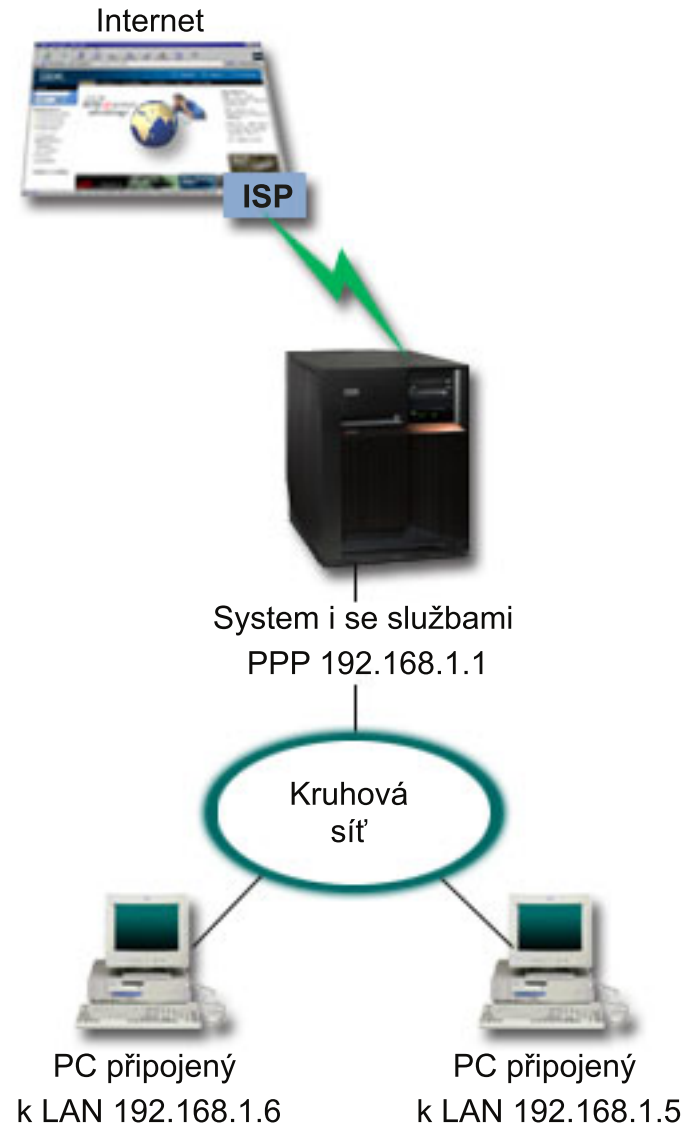
“Oblast linek” na stránce 49
Tuto službu linky vyberte, chcete-li nastavit, aby připojení PPP používalo linku z oblasti linek. Když je zahájeno připojení PPP, systém vybere nepoužívanou linku z oblasti linek. U profilů volání na vyžádání systém vybírá linku až tehdy, když detekuje provoz TCP/IP pro vzdálený systém.

Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu

Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. K připojení systému k některému ISP (poskytovateli internetových služeb) mohou použít modem. PC klienti připojení k síti LAN mohou s Internetem komunikovat tak, že používají operační systém i5/OS jako bránu.

Situace

Podniková aplikace, kterou vaše společnost používá, vyžaduje, aby uživatelé měli přístup k Internetu. Jelikož aplikace nevyžaduje velké přenosy dat, musíte být schopni k připojení systému a PC klientů v síti LAN používat modem. Tuto situaci znázorňuje následující obrázek.



Obrázek 5. Připojení podnikové sítě LAN k Internetu pomocí modemu

Řešení

K připojení systému k poskytovateli internetových služeb (ISP) můžete použít svůj integrovaný (nebo jiný kompatibilní) modem. Je třeba vytvořit profil odesílatele, pomocí něhož se k ISP zřídí připojení PPP.

Jakmile vytvoříte připojení mezi systémem a ISP, vaše počítače připojené k síti LAN budou moci komunikovat s Internetem, přičemž budou využívat systém jako bránu. Ujistěte se, že v profilu původce je zapnutá volba Skrýt adresy, aby klienti LAN, kteří mají soukromé adresy, mohli komunikovat s Internetem.

Když jsou nyní váš systém i síť připojeny k Internetu, je třeba, abyste se seznámili s bezpečnostními riziky. Spolupracujte se svým ISP, abyste poznali jeho strategii zabezpečení ochrany dat, a podnikněte další kroky k ochraně svého systému a sítě.

Podle toho, jak využíváte Internet, byste se měli zajímat o šířku pásma.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci z produktu System i Navigator, postupujte takto:

1. Nakonfigurujte profil připojení odesílatele na systému.

   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 oblast linek v závislosti na vašem prostředí.
2. Na stránce Obecné ve vlastnostech nového profilu PPP zadejte jméno a popis profilu odesílatele.
3. Klepněte na **Připojení** a otevře se stránka 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. Pokud vyberete jako prostředek interní modem, potom se provede automatický výběr typu modemu a nastavení typu rámcování.
   b. 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 **Autentizace** a otevře se stránka Autentizace, kde vyberte volbu **Povolit vzdálenému systému ověřit identitu tohoto serveru iSeries**. Vyberte si autentizační protokol a zadejte požadované jméno uživatele nebo heslo.
6. Klepněte na **Nastavení TCP/IP** a otevřete stránku TCP/IP.
   a. Vyberte volbu **Přiřazená vzdáleným systémem** pro adresy IP lokálních i vzdálených systémů.
   b. Vyberte volbu **Přidat vzdálený systém jako předvolenou předepsanou cestu**.
   c. Zaškrtněte volbu **Skrýt adresy**, aby vaše interní adresy IP nemohly být směrovány na Internet.
7. Klepněte na **DNS** a otevře se stránka DNS, kde zadejte adresu IP serveru DNS, kterou vám poskytl ISP.
8. Klepnutím na tlačítko **OK** profil dokončete.

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

Poznámka: Dbejte také na to, aby ostatní systémy ve vaší síti měly správně definováno směrování a aby se tak přenosy TCP/IP směrované na Internet z těchto systémů odesílaly přes systém.

Související pojmy

"Plánování PPP" na stránce 30
Plánování PPP (Point-to-Point Protocol) zahrnuje vytváření a správu připojení PPP.

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Související odkazy

“Oblast linek” na stránce 49
Tuto službu linky vyberte, chcete-li nastavit, aby připojení PPP používalo linku z oblasti linek. Když je zahájeno připojení PPP, systém vybere nepoužívanou linku z oblasti linek. U profilů volání na vyžádání systém vybírá linku až tehdy, když detekuje provoz TCP/IP pro vzdálený systém.

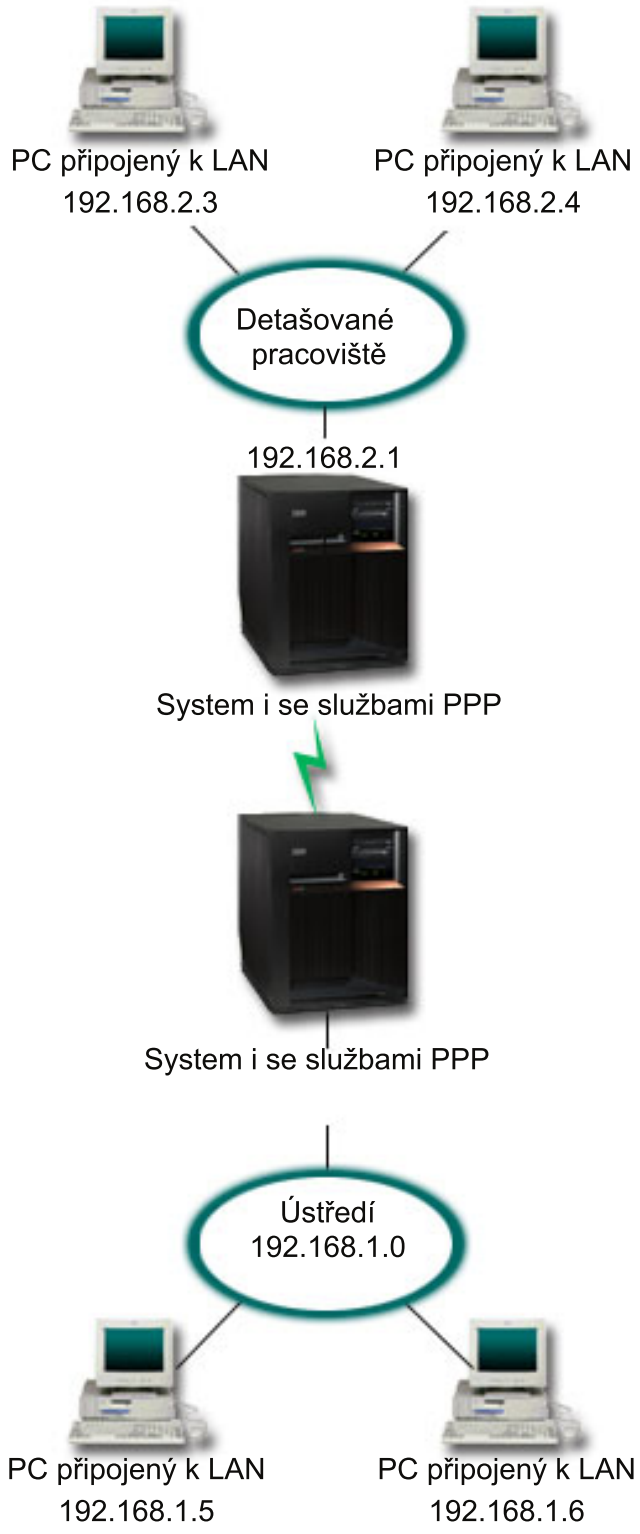
“Konfigurace linky” na stránce 48
V konfiguraci linky se definuje typ služby linky, kterou váš profil připojení PPP používá pro ustanovení připojení.

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 propojit dvě sítě LAN tak, že se vytvoří připojení mezi systémem v ústředí a jiným systémem v pobočce.

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 pro zadávání dat. Množství vyměněných dat není důvodem pro koupi fyzického síťového připojení, takže se pro propojení těchto dvou sítí rozhodnete používat modemy.



Obrázek 6. Propojení podnikové sítě a vzdálené sítě pomocí modemu

Řešení

Protokol PPP lze využít k vzájemnému propojení dvou sítí LAN - vytvoří se připojení mezi jednotlivými systémy, jak znázorňuje obrázek. V tomto případě předpokládejme, že vzdálená kancelář iniciuje připojení s ústředím firmy. Budete konfigurovat profil odesílatele na vzdáleném systému a profil příjemce 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 adres IP (v tomto příkladu 192.168.2, 192.168.3, 192.168.1.6 a 192.168.1.5). Musí být také aktivováno zasílání adres IP 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.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci z produktu System i Navigator, postupujte takto:

1. Budete konfigurovat profil odesílatele na vzdáleném systému ústředí společnosti.

   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 oblast linek v závislosti na vašem prostředí.
2. Na stránce Obecné ve vlastnostech nového profilu PPP zadejte jméno a popis profilu odesílatele.
3. Klepněte na **Připojení** a otevře se stránka 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 **Modem** a otevřete 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 systému ústředí společnosti. Dbejte na to, abyste zahrnuli případně požadovanou předponu.
5. Klepněte na **Autentizace** a otevře se stránka Autentizace, kde vyberte volbu **Povolit vzdálenému systému ověřit identitu tohoto serveru iSeries**. Vyberte volbu **Požadovat šifrované heslo (CHAP-MD5)** a zadejte požadované jméno uživatele a heslo.
6. Klepněte na **Nastavení TCP/IP** a otevřete stránku nastavení TCP/IP.
   a. Jako lokální adresu IP vyberte adresu IP rozhraní LAN vzdálené kanceláře (192.168.2.1) z výběrového rámečku **Použít pevnou adresu IP**.
   b. Jako adresu IP 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 připojení příjemce na systému ústředí společnosti.

   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 oblast linek v závislosti na vašem prostředí.
8. Na stránce Obecné ve vlastnostech nového profilu PPP zadejte jméno a popis profilu příjemce.
9. Klepněte na **Připojení** a otevře se stránka 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 **Modem** a otevřete 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 **Autentizace** a otevře se stránka 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 **Nastavení TCP/IP** a otevřete stránku nastavení TCP/IP.
    a. Jako lokální adresu IP vyberte z rámečku pro **výběr** adresu IP rozhraní systému ústředí (192.168.1.1).
    b. Jako adresu IP vzdáleného systému vyberte volbu **Na základě ID uživatele vzdáleného systému**. Objeví se dialog **Adresy IP definované jménem uživatele**. Klepněte na tlačítko **Přidat**. Vyplňte pole pro jméno volajícího uživatele, adresu IP a masku podsítě. V našem scénáři jsou správné následující hodnoty:
       - Jméno volajícího uživatele: Remote_site
       - Adresa IP: 192.168.2.1
       - Maska podsítě: 255.255.255.0

       Klepněte na **OK** a znovu klepněte na **OK**, čímž se vrátíte na stránku nastavení TCP/IP.
    c. Vyberte volbu **Směrování pomocí IP**, čímž umožníte ostatním systémům v síti používat tento systém jako bránu.
12. Klepněte na **OK**, čímž dokončíte profil příjemce.

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Související odkazy

“Konfigurace linky” na stránce 48
V konfiguraci linky se definuje typ služby linky, kterou váš profil připojení PPP používá pro ustanovení připojení.

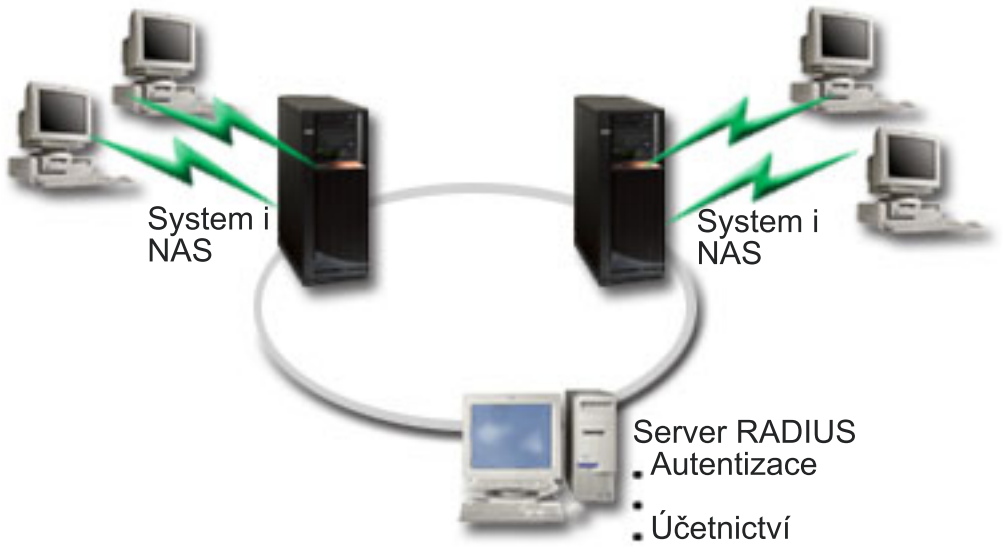
“Oblast linek” na stránce 49
Tuto službu linky vyberte, chcete-li nastavit, aby připojení PPP používalo linku z oblasti linek. Když je zahájeno připojení PPP, systém vybere nepoužívanou linku z oblasti linek. U profilů volání na vyžádání systém vybírá linku až tehdy, když detekuje provoz TCP/IP pro vzdálený systém.

Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS

Server NAS (Network Access Server) spuštěný na systému může směrovat požadavky na autentizaci volajících klientů na samostatný server RADIUS. Jestliže dojde k autentizaci, může server RADIUS také řídit adresy IP přiřazené uživatelům.

Situace

Do sítě vašeho podniku se telefonicky připojují vzdálení uživatelé ke dvěma systémům. Potřebujete způsob, jak centralizovat autentizaci, služby a účtování, aby jeden systém mohl vyřizovat požadavky na ověřování ID a hesel uživatelů a určovat, které adresy IP jsou jim přiřazené.



Obrázek 7. Autentizace vytáčených připojení pomocí serveru RADIUS

Řešení

Když se uživatelé pokusí o připojení, server NAS (Network Access Server) spuštěný na systémech odešle autentizační informace na server 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 adresy IP a aktivoval účtování za účelem sledování aktivity uživatele a využití. Chcete-li podporovat služby RADIUS, je třeba, abyste na systému definovali server RADIUS NAS.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci z produktu System i Navigator, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Síť**, klepněte pravým tlačítkem myši na **RAS (Služby vzdáleného přístupu)** a vyberte **Služby**.
2. Na kartě **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 **Adresa IP lokálního systému** zadejte adresu IP rozhraní používanou pro připojení k serveru RADIUS.
   b. Do rámečku **Adresa IP serveru** zadejte adresu IP pro server RADIUS.
   c. Do rámečku **Heslo** zadejte heslo používané k identifikaci systému na serveru RADIUS.
   d. Do rámečku **Port** zadejte port na systému používaný ke komunikaci se serverem RADIUS. Pro autentizační server je předvolený port 1812, pro účtovací server je to port 1813.
6. Klepněte na **OK**.
7. V prostředí produktu System i Navigator rozbalte **Síť → Služby vzdáleného přístupu**.
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 volbu **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
10. Vyberte **Vzdálená autentizace pomocí serveru RADIUS**.
11. Vyberte autentizační protokol (PAP nebo CHAP-MD5). Tento protokol musí používat také server RADIUS.
12. Vyberte volbu **Povolit RADIUS pro editování a účtování připojení**.
13. Klepnutím na **OK** uložíte změnu 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 telefonicky připojují pomocí tohoto profilu připojení, systém odešle informace o autentizaci 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.

Související úlohy

"Povolení služeb RADIUS a DHCP pro profily připojení" na stránce 58
Pokyny pro povolení služeb RADIUS nebo DHCP (Dynamic Host Configuration Protocol) pro profily připojení příjemců PPP.

Související odkazy

"Autentizace systému" na stránce 41
Na platformě System i podporují připojení PPP několik voleb pro autentizaci vzdálených klientů volajících na systém, a také připojení k ISP nebo k jinému systému, na který systém volá.

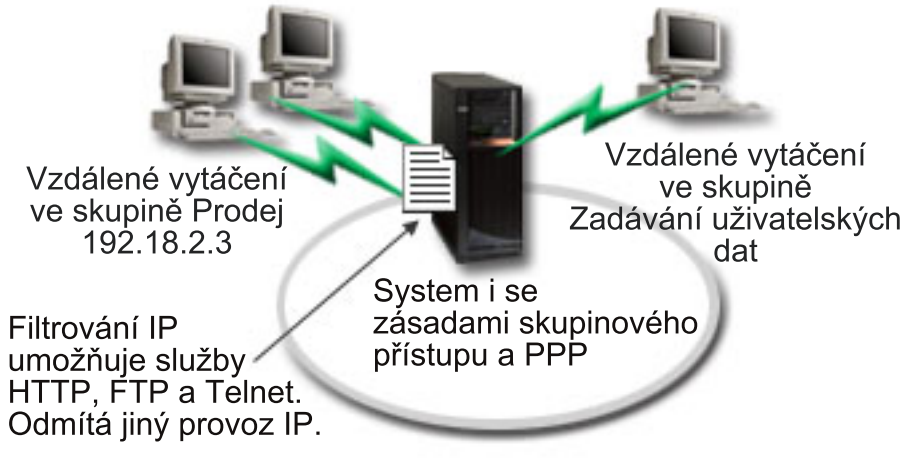
"Přehled o protokolu RADIUS (Remote Authentication Dial In User Service)" na stránce 43
RADIUS (Remote Authentication Dial in User Service) je standardní internetový protokol, který poskytuje služby centralizované autentizace, účtování a správy IP uživatelům vzdáleného přístupu na distribuované vytáčené síti.

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

Zásady 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 adresám IP ve vaší síti.

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 dalším aplikacím. Lidé z ostatních společností potřebují 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 nebude zaručovat dostatečnou kontrolu. Potřebujete nějak definovat nastavení a možnosti připojení pro několik odlišných skupin uživatelů, kteří se běžně připojují k tomuto systému přes telefonní linku.



Obrázek 8. Nastavení vytáčených připojení s uplatněním zásady skupinového nastavení

Řešení

Potřebujete použít jedinečná filtrovací omezení IP na dvě různé skupiny uživatelů. Toho dosáhnete tak, že vytvoříte zásady přístupu skupin a pravidla filtrování IP. Zásady přístupu skupin se odkazují na pravidla filtrování IP, takže nejprve musíte vytvořit pravidla filtrování. V tomto příkladu musíte vytvořit filtr PPP, který má zahrnovat pravidla filtrování IP pro zásadu přístupu skupiny obchodních partnerů IBM. Tato pravidla filtrování povolí služby HTTP, FTP a Telnet, avšak zamezí přístupu ke všem ostatním přenosům a službám TCP/IP na systému. Tento scénář pouze zobrazuje pravidla filtrování potřebná pro skupinu prodeje; podobné filtry byste si však mohli také nastavit pro skupinu Zadávání dat.

Nakonec si musíte vytvořit zásady přístupu skupiny (vždy jednu pro jednu skupinu), čímž svou skupinu definujete. Zásada přístupu skupiny vám umožňuje definovat běžné atributy připojení pro uživatele ve skupině. Přidáte-li zásadu přístupu skupin do Ověřovacího seznamu na systému, budete moci použít toto nastavení připojení během procesu autentizace. Zásada přístupu skupiny definuje několik nastavení pro relaci uživatele včetně možnosti uplatnit pravidla filtrování IP, která omezí adresy IP a služby TCP/IP, které jsou uživateli v dané relaci dostupné.

Vzorová konfigurace

Chcete-li nastavit vzorovou konfiguraci z produktu System i Navigator, postupujte takto:

1. Vytvořte identifikátor filtru PPP a filtry pro pravidla paketu IP, které specifikují povolení a omezení pro tuto zásadu přístupu skupiny.
   a. V prostředí produktu System i Navigator rozbalte **Síť → Služby vzdáleného přístupu**.
   b. Klepněte na **Profily připojení příjemce** a vyberte Zásady přístupu skupiny.
   c. Klepněte pravým tlačítkem myši na předdefinovanou skupinu, zobrazenou v podokně na pravé straně a vyberte **Vlastnosti**.

      Poznámka: Pokud chcete vytvořit nové zásady přístupu skupiny, klepněte pravým tlačítkem myši na **Zásady přístupu skupiny** a vyberte **Nové zásady přístupu skupiny**. Vyplňte kartu **Obecné**. Potom vyberte kartu **Nastavení TCP/IP** a pokračujte krokem e uvedeným níže.
   d. Vyberte kartu **Nastavení TCP/IP** a klepněte na volbu **Rozšířené**.
   e. Vyberte volbu **Použít pro toto připojení pravidla paketu IP**. Pak klepněte na **Editovat soubor pravidel**. Tak spustíte editor pravidel paketu IP a otevřete soubor PPP pravidlel filtrování paketu.
   f. Otevřete nabídku **Vložit** a vyberte volbu **Filtry**, abyste mohli přidat sady filtrů. Na kartě **Obecné** definujte sady filtrů a na kartě **Služby** definujte službu, kterou povolujete, například HTTP. Následující sada filtrů,

″services_rules,″, umožní služby HTTP, FTP a Telnet. Pravidla filtrování obsahují implicitně omezovací příkazy, které zamezují všechny služby TCP/IP nebo přenosy IP, jež nejsou výslovně povoleny.

Poznámka: Adresy IP 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

### 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 = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

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

g. Otevřete nabídku **Vložit** a vyberte **Filtrovací rozhraní**. Pomocí filtrovacího rozhraní můžete vytvořit identifikátor filtru PPP a zahrnout sady filtrů, které jste definovali.
   1) Na kartě **Obecné** zadejte jako identifikátor filtru PPP permitted_services.
   2) Na kartě **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 zásadu přístupu skupiny.

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

h. Změny uložte a ukončete práci. Pokud budete později potřebovat tyto změny anulovat, zadejte do znakově orientovaného rozhraní příkaz RMVTCPTBL *ALL. Tak odstraníte všechna pravidla filtrování a NAT na systému.

i. V dialogu **Rozšířená nastavení TCP/IP** ponechejte okénko **Identifikátor filtru PPP** prázdné a klepněte na tlačítko **OK**, čímž práci ukončíte. Později byste měli použít identifikátor filtru, který jste právě vytvořili, na zásadu přístupu skupiny, nikoliv na tento profil připojení.

2. Definujte novou zásadu přístupu skupiny pro tuto skupinu uživatelů.
   a. V prostředí produktu System i Navigator rozbalte **Síť → RAS (Služby vzdáleného přístupu) → Profily připojení příjemce**.

b. Klepněte pravým tlačítkem na ikonu **Zásada přístupu skupiny** a vyberte volbu **Nová zásada přístupu skupiny**. Produkt System i Navigator zobrazí dialog **Definice nové zásady přístupu skupiny**.
c. Na stránce Obecné zadejte jméno a popis zásady přístupu skupiny.
d. Na stránce Nastavení TCP/IP:
   - Vyberte volbu **Použít pro toto připojení pravidla paketu IP** a zvolte identifikátor filtru PPP **permitted_services**.
e. Vyberte **OK**, čímž uložíte zásadu přístupu skupiny.

3. Použijte zásadu přístupu skupiny na uživatele, kteří jsou přidruženi k této skupině.
   a. Otevřete profil příjemce připojení, kterým se řídí tato vytáčená připojení.
   b. Na stránce Autentizace u profilu příjemce připojení vyberte ověřovací seznam, který obsahuje autentizační informace o uživatelích, a klepněte na **Otevřít**.
   c. Vyberte uživatele ze skupiny prodeje, na kterého chcete uplatnit zásadu přístupu skupiny, a klepněte na **Otevřít**.
   d. Klepněte na tlačítko **Použít pro uživatele zásadu skupiny** a vyberte zásadu přístupu skupiny definovanou v kroku 2.
   e. Kroky zopakujte pro všechny uživatele ve skupině prodeje.

Související pojmy

“Konfigurace zásady přístupu skupiny” na stránce 56
Složka **Zásady přístupu skupiny** 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.

“Podpora zásad skupiny” na stránce 3
S podporou zásad skupiny mohou správci sítě definovat zásady skupin podle uživatelů pro správu prostředků. K určitým uživatelům je možné přiřadit zásady pro řízení přístupu, když se přihlásí k relaci protokolu PPP (Point-to-Point Protocol) nebo L2TP (Layer Two Tunneling Protocol).

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

“Použití pravidel filtrování IP na připojení PPP” na stránce 57
Soubor pravidel paketů můžete použít pro omezení přístupu k adresám IP pro uživatele nebo skupiny ve vaší síti.

Související odkazy

“Ověřovací seznam” na stránce 43
Ověřovací seznam se používá pro ukládání ID a hesel vzdálených uživatelů.

“Autentizace systému” na stránce 41
Na platformě System i podporují připojení PPP několik voleb pro autentizaci vzdálených klientů volajících na systém, a také připojení k ISP nebo k jinému systému, na který systém volá.

Související informace

Filtrování IP a převod síťových adres (NAT)

Scénář: Použití L2TP pro sdílení modemu mezi logickými oddíly

Musíte nastavit virtuální Ethernet přes čtyři logické oddíly na disku. Přejete si, aby vybrané logické oddíly sdílely modem pro přístup do vnější sítě LAN.

Situace

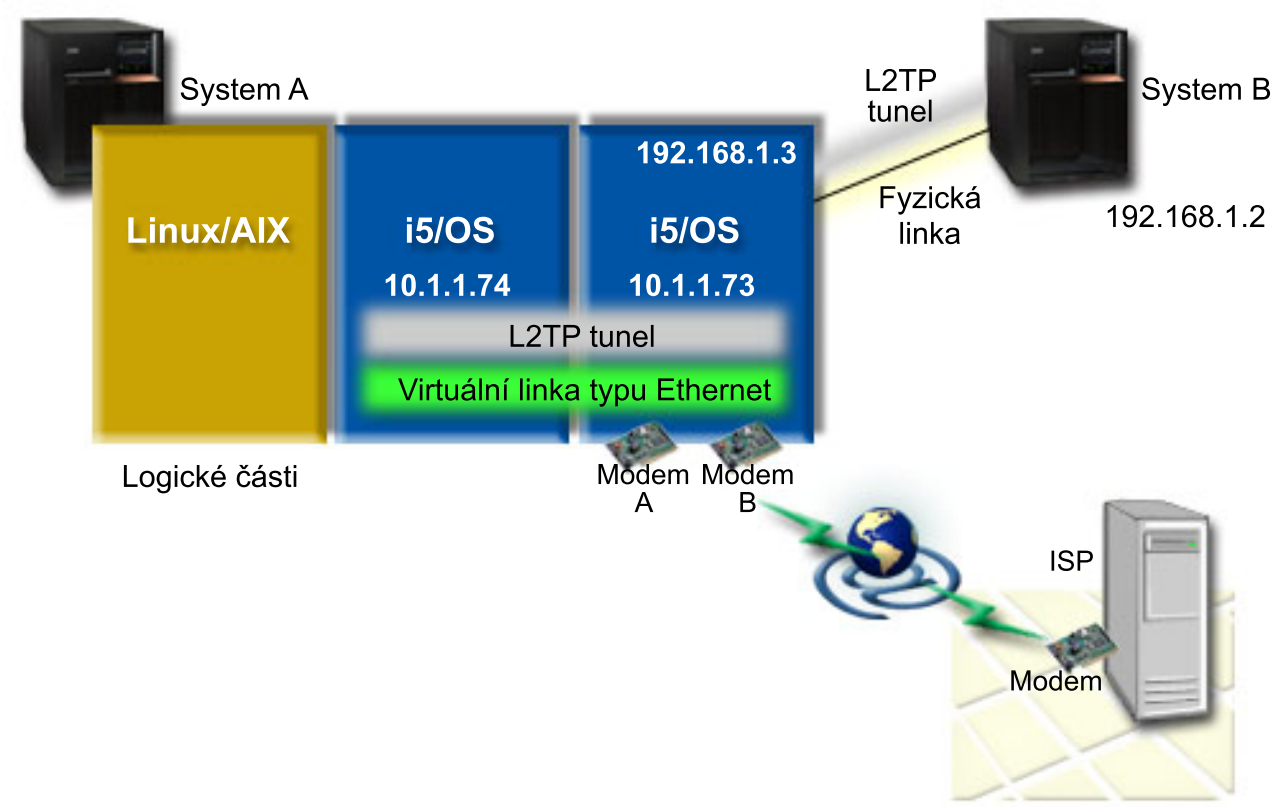
Jste systémový administrátor ve středně velké společnosti. Měli byste provést aktualizaci vašeho počítače, ale vy byste chtěli udělat ještě více; chcete váš hardware zjednodušit. Začnete tím, že sjednotíte práci tří starých systémů a převedete ji na jeden systém. Na systému vytvoříte tři logické oddíly. Nový systém obsahuje interní modem 2793. Je to jediný I/O procesor (IOP), který umožňuje podporu PPP. Máte rovněž starý modem 7852–400 ECS (electronic customer support).

Řešení

Více systémů a oddílů může sdílet stejný modem pro vytáčené spojení, není tedy třeba, aby každý systém nebo oddíl měly vlastní modem. To je možné tehdy, když používáte tunely L2TP a konfigurujete profily L2TP, které umožňují odchozí volání. Ve vaší síti se tunely budou spouštět přes virtuální síť Ethernet a přes fyzickou síť. Fyzická linka je připojena do jiného systému, který sdílí modemy ve vaší síti.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítě s tímto scénářem:



Obrázek 9. Více systémů, které sdílejí stejný modem pro vytáčené spojení

Nezbytné předpoklady a podmínky

Systém A musí splňovat následující požadavky na nastavení:

- Instalace systému i5/OS verze 5, vydání 3 nebo novější v oblasti, která vlastní modely podporující ASYNC.
- Hardware, který vám umožní rozdělení systému na oddíly.
- Produkty System i Access for Windows a System i Navigator (konfigurační a servisní komponenta produktu System i Navigator), verze 5, vydání nebo novější.
- Máte na systému vytvořené alespoň dva logické oddíly (LPAR). Na oddílech, které vlastní modem, musí být nainstalován systém i5/OS V5R3 nebo pozdější verze. Ostatní oddíly mohou mít nainstalovaný operační systém OS/400 V5R2, i5/OS V5R3, Linux, nebo AIX. Oddíly v tomto scénáři používají buď operační systém i5/OS nebo Linux.
- Máte virtuální síť Ethernet, určenou pro komunikaci mezi oddíly.

Systém B musí mít nainstalován licenční program a relevantní komponenty produktu System i Navigator: System i Access for Windows a System i Navigator (konfigurační a servisní komponenta produktu System i Navigator) V5R2 nebo novější.

Související informace

Logické oddíly

Podrobný scénář: Použití L2TP pro sdílení modemu mezi logickými oddíly

Po splnění všech nezbytných předchozích podmínek jste připraveni ke konfiguraci profilů L2TP.

Krok 1: Konfigurace terminátoru profilu L2TP pro rozhraní na oddílu, který komunikuje s modemy:

Chcete-li vytvořit nový profil terminátoru pro libovolné rozhraní, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***systém*** → **Síť** → **Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem myši na **Profily připojení příjemce** a vyberte **Nový profil**.
3. V nabídce nastavení stránky vyberte následující volby a klepněte na tlačítko **OK**:
   - **Typ protokolu**: PPP.
   - **Typ připojení**: L2TP (virtuální linka).
   - **Provozní režim**: terminátor (síťový server).
   - **Typ služby linky**: jediná linka.
4. Na kartě **Nový profil - Obecný** dokončete nastavení těchto polí:
   - **Jméno**: vnější.
   - **Popis**: připojení příjemce pro odchozí vytáčení.
   - Vyberte **Start profilu s TCP**.
5. Na kartě **Nový profil - Připojení** dokončete nastavení těchto polí.
   - **Adresa IP koncového bodu lokálního tunelu**: libovolná.
   - **Jméno virtuální linky**: vnější. Tato linka nemá přiřazené fyzické rozhraní. Virtuální linka popisuje různé charakteristiky profilu PPP. Poté, co se otevře okno Vlastnosti linky L2TP, klepněte na kartu **Autentizace** a zadejte název hostitele systému. Klepněte na **OK** a vrátíte se na kartu **Připojení** v okně Vlastnosti nového profilu PPP.
6. Klepněte na **Povolit navázání odchozího volání.** Objeví se dialog **Vlastnosti vytáčení odchozího volání**.
7. Ve volbě Vlastnosti vytáčení odchozího volání vyberte typ služby linky.
   - **Typ služby linky**: Oblast linek.
   - **Jméno**: volající.
   - Klepněte na **Nová**. Objeví se dialog **Vlastnosti nové oblasti linek**.
8. V okně Vlastnosti nové oblasti linek vyberte linky a modemy, kterým chcete povolit odchozí volání, a klepněte na **Přidat**. Pokud potřebujete tyto linky definovat, vyberte **Nová linka**. Rozhraní na oddílu, který komunikuje s příslušnými modemy, se pokusí použít kteroukoliv otevřenou linku z oblasti linek. Otevře se okno Vlastnosti nové linky.
9. Na kartě **Vlastnosti nové linky Obecné** zadejte informace do následujících polí:
   - **Jméno**: linka 1.
   - **Popis**: první linka a první modem oblasti linek (interní modem 2793).
   - **Hardwarový prostředek**: cmn03 (komunikační port).
10. Na všech ostatních kartách potvrďte předvolby a klepněte na **OK**, abyste se vrátili do okna Vlastnosti nové oblasti linek.
11. V okně Vlastnosti nové oblasti linek vyberte linky a modemy, kterým chcete povolit odchozí volání, a klepněte na **Přidat**. Ověřte, že pro oblast je vybraný modem 2793.
12. Vyberte **Nová linka** a přidejte modem ECS 7852–400. Otevře se okno Vlastnosti nové linky.
13. Na kartě **Vlastnosti nové linky Obecné** zadejte informace do následujících polí:

- **Jméno**: linka 2.
- **Popis**: druhá linka a druhý modem pro oblast linek (externí modem ECS 7852-400).
- **Hardwarový prostředek**: cmn04 (port V.24).
- **Rámcování**: asynchronní.

14. Na kartě **Vlastnosti nové linky - Modem** vyberte externí modem (7852–400) a klepněte na **OK**, abyste se vrátili do okna Vlastnosti nové oblasti linek.
15. Vyberte libovolné jiné linky, které chcete přidat do oblasti linek a klepněte na **Přidat**. V tomto příkladu si ověřte, že dva nové modemy, které jste dříve přidali, jsou uvedeny v poli **Vybrané linky pro oblast** a poté klepněte na **OK**, abyste se vrátili zpět do okna Vlastnosti vytáčení odchozího volání.
16. V okně Vlastnosti vytáčení odchozího volání zadejte předvolená čísla pro vytáčení a klepněte na **OK**, abyste se vrátili do okna Vlastnosti nového profilu PPP.

    Poznámka: Tato čísla, která se budou často volat z ostatních systémů přes příslušné modemy, mohou být něco jako váš ISP (poskytovatel internetových služeb). Pokud ostatní systémy zadají číslo z *PRIMARY nebo *BACKUP, bude se aktuálně vytáčet jedno z čísel, uvedených v tomto seznamu. Pokud ostatní systémy uvedou vlastní číslo, použije se místo předvoleného.
17. Na kartě **Nastavení TCP/IP** vyberte následující hodnoty:
    - **Adresa IP lokálního systému**: žádná.
    - **Adresa IP vzdáleného systému**: žádná.

    Poznámka: Pokud chcete použít profil k ukončení relací L2TP, musíte vybrat lokální adresu IP, která bude znázorňovat systém. Jako adresu IP vzdáleného systému můžete použít oblast adres, který je ve stejné podsíti jako váš systém. Všechny relace L2TP budou používat adresy IP z této oblasti.
18. Na kartě **Autentizace** potvrďte všechny předvolené hodnoty.

Nyní jste dokončili konfiguraci profilu terminátoru L2TP na oddíly s modemy. V dalším kroku potřebujete nakonfigurovat vzdálené vytáčení L2TP, profil odesílatele pro 10.1.1.74.

Související odkazy

“Podpora profilů více připojení” na stránce 50
Profily dvoubodových připojení, které podporují více připojení, vám umožňují mít jeden profil připojení, který obslouží mnoho digitálních, analogových nebo L2TP volání.

Krok 2: Konfigurace profilu odesílatele L2TP na 10.1.1.74:

Tyto kroky vás provedou profilem odesílatele L2TP (Layer Two Tunneling Protocol):

1. V prostředí produktu System i Navigator rozbalte **10.1.1.74 → Síť → Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem myši na **Profily připojení odesílatele** a vyberte **Nový profil**.
3. V nabídce nastavení stránky vyberte následující volby a klepněte na tlačítko **OK**:
   - **Typ protokolu**: PPP.
   - **Typ připojení**: L2TP (virtuální linka).
   - **Provozní režim**: vzdálené vytáčení.
   - **Typ služby linky**: jediná linka.
4. Na kartě **Obecné** dokončete nastavení následujících polí:
   - **Jméno**: toModem.
   - **Popis**: odesílatel příchozího spojení k oddílu, který komunikuje s modemem.
5. Na kartě **Připojení** dokončete nastavení následujících polí:

   Název virtuální linky: toModem. Tato linka nemá přiřazené fyzické rozhraní. Virtuální linka popisuje různé charakteristiky profilu PPP. Otevře se okno Vlastnosti linky L2TP.
6. Na kartě **Obecné** zadejte popis virtuální linky.

7. Na kartě **Autentizace** zadejte jméno lokálního hostitelského systému oddílu a klepněte na **OK**, abyste se vrátili zpět na stránku Připojení.
8. Do pole **Vzdálená telefonní čísla** přidejte *PRIMARY a *BACKUP. Tato volba umožní, aby profil mohl používat stejná telefonní čísla jako terminátor (koncový znak) profilu na oddílu, který komunikuje s modemy.
9. Do pole **Hostitelské jméno nebo adresa IP koncového bodu vzdáleného tunelu** zadejte adresu koncového bodu vzdáleného tunelu (10.1.1.73).
10. Na kartě **Autentizace** vyberte volbu **Povolit vzdálenému systému ověřit identitu tohoto serveru iSeries**.
11. V souladu s použitím autentizačního protokolu, vyberte volbu **Požadovat zakódované heslo (CHAP-MD5)**. Standardně je také označena volba **Povolit rozšířený autentizační protokol**.

    Poznámka: Protokol by měl odpovídat kterémukoliv protokolu užívanému také na systému, který voláte.
12. Zadejte vaše jméno uživatele a heslo.

    Poznámka: Jméno uživatele a heslo musí odpovídat kterémukoli platnému jménu uživatele a heslu na systému, který voláte.
13. Přejděte na kartu **Nastavení TCP/IP** a ověřte povinná pole:
    - **Adresa IP lokálního systému**: přiřadí vzdálený systém.
    - **Adresa IP vzdáleného systému**: přiřadí vzdálený systém.
    - **Směrování**: dodatečné směrování není povinné.
14. Klepnutím na **OK** uložíte profil PPP.

Krok 3: Konfigurace profilu pro vzdálené připojení L2TP pro 192.168.1.2:

Můžete konfigurovat profil vzdáleného vytáčení L2TP (Layer Two Tunneling Protocol) pro 192.168.1.2 opakováním Kroku 2 a změnou adresy koncového bodu vzdáleného tunelu na 192.168.1.3 (fyzické rozhraní, ke kterému se připojuje systém B).

Poznámka: Tato adresa je fiktivní a používá se pouze pro ukázkové účely.

Krok 4: Testování spojení:

Když dokončíte konfiguraci obou systémů, měli byste otestovat schopnost připojení, abyste se ujistili, že systémy pro připojení k vnějším sítím používají sdílený modem.

1. Ujistěte se, že je aktivní profil terminátoru L2TP (Layer Two Tunneling Protocol).
   a. V prostředí produktu System i Navigator rozbalte **10.1.1.73 → Síť → RAS (Služby vzdáleného přístupu) → Profily připojení příjemce**.
   b. V podokně na pravé straně najděte požadovaný profil (toExternal) a ověřte, že pole **Stav** je Aktivní. Pokud není aktivní, klepněte pravým tlačítkem myši na profil a vyberte volbu **Start**.
2. Spusťte profil Vzdálené vytáčení na 10.1.1.74.
   a. V prostředí produktu System i Navigator rozbalte **10.1.1.74 → Síť → RAS (Služby vzdáleného přístupu) → Profily připojení odesílatele**.
   b. V podokně na pravé straně najděte požadovaný profil (toModem) a ověřte, že pole **Stav** je Aktivní. Pokud není aktivní, klepněte pravým tlačítkem myši na profil a vyberte volbu **Start**.
3. Spusťte profil Vzdálené vytáčení na systému B.
   a. V prostředí produktu System i Navigator rozbalte **192.168.1.2 → Síť → RAS (Služby vzdáleného přístupu) → Profily připojení odesílatele**.
   b. V podokně na pravé straně najděte profil, který jste vytvořili, a ověřte, že pole **Stav** je Aktivní. Pokud není aktivní, klepněte pravým tlačítkem myši na profil a vyberte volbu **Start**.
4. Pokud je to možné, otestujte spojení s poskytovatelem služeb sítě Internet (ISP) nebo s jiným místem určení, pro něž chcete ověřit, že oba profily budou v případě vytáčení aktivní. Pokuste se otestovat spojení jak z 10.1.1.74, tak i z 192.168.1.2.

5. Případně také můžete zkontrolovat stav připojení.
   a. V prostředí produktu System i Navigator rozbalte **systém → Síť → RAS (Služby vzdáleného přístupu) → Profily připojení odesílatele**.
   b. V podokně na pravé straně klepněte pravým tlačítkem myši na profil, který jste vytvořili a vyberte **Připojení**. V okně Stav připojení můžete vidět, které profily jsou aktivní, neaktivní, připojené, atd.

Plánování PPP

Plánování PPP (Point-to-Point Protocol) zahrnuje vytváření a správu připojení PPP.

Související odkazy

"Scénář: Připojení vzdálených volajících klientů k systému" na stránce 12
Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

"Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu" na stránce 15
Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. K připojení systému k některému ISP (poskytovateli internetových služeb) mohou použít modem. PC klienti připojení k síti LAN mohou s Internetem komunikovat tak, že používají operační systém i5/OS jako bránu.

"Informace související s RAS (Služby vzdáleného přístupu)" na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Požadavky na software a hardware

Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, platforma System i, může být buď odesílatelem, nebo příjemcem.

Systém musí splňovat následující předpoklady, aby k němu vzdálené systémy mohly přistupovat.

- Produkt System i Navigator s podporou 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 s nainstalovaným produktem System i Access for Windows 95 nebo novějším s produktem System i Navigator.
- Instalovaný adaptér.

  Můžete si vybrat některý z následujících adaptérů:
  - 2699*: dvoulinkový WAN IOA (input/output adapter).
  - 2720*: PCI WAN/Twinaxial IOA.
  - 2721*: PCI dvoulinkový WAN IOA.
  - 2745*: PCI dvoulinkový WAN IOA (nahrazuje IOA 2721).
  - 2742*: dvoulinkový IOA (nahrazuje IOA 2745).
  - 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.
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: adaptér Ethernet pro připojení PPPoE.
  - 2793/576C*: dvouportový WAN IOA modem s V.92 integrovaným na portu 1 a standardním komunikačním rozhraním na portu 2. Chcete-li používat port 2, je nutný externí modem nebo adaptér terminálu ISDN s příslušným kabelem.
  - 2805: čtyřportový WAN IOA s integrovaným analogovým modem s integrovaným V.92. Nahrazuje modely 2761 a 2772.

* Tyto adaptéry vyžadují externí modem V.90 (nebo novější) nebo adaptér terminálu ISDN a kabel RS-232 (EIA 232) 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.

Související odkazy

"Profily připojení" na stránce 2
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.

"Modemy" na stránce 37
Pro připojení PPP lze používat externí i interní modemy.

"CSU/DSU" na stránce 37
CSU (channel service unit) je zařízení, které připojuje terminál k digitální lince. DSU (data service unit) je zařízení, které provádí ochranné a diagnostické funkce pro telefonní linku. Tato dvě zařízení se obvykle dodávají jako jedna jednotka CSU/DSU.

"Adaptéry terminálu ISDN" na stránce 37
ISDN (Integrated Services Digital Network) vám poskytuje digitální připojení, které vám umožní komunikovat pomocí libovolné kombinace hlasu, dat, videa a dalších multimediálních aplikací.

Alternativy připojení

Protokol 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 (High-level Data Link Control) pro zapouzdření datagramů přenášených na asynchronních i synchronních telekomunikačních linkách.

Zatímco PPP podporuje širokou škálu typů linek, SLIP (Serial Line Internet Protocol) 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

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 RS-232 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 zásada, 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 zůstávat připojeny, když telefonní linka přijímá příchozí hovor nebo čeká na volání.

Digitální služby a DDS (Digital Data Services)

S protokoly PPP lze použít digitální služby a DDS (Digital Data Services).

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.

Digitální datové služby

Digitální datové služby (DDS) jsou úplným základem datových služeb. Linky DDS jsou pronajatá 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 *CSU/DSU*, které slouží místo modemu v analogovém uspořádání. DDS má fyzická omezení, která souvisejí hlavně se vzdáleností mezi CSU/DSU a ústřednou telefonní společnosti. DDS pracuje nejlépe, když je vzdálenost menší než 9 000 m (30 000 stop). 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 ústředen 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.

Související odkazy

“CSU/DSU” na stránce 37
CSU (channel service unit) je zařízení, které připojuje terminál k digitální lince. DSU (data service unit) je zařízení, které provádí ochranné a diagnostické funkce pro telefonní linku. Tato dvě zařízení se obvykle dodávají jako jedna jednotka CSU/DSU.

“Komutovaná linka 56”
Jestliže nepotřebujete trvalé připojení, můžete ušetřit peníze tak, že použijete komutovanou digitální službu, které se běžně říká *komutovaná linka 56 (SW56)*.

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 (Digital Data Services) v tom, že DTE (Data Terminal Equipment) 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.

Související odkazy

"Digitální služby a DDS (Digital Data Services)" na stránce 32
S protokoly PPP lze použít digitální služby a DDS (Digital Data Services).

"ISDN (Integrated Services Digital Network)"
ISDN (Integrated Services Digital Network) poskytuje digitální připojení dvou koncových bodů po komutované lince. ISDN může přenášet hlas i data na stejném připojení.

ISDN (Integrated Services Digital Network)

ISDN (Integrated Services Digital Network) poskytuje digitální připojení dvou koncových bodů po komutované lince. 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 64 kbps 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 5 400 m (18 000 stop) 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 RS-232 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. S touto technologií může adaptér terminálu fungovat také jako digitální systém pro klienty V.92.

Obvykle se budete chtít připojit k adaptéru terminálu ISDN přes sériové rozhraní RS-232 pomocí asynchronního protokolu při rychlostech až do 230,4 kbps. Maximální přenosová rychlost na systému však pro asynchronní přenos přes RS-232 činí 115,2 kbps. To nás bohužel omezuje na maximální přenosovou rychlost 11,5 Kbps, kdežto adaptér terminálu s více linkami může přenášet za sekundu až 14 nebo 16 KB nekomprimovaných dat. Některé adaptéry terminálu podporují synchronní přenosy přes RS-232 při rychlostech 128 kbps, ale maximální rychlost synchronního přenosu přes rozhraní RS232 na systému je 64 kbps.

Systém je schopen provozovat asynchronní přenosy přes rozhraní V.35 při rychlostech až 230,4 kbps, ale výrobci adaptérů terminálů obvykle takovou konfiguraci nenabízejí. Konvertory rozhraní, které konvertují RS-232 na rozhraní V.35, by snad byly vhodným řešením tohoto problému, ale pro systém nebyl tento přístup dosud vyhodnocen. 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.

Související odkazy

"Komutovaná linka 56" na stránce 32
Jestliže nepotřebujete trvalé připojení, můžete ušetřit peníze tak, že použijete komutovanou digitální službu, které se běžně říká *komutovaná linka 56 (SW56)*.

"Adaptéry terminálu ISDN" na stránce 37
ISDN (Integrated Services Digital Network) vám poskytuje digitální připojení, které vám umožní komunikovat pomocí libovolné kombinace hlasu, dat, videa a dalších multimediálních aplikací.

T1/E1 a částečná připojení T1

T1/E1 a částečná připojení T1 jsou dva druhy platných alternativ připojení.

T1/E1

Připojení T1 spojuje celkem dvacet čtyři kanálů 64-kbps Kbps (DS0) TDM (time-division 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 dva 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 (private branch exchanges) využívá službu T1 pro import více volacích obvodů přes jednu linku T1, místo aby měly 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 Adresa IP (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 T1 (1,544 mbps) a T3 (45 mbps). O přenosu rámce můžete přemýšlet jako o způsobu využití stávajících linek T1 a T3, které vlastní poskytovatel služeb. Většina telefonních společností nyní poskytuje službu přenosu rámce těm zákazníkům, kteří chtějí připojení s rychlostí od 56 kbps do T1. (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 (asynchronous transfer mode).

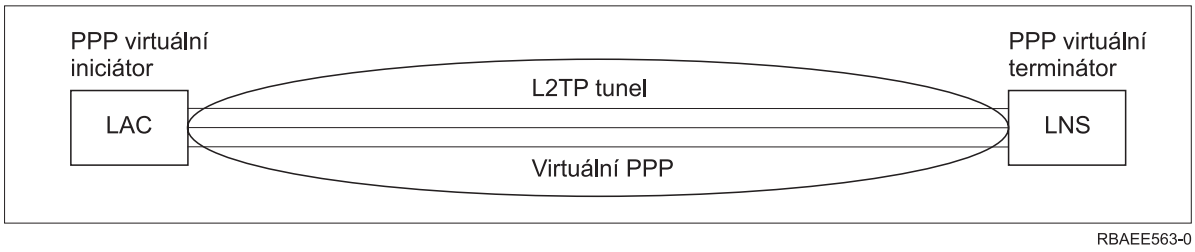
Podpora L2TP (tunelování) pro připojení PPP

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).

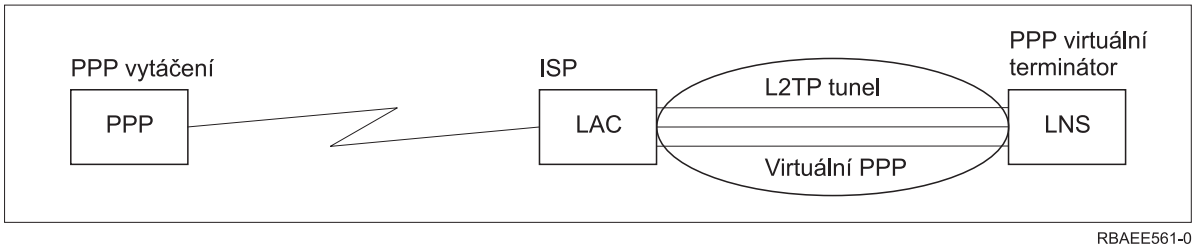
Protokol L2TP (Layer Two Tunneling Protocol)

Pomocí tunelů L2TP (Layer Two Tunneling Protocol) je možné oddělit místo, kde končí vytáčený protokol, a místo, kde je poskytován přístup k síti. Z tohoto důvodu je někdy protokol L2TP označován jako *Virtuální PPP*.

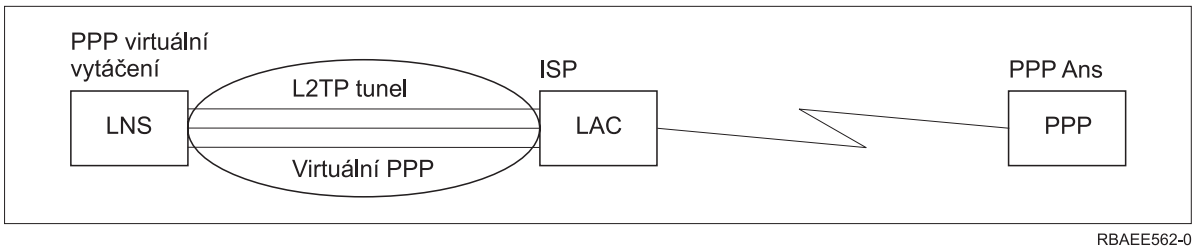
Toto obrázky ilustrují tři odlišné příklady implementace tunelu L2TP.



Obrázek 10. PPP virtuální iniciátor nebo PPP virtuální terminátor



Obrázek 11. PPP iniciátor vytáčení nebo PPP virtuální terminátor



Obrázek 12. PPP virtuální vytáčení nebo PPP virtuální příjem

Protokol vícenásobných připojení je dokumentovaný jako norma RFC-2661 (Request for Comment). 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.

Související informace

Scénář: Ochrana nepovinného tunelu L2TP pomocí IPSec

Editor RFC

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, který je odesílá na síťový server L2TP (LNS). Při používání nepovinného tunelu nepotřebuje ISP podporu L2TP a indikátor tunelu L2TP zůstává na stejném systému jako vzdálený klient. V tomto modelu se tunel rozkládá na celé relaci PPP (Point-to-Point Protocol) 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.

Ve výsledku uživatel odešle pakety PPP na koncentrátor přístupů protokolu L2TP poskytovatele internetových služeb. ISP zabalí pakety v L2TP a odešle je v tunelu na síťový server L2TP (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 kanceláří, 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 přesměrování 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 přesměrují bránou L2TP pro více přechodů do cílového LNS a přenosy z cílového LNS se přesměrují do klientského LAC.

Podpora PPPoE (DSL) pro připojení PPP

DSL (digital Subscriber Line) 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).

DSL 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 kbps) dosahuje teoretické mezní hodnoty této technologie. Technologie DSL umožňuje dosahovat na linkách s kroucenou dvoulinkou 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. PPP se obvykle používá pro sériovou komunikaci jako například pro vytáčená modemová připojení. Mnozí poskytovatelé internetové služby DSL nyní používají PPPoE (PPP over Ethernet), protože má rozšířené funkce pro přihlašování a zabezpečení dat.

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 jednouživatelskou telefonní linku (POTS rozdělovač kanálů umožňuje simultánní sdílení linky). Ačkoli DSL modemy vypadají podobně jako konvenční analogové modemy, poskytují mnohem větší propustnost.

Příslušenství pro připojení

K práci s připojeními přes protokol PPP využívá systém modemy, terminálové adaptéry ISDN (Integrated Services Digital Network), adaptéry Token-ring, adaptéry Ethernet nebo zařízení CSU/DSU.

Toto jsou čtyři typy komunikačních zařízení, která můžete ve svém prostředí PPP používat:

- modemy
- CSU/DSU
- adaptéry terminálu ISDN
- adaptéry Ethernet (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.

Systém má předdefinováno mnoho modelů modemů a lze definovat i nové modely prostřednictvím produktu System i 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.

Ke zřízení připojení PPP můžete použít modem ECS, který je dodáván spolu se systémem. Ve starších systémech se jako modem electronic využíval externí modem IBM 7852-400. Tento modem byl nahrazen modemem MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. U novějších systémů lze jako modem ECS použít interní modemy 2771, 2793 nebo libovolné jiné podporované interní modemy.

Související odkazy

“Požadavky na software a hardware” na stránce 30
Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, platforma System i, může být buď odesílatelem, nebo příjemcem.

CSU/DSU

CSU (channel service unit) je zařízení, které připojuje terminál k digitální lince. DSU (data service unit) 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.

Související odkazy

“Požadavky na software a hardware” na stránce 30
Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, platforma System i, může být buď odesílatelem, nebo příjemcem.

“Digitální služby a DDS (Digital Data Services)” na stránce 32
S protokoly PPP lze použít digitální služby a DDS (Digital Data Services).

Adaptéry terminálu ISDN

ISDN (Integrated Services Digital Network) vám poskytuje digitální připojení, které vám umožní komunikovat pomocí libovolné kombinace hlasu, dat, videa a dalších multimediálních aplikací.

Budete muset ověřit, zda je váš adaptér terminálu schválený pro použití na systému.

Při konfiguraci adaptéru terminálu proveďte následující kroky:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
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 kartě **Obecné**. Neopomeňte jako komunikační zařízení uvést adaptér terminálu ISDN.
4. Vyberte kartu **Parametry ISDN**.
5. Přidejte nebo změňte vlastnosti ISDN na kartě **Parametry ISDN** tak, aby vyhovovaly vlastnostem, které vyžaduje váš adaptér terminálu.

Související úlohy

"Příklad: Konfigurace adaptéru terminálu ISDN" na stránce 53
Tento příklad demonstruje, jak konfigurovat adaptéry terminálu ISDN.

Související odkazy

"Požadavky na software a hardware" na stránce 30
Prostředí PPP vyžaduje, abyste měli dva nebo více počítačů, které podporují protokol PPP. Jeden z těchto počítačů, platforma System i, může být buď odesílatelem, nebo příjemcem.

"ISDN (Integrated Services Digital Network)" na stránce 33
ISDN (Integrated Services Digital Network) poskytuje digitální připojení dvou koncových bodů po komutované lince. ISDN může přenášet hlas i data na stejném připojení.

Doporučení adaptéru terminálu ISDN:

Existuje několik různých adaptérů terminálu, které lze použít.

Doporučený externí adaptér terminálu ISDN (Integrated Services Digital Network), neboli modem ISDN, je **3Com/U.S. Robotics Courier I ISDN V.Everything**. Podporuje analogová modemová připojení V.35, připojení V.90 (X2), V.92 a vícenásobná připojení PPP prostřednictvím linky ISDN v režimu odesílatele zprávy i odpovědi na systému. Rovněž automaticky podporuje na připojení ISDN PPP autentizační protokol CHAP (Challenge Handshake Authentication). 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 systému.** Zatímco probíhá vyjednávání autentizace PAP se systémem, adaptér terminálu Courier I odpovídá na výzvy CHAP pocházející ze strany příjemce. Odpovědi PAP se na připojení ISDN neobjevují.
- **Připojení, na která systém odpovídá.** Pokud se na základě konfigurace odpovědi systému otevře autentizace systému s výzvou CHAP, vyžaduje Courier I autentizeci CHAP volající stranou. Pokud systém zahájí autentizaci pomocí PAP, adaptér terminálu Courier I se pomocí PAP ověří.

Jestliže používáte modem Courier I starší verze než 1999, ověřte, zda je tento modem připojen k systému pomocí kabelu V.35, abyste získali 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 verzi V.35 tohoto adaptéru terminálu již nelze získat od jiných dodavatelů, ale některé verze V.35 mohou ještě u jiných dodavatelů být. Verze RS-232 se i přes poněkud omezený výkon na systému stále doporučuje, neboť připojení RS-232 jsou omezena na 115,2 KB.

Neopomeňte nastavit rychlost linky V.35 na systému na 230,4 kbps.

Omezení adaptérů terminálu ISDN:

Adaptéry terminálu v tomto tématu byly hodnoceny. Doporučují se pouze pro iniciaci vzdálených připojení ISDN ze systému.

3Com Impact IQ ISDN:

Tento adaptér terminálu se pro server System i 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 systému větší rychlostí než 115 200 bps.
- Adaptér terminálu nepodporuje automaticky protokol CHAP (Challenge Handshake Authentication). Pokud jste nastavili S84 na 0, provede se autentizace CHAP.
- Systém, který monitoruje signál DSR (data set ready) z adaptéru terminálu, není schopen určit, kdy připojení skončilo. To představuje pro systém potenciální riziko zabezpečení.

Motorola BitSurfr Pro ISDN:

Tento adaptér terminálu se pro server System i 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 systému větší rychlostí než 115 200 bps.
- Adaptér terminálu nepodporuje automaticky autentizaci CHAP. Avšak nastavení @M2=C umožňuje systému autentizaci provádět.
- Adaptér terminálu neumožňuje automatické odpovídání na jednolinková 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 dat nepracuje s tímto adaptérem terminálu správně. To vede ke snížení výkonu, když systém odesílá data přes vícenásobné připojení PPP Multilink.

Práce s adresou IP

Připojení PPP umožňuje několik různých množin voleb pro správu adres IP v závislosti na typu profilu připojení.

- DHCP může centrálně spravovat přiřazování adres IP ve vaší síti. Dozvíte se, jak na síti nastavit a spravovat služby DHCP. Viz Protokol DHCP (Dynamic Host Configuration Protocol)
- DNS vám může pomoci spravovat hostitelská jména a jejich přidružené adresy IP. Dozvíte se, jak v síti nastavit a spravovat služby DNS. Viz DNS (Domain Name System)
- BOOTP se používá k přiřazování klientských pracovních stanic systému a k přiřazování adres IP těmto stanicím. Dozvíte se, jak v síti nastavit a spravovat služby BOOTP. Viz Protokol Bootstrap

Související odkazy

“Scénář: Připojení systému ke koncentrátoru přístupu PPPoE” na stránce 10
Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

Filtrování IP paketů

Filtrování IP paketů omezuje služby pro jednotlivé uživatele, když se přihlašují do sítě.

Filtrování paketů může povolit nebo odepřít přístup v závislosti na místu určení adres IP, portů nebo obojího. Uplatňují se různé zásady 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 pravidla filtrování na určitou kategorii uživatelů. Pravidla filtrování paketů nejsou sama o sobě definována v PPP, ale jsou definována pod pravidly pro IP pakety v rámci produktu System i Navigator.

Pro připojení L2TP byste měli použít VPN s filtrováním IPSec, aby byl chráněn provoz v síti.

Související odkazy

“Scénář: Připojení systému ke koncentrátoru přístupu PPPoE” na stránce 10
Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

Související informace

Filtrování IP a převod síťových adres (NAT)

VPN (Virtual Private Networking)

Strategie správy adres IP

Než začnete konfigurovat profil připojení PPP, měli byste dobře znát strategii správy adres IP 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 adresy IP definované pro profil odesílatele se obvykle budou definovat jako *přiřazené vzdáleným systémem*. To umožňuje administrátorům na vzdáleném systému ovládat adresy IP, 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 adresy IP.

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

Další otázkou je, zda chcete povolit skrývání adres IP. Pokud se například systém připojuje k Internetu prostřednictvím ISP, mohlo by se stát, že by síť připojená za systémem také získala přístup k Internetu. Systém bude vlastně ″skrývat″ adresy IP systémů v síti za lokální adresu IP přiřazenou od ISP, jakoby veškerý provoz pocházel ze systému. Zvažte také otázku dodatečného směrování jak pro systémy v síti LAN (aby jejich internetové přenosy byly posílány na systém), tak i pro systém; v tom případě by bylo nutné zaškrtnout volbu **Přidat vzdálený systém jako předvolenou přenosovou cestu**.

Profily připojení příjemce

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

Lokální adresy IP

Pro jediný profil příjemce můžete na systému definovat jedinečnou adresu IP nebo používat adresu existující. Pro profily příjemců definovaných pro podporu souběžných vícenásobných připojení musíte použít existující lokální adresu IP. Pokud nejsou k dispozici žádné existující lokální adresy IP, můžete za tímto účelem vytvořit virtuální adresu IP.

Adresy IP vzdáleného systému

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

Poznámka: Chcete-li, aby byl vzdálený systém považován za součást sítě LAN, je třeba nakonfigurovat směrování adres IP, zadat adresu IP z rozsahu adres IP systémů připojených k síti LAN-attached a ověřit, že přesměrování pomocí IP je povoleno jak pro tento profil připojení, tak i pro systém.

Tabulka 8. Volby přiřazení adresy IP v profilu připojení příjemce

Volba	Popis
fixní adresa IP	Definujete jedinou adresu IP, která se má předat vzdáleným uživatelům, když se připojí. Jedná se o výhradně hostitelskou adresu IP (maska podsítě je 255.255.255.255) a slouží pouze pro profily příjemců jediného připojení.
oblast adres	Můžete definovat počáteční adresu IP a pak rozsah udávající, kolik dalších dodatečných adres IP se má definovat. Každý uživatel, který se připojí, pak dostane jedinečnou adresu IP z definovaného rozmezí. Jedná se o výhradně hostitelskou adresu IP (maska podsítě je 255.255.255.255) a slouží pouze pro profily příjemců více připojení.
RADIUS	Vzdálenou adresu IP a její masku podsítě určí server Radius. To je možné pouze tehdy, pokud je definováno následující: • Podpora serveru Radius v oblasti autentizace a adresování IP je povolena v konfiguraci služeb serveru RAS (Služby vzdáleného přístupu). • Autentizace je povolena pro profil připojení příjemce a je definováno, že autentizace se provádí na dálku serverem Radius.
DHCP	Vzdálenou adresu IP určuje přímo nebo nepřímo server DHCP pomocí předávání DHCP. To je možné jen tehdy, pokud byla povolena podpora DHCP v konfiguraci služeb serveru RAS. Jedná se o výhradně hostitelskou adresu IP (maska podsítě je 255.255.255.255).
na základě ID uživatele vzdáleného systému	Vzdálená adresa IP se určuje podle ID uživatele definovaného pro vzdálený systém, když se provádí jeho autentizace. To umožňuje administrátorovi přiřadit různé vzdálené adresy IP (a jejich přiřazené masky podsítě) uživateli, který se připojí. To rovněž umožňuje definovat dodatečné přenosové cesty pro každý z těchto ID uživatele, takže pro známého vzdáleného uživatele můžete prostředí přesně upravit. Má-li tato funkce řádně fungovat, musí být povolena autentizace.
definování dodatečných adres IP na základě ID uživatele vzdáleného systému	Tato volba vám umožňuje definovat adresy IP založené na ID uživatele vzdáleného systému. Tato volba se automaticky volí (a musí se použít), jestliže je zásada přiřazování vzdálených adres IP definována jako **Na základě ID uživatele vzdáleného systému**. Tato volba je také povolena pro tyto zásady přiřazování adres: fixní adresa IP a oblast adres. Když se vzdálený uživatel připojí k systému, provede se vyhledávání, aby se zjistilo, zda není některá vzdálená IP adresa definována specificky pro tohoto uživatele. Pokud ano, použije se pro připojení tato adresa IP, maska a sada možných přenosových cest. Jestliže uživatel není definován, pak adresa IP nabývá předem stanovené hodnoty definované fixní adresy IP nebo další adresy z oblasti adres IP.
povolení vzdálenému systému definovat svou vlastní adresu IP	Tato volba umožňuje vzdálenému uživatelům definovat své vlastní adresy IP, pokud o to požádají. Pokud nepožadují použití své vlastní adresy IP, vzdálená adresa IP se určí definovanou zásadou přiřazování adres IP vzdáleného systému. Tato volba je zpočátku zablokována a měli byste ji použít po pečlivém uvážení.
směrování adres IP	Jestliže volající klient potřebuje přístup k některé adrese IP v síti LAN, k níž systém patří, musí mít klient i systém správně konfigurováno směrování adres IP.

Autentizace systému

Na platformě System i podporují připojení PPP několik voleb pro autentizaci vzdálených klientů volajících na systém, a také připojení k ISP nebo k jinému systému, na který systém volá.

Systém podporuje několik metod údržby informací o autentizaci. Tyto metody zahrnují jednoduché ověřovací seznamy na systému, které obsahují seznamy oprávněných uživatelů a jejich hesla pro podporu serverů RADIUS (Remote Authentication Dial In User Service). Servery RADIUS udržují podrobné informace o uživatelích sítě. Systém také podporuje několik voleb pro šifrování informací o ID a heslech uživatelů v rozsahu od jednoduché výměny hesel až po podporu protokolem CHAP-MD5 (Challenge Handshake Authentication Protocol). Na kartě **Autentizace** v profilu připojení produktu System i Navigator můžete specifikovat své požadavky na autentizaci systému, včetně ID a hesla uživatele, které se používají k ověřování systému při odchozím volání.

Související odkazy

"Scénář: Připojení systému ke koncentrátoru přístupu PPPoE" na stránce 10
Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

"Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS" na stránce 20
Server NAS (Network Access Server) spuštěný na systému může směrovat požadavky na autentizaci volajících klientů na samostatný server RADIUS. Jestliže dojde k autentizaci, může server RADIUS také řídit adresy IP přiřazené uživatelům.

"Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP" na stránce 22
Zásady 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 adresám IP ve vaší síti.

CHAP-MD5 (Challenge Handshake Authentication Protocol with 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 protokol PAP (Password Authentication Protocol). Tento protokol je účinný proti pokusům o získání přístupu zásadou opakování nebo zásadou pokusu a omylu. Autentizace CHAP může při připojení proběhnout více než jednou.

Systém, 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. Systém, který provádí autentizaci, zkontroluje odpověď na základě výpočtu, který sám provedl. Autentizace je úspěšná, pokud se hodnoty shodují; v opačném případě se připojení ukončí.

Související odkazy

"Scénář: Připojení vzdálených volajících klientů k systému" na stránce 12
Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

"PAP (Password Authentication Protocol)"
Protokol PAP (Password Authentication Protocol) používá dvoucestné navazování spojení, aby poskytl peer systému snadnou zásadu pro prokázání své totožnosti.

EAP (Extensible Authentication Protocol)

EAP (Extensible Authentication Protocol) umožňuje autentizačním modulům od jiných dodavatelů 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 o zařízení ochrany dat třetí strany. Protokol EAP chrání zabezpečené VPN (virtual private networks) před hackery (počítačovými piráty), kteří při napadání systémů používají zjišťování hesla pomocí slovníků a hádání. Protokol EAP vylepšuje protokol PAP (Password Authentication Protocol) a CHAP (Challenge Handshake Authentication Protocol).

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

Systém nepodporuje přímo protokol EAP. Můžete však použít vzdálenou autentizaci se serverem RADIUS (Remote Authentication Dial In User Service), který může podporovat některá další výše popsaná schémata autentizace.

PAP (Password Authentication Protocol)

Protokol PAP (Password Authentication Protocol) používá dvoucestné navazování spojení, aby poskytl peer systému snadnou zásadu 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.

Související odkazy

"CHAP-MD5 (Challenge Handshake Authentication Protocol with MD5)" na stránce 42
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.

Přehled o protokolu RADIUS (Remote Authentication Dial In User Service)

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. Systém, který funguje jako NAS, odesílá informace o uživateli a připojení na server RADIUS, který je k němu přiřazen, prostřednictvím standardního protokolu RADIUS definovaného v RFC 2865.

Servery RADIUS reagují na přijaté požadavky uživatelů na připojení tím, že uživatele autentizují a následně vracejí všechny nezbytné konfigurační informace serveru NAS (systému), který pak může autentizovaným volajícím uživatelům poskytnout oprávněné služby.

Pokud nelze server RADIUS dosáhnout, systém může směrovat požadavky na autentizaci na alternativní server. Tak je možné, aby podniky umožňovaly svým uživatelům službu vytáčení 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. To mohou být soubory hesel operačního systému UNIX, Kerberos, komerční systém zabezpečení dat nebo na zakázku vyvynutý systém zabezpečení dat. Server Radius odešle zpět systému informace o všech službách, které je autentizovaný uživatel oprávněn používat, jako je například adresa IP. Podobným způsobem se vyřizují i účtovací požadavky serveru 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.

Související odkazy

"Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS" na stránce 20
Server NAS (Network Access Server) spuštěný na systému může směrovat požadavky na autentizaci volajících klientů na samostatný server RADIUS. Jestliže dojde k autentizaci, může server RADIUS také řídit adresy IP přiřazené uživatelům.

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. Záznamy 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 získáte v online nápovědě.

Související odkazy

"Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP" na stránce 22
Zásady 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 adresám IP ve vaší síti.

Pokyny ohledně šířky pásma - vícenásobné připojení

Pro provádění určitých úkolů je často zapotřebí větší šířka pásma, která však není nutná vždy.

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 RFC-1990 (Request for Comment).

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. RFC-2125 dokumentuje oba protokoly PPP: BAP (Bandwidth Allocation Protocol) a BACP (Bandwidth Allocation Control Protocol).

Související informace

Editor RFC

Konfigurace PPP

Než budete moci používat PPP pro nastavení připojení PPP, musíte konfigurovat prostředí PPP.

Související odkazy

“Informace související s RAS (Služby vzdáleného přístupu)” na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Vytvoření profilu připojení

Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Profil připojení je logické znázornění následujících atributů připojení:

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

Služby RAS (Služby vzdáleného přístupu), v adresáři Síť, obsahují následující objekty:

- Profily připojení odesílatele.
- Profily připojení příjemce.
- **Modemy.**

Při vytváření profilu připojení proveďte následující kroky:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
2. Vyberte jednu z následujících voleb:
   - Klepněte pravým tlačítkem myši na **Profily připojení odesílatele**, abyste mohli nastavit systém jako systém pro iniciaci.
   - Klepněte pravým tlačítkem myši na **Profily připojení příjemce**, abyste mohli nastavit systém jako systém, který umožňuje příchozí připojení 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 informace získáte v online nápovědě.

   Související úlohy

   “Přiřazení modemu k popisu linky” na stránce 54
   Toto téma demonstruje kroky pro přidružení modemu k popisu linky.

   Související odkazy

   “Scénář: Připojení systému ke koncentrátoru přístupu PPPoE” na stránce 10
   Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

   “Scénář: Připojení vzdálených volajících klientů k systému” na stránce 12
   Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

   “Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu” na stránce 15
   Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. K připojení systému k některému ISP (poskytovateli internetových služeb) mohou použít modem. PC klienti připojení k síti LAN mohou s Internetem komunikovat tak, že používají operační systém i5/OS jako bránu.

   “Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu” na stránce 17
   Modem vám umožňuje, aby si dvě vzdálená pracoviště (například ústředí a pobočka) vzájemně vyměňovala data. Pomocí PPP lze propojit dvě sítě LAN tak, že se vytvoří připojení mezi systémem v ústředí a jiným systémem v pobočce.

   “Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP” na stránce 22
   Zásady 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 adresám IP ve vaší síti.

Typ protokolu: PPP nebo SLIP (Serial Line Internet Protocol)

Protokol PPP nahrazuje protokol SLIP (Serial Line Internet Protocol), který lze také volit pro dvoubodová připojení.

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 SLIP definovaný v RFC (Request for Comment) se na Internetu nikdy nestal standardem kvůli následujícím nedostatkům:

- SLIP nemá žádný standardní způsob, jak definovat adresování IP 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.

Protokol SLIP se v současnosti stále používá a operační systém i5/OS jej nadále podporuje. IBM však při nastavování dvoubodového připojení doporučuje používat protokol 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 systém používá nové připojení PPP.

Chcete-li zadat výběry režimu, proveďte následující kroky:

1. Vyberte jeden z následujících typů připojení:
   - komutovaná linka
   - pronajatá linka
   - L2TP (Layer Two Tunneling Protocol) (virtuální linka).
   - Linka PPPoE (Point-to-Point Protocol over Ethernet).
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:

Pokud používáte modem (vnitřní nebo vnější) nebo adaptér terminálu externí ISDN (Integrated Services Digital Network) k připojení přes telefonní linku, vyberte připojení přes komutovanou linku.

Připojení typu komutované linky má následující provozní režimy:

Odpověď

Tento provozní režim zvolte tehdy, chcete-li povolit vzdálenému systému přístup k systému.

Vytáčení

Tento provozní režim zvolte tehdy, chcete-li povolit systému, aby inicioval připojení ke vzdálenému systému.

Vytáčení na požádání (pouze vytáčení)

Tento provozní režim zvolte tehdy, chcete-li systému povolit, aby se automaticky připojoval ke vzdálenému systému, když je v systému detekován provoz TCP/IP. Připojení se ukončí, když se dokončí datový přenos a po určitou dobu se nevyskytne provoz TCP/IP.

Vytáčení na požádání (vyhrazený peer s možností odpovídat)

Tento provozní režim zvolte tehdy, chcete-li systému povolit příjem volání od vyhrazeného vzdáleného systému. Tento provozní režim systému rovněž umožňuje iniciovat připojení ke vzdálenému systému, jakmile se objeví provoz TCP/IP určený pro vzdálený systém. Jestliže oba systémy používají operační systém i5/OS a oba používají tento provozní režim, dochází k provozu TCP/IP mezi těmito dvěma systémy podle potřeby, 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, máte-li vyhrazený spoj mezi lokálním a vzdáleným systémem. Pokud máte pronajatou linku, nepotřebujete k 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 zvolte, chcete-li vzdálenému systému povolit přístup k systému přes vyhrazený spoj. Tento provozní režim se odkazuje na profil odpovědi použitý pro pronajatou linku.

iniciátor

Tento provozní režim zvolte, chcete-li umožnit systému přístup ke vzdálenému 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 vaším systémem a vzdáleným systémem. Když budete používat tunel L2TP 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 zvolte, chcete-li vzdálenému systému umožnit přístup k systému tunelem L2TP.

iniciátor

Tento provozní režim zvolte, chcete-li systému umožnit připojení ke vzdálenému systému tunelem L2TP.

vzdálené vytáčení

Tento provozní režim zvolte, chcete-li systému povolit, aby se připojoval k jinému systému nebo k ISP tunelem L2TP an nařizoval ISP vytáčení vzdáleného klienta PPP.

iniciátor pro více přechodů

Tento provozní režim zvolte, chcete-li systému povolit, aby vytvářel připojení s více přechody.

Poznámka: Profil terminátoru L2TP, k němuž je tento iniciátor pro více přechodů přidružený, 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.

Linka PPPoE:

Připojení PPPoE (Point-to-Point over Ethernet) využívají virtuální linku pro zasílání dat PPP (přes adaptér Ethernet) na model DSL (Digital Subscriber) modem poskytovaný vaším ISP. Tento modem je rovněž připojen k síti LAN umístěné na Ethernetu.

To umožňuje přístup k vysokorychlostnímu Internetu pro uživatele sítě LAN prostřednictvím relací PPP na operačním systému i5/OS. Jakmile se zahájí připojení mezi systémem a ISP, mohou jednotliví uživatelé v síti LAN spouštět jedinečné relace s ISP přes PPPoE.

PPPoE je jediný používaný protokol pro profily odesílatele připojení. Připojení předpokládají 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.

Související odkazy

"Scénář: Připojení systému ke koncentrátoru přístupu PPPoE" na stránce 10
Mnoho ISP nabízí vysokorychlostní přístup k Internetu prostřednictvím DSL s použitím protokolu PPPoE (Point-to-Point Protocol over Ethernet). Můžete systém připojit k těmto ISP, které poskytnou širokopásmové připojení, které zachovává výhody protokolu PPP.

"Scénář: Připojení vzdálených volajících klientů k systému" na stránce 12
Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

"Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu" na stránce 15
Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. K připojení systému k některému ISP (poskytovateli internetových služeb) mohou použít modem. PC klienti připojení k síti LAN mohou s Internetem komunikovat tak, že používají operační systém i5/OS jako bránu.

"Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu" na stránce 17
Modem vám umožňuje, aby si dvě vzdálená pracoviště (například ústředí a pobočka) vzájemně vyměňovala data. Pomocí PPP lze propojit dvě sítě LAN tak, že se vytvoří připojení mezi systémem v ústředí a jiným systémem v pobočce.

Jediná linka:

Chcete-li definovat linku protokolu PPP (Point-to-Point), která je přidružena k analogovému modelu, vyberte tuto službu linky. Tato volba se také používá pro pronajaté linky, u kterých se modem nepožaduje. Profil připojení PPP používá vždy tentýž prostředek komunikačního portu systému i5/OS.

Pokud to budete požadovat, můžete jedinou analogovou linku konfigurovat jako sdílenou mezi profilem příjmu a profilem vytáčeného připojení. 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″. Poté se ustanoví odchozí připojení. Jakmile se připojení ukončí, profil vytáčení vrátí linku profilu odpovědi, který bude znovu připraven na příjem příchozích připojení. Chcete-li povolit funkci sdílení, klepněte na kartu **modem**, 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 připojení 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.

Oblast linek:

Tuto službu linky vyberte, chcete-li nastavit, aby připojení PPP používalo linku z oblasti linek. Když je zahájeno připojení PPP, systém vybere nepoužívanou linku z oblasti linek. U profilů volání na vyžádání systém vybírá linku až tehdy, když detekuje provoz TCP/IP pro vzdálený systém.

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

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

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

Výhody používání oblasti linek:

- Neváže te 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 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 s oblastmi linek, čímž budete prostředky využívat efektivněji.

  Systém vybere linku z oblasti linek pouze tehdy, když používá 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 oblast linek, aby toto prostředí fungovalo. Můžete vytvořit čtyři profily připojení vytáčení na požádání, přičemž každý z těchto profilů se bude odvolávat na 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 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 ″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.

Konfigurace oblasti linek

Oblasti linek se definují v rámci profilu připojení. Při konfiguraci základní oblasti linek postupujte takto:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Vytváření sítě → RAS (Služby vzdáleného přístupu)**.
2. Vytvořte profil připojení buď pro vytáčení, nebo pro přijímaná volání. Vyberte si z jedné z následujících voleb:
   - Klepněte pravým tlačítkem myši na **Profily připojení odesílatele**, abyste mohli nastavit systém jako systém pro iniciaci spojení se vzdáleným systémem.
   - Klepněte pravým tlačítkem myši na **Profily připojení příjemce**, abyste mohli nastavit systém jako systém, který umožňuje příchozí připojení vzdálených systémů a uživatelů.
3. Vyberte **Nový profil**.

4. Pro profil odesílatele (odchozí volání) vyberte: PPP, Komutovaná linka a Provozní režim (typické vytáčení). Pro konfiguraci linky vyberte **Oblast linek**. Klepněte na **OK** a produkt System i Navigator otevře okno vlastností pro tento profil připojení.

   Poznámka: Oblast linek můžete také vybrat, vytváříte-li Profily připojení příjemce. Volba Oblast linek může a nemusí být uvedena, v závislosti na hodnotách následujících polí: typ protokolu, typ připojení a provozní režim.
5. Na stránce Obecné uveďte jméno profilu a zadejte popis.
6. Na stránce Připojení zadejte jméno oblasti linek a klepněte na **Nový**. Vyvoláte tím dialog **Vlastnosti nové oblasti linek**, kde se zobrazí všechny dostupné linky a modemy pro daný systém.
7. Vyberte linky, které chcete používat a přidejte je do oblasti. Klepnutím na volbu **Nová linka** můžete také definovat novou linku.
8. Klepněte na **OK** , abyste uložili tuto oblast linek a vraťte se na Vlastnosti nového profilu dvoubodového spojení (PPP).
9. Doplňte potřebné informace na ostatních stránkách (například nastavení TCP/IP a autentizace).
10. Profil připojení bude procházet seznam dostupných linek (bez oblasti) dokud zdroj nebude dostupný a nepoužije tuto linku pro připojení. Další rady najdete v nápovědě produktu System i Navigator.

Související odkazy

“Scénář: Připojení vzdálených volajících klientů k systému” na stránce 12
Vzdálení uživatelé, jako například lidé pracující doma nebo mobilní klienti, často vyžadují přístup do sítě své firmy. Tito volající klienti mohou získat přístup do systému prostřednictvím protokolu PPP.

“Scénář: Připojení podnikové sítě LAN k Internetu pomocí modemu” na stránce 15
Administrátoři obvykle instalují podnikové sítě, které umožňují zaměstnancům přístup k Internetu. K připojení systému k některému ISP (poskytovateli internetových služeb) mohou použít modem. PC klienti připojení k síti LAN mohou s Internetem komunikovat tak, že používají operační systém i5/OS jako bránu.

“Scénář: Propojení hlavní podnikové sítě a vzdálené sítě pomocí modemu” na stránce 17
Modem vám umožňuje, aby si dvě vzdálená pracoviště (například ústředí a pobočka) vzájemně vyměňovala data. Pomocí PPP lze propojit dvě sítě LAN tak, že se vytvoří připojení mezi systémem v ústředí a jiným systémem v pobočce.

Podpora profilů více připojení:

Profily dvoubodových připojení, které podporují více připojení, vám umožňují mít jeden profil připojení, který obslouží mnoho digitálních, analogových nebo L2TP volání.

To je užitečné v případě, že chcete, aby se více uživatelů připojovalo k systému, ale nechcete uvádět zvláštní profil dvoubodového připojení pro obsluhu každé linky. Tato funkce je zvláště užitečná pro 4portový integrovaný modem 2805, u něhož jeden adaptér používá čtyři linky.

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

Adresa IP lokálního systému pro profily více připojení

S profily více připojení můžete používat lokální adresu IP, ale musí jít o existující adresu IP definovanou na systému. Pomocí rozbalovacího seznamu lokálních adres IP si můžete vybrat existující adresu IP. Pokud jako lokální adresu IP pro protokol PPP zvolíte adresu IP lokálního systému, budou vzdálení uživatelé moci přistupovat k prostředkům na lokální síti. Musíte také definovat adresy IP, které jsou v oblasti adres IP, aby byly ve stejné síti jako lokální adresa IP lokálního systému.

Pokud lokální adresu IP systému nemáte nebo pokud nechcete, aby měli vzdálení uživatelé přístup k síti LAN, je třeba, abyste pro svůj systém definovali virtuální adresu IP. Virtuální adresa IP je také známá jako bezobvodové rozhraní.

Vaše profily dvoubodového připojení mohou používat tuto adresu IP jako svou lokální adresu IP. Jelikož tato virtuální adresa IP není vázána k žádné fyzické síti, nebude automaticky předávat provoz ostatním sítím připojeným k systému.

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

1. V prostředí produktu System i Navigator, rozbalte systém a klepněte na **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 adresu IP, jakmile ji vytvoříte. Pomocí rozbalovacího seznamu v poli **Lokální adresa IP**, které je na stránce Nastavení TCP/IP, vyberte adresu IP, kterou chcete použít se svým profilem.

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

Oblasti adres IP vzdáleného systému pro profily více připojení

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

Omezení oblasti linek

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

- V daném okamžiku může konkrétní linka existovat pouze v jedné oblasti linek. Když linku odejmete z oblasti linek, můžete ji použít v jiné oblasti linek.
- Když spouštíte profil připojení, který používá oblast linek, všechny linky v 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 v oblasti linek žádné linky, každý spouštěný profil se ihned ukončí.
- Když spustíte profil jediného připojení, který má oblast linek, systém použije pouze jednu linku z oblasti linek. Jestliže spustíte profil více připojení, který používá tutéž oblast linek, všechny zbývající linky v oblasti linek lze využít.

  Související úlohy

  “Krok 1: Konfigurace terminátoru profilu L2TP pro rozhraní na oddílu, který komunikuje s modemy” na stránce 27
  Chcete-li vytvořit nový profil terminátoru pro libovolné rozhraní, postupujte takto:

Oblast adres IP vzdáleného systému:

Systém může používat oblast adres IP vzdáleného systému pro příjem nebo ukončování profilu dvoubodového připojení, který se používá s více příchozími připojeními.

To zahrnuje L2TP a oblasti linek a maximálním počtem připojení větším než jedna. Tato funkce systému umožňuje přiřazovat jedinečnou vzdálenou adresu IP ke každému příchozímu připojení.

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

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

- Více než jeden profil připojení může uvádět stejnou oblast adres. Pokud se však používají všechny adresy IP uvedené v oblasti, každý další požadavek na připojení se odmítá do doby, než se jiné připojení ukončí a tím dá k dispozici volnou adresu IP.
- Chcete-li alokovat určité adresy IP pro některé vzdálené systémy, zatímco chcete jiným příchozím systémům povolit používání adresy IP z oblasti, proveďte následující kroky:
  1. Povolte ověřování vzdáleného systému na kartě **Autentizace**, aby mohlo být zjištěno jméno uživatele vzdáleného systému.
  2. Definujte rozsah vzdálených adres IP pro všechny příchozí požadavky na připojení, které nevyžadují konkrétní adresu IP.
  3. Definujte adresy IP pro konkrétní uživatele tak, že zaškrtnete volbu **Definovat přídavné adresy IP na základě ID uživatele vzdáleného systému**, a pak klepněte na volbu **Adresa IP definovaná na základě jména uživatele**.

  Když se vzdálený uživatel připojí, systém určí, zda je pro daného uživatele definována specifická adresa IP. Pokud ano, předá se adresa IP vzdálenému systému; v opačném případě se vrátí adresa IP z oblasti vzdálených adres IP.

Konfigurace modemu pro PPP

Modem vám poskytuje schopnosti analogového připojení (pronajatá linka a komutovaná linka). Pro svá analogová připojení PPP můžete používat externí modem, interní modem, externí modem nebo adaptér terminálu ISDN.

Související odkazy

“Odstraňování problémů s PPP” na stránce 61
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.

Konfigurace nového modemu

Můžete nakonfigurovat nový modem s pomocí existujícího popisu modemu, nebo můžete popis modemu založit na předchozím popisu modemu.

Jak konfigurovat nový modem, postupujte takto:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
2. Klepněte pravým tlačítkem myši na **Modemy** a vyberte **Nový modem**.
3. Na kartě **Obecné** zadejte správné hodnoty do všech okének.
4. Volitelné: Pokud chcete přidat nějaké inicializační příkazy pro modem, klepněte na kartu **Přídavné parametry**.
5. Klepnutím na **OK** uložíte své záznamy a uzavřete stránku Vlastnosti nového modemu.

Použití existujícího popisu modemu

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

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
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.

Vytvoření popisu modemu, který je založený na předchozím popisu modemu

Chcete-li vytvořit popis modemu, který je založený na předchozím popisu modemu, proveďte následující kroky:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
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.

Související odkazy

"Odstraňování problémů s PPP" na stránce 61
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.

Nastavení příkazového řetězce modemu

Můžete si vyhledat ekvivalentní příkazové řetězce v uživatelské příručce ke svému modemu. V popisu modemu použijte výrobcem doporučené nastavení.

Tabulka 9. Modemy definované na systému a příkazové řetězce

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

Tento příklad demonstruje, jak konfigurovat adaptéry terminálu ISDN.

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
2. Klepněte pravým tlačítkem myši na **Modemy** a vyberte **Nový modem**.
3. Na kartě **Obecné** zadejte správné hodnoty do všech **okének**.
4. Volitelné: Pokud chcete přidat nějaké inicializační příkazy pro modem, klepněte na kartu **Parametry 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, které systém může provádět za účelem nápravy chyb.

   Proto by tyto příkazy měly obsahovat a být omezeny následujícími nastaveními:

- 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 znak CR pro indikaci délky parametru.
- Ukládání a aktivace nových nastavení, aby se obnovovala po vynulování nebo po vypnutí systému.
- Testovací příkaz aktivního stavu rozhraní *U* (ATD*x*), který systému umožňuje určit, kdy bylo dosaženo 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 přidruží k popisu linky.
6. Klepnutím na **OK** uložíte své záznamy a uzavřete stránku Vlastnosti nového modemu.

Související odkazy

“Adaptéry terminálu ISDN” na stránce 37
ISDN (Integrated Services Digital Network) vám poskytuje digitální připojení, které vám umožní komunikovat pomocí libovolné kombinace hlasu, dat, videa a dalších multimediálních aplikací.

Přiřazení modemu k popisu linky

Toto téma demonstruje kroky pro přidružení modemu k popisu linky.

1. V prostředí produktu System i Navigator vyberte svůj systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu) → Profily připojení odesílatelů nebo ″Profily připojení příjemců″**.
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 kartu **Připojení** a klepněte na **Nové**.
   - Zadejte jméno konfigurace linky.
   - Klepnutím na **Nová** otevřete okno Vlastnosti nové linky.
4. V okně Vlastnosti nové linky klepněte na kartu **Modem** a vyberte modem ze seznamu. Vybraný modem se přidruží k tomuto popisu linky. Pro interní modemy byste vždy měli vybrat odpovídající definici modemu. Další informace naleznete v online nápovědě.

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 kartě **Modem** v okně konfigurace linky PPP. Linky PPP můžete konfigurovat na kartě **Připojení** u profilů připojení příjemce a odesílatele.

Související úlohy

“Vytvoření profilu připojení” na stránce 44
Prvním krokem při konfiguraci připojení PPP mezi systémy je vytvoření profilu připojení na systému.

Konfigurace vzdáleného PC

Chcete-li se připojit k platformě z PC, který pracuje s některým 32bitovým operačním systémem Windows, přesvědčte se, že je modem správně nainstalován a nakonfigurován a že máte na svém PC nainstalován protokol TCP/IP a telefonické připojení sítě.

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

- Typ telefonického připojení by měl být **PPP**.
- Používáte-li šifrovaná hesla, je třeba, abyste používali autentizační protokol CHAP-MD5 (MS-CHAP není operačním systémem i5/OS podporován). Některé verze operačního systému 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 (Password Authentication Protocol). Žádný jiný typ nezabezpečeného protokolu nebude systém podporovat.
- Adresování IP je obvykle definováno vzdáleným systémem, nebo operačním systémem i5/OS. Máte-li v úmyslu použít alternativní zásady adresování IP (například definování svých vlastních adres IP), zajistěte, aby byl systém konfigurován tak, aby přijímal vaši zásadu adresování.
- Přidejte adresu IP DNS, pokud je to vhodné pro dané prostředí.

Konfigurace přístupu k Internetu přes AT & T Global Network

Pro komunikaci s AT&T Global Network jsou nutné zvláštní profily.

Chcete-li získat přístup k této službě, můžete použít průvodce vytáčeným 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 následující typy aplikací:

- **Výměna pošty**: Umožňuje pravidelně odebírat poštu z jednoho účtu AT&T Global Network a odesílat ji na váš systém, odkud je distribuována uživatelům produktu Lotus Mail nebo uživatelům protokolu SMTP (Simple Mail Transfer Protocol).
- **Telefonické připojení do sítě**: Používejte aplikace pro vytáčené 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).
- 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.
- 2793/576C: 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 modem 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:

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

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

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
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

Můžete použít průvodce připojením, kteří vám pomohou s konfigurací profilu připojení.

Průvodce novým vytáčeným připojením

Tento průvodce popisuje kroky konfigurace profilu připojení přes vytáčenou linku tak, abyste získali přístup k vašemu ISP (poskytovateli služeb sítě Internet) nebo k síti Internet. Budete muset u správce sítě nebo ISP zjistit určité informace, abyste mohli tohoto průvodce dokončit. Další informace pro dokončení tohoto průvodce získáte v online nápovědě.

IBM Universal Connection Wizard

Tento průvodce popisuje konfigurací profilu, který může být použit softwarem elektronické podpory zákazníka (ECS) pro připojení k IBM. Podpora elektronických služeb umožňuje monitorování jedinečného systémového prostředí i5/OS, aby vám mohly být doporučeny úpravy určené konkrétně pro váš systém a situaci.

Související informace

Univerzální připojení

Konfigurace zásady přístupu skupiny

Složka **Zásady přístupu skupiny** 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.

Chcete-li konfigurovat novou zásadu přístupu skupiny, postupujte takto:

1. V prostředí System i vyberte svůj systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu) → Profily připojení příjemců**.
2. Klepněte pravým tlačítkem myši na **Zásady přístupu skupiny** a vyberte **Nová zásada přístupu**.
3. Na kartě **Obecné** zadejte jméno a popis nové zásady přístupu skupiny.
4. Klepněte na kartu **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 6. Jelikož neznáte typ nastavení linky, dokud se připojení neuskuteční, je předvolená hodnota vždy 1. Zásadu 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 zásada 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 kartu **Nastavení TCP/IP** povolíte libovolné z následujících nastavení:

   Povolit vzdálenému systému přístup k ostatním sítím (směrování pomocí IP). Tato volba uvádí, zda chcete směrování pomocí protokolu IP. Pokud vyberete tuto volbu, povolíte, aby systém pracoval pro toto připojení jako směrovač. Tak mohou datagramy protokolu IP, které nejsou určeny pro tento systém, projít tímto systémem do připojené sítě. Jestliže necháte toto pole nevyplněné, protokol IP vyřadí ze vzdáleného systému datagramy, které nejsou určeny pro žádnou z adres, jež jsou pro tento systém lokální.

   Kvůli zabezpečení dat možná směrování pomocí protokolu IP nebudete chtít povolit. Poskytovatel služeb sítě Internet (ISP) naopak obvykle směrování pomocí protokolu IP poskytuje. Pamatujte, že toto bude fungovat pouze tehdy, když je povoleno postoupení datagramů pomocí protokolu IP v celém systému; jinak bude tato volba ignorována, i když bude označena. Postoupení datagramů pomocí protokolu IP v celém systému lze zobrazit prostřednictvím karty **Obecné** na stránce Vlastnosti IPv4.

Požadovat komprimaci hlavičky TCP/IP (VJ). Tato volba uvádí, zda chcete, aby protokol IP komprimoval informace v hlavičce poté, co vytvoří 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, ustanoví systém připojení, které kompresi nepoužívá.

Použít pro toto připojení pravidla paketu IP. Tato volba uvádí, zda chcete na tuto zásadu skupiny použít nějaké pravidlo filtrování. Pravidla filtrování řídí přenosy IP v síti. Komponentu filtrování IP paketů můžete použít k ochraně vašeho systému tím, že filtruje pakety podle pravidel, která zadáte. Tato pravidla se zakládají na informacích v záhlaví paketu.

Použití zásad skupiny na uživatele se vzdáleným přístupem

Když dokončíte nastavení vlastností dvoubodového připojení nového profilu připojení příjemce, můžete na uživatele se vzdáleným přístupem použít zásadu skupiny.

Chcete-li použít zásadu skupiny na uživatele se vzdáleným přístupem, postupujte takto:

1. Klepněte na **Autentizace** a otevře se stránka autentizace.
2. Klepněte na **Požadovat, aby tento server iSeries ověřil identitu vzdáleného systému**.
3. Vyberte volbu **Lokální autentizace pomocí ověřovacího seznamu**.
4. Jestliže existuje ověřovací seznam, vyberte jej ze 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 okně Přidat uživatele vyplňte následující informace:
   a. Vyberte autentizační protokol, pro který je jméno uživatele definované.
   b. 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 22314), EAP (Extensible Authentication Protocol) a PAP (Password Authentication Protocol).
   c. Zaškrtněte volbu **Použít pro uživatele zásadu skupiny**, vyberte zásadu skupiny ze seznamu a klepněte na **Otevřít**.

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

Související odkazy

"Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP" na stránce 22
Zásady 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 adresám IP ve vaší síti.

Související informace

Filtrování IP a převod síťových adres (NAT)

Použití pravidel filtrování IP na připojení PPP

Soubor pravidel paketů můžete použít pro omezení přístupu k adresám IP pro uživatele nebo skupiny ve vaší síti.

Téma Filtrování paketů IP a NAT v aplikaci Informační centrum popisuje, jak vytvářet pravidla IP paketů, na která se můžete odkazovat v profilu připojení PPP.

Existující pravidla filtrování IP paketů můžete zobrazit 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 ze seznamu.
3. Klepněte na **OK**, chcete-li použít filtr PPP pro profil připojení.

- Uživatelská úroveň
  1. Otevřete existující zásady přístupu skupiny nebo vytvořte novou zásadu přístupu skupiny.
  2. Klepněte na stránku Nastavení TCP/IP.
  3. Zaškrtněte volbu **Použít pro toto připojení pravidla paketu IP** a vyberte identifikátor filtru PPP ze seznamu.
  4. Klepnutím na **OK** použijete filtr PPP.

Související odkazy

"Scénář: Správa přístupu vzdálených uživatelů k prostředkům pomocí zásad skupin a filtrování IP" na stránce 22
Zásady 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 adresám IP ve vaší síti.

Povolení služeb RADIUS a DHCP pro profily připojení

Pokyny pro povolení služeb RADIUS nebo DHCP (Dynamic Host Configuration Protocol) pro profily připojení příjemců PPP.

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**.
2. Klepněte pravým tlačítkem myši na **RAS (Služby vzdáleného přístupu)** a vyberte **Služby**.
3. Klepněte na kartu **DHCP-WAN**. Tím automaticky povolíte DHCP a detekuje se, který server DHCP a agenti přenosu (pokud vůbec nějací) jsou spuštěny v systému.
4. Chcete-li aktivovat služby RADIUS, klepněte na kartu **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 tlačítko **OK** se vraťte do prostředí produktu System i Navigator.

Související odkazy

"Scénář: Autentizace vytáčených připojení pomocí RADIUS NAS" na stránce 20
Server NAS (Network Access Server) spuštěný na systému může směrovat požadavky na autentizaci volajících klientů na samostatný server RADIUS. Jestliže dojde k autentizaci, může server RADIUS také řídit adresy IP přiřazené uživatelům.

Správa PPP

Toto téma obsahuje informace o úlohách správy PPP, které můžete na systému provádět.

Související odkazy

"Informace související s RAS (Služby vzdáleného přístupu)" na stránce 62
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Nastavení vlastností profilů připojení PPP

Při vytváření profilu připojení obvykle v okně Nastavení profilu dvoubodového spojení vyberete protokol, typ připojení a provozní režim nového profilu připojení.

Jakmile zadáte své volby do tohoto okna, zobrazí se list vlastností profilu připojení. Výběr, který uvedete v 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 okna Vlastnosti nového profilu dvoubodového spojení můžete použít toto vodítko. Nastavení, která vyberete na každé stránce, závisí na vašem prostředí a typu připojení, které konfigurujete. Online nápověda produktu System i Navigator popisuje každou volbu, která se objevuje v dialogovém okně. Další informace naleznete v příkladech a procedurách PPP.

Monitorování aktivity PPP

Pomocí produktu System i Navigator můžete zobrazit profil připojení a protokol relace.

Něco o úlohách připojení PPP:

- Existují dvě řídicí úlohy PPP, které se používají pro správu jednotlivých vláken připojení PPP. Tyto úlohy se provádějí v subsystému QSYSWRK:
  - QTPPPCTL - Hlavní řídicí úloha PPP. Tato úloha spravuje všechna vlákna připojení PPP.
  - QTPPPL2TP - Server L2TP. Tato úloha spravuje ustanovení tunelu L2TP a spouští se pouze tehdy, když je v daný okamžik spuštěný profil L2TP.
- Vlákna připojení PPP v úlohách QTPPPCTL jsou spuštěny pod jménem uživatele QTCP.
- Úlohy připojení SLIP se spouštějí v subsystému QSYSWRK pod jménem uživatele QTCP. Existují dva typy jmen úloh SLIP:
  - QTPPDIAL*nn* jsou úlohy odchozího připojení, kde *nn* je libovolné číslo od 1 do 99.
  - QTPPANS*nnn* jsou úlohy příchozího připojení, kde *nnn* je libovolné číslo od 1 do 999.

Práce s komunikačními profily:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**. 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 **Připojení** otevírá okno pro zobrazení informací o všech připojeních, která jsou přidružena k profilu. Informace mohou zahrnovat připojovací data pro aktuální připojení, dřívější připojení, nebo obojí. Volby pro zobrazení výstupu úlohy, podrobností pro připojení, protokolů volání nebo protokolů zpráv pro každé dostupné připojení.
   - Volba **Vlastnosti** otevírají stránky vlastností, které zobrazují aktuální vlastnosti připojení.

Zobrazení informací o připojení:

1. V prostředí produktu System i Navigator vyberte váš systém a rozbalte **Síť → RAS (Služby vzdáleného přístupu)**. 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, ID vlákna, adresy IP lokálního nebo vzdáleného systému a jméno úlohy PPP, mohou být uvedeny v závislosti na stavu každé PPP úlohy.
3. Chcete-li zobrazit výstup úlohy, podrobnosti pro připojení, protokoly volání nebo protokoly zpráv, klepněte pravým tlačítkem na připojení a tlačítka se povolí.
4. Chcete-li zobrazit QTPPPCTL, klepněte na **Úlohy**. Z okna pro připojení klepněte pravým tlačítkem na jméno úlohy a vyberte **Tiskový výstup** nebo **Protokol úlohy** a zobrazí se informace o všech vláknech přiřazených k úloze QTPPPCTL.
5. Chcete-li zobrazit podrobnosti o připojení, klepněte na **Podrobnosti**. Podrobnosti lze zobrazovat pouze pro momentálně aktivní připojení. Okno podrobností připojení vám umožňuje prohlédnout si další informace o tomto konkrétním připojení.
6. Chcete-li zobrazit protokoly volání, klepněte na **Protokol volání**.
7. Chcete-li zobrazit protokoly zpráv, klepněte na **Protokol zpráv**.

Práce s výstupem z PPP ze systému:

Chcete-li pracovat s výstupem z PPP, zadejte příkaz WRKTCPPTP v příkazovém řádku systému:

- 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). Poté použijte příkaz WRKSPLF pro přístup k tiskovému výstupu.

Stav připojení:

Stav profilu připojení se zobrazuje v poli **Stav** u daného profilu v seznamu profilů připojení, pod volbou **Síť → RAS (Služby vzdáleného přístupu)** poté, co vyberete profily odesílatele nebo příjemce. Stav jednotlivého připojení se zobrazuje pomocí okna Připojení.

Tabulka 10. Popis primárního stavu

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)	Systém 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.

Tabulka 11. Popis sekundárního stavu

Popis sekundárního stavu	**Vysvětlení**
Initializing modem (Inicializace modemu)	Inicializace modemu při spouštění vytáčeného 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 adres IP)	Připojení PPP skončilo kvůli problémům při vyjednávání IP.

Tabulka 11. Popis sekundárního stavu (pokračování)

Popis sekundárního stavu	Vysvětlení
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.

Odstraňování problémů s PPP

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.

Aktuální a podstatné informace o PTF a odstraňování problémů najdete na webové stránce TCP/IP for i5/OS . Na této webové stránce jsou uvedeny nejnovější informace, které nahrazují informace obsažené v této části a převažují nad nimi.

1. Požadované výchozí informace:
   - Typ vzdáleného hostitele, operační systém a úroveň.
   - Úroveň hostitelského operačního systému i5/OS.
   - Všechny výstupní soubory jsou uloženy do výstupní fronty se stejným jménem jako je jméno profilu.
   - Protokoly úloh QTPPPCTL a QTPPPL2TP (v případě profilu L2TP).
   - Skript pro spojení, který 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 WRKTCPPTP tiskne nastavení profilu.
   - Typ a model modemu.
   - Příkazové řetězce modemu.
   - Sledování komunikace.

Publikace ITSO Redbook V4 TCP/IP for AS/400: More Cool Things Than Ever pokrývá následující problémy s PPP. Tato publikace rovněž poskytuje podrobné informace o řešení problémů.

Pro zjištění problémů a jejich řešení prohlédněte kontrolní seznam v následující tabulce.

Tabulka 12. Problémy s protokoly PPP v publikaci Redbook ITSO

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 *asynchronní*, nebo *synchronní*. Další informace naleznete v příručce k modemu.
AT příkazy modemu Modem, který se snažíte použít, není v seznamu modemů předdefinovaném v produktu System i Navigator.	Vytvořit nový modem.

Tabulka 12. Problémy s protokoly PPP v publikaci Redbook ITSO (pokračování)

Problém	Řešení
Uživatelé a hesla PPP Při pokusu o připojení PPP se objevují chyby jména uživatele a hesla.	• 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.
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.

Související pojmy

"Konfigurace modemu pro PPP" na stránce 52
Modem vám poskytuje schopnosti analogového připojení (pronajatá linka a komutovaná linka). Pro svá analogová připojení PPP můžete používat externí modem, interní modem, externí modem nebo adaptér terminálu ISDN.

"Konfigurace nového modemu" na stránce 52
Můžete nakonfigurovat nový modem s pomocí existujícího popisu modemu, nebo můžete popis modemu založit na předchozím popisu modemu.

Související odkazy

"Informace související s RAS (Služby vzdáleného přístupu)"
Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Informace související s RAS (Služby vzdáleného přístupu)

Příručky IBM Redbooks a webové stránky obsahují informace související s kolekcí témat týkajících se služeb RAS. Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

IBM Redbooks

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

Webové stránky

Nejnovější PTF a aktuální informace o konfiguraci PPP a L2TP najdete pod odkazem PPP na webové stránce TCP/IP for i5/OS . Na této webové stránce jsou uvedeny nejnovější informace, které nahrazují informace obsažené v této kolekci témat a převažují nad nimi.

Související odkazy

"Soubor PDF pro RAS (Služby vzdáleného přístupu)" na stránce 1
Tyto informace můžete prohlížet a tisknout ve formátu PDF.

Dodatek. Poznámky

Tyto informace byly vypracovány pro produkty a služby nabízené ve Spojených státech.

IBM nemusí v ostatních zemích nabízet produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve Vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoliv funkčně ekvivalentní produkt, program či službu neporušující práva IBM na duševní vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli Vám neuděluje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Česká republika, spol. s r.o.
North Castle Drive
Armonk, NY 10504-1785
USA

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve Vaší zemi nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, “ JAKÁ JE” (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností v určitých transakcích, a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči Vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Česká republika, spol. s r.o.
Software Interoperability Coordinator, Department YBWA
Česká republika

Rochester, MN 55901
USA

Informace tohoto typu mohou být dostupné za odpovídajících podmínek. V některých případech připadá v úvahu zaplacení poplatku.

Zde popsaný licencovaný program a všechny licencované materiály, které jsou pro něj k dispozici, poskytuje IBM na základě smlouvy IBM Customer Agreement, Mezinárodní licenční smlouvy IBM na programy, smlouvy IBM License Agreement for Machine Code, nebo jiné ekvivalentní smlouvy mezi námi.

Všechny uváděné údaje o výkonu byly zjišťovány v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou výrazně lišit. Některá měření byla provedena v systémech s vývojovým prostředím a neexistuje žádná záruka, že tato měření budou stejná v obecně dostupných systémech. Kromě toho byla některá měření odhadnuta extrapolací. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit vhodnost údajů pro svá specifická prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit přesnost údajů o výkonu, kompatibilitě nebo jiná tvrzení, která se k těmto produktům vztahují. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Tyto publikace obsahují příklady údajů a sestav používaných v každodenních obchodních činnostech. Abyste si udělali co neúplnější představu, obsahují příklady názvy konkrétních podniků, firemních značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami, používanými ve skutečných obchodních podnicích, je čistě náhodná.

COPYRIGHT

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které demonstrují techniku programování na různých operačních systémech. Tyto vzorové programy můžete kopírovat, modifikovat a distribuovat v jakékoliv formě za účelem vývoje, používání, prodeje nebo distribuce aplikačních programů, podřizujících se aplikačnímu programovému rozhraní pro daný operační systém, pro který byly tyto vzorové programy napsány, bez jakýchkoliv poplatků výrobci. Tyto příklady nebyly přísně testovány za všech podmínek. Z tohoto důvodu nemůže IBM zaručit nebo odvodit jejich spolehlivost, obsluhovatelnost nebo funkčnost.

Každá kopie nebo část těchto vzorových programů nebo odvozených prací musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů společnosti IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Tyto publikace týkající se tématu RAS (Služby vzdáleného přístupu): Připojení PPP jsou určeny pro programovací rozhraní, která umožňující zákazníkům psát programy za účelem získání sluežb operačního systému i5/OS.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

AIX
AS/400
eServer

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

Adobe, logo Adobe, PostScript a logo PostScript jsou buď registrované ochranné známky nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech a případně dalších jiných zemích.

Linux je registrovaná ochranná známka, jejímž majitelem je Linus Torvalds, ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka společnosti The Open Group ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.