



Systemy IBM - iSeries

Networking

Dynamic Host Configuration Protocol

Verze 5, vydání 4





Systemy IBM - iSeries

Networking

Dynamic Host Configuration Protocol

Verze 5, vydání 4

Poznámka

Dříve než použijete tyto informace a produkt, který podporují, nezapomeňte si přečíst informace uvedené v části “Poznámky”, na stránce 53.

Páté vydání (únor 2006)

Toto vydání se týká verze 5, vydání 4, modifikace 0 operačního systému IBM i5/OS (5722-SS1) a všech následných vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nemůže být spuštěna na žádném počítači RISC (reduced instruction set computer), ani na modelech CISC.

© Copyright International Business Machines Corporation 1998, 2006. Všechna práva vyhrazena.

Obsah

Protokol DHCP (Dynamic Host Configuration Protocol) 1

Tisknutelné PDF	1
Koncepce DHCP	1
Vzájemné působení klienta a serveru DHCP	1
Pronájem	3
Agenti přenosu a směrovače	5
Podpora klienta DHCP	6
BOOTP	6
Dynamické aktualizace	7
Vyhledávání voleb DHCP	8
Příklady DHCP	21
Příklad: Jednoduchá podsít DHCP	21
Příklad: Vícenásobné podsítě TCP/IP	23
Příklad: DHCP a multihoming	25
Příklad: DNS a DHCP na stejném serveru iSeries	28
Příklad: DNS a DHCP na různých serverech iSeries	30
Příklad: PPP a DHCP na jednom serveru iSeries	32
Příklad: Profil DHCP a PPP na různých serverech iSeries	34
Plánování DHCP	37
Otázky týkající se topologie sítě	38

Konfigurace DHCP	40
Konfigurace serveru DHCP a agenta přenosu BOOTP/DHCP	41
Konfigurování klientů, aby mohli používat DHCP	42
Konfigurování serveru DHCP, aby mohl odesílat dynamické aktualizace na server DNS	45
Správa pronajatých IP adres	45
Odstraňování problémů se serverem DHCP	46
Shromažďování podrobných informací o chybách DHCP	46
Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci	47
Problém: Přiřazování duplicitních IP adres ve stejné síti	48
Problém: DHCP neaktualizuje záznamy DNS	48
Problém: Protokol úloh DHCP uvádí zprávy DNS030B s chybou č. 1 ze 3447	49
Související informace o DHCP	50

Dodatek. Poznámky 53

Informace o programovacím rozhraní	54
Ochranné známky	54
Ustanovení a podmínky	55

Protokol DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) je standard TCP/IP, který centrální server používá při správě IP adres a jiných podrobností konfigurace pro celou síť.

Server DHCP odpovídá na požadavky klientů a dynamicky jim přiřazuje vlastnosti.

Tisknutelné PDF

Tuto volbu použijte k zobrazení a tisku těchto informací ve formátu PDF.


Chcete-li si prohlédnout nebo stáhnout PDF verzi tohoto dokumentu, vyberte odkaz DHCP (přibližně 1399 KB).

Uložení souborů ve formátu PDF

Pokud chcete uložit soubor PDF na pracovní stanici, abyste si ho mohli prohlédnout nebo vytisknout, postupujte takto:

1. Klepněte pravým tlačítkem myši na soubor ve formátu PDF (klepněte pravým tlačítkem myši na výše uvedený řádek).
2. Klepněte na volbu pro lokální uložení souboru ve formátu PDF.
3. Zadejte cestu do adresáře, ve kterém chcete soubor ve formátu PDF uložit.
4. Klepněte na **Save (Uložit)**.

Stažení aplikace Adobe Reader

- Chcete-li zobrazit nebo tisknout tyto soubory ve formátu PDF, potřebujete program Adobe Reader. Jeho bezplatnou kopii si můžete stáhnout z webové stránky společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepce DHCP

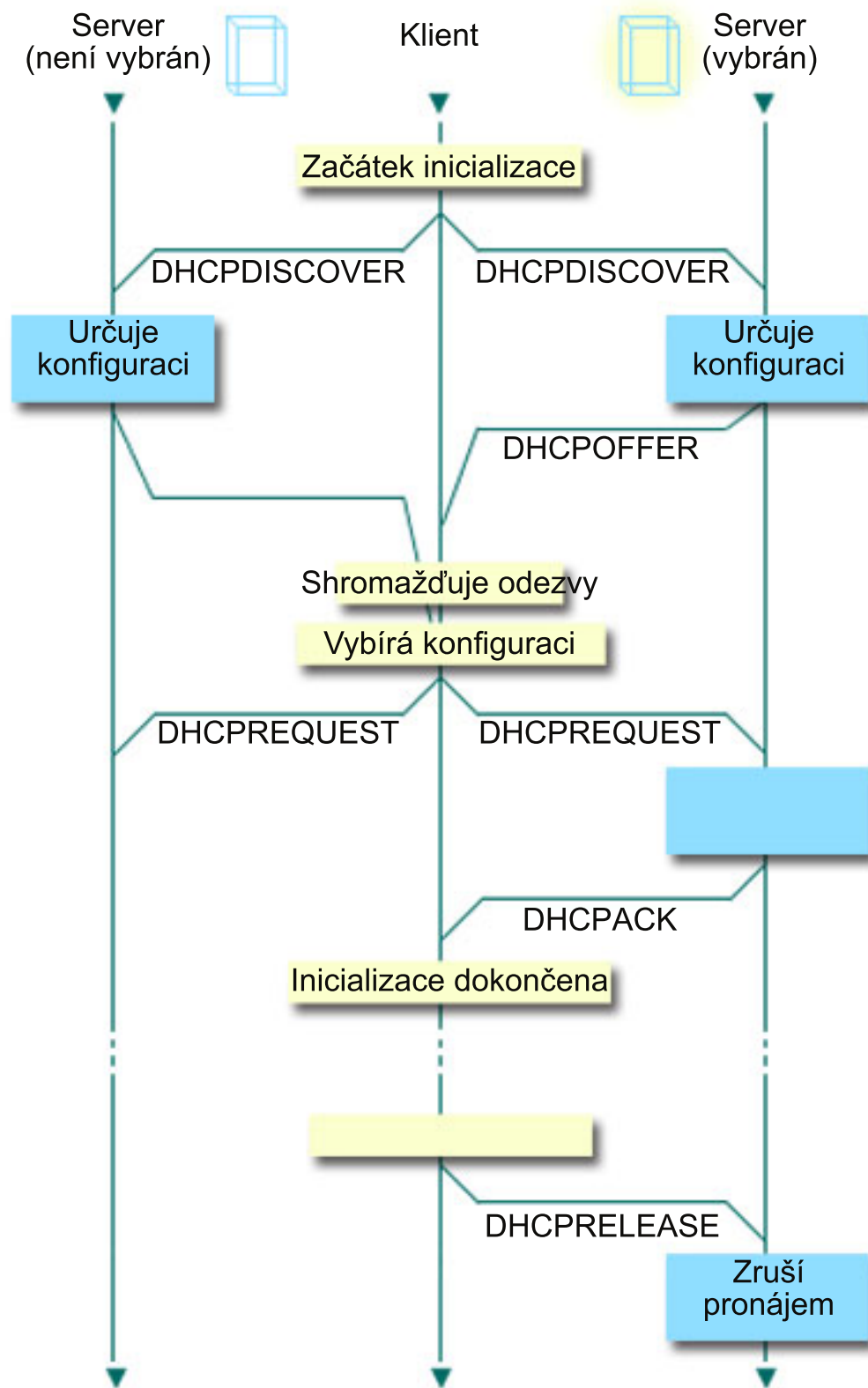
Jak DHCP vzájemně působí s klientem a jak DHCP pracuje v síti.

DHCP poskytuje automatickou metodu pro dynamickou konfiguraci klienta. Klienti, které DHCP podporuje, získávají ze serveru automaticky vlastní IP adresu a parametry konfigurace. Tento proces probíhá v řadě kroků.

Vzájemné působení klienta a serveru DHCP

Klient získává informace o DHCP ze serveru a odesílají se určité zprávy mezi klientem a serverem. DHCP získává a vrací pronájmy.

DHCP poskytuje automatickou metodu pro dynamickou konfiguraci klienta. Klienti, které DHCP podporuje, získávají ze serveru automaticky vlastní IP adresu a parametry konfigurace. Tento proces probíhá v řadě kroků, které jsou zobrazeny na následujícím obrázku.



Obrázek 1. Vzájemné působení klienta a serveru DHCP

Klient požaduje informace o DHCP: DHCPDISCOVER

Nejdříve klient odešle zprávu DISCOVER požadující IP adresu. Zpráva DISCOVER obsahuje identifikátor, který je pro tohoto klienta jedinečný (obvykle MAC adresa). Zpráva může také obsahovat jiné požadavky,

jako požadované volby (například maska podsítě, server jmen domény, jméno domény nebo statickou přenosovou cestu). Zpráva je odeslána jako vysílání. Pokud síť obsahuje směrovače, mohou být tyto směrovače konfigurovány tak, aby poslaly pakety DISCOVER na servery DHCP v připojených sítích.

Server DHCP nabízí informace klientovi: DHCP OFFER

Jakýkoliv server DHCP, který přijímá zprávu DISCOVER, může v odpovědi odeslat zprávu OFFER. Existuje několik důvodů, proč server DHCP nemusí odeslat zprávu OFFER zpět klientovi. Nejčastějším důvodem je, že všechny dostupné adresy jsou zrovna pronajaty, není konfigurována podsít nebo klient není podporován. Pokud server DHCP odesílá v odpovědi zprávu OFFER, pak DHCP OFFER bude obsahovat dostupnou IP adresu a všechny ostatní informace o konfiguraci, která je definovaná v nastavení DHCP.

Klient přijímá nabídku serveru DHCP: DHCP REQUEST

Klient přijímá zprávu OFFER ze serverů DHCP, které odpovídají na DISCOVER. Klient porovná nabídky s nastavením, které požadoval, a potom vybere server, který chce použít. Odešle zprávu REQUEST, čímž přijme nabídku, a označí server, který vybral. Tato zpráva je vyslána do celé sítě a sdělí všem serverům DHCP, který server byl vybrán.

Server DHCP potvrdí klienta a pronajme IP adresu: DHCP ACK

Pokud server přijme zprávu REQUEST, označí adresu jako pronajatou. Servery, které nejsou vybrány, vrátí nabízené adresy do dostupné společné oblasti. Vybraný server odešle klientovi potvrzení (DHCP ACK), které obsahuje další informace o konfiguraci.

Klient nyní může používat IP adresu a parametry konfigurace. Klient bude používat tato nastavení, dokud nevyprší pronájem, nebo dokud klient neodešle serveru zprávu DHCP RELEASE a neukončí tak sám pronájem.

Klient se pokouší obnovit pronájem: DHCP REQUEST, DHCP ACK

Klient začne obnovovat pronájem, když uplyne polovina doby pronájmu. Klient žádá obnovení pronájmu prostřednictvím zprávy REQUEST, kterou odešle serveru. Pokud server žádost přijme, odešle klientovi zprávu DHCP ACK. Pokud server na žádost neodpoví, může klient nadále používat IP adresu a informace o konfiguraci, dokud nevyprší pronájem. Dokud je pronájem aktivní, server ani klient nemusí procházet procesem DHCP DISCOVER a DHCP REQUEST. Když pronájem vyprší, musí klient začít znovu s procesem DHCP DISCOVER.

Klient ukončí pronájem: DHCP RELEASE

Klient ukončí pronájem zprávu RELEASE, kterou odešle serveru DHCP. Server vrátí klientovi IP adresu do dostupné společné oblasti adres.

Související pojmy

“Agenti přenosu a směrovače” na stránce 5

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

“Pronájemy”

Zde naleznete informace o tom, jaké jsou DHCP pronájemy, a některé otázky, které je třeba zvážit při určování doby pronájmu pro klienty DHCP.

“Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci” na stránce 47

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

Pronájemy

Zde naleznete informace o tom, jaké jsou DHCP pronájemy, a některé otázky, které je třeba zvážit při určování doby pronájmu pro klienty DHCP.

Když server DHCP odešle klientovi informace o konfiguraci, jsou tyto informace odeslány společně s dobou pronájmu. Tou se rozumí doba, po kterou klient může používat IP adresu, která mu byla přiřazena. Během doby pronájmu nemůže server DHCP přiřadit tuto IP adresu žádným jiným klientům. Účelem pronájmu je omezit dobu, po kterou může klient používat IP adresu. Pronájem zabraňuje nepoužívaným klientům zabírat IP adresy v případě, že existuje více klientů

než adres. Umožňuje také administrátorovi provádět v omezené době změny v konfiguraci všech klientů v síti. Když pronájem skončí, bude klient požadovat od DHCP nový pronájem. Pokud se změnila konfigurační data, budou klientovi v tomto okamžiku odeslána nová data.

Obnova pronájmu

Klient začne obnovovat pronájem, když uplyne polovina doby pronájmu. Například u 24hodinového pronájmu se klient pokusí obnovit pronájem po 12 hodinách. Klient požaduje obnovu pomocí zprávy DHCPREQUEST, kterou odešle serveru. Požadavek na obnovu obsahuje aktuální IP adresu a informace o konfiguraci klienta.

Pokud server přijme požadavek, odešle klientovi zpět zprávu DHCPACK. Pokud server na žádost neodpoví, může klient nadále používat IP adresu a informace o konfiguraci, dokud nevyprší pronájem. Jestliže pronájem je aktivní, server ani klient nemusí procházet procesem DHCPDISCOVER a DHCPREQUEST. Když pronájem vyprší, musí klient začít znovu s procesem DHCPDISCOVER.

Pokud je server nedostupný, může klient nadále používat přiřazenou adresu až do vypršení doby pronájmu. Ve výše uvedeném příkladu má klient 12 hodin do ukončení pronájmu od doby, kdy se poprvé pokusil obnovit pronájem. Během 12hodinového výpadku nemohou noví uživatelé dostat nové pronájmy, ale současně nevyprší pronájem u žádného počítače, který byl v době zahájení výpadku zapnutý.

Jak zjistit trvání pronájmu

Předvolená doba pronájmu u serveru DHCP je 24 hodin. Doba, na kterou nastavíte pronájem, závisí na několika faktorech. Budete muset zvážit své cíle, modely využití uzlu a uspořádání služeb pro server DHCP. Následující otázky vám mohou pomoci při stanovení vhodné doby pronájmu:

Máte více uživatelů než adres?

Pokud ano, měla by být doba pronájmu krátká, aby klienti nemuseli čekat na ukončení nepoužívaných pronájmů.

Znáte minimum času, který potřebujete k podpoře?

Pokud je váš typický uživatel přihlášen minimálně jednu hodinu, naznačuje to, že doba pronájmu by měla být minimálně jednu hodinu.

Jaký přenos zpráv DHCP dokáže vaše síť zvládnout?

Pokud máte velký počet klientů nebo pomalé komunikační linky, po kterých jsou přenášeny pakety DHCP, může provoz sítě působit problémy. Čím kratší je doba pronájmu, tím větší je přenos kvůli zátěži serveru a síť kvůli požadavkům na obnovu v síti.

Jakým druhem servisního plánu disponujete a do jaké míry může váš server zvládnout výpadek?

Zvažte jakoukoliv obvyklou údržbu a její možný vliv na výpadek. Pokud je doba pronájmu alespoň dvojnásobně delší než výpadek serveru, potom spuštění klienti neztratí svůj pronájem. Pokud máte dobrou představu o nejdelším možném výpadku serveru, můžete se takovým problémům vyhnout.

V jakém síťovém prostředí je server DHCP? Co dělá typický klient?

Zvažte, co dělá klient v síti, kterou obsluhuje server DHCP. Pokud máte například prostředí, kde jsou klienti hlavně mobilní a připojují se k síti v různou dobu, obvykle pouze jednou nebo dvakrát za den kvůli kontrole elektronické pošty, můžete žádat poměrně krátkou dobu pronájmu. V tom případě není nutné mít pro každého klienta nastavenou jednu IP adresu. Když omezíte dobu pronájmu, můžete při podpoře mobilních klientů použít méně IP adres.

Pokud ale máte kancelářské prostředí, kde většina zaměstnanců má primární pracovní stanice na pevném místě, může být vhodnější doba pronájmu 24 hodin. V tomto prostředí může být také nezbytné mít dostupnou IP adresu pro každého klienta, který se v pracovní době připojuje k síti. Pokud v takovém případě zadáte kratší dobu pronájmu, server DHCP bude jednat s klientem o obnově pronájmu mnohem častěji, což by způsobovalo velké zatížení provozu sítě.

Jak často se mění konfigurace sítě?

Pokud se topologie sítě mění poměrně často, bylo by lepší zvolit kratší dobu pronájmu. Dlouhá doba pronájmu

může být nevýhodná v případech, kdy potřebujete změnit parametry konfigurace. Délka pronájmu může ovlivnit to, zda budete muset restartovat každého postiženého klienta nebo zda vám postačí čekat po určitou dobu, než se obnoví pronájem.

Pokud se topologie sítě mění jen zřídka a ve společné oblasti adres máte dostatek IP adres, můžete nakonfigurovat DHCP, aby používal nekonečný pronájem - pronájem, který nikdy nevyprší. Nekonečné pronájmy se však nedoporučují. Pokud použijete nekonečný pronájem, je IP adresa pronajata klientovi na nekonečně dlouhou dobu. Tito klienti nemusí po obdržení nekonečného pronájmu procházet procesem obnovy pronájmu. Jakmile je klientovi přiřazen nekonečný pronájem, nemůže být tato adresa přiřazena jinému klientovi. Proto mohou nastat problémy s nekonečnými pronájmy v případě, kdy chcete tomuto klientovi přiřadit novou IP adresu nebo později pronajmout klientovu IP adresu jinému klientovi.

Můžete mít v síti klienty, jako je například souborový server, kteří budou vždy dostávat stejnou IP adresu. Namísto nekonečného pronájmu byste měli tomuto klientovi přiřadit určitou adresu a dát mu dlouhou dobu pronájmu. Klient si ji sice musí pronajmout na zadanou dobu a pronájem obnovovat, ale server obdrží IP adresu pouze pro tohoto klienta. Když potom například získáte nový souborový server, můžete změnit pouze identifikátor klienta (MAC adresu) a server dá novému souborovému serveru stejnou adresu. Pokud jste dali nekonečný pronájem, potom server DHCP nemůže znovu vydat tuto adresu, dokud není tento pronájem explicitně vymazán.

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Související odkazy

“Vzájemné působení klienta a serveru DHCP” na stránce 1

Klient získává informace o DHCP ze serveru a odesílají se určité zprávy mezi klientem a serverem. DHCP získává a vrací pronájmy.

Agenti přenosu a směrovače

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

Klienti DHCP zpočátku vysílají pakety DISCOVER, protože nevědí, ke které síti jsou připojeni. V některých sítích nemusí být server DHCP ve stejné síti LAN jako klient. Proto je nezbytné postoupit klientovy odeslané pakety DHCP do sítě LAN, kde se nachází server DHCP. Některé směrovače jsou konfigurovány tak, aby přesměrovaly pakety DHCP. Pokud váš směrovač podporuje přesměrování paketů DHCP, nemusíte nic dělat. Mnohé směrovače však nepřesměřují pakety, které mají cílovou IP adresu adresy plošného vysílání (pakety DHCP). V tomto případě, kdy směrovač nemůže přesměrovat pakety DHCP, musí mít síť LAN agenta přenosu BOOTP/DHCP, který přesměruje pakety DHCP do sítě LAN se serverem DHCP. Ukázkou sítě používající agenta přenosu a směrovač uvádí téma *Příklad: Profil DHCP a PPP na různých serverech iSeries*.

Kvůli tomu, že server DHCP je v samostatné síti, budou muset mít vaši klienti v každém případě definovanou volbu směrovače (volba 3), která uvádí IP adresu směrovače připojovacího jejich síť k síti se serverem DHCP.

Pokud podle tohoto scénáře nepoužijete agenta přenosu BOOTP/DHCP, budete muset kvůli obsluze těchto klientů přidat server DHCP k druhé síti LAN. Při rozhodování o tom, kolik serverů DHCP je třeba mít v síti, vám pomůže téma *Otázky týkající se topologie sítě*.

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

“Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci” na stránce 47

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

Související úlohy

“Konfigurace serveru DHCP a agenta přenosu BOOTP/DHCP” na stránce 41

Toto téma vysvětluje, jaký software potřebujete, abyste mohli konfigurovat server iSeries DHCP. Také obsahuje instrukce popisující jak pracovat s konfigurací DHCP, jak používat nástroj pro administraci serveru DHCP (DHCP Server Monitor Program) a jak nastavit agenta přenosu DHCP/BOOTP.

Související odkazy

“Vzájemné působení klienta a serveru DHCP” na stránce 1

Klient získává informace o DHCP ze serveru a odesílají se určité zprávy mezi klientem a serverem. DHCP získává a vrací pronájmy.

“Příklad: Profil DHCP a PPP na různých serverech iSeries” na stránce 34

Zde se dozvíte, jak nastavit dva servery iSeries jako síťový server DHCP a agenta přenosu DHCP/BOOTP pro dvě sítě LAN a vzdálené klienty připojené přes komutovanou linku.

Podpora klienta DHCP

Pomocí DHCP můžete spravovat každého klienta v síti namísto správy všech klientů jako velké skupiny (podsítí).

Tato metoda nastavení DHCP umožňuje klientům identifikovaným serverem DHCP přijmout IP adresu a informace o konfiguraci.

Lidé často uvažují o používání DHCP kvůli přidělování IP adres ze společné oblasti adres podsítí klientů. Když používáte podsítě, může každý klient, který požaduje ze sítě informace o DHCP, obdržet IP adresu ze společné oblasti adres, za předpokladu, že administrátor DHCP explicitně tyto adresy nevyloučil. Server DHCP je však také schopen opačné činnosti - omezit službu DHCP pouze na určité klienty.

Server DHCP může omezit službu jak na úrovni individuálního klienta, tak podle typu klienta (BOOTP nebo DHCP). Při omezení služby na úrovni individuálního klienta musíte v konfiguraci DHCP individuálně identifikovat každého síťového klienta. Každý klient je identifikován podle ID klienta (obvykle je to MAC adresa). Pouze ti klienti, kteří jsou identifikováni v konfiguraci DHCP, dostanou od serveru DHCP IP adresu a informace o konfiguraci. Pokud klient není uveden v konfiguraci DHCP, je mu odepřena služba serveru DHCP. Tato metoda zabraňuje neznámým hostitelům získávat od serveru DHCP IP adresy a informace o konfiguraci.

Pokud chcete mít ještě větší kontrolu nad síťovými klienty a informacemi o konfiguraci, které tyto klienti získávají, můžete nastavit klienty DHCP tak, aby získávali statickou IP adresu namísto IP adresy ze společné oblasti adres. Pokud nastavíte klienta tak, aby získával definovanou IP adresu, měl by tento klient být jediným klientem, který může obdržet tuto IP adresu, abyste se vyhnuli překrývání adres. Pokud používáte dynamické přidělování IP adres, bude přiřazování IP adres klientům spravovat server DHCP.

V širším významu může server DHCP omezit služby klientovi podle typu klienta, BOOTP nebo DHCP. Server DHCP může odmítnout službu pro klienty BOOTP.

Související pojmy

“BOOTP”

Toto téma popisuje, co je BOOTP, a uvádí určitou historii o BOOTP a DHCP.

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

BOOTP

Toto téma popisuje, co je BOOTP, a uvádí určitou historii o BOOTP a DHCP.

Protokol BOOTP (Bootstrap protocol) je hostitelský konfigurační protokol, který byl používán před tím, než byl vyvinut protokol DHCP. Podpora BOOTP je zkrácenou verzí protokolu DHCP. V BOOTP jsou klienti definováni MAC adresou a je jim přiřazena určitá IP adresa. V podstatě se dá říci, že každý klient v síti je mapován na IP adresu.

Neexistuje zde žádné dynamické přiřazení adresy, každý klient v síti musí být označen v BOOTP a klienti mohou přijmout pouze omezené množství informací o konfiguraci ze serveru BOOTP.

Vzhledem k tomu, že DHCP je založen na BOOTP, server DHCP může podporovat klienty BOOTP. Pokud nyní používáte BOOTP, můžete nastavit a používat DHCP, aniž by to mělo vliv na klienty BOOTP. Aby bylo možné úspěšně podporovat klienty BOOTP, musíte zadat IP adresu a volbu jména zaváděcího souboru (volba 67) a podpora BOOTP musí být zapnuta pro celý server nebo různé podsítě.

Použití DHCP při podpoře klientů BOOTP je nadřazeno nad použitím serveru BOOTP. Dokonce i když používáte DHCP při podpoře klientů BOOTP, je každý klient BOOTP v podstatě mapován na jednu IP adresu, a tuto adresu proto nemůže znovu použít jiný klient. V tomto případě je však výhodou používání DHCP to, že není třeba konfigurovat prosté mapování klientů BOOTP na IP adresy. Server DHCP bude stále dynamicky přiřazovat IP adresy klientovi BOOTP ze společné oblasti adres. Jakmile je klientovi BOOTP přiřazena IP adresa, pak je tato adresa trvale vyhrazena tomuto klientovi, dokud vyhrazenou adresu explicitně nevymažete. Nakonec můžete uvažovat o konverzi klientů BOOTP na DHCP kvůli snadnější hostitelské správě konfigurace.

Související pojmy

“Podpora klienta DHCP” na stránce 6

Pomocí DHCP můžete spravovat každého klienta v síti namísto správy všech klientů jako velké skupiny (podsítí).
BOOTP

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Dynamické aktualizace

Můžete používat server DHCP společně se serverem DNS při dynamické aktualizaci informací o klientovi v DNS, když DHCP přiřazuje klientovi IP adresu.

DNS (Domain Name System) je systém distribuované databáze pro správu hostitelských jmen a přiřazených IP adres. DNS umožňuje uživatelům vyhledat hostitele pomocí jednoduchých jmen, jako je "www.příklad.com", namísto IP adres (xxx.xxx.xxx.xxx).

V minulosti byla všechna data DNS uložena ve statických databázích. Všechny zdrojové soubory DNS musel vytvářet a udržovat administrátor. Nyní mohou být servery DNS provozující BIND 8 konfigurovány tak, aby při dynamické aktualizaci zónových dat přijímaly požadavky z jiných zdrojů.

Server DHCP můžete konfigurovat tak, aby odesílal aktualizované požadavky na server DNS pokaždé, když přiřazuje novou adresu hostiteli. Tento automatizovaný proces snižuje náročnost správy serveru DNS v rychle rostoucích nebo měnících se sítích TCP/IP a v sítích, kde hostitelé často mění umístění. Když klient, který používá DHCP, obdrží IP adresu, jsou tato data ihned odeslána serveru DNS. Pomocí této metody může DNS pokračovat v úspěšném řešení dotazů pro hostitele, dokonce i když se jejich IP adresy mění.

Můžete konfigurovat DHCP, tak aby aktualizoval záznamy mapování adres (A), záznamy PTR (reverse-lookup pointer) nebo oba typy záznamů namísto klienta. Záznam A mapuje klientovo DNS jméno na IP adresu. Záznam PTR mapuje hostitelovu IP adresu na hostitelské jméno. Když se změní klientova adresa, může DHCP automaticky odeslat aktualizaci do serveru DNS, takže ostatní hostitelé v síti mohou klienta najít na jeho nové adrese pomocí dotazů DNS. Pro každý dynamicky aktualizovaný záznam bude napsán textový záznam (TXT), který indikuje, že tento záznam byl napsán pomocí DHCP.

Poznámka: Pokud nastavíte DHCP tak, aby aktualizoval pouze záznamy PTR, musíte konfigurovat DNS a umožnit klientům aktualizaci, aby každý klient mohl aktualizovat svůj záznam A.

Dynamické zóny jsou zabezpečeny pomocí seznamu autorizovaných zdrojů, kterým je umožněno odesílat aktualizace. DNS před aktualizací zdrojových záznamů ověří, zda došlé pakety požadavků přicházejí od autorizovaného zdroje.

Dynamické aktualizace mezi DNS a DHCP mohou být provedeny na jednom serveru iSeries, různých serverech iSeries nebo na jiných serverech, které umožňují dynamické aktualizace.

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

“Problém: DHCP neaktualizuje záznamy DNS” na stránce 48

Server iSeries DHCP je schopen dynamicky aktualizovat zdrojové záznamy DNS. Chyby dynamické aktualizace mohou být způsobeny selháním aktualizace záznamů DNS.

Související úlohy

“Konfigurování serveru DHCP, aby mohl odesílat dynamické aktualizace na server DNS” na stránce 45

Můžete konfigurovat servery DHCP a DNS, aby bylo možné dynamicky aktualizovat zdrojové záznamy DNS, když server DHCP pronajímá klientovi IP adresu.

Konfigurování serveru DNS, aby mohl přijímat dynamické aktualizace

Související informace

Server jmen domény (DNS)

Záznamy prostředků

Vyhledávání voleb DHCP

DHCP má mnoho konfiguračních voleb, které mohou být odeslány klientovi v případě požadavků na informace od serveru DHCP. Můžete použít nástroj pro vyhledávání, který popisuje všechny volby DHCP.

Volby DHCP definují dodatečná konfigurační data, která server DHCP předává klientovi společně s IP adresou. Typické volby zahrnují masku podsítě, jméno domény, IP adresy směrovače, IP adresy serveru DNS a statické přenosové cesty.

Standardní volby DHCP založené na definicích, které uvádí RFC 2132: DHCP Options and BOOTP Vendor Extensions, jsou popsány v následující tabulce. Uživatelsky přizpůsobené volby můžete také nakonfigurovat na stránce **Volby** aplikace iSeries Navigator.

Tabulka 1.

Číslo volby	Volba	Popis												
1	Maska podsítě	<p>Volba masky podsítě uvádí masku podsítě klienta, jak je uvedeno v RFC 950. Pokud je v odpovědi DHCP uvedena jak volba pro masku podsítě, tak i volba pro směrovač, pak musí být uvedena volba pro masku podsítě jako první.</p> <p>Kód volby pro masku podsítě je 1 a její délka je 4 oktety.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Subnet mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG530-0</p>	Code	Len	Subnet mask				1	4	m1	m2	m3	m4
Code	Len	Subnet mask												
1	4	m1	m2	m3	m4									
2	Časový posun	<p>Pole časového posunu uvádí odchylku podsítě klienta od času UTC ve vteřinách. Odchylka je vyjádřena dvěma doplňkovými 32bitovými celými čísly. Kladná odchylka znamená, že lokalita je východně od nultého poledníku, a záporná odchylka znamená, že lokalita je západně od nultého poledníku.</p> <p>Kód volby časového posunu je 2 a její délka je 4 oktety.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Time offset</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>4</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG531-0</p>	Code	Len	Time offset				2	4	n1	n2	n3	n4
Code	Len	Time offset												
2	4	n1	n2	n3	n4									

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis									
3	Směrovač	<p>Volba pro směrovač uvádí seznam IP adres směrovačů v podsíti klienta. Směrovače by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro směrovač je 3. Minimální délka volby pro směrovač je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>3</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG511-0</p>	3	n	a1	a2	a3	a4	a1	a2	...
3	n	a1	a2	a3	a4	a1	a2	...			
4	Server času	<p>Volba pro server času obsahuje seznam serverů času podle RFC 868, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server času je 4. Minimální délka volby pro server času je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>4</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG512-0</p>	4	n	a1	a2	a3	a4	a1	a2	...
4	n	a1	a2	a3	a4	a1	a2	...			
5	Server jmen	<p>Volba pro server jmen uvádí seznam serverů jmen podle IEN 116, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server jmen je 5. Minimální délka volby pro server jmen je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>5</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG513-0</p>	5	n	a1	a2	a3	a4	a1	a2	...
5	n	a1	a2	a3	a4	a1	a2	...			
6	Server jmen domény	<p>Volba pro server jmen domény uvádí seznam serverů jmen DNS (STD 13, RFC 1035), které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server jmen domény je 6. Minimální délka volby pro server jmen domény je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>6</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG514-0</p>	6	n	a1	a2	a3	a4	a1	a2	...
6	n	a1	a2	a3	a4	a1	a2	...			
7	Server protokolu	<p>Volba pro server protokolu obsahuje seznam serverů protokolu podle MIT-LCS UDP, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server protokolu je 7. Minimální délka volby pro server protokolu je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>7</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG515-0</p>	7	n	a1	a2	a3	a4	a1	a2	...
7	n	a1	a2	a3	a4	a1	a2	...			

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis									
8	Server Cookie	<p>Volba pro server cookie obsahuje seznam serverů cookie podle RFC 865, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server cookie je 8. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>8</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG516-0</p>	8	n	a1	a2	a3	a4	a1	a2	...
8	n	a1	a2	a3	a4	a1	a2	...			
9	Server LPR	<p>Volba pro server LPR obsahuje seznam serverů LPR podle RFC 1179, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server LPR je 9. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>9</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG517-0</p>	9	n	a1	a2	a3	a4	a1	a2	...
9	n	a1	a2	a3	a4	a1	a2	...			
10	Server Impress	<p>Volba pro server Impress (Imagen Impress) obsahuje seznam serverů Impress, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server Impress je 10. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>10</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG518-0</p>	10	n	a1	a2	a3	a4	a1	a2	...
10	n	a1	a2	a3	a4	a1	a2	...			
11	Server umístění prostředků	<p>Tato volba obsahuje seznam serverů RLP (Resource Location podle RFC 887), které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 11. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>11</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG519-0</p>	11	n	a1	a2	a3	a4	a1	a2	...
11	n	a1	a2	a3	a4	a1	a2	...			
12	Jméno hostitele	<p>Tato volba obsahuje jméno klienta. Jméno může nebo nemusí být kvalifikováno ve jméně lokální domény (viz část 3.17, která obsahuje informace o preferovaném způsobu získávání jména domény). Informace o omezení znakové sady najdete v RFC 1035.</p> <p>Kód této volby je 12 a její minimální délka je 1.</p> <p>Code Len Host name</p> <table border="1"> <tr> <td>12</td> <td>n</td> <td>h1</td> <td>h2</td> <td>h3</td> <td>h4</td> <td>h5</td> <td>h6</td> <td>...</td> </tr> </table> <p>RZAKG520-0</p>	12	n	h1	h2	h3	h4	h5	h6	...
12	n	h1	h2	h3	h4	h5	h6	...			
13	Velikost zaváděcího souboru	<p>Tato volba uvádí délku předvoleného zaváděcího obrazu klienta (v 512oktetových blocích). Délka souboru je uvedena ve formátu 16bitového celého čísla bez znaménka.</p> <p>Kód této volby je 13 a její délka je 2.</p> <p>Code Len File size</p> <table border="1"> <tr> <td>13</td> <td>2</td> <td>11</td> <td>12</td> </tr> </table> <p>RZAKG541-0</p>	13	2	11	12					
13	2	11	12								

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis							
14	Soubor pro výpis paměti	<p>Tato volba uvádí cestu souboru, do kterého by se měl v případě havárie provádět výpis paměti klienta. Cesta je naformátována jako znakový řetězec obsahující znaky ze znakové sady NVT ASCII.</p> <p>Kód této volby je 14. Její minimální délka je 1.</p> <p>Code Len Dump file pathname</p> <table border="1"> <tr> <td>14</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </table> <p>RZAKG521-0</p>	14	n	n1	n2	n3	n4	...
14	n	n1	n2	n3	n4	...			
15	Jméno domény	<p>Tato volba uvádí jméno domény, které by měl klient používat při zpracování hostitelských jmen prostřednictvím DNS.</p> <p>Kód této volby je 15. Její minimální délka je 1.</p> <p>Code Len Domain name</p> <table border="1"> <tr> <td>15</td> <td>n</td> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>...</td> </tr> </table> <p>RZAKG522-0</p>	15	n	d1	d2	d3	d4	...
15	n	d1	d2	d3	d4	...			
16	Odkládací server	<p>Zde je uvedena IP adresa odkládacího serveru klienta.</p> <p>Kód této volby je 16 a její délka je 4.</p> <p>Code Len Swap server address</p> <table border="1"> <tr> <td>16</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> </tr> </table> <p>RZAKG523-0</p>	16	n	a1	a2	a3	a4	
16	n	a1	a2	a3	a4				
17	Cesta ke kořenovému serveru	<p>Tato volba uvádí název cesty, která obsahuje kořenový disk klienta. Cesta je naformátována jako znakový řetězec obsahující znaky ze znakové sady NVT ASCII.</p> <p>Kód této volby je 17. Její minimální délka je 1.</p> <p>Code Len Root disk pathname</p> <table border="1"> <tr> <td>17</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </table> <p>RZAKG524-0</p>	17	n	n1	n2	n3	n4	...
17	n	n1	n2	n3	n4	...			
18	Cesta k souboru rozšíření	<p>Řetězec, který udává soubor, jež je možné načíst pomocí TFTP a jenž obsahuje informace, které je možné s následujícími výjimkami interpretovat stejně jako 64oktetové pole rozšířené dodavatelem v rámci odezvy BOOTP:</p> <ul style="list-style-type: none"> • Délka souboru není omezená. • všechny odkazy na příznak 18 (tj. instance pole Cesty rozšíření BOOTP) v souboru jsou ignorovány <p>Kód této volby je 18. Její minimální délka je 1.</p> <p>Code Len Extensions pathname</p> <table border="1"> <tr> <td>18</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </table> <p>RZAKG525-0</p>	18	n	n1	n2	n3	n4	...
18	n	n1	n2	n3	n4	...			
19	Směrování pomocí IP	<p>Tato volba uvádí, zda klient může nakonfigurovat svou vrstvu IP pro směrování paketů. Hodnota 0 znamená zakázat směrování IP, hodnota 1 znamená povolit směrování IP.</p> <p>Kód této volby je 19 a její délka je 1.</p> <p>Code Len Value</p> <table border="1"> <tr> <td>19</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG544-0</p>	19	1	0/1				
19	1	0/1							

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis																																					
20	Směrování na nelokální zdrojový systém	<p>Tato volba uvádí, zda klient může nakonfigurovat svou vrstvu IP tak, aby umožňovala směrování datagramů s nelokálními zdrojovými přenosovými cestami. Hodnota 0 znamená zakázat směrování takových datagramů, hodnota 1 znamená povolit směrování.</p> <p>Kód této volby je 20 a její délka je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>20</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG545-0</p>	Code	Len	Value	20	1	0/1																															
Code	Len	Value																																					
20	1	0/1																																					
21	Filtr zásady	<p>Tato volba uvádí filtry zásad pro směrování na nelokální zdrojový systém. Filtry se skládají ze seznamu IP adres a masek, které uvádějí páry cíl/maska, pomocí kterých se mají filtrovat příchozí směrování na zdrojový systém.</p> <p>Každý datagram směrování na zdrojový systém, jehož následná adresa neodpovídá jednomu z filtrů, bude klientem vyřazen.</p> <p>Kód této volby je 21. Minimální délka této volby je 8 a délka musí být vždy násobkem 8.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Address 1</th> <th colspan="4">Mask 1</th> </tr> </thead> <tbody> <tr> <td>21</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="4">Address 2</th> <th colspan="4">Mask 2</th> </tr> </thead> <tbody> <tr> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>m1</td> <td>m2</td> <td>m3</td> <td>m4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG510-0</p>	Code	Len	Address 1				Mask 1				21	n	a1	a2	a3	a4	m1	m2	m3	m4	Address 2				Mask 2				a1	a2	a3	a4	m1	m2	m3	m4	...
Code	Len	Address 1				Mask 1																																	
21	n	a1	a2	a3	a4	m1	m2	m3	m4																														
Address 2				Mask 2																																			
a1	a2	a3	a4	m1	m2	m3	m4	...																															
22	Maximální velikost opětovného skládání datagramu	<p>Tato volba uvádí maximální velikost datagramu, který může klient připravit k opětovnému složení. Velikost je uvedena ve tvaru 16bitového celého čísla bez uvedení znaménka. Minimální přípustná hodnota je 576.</p> <p>Kód této volby je 22 a její délka je 2.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="2">Size</th> </tr> </thead> <tbody> <tr> <td>22</td> <td>2</td> <td>s1</td> <td>s2</td> </tr> </tbody> </table> <p>RZAKG542-0</p>	Code	Len	Size		22	2	s1	s2																													
Code	Len	Size																																					
22	2	s1	s2																																				
23	Předvolená doba platnosti IP	<p>Tato volba uvádí předvolenou dobu platnosti, kterou by měl klient používat u odchozích datagramů. Doba platnosti TTL je uvedena v oktetovém formátu a její hodnota je mezi 1 a 255.</p> <p>Kód této volby je 23 a její délka je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>TTL</th> </tr> </thead> <tbody> <tr> <td>23</td> <td>1</td> <td>ttl</td> </tr> </tbody> </table> <p>RZAKG546-0</p>	Code	Len	TTL	23	1	ttl																															
Code	Len	TTL																																					
23	1	ttl																																					
24	Časový limit stárnutí MTU cesty	<p>Tato volba uvádí časový limit (ve vteřinách), který se používá při stárnutí hodnot MTU cesty zjištěných mechanismem, jenž byl nadefinován ve standardu RFC 1191. Časový limit je uveden ve tvaru 32bitového celého čísla bez uvedení znaménka.</p> <p>Kód této volby je 24 a její délka je 4.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Timeout</th> </tr> </thead> <tbody> <tr> <td>24</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </tbody> </table> <p>RZAKG532-0</p>	Code	Len	Timeout				24	4	t1	t2	t3	t4																									
Code	Len	Timeout																																					
24	4	t1	t2	t3	t4																																		

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis							
25	Tabulka MTU cesty	<p>Tato volba uvádí tabulku velikostí MTU, která se používá při zjišťování MTU cest podle definice ve standardu RFC 1191. Tabulka je naformátována jako seznam 16bitových celých čísel bez uvedení znaménka, seřazených od nejmenšího po největší. Minimální hodnota MTU nesmí být menší než 68.</p> <p>Kód této volby je 25. Její minimální délka je 2 a délka musí být násobkem 2.</p> <p>Code Len Size 1 Size 2</p> <table border="1"> <tr> <td>25</td> <td>n</td> <td>s1</td> <td>s2</td> <td>s1</td> <td>s2</td> <td>...</td> </tr> </table> <p>RZAKG526-0</p>	25	n	s1	s2	s1	s2	...
25	n	s1	s2	s1	s2	...			
26	Rozhraní MTU	<p>Tato volba uvádí MTU, které se má na tomto rozhraní používat. MTU je zadána jako 16bitové celé číslo bez uvedení znaménka. Minimální přípustná hodnota MTU je 68.</p> <p>Kód této volby je 26 a její délka je 2.</p> <p>Code Len MTU</p> <table border="1"> <tr> <td>26</td> <td>2</td> <td>m1</td> <td>m2</td> </tr> </table> <p>RZAKG543-0</p>	26	2	m1	m2			
26	2	m1	m2						
27	Všechny podsítě jsou lokální	<p>Tato volba uvádí, zda klient může předpokládat, že všechny podsítě sítě IP, ke které je klient připojen, používají stejnou MTU jako podsítě té sítě, ke které je klient přímo připojen. Hodnota 1 znamená, že všechny podsítě sdílejí stejnou MTU. Hodnota 0 znamená, že klient by mohl předpokládat, že některé podsítě přímo připojené sítě mohou mít menší MTU.</p> <p>Kód této volby je 27 a její délka je 1.</p> <p>Code Len Value</p> <table border="1"> <tr> <td>27</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG547-0</p>	27	1	0/1				
27	1	0/1							
28	Adresa plošného vysílání	<p>Tato volba uvádí adresu plošného vysílání, která se používá v podsíti klienta. Přípustné hodnoty adres vysílání jsou uvedeny v části 3.2.1.3 standardu RFC 2132.</p> <p>Kód této volby je 28 a její délka je 4.</p> <p>Code Len Broadcast address</p> <table border="1"> <tr> <td>28</td> <td>4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> </tr> </table> <p>RZAKG533-0</p>	28	4	b1	b2	b3	b4	
28	4	b1	b2	b3	b4				
29	Provést vyhledání masky	<p>Tato volba uvádí, zda klient může provádět zjišťování masky podsítě pomocí ICMP. Hodnota 0 znamená, že klient by neměl provádět zjišťování masky. Hodnota 1 znamená, že klient by mohl provádět zjišťování masky.</p> <p>Kód této volby je 29 a její délka je 1.</p> <p>Code Len Value</p> <table border="1"> <tr> <td>29</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG548-0</p>	29	1	0/1				
29	1	0/1							

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis																																					
30	Dodavatel masky	<p>Tato volba uvádí, zda klient může odpovídat na požadavek na masku podsítě pomocí ICMP. Hodnota 0 znamená, že klient by neměl odpovídat. Hodnota 1 znamená, že klient může odpovídat.</p> <p>Kód této volby je 30 a její délka je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>30</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG549-0</p>	Code	Len	Value	30	1	0/1																															
Code	Len	Value																																					
30	1	0/1																																					
31	Provést vyhledání směrovače	<p>Tato volba uvádí, zda klient může vyžadovat směrovače pomocí mechanismu vyhledávání směrovačů nadefinovaným ve standardu RFC 1256. Hodnota 0 znamená, že klient by neměl provádět vyhledávání směrovače. Hodnota 1 znamená, že klient může provádět vyhledávání směrovače.</p> <p>Kód této volby je 31 a její délka je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>31</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG550-0</p>	Code	Len	Value	31	1	0/1																															
Code	Len	Value																																					
31	1	0/1																																					
32	Volba adresy pro vyžádání směrovače	<p>Tato volba uvádí adresu, na kterou by měl klient přenést požadavky na vyžádání směrovače.</p> <p>Kód této volby je 32 a její délka je 4.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Address</th> </tr> </thead> <tbody> <tr> <td>32</td> <td>4</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> </tr> </tbody> </table> <p>RZAKG534-0</p>	Code	Len	Address				32	4	a1	a2	a3	a4																									
Code	Len	Address																																					
32	4	a1	a2	a3	a4																																		
33	Statická přenosová cesta	<p>Tato volba uvádí seznam statických přenosových cest, které by měl klient nainstalovat do své směrovací tabulky. Pokud je uvedeno ke stejnému cíli více přenosových cest, jsou uvedeny v sestupném pořadí priorit.</p> <p>Přenosové cesty se skládají se seznamu párů IP adres. První adresa je cílová adresa a druhá adresa je směrovačem k cíli.</p> <p>Předvolená přenosová cesta (0.0.0.0) je neplatným cílem statické přenosové cesty.</p> <p>Kód této volby je 33. Minimální délka této volby je 8 a délka musí být vždy násobkem 8.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Destination 1</th> <th colspan="4">Router 1</th> </tr> </thead> <tbody> <tr> <td>33</td> <td>n</td> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>r1</td> <td>r2</td> <td>r3</td> <td>r4</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="4">Destination 2</th> <th colspan="4">Router 2</th> </tr> </thead> <tbody> <tr> <td>d1</td> <td>d2</td> <td>d3</td> <td>d4</td> <td>r1</td> <td>r2</td> <td>r3</td> <td>r4</td> <td>...</td> </tr> </tbody> </table> <p>RZAKG509-0</p>	Code	Len	Destination 1				Router 1				33	n	d1	d2	d3	d4	r1	r2	r3	r4	Destination 2				Router 2				d1	d2	d3	d4	r1	r2	r3	r4	...
Code	Len	Destination 1				Router 1																																	
33	n	d1	d2	d3	d4	r1	r2	r3	r4																														
Destination 2				Router 2																																			
d1	d2	d3	d4	r1	r2	r3	r4	...																															
34	Zapouzdření koncového návěští	<p>Tato volba uvádí, zda klient může vyjednávat používání koncového návěští (RFC 893), pokud používá protokol ARP. Hodnota 0 znamená, že klient by se neměl pokoušet používat koncová návěští. Hodnota 1 znamená, že klient se může pokusit používat koncová návěští.</p> <p>Kód této volby je 34 a její délka je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>34</td> <td>1</td> <td>0/1</td> </tr> </tbody> </table> <p>RZAKG573-0</p>	Code	Len	Value	34	1	0/1																															
Code	Len	Value																																					
34	1	0/1																																					

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis						
35	Časový limit paměti cache ARP	<p>Tato volba uvádí časový limit záznamů paměti cache ARP ve vteřinách. Časový limit se uvádí ve tvaru 32bitového celého čísla bez uvedení znaménka.</p> <p>Kód této volby je 35 a její délka je 4.</p> <p>Code Len Time</p> <table border="1"> <tr> <td>35</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </table> <p>RZAKG535-0</p>	35	4	t1	t2	t3	t4
35	4	t1	t2	t3	t4			
36	Zapouzdření Ethernetu	<p>Tato volba uvádí, zda klient může používat zapouzdření Ethernetu verze 2 (RFC 894) nebo IEEE 802.3 (RFC 1042), je-li jeho rozhraním Ethernet. Hodnota 0 znamená, že klient by měl používat zapouzdření podle RFC 894. Hodnota 1 znamená, že klient by měl používat zapouzdření podle RFC 1042.</p> <p>Kód této volby je 36 a její délka je 1.</p> <p>Code Len Value</p> <table border="1"> <tr> <td>36</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG551-0</p>	36	1	0/1			
36	1	0/1						
37	Předvolená doba platnosti pro TCP	<p>Tato volba uvádí předvolenou dobu platnosti (TTL), kterou by měl klient používat při odesílání segmentů TCP. Hodnota je uvedena jako 8bitové celé číslo bez uvedení znaménka. Minimální hodnota je 1.</p> <p>Kód této volby je 37 a její délka je 1.</p> <p>Code Len TTL</p> <table border="1"> <tr> <td>37</td> <td>1</td> <td>n</td> </tr> </table> <p>RZAKG552-0</p>	37	1	n			
37	1	n						
38	Interval trvání platnosti TCP	<p>Tato volba uvádí interval (ve vteřinách), po který by měl klient TCP čekat, než odešle zprávu o trvání platnosti ve spojení TCP. Časový limit se uvádí ve tvaru 32bitového celého čísla bez uvedení znaménka. Hodnota nula znamená, že klient nebude generovat zprávy o trvání platnosti ve spojení, pokud o to nebude výslovně požádán nějakou aplikací.</p> <p>Kód této volby je 38 a její délka je 4.</p> <p>Code Len Time</p> <table border="1"> <tr> <td>38</td> <td>4</td> <td>t1</td> <td>t2</td> <td>t3</td> <td>t4</td> </tr> </table> <p>RZAKG536-0</p>	38	4	t1	t2	t3	t4
38	4	t1	t2	t3	t4			
39	Přebytečný bajt ve zprávě o trvání platnosti TCP	<p>Tato volba uvádí, zda by měl klient odesílat ve zprávě o trvání platnosti TCP přebytečný oktet z důvodů kompatibility se staršími implementacemi. Hodnota 0 znamená, že přebytečný oktet nebude odesílán. Hodnota 1 znamená, že přebytečný oktet by měl být odesílán.</p> <p>Kód této volby je 39 a její délka je 1.</p> <p>Code Len Value</p> <table border="1"> <tr> <td>39</td> <td>1</td> <td>0/1</td> </tr> </table> <p>RZAKG553-0</p>	39	1	0/1			
39	1	0/1						

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis											
40	Doména NIS	<p>Tato volba uvádí jméno domény NIS klienta. Doména je naformátována jako znakový řetězec obsahující znaky ze znakové sady NVT ASCII.</p> <p>Kód této volby je 40. Její minimální délka je 1.</p> <p>Code Len NIS Domain name</p> <table border="1"> <tr> <td>40</td> <td>n</td> <td>n1</td> <td>n2</td> <td>n3</td> <td>n4</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG540-0</p>	40	n	n1	n2	n3	n4	...				
40	n	n1	n2	n3	n4	...							
41	Servery NIS	<p>Tato volba uvádí seznam IP adres, určujících servery NIS, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 41. Její minimální délka je 4 a délka musí být násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>41</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG556-0</p>	41	n	a1	a2	a3	a4	a1	a2	...		
41	n	a1	a2	a3	a4	a1	a2	...					
42	Volba serverů NTP	<p>Tato volba uvádí seznam IP adres, určujících servery NTP, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 42. Její minimální délka je 4 a délka musí být násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>42</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG557-0</p>	42	n	a1	a2	a3	a4	a1	a2	...		
42	n	a1	a2	a3	a4	a1	a2	...					
44	Server jmen NetBIOS přes TCP/IP	<p>Volba NBNS (NetBIOS name server) - server jmen NetBIOS - uvádí seznam serverů jmen NBNS podle standardu RFC 1001/1002, seřazený podle preferencí.</p> <p>Kód této volby je 44. Minimální délka této volby je 4 oktety a její délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>44</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG558-0</p>	44	n	a1	a2	a3	a4	b1	b2	b3	b4	...
44	n	a1	a2	a3	a4	b1	b2	b3	b4	...			
45	Server pro distribuci datagramu NetBIOS přes TCP/IP	<p>Volba NBDD (NetBIOS datagram distribution server) - server pro distribuci datagramu NetBIOS přes TCPIP - uvádí seznam serverů NBDD podle standardu RFC 1001/1002, seřazený podle preferencí.</p> <p>Kód této volby je 45. Minimální délka této volby je 4 oktety a její délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>45</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>b1</td> <td>b2</td> <td>b3</td> <td>b4</td> <td>...</td> </tr> </table> <p style="text-align: right;">RZAKG559-0</p>	45	n	a1	a2	a3	a4	b1	b2	b3	b4	...
45	n	a1	a2	a3	a4	b1	b2	b3	b4	...			

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis																		
46	Typ uzlu NetBIOS přes TCP/IP	<p>Volba Typ uzlu NetBIOS umožňuje, aby konfigurovatelní klienti NetBIOS přes TCP/IP byli nakonfigurováni v souladu s popisem standardu RFC 1001/1002. Hodnota je zadána ve tvaru jednoho oktetu, který určuje typ klienta:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Node type</th> </tr> </thead> <tbody> <tr> <td>0x1</td> <td>B-node</td> </tr> <tr> <td>0x2</td> <td>P-node</td> </tr> <tr> <td>0x4</td> <td>M-node</td> </tr> <tr> <td>0x8</td> <td>H-node</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG554-0</p> <p>Ve výše uvedeném grafu označení '0x' určuje číslo v hexadecimálním formátu (base-16).</p> <p>Kód této volby je 46. Délka této volby je vždy 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th>Node type</th> </tr> </thead> <tbody> <tr> <td>46</td> <td>1</td> <td>see above</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG555-0</p>	Value	Node type	0x1	B-node	0x2	P-node	0x4	M-node	0x8	H-node	Code	Len	Node type	46	1	see above		
Value	Node type																			
0x1	B-node																			
0x2	P-node																			
0x4	M-node																			
0x8	H-node																			
Code	Len	Node type																		
46	1	see above																		
47	Rozsah NetBIOS přes TCP/IP	<p>Volba Rozsah NetBIOS uvádí parametr klienta Rozsah NetBIOS přes TCP/IP, který je uveden ve standardu RFC 1001/1002.</p> <p>Kód této volby je 47. Minimální délka této volby je 1.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="5">NetBIOS scope</th> </tr> </thead> <tbody> <tr> <td>47</td> <td>n</td> <td>s1</td> <td>s2</td> <td>s3</td> <td>s4</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG528-0</p>	Code	Len	NetBIOS scope					47	n	s1	s2	s3	s4	...				
Code	Len	NetBIOS scope																		
47	n	s1	s2	s3	s4	...														
48	Server fontů systému X Window	<p>Tato volba uvádí seznam serverů fontů systému X Window, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 48. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Address 1</th> <th colspan="3">Address 2</th> </tr> </thead> <tbody> <tr> <td>48</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG560-0</p>	Code	Len	Address 1				Address 2			48	n	a1	a2	a3	a4	a1	a2	...
Code	Len	Address 1				Address 2														
48	n	a1	a2	a3	a4	a1	a2	...												
49	Správce obrazovky systému X Window	<p>Tato volba uvádí seznam IP adres systémů, na kterých je spuštěna aplikace správce obrazovky systému X Window a které jsou klientovi k dispozici.</p> <p>Adresy by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 49. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Address 1</th> <th colspan="3">Address 2</th> </tr> </thead> <tbody> <tr> <td>49</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: center;">RZAKG561-0</p>	Code	Len	Address 1				Address 2			49	n	a1	a2	a3	a4	a1	a2	...
Code	Len	Address 1				Address 2														
49	n	a1	a2	a3	a4	a1	a2	...												

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis									
51	Doba pronájmu IP adresy	<p>Tato volba se používá v požadavku klienta (DHCPDISCOVER nebo DHCPREQUEST) a dovoluje klientovi žádat o dobu pronájmu IP adresy. V odpovědi serveru (DHCPOFFER) server DHCP použije tuto volbu ke specifikaci doby pronájmu, kterou hodlá nabídnout.</p> <p>Čas je uveden ve vteřinách a je zadán ve tvaru 32bitového celého čísla bez uvedení znaménka.</p> <p>Kód této volby je 51 a její délka je 4.</p> <p>Code Len Lease time</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">51</td> <td style="text-align: center;">4</td> <td style="text-align: center;">t1</td> <td style="text-align: center;">t2</td> <td style="text-align: center;">t3</td> <td style="text-align: center;">t4</td> </tr> </table> <p style="text-align: right;">RZAKG537-0</p>	51	4	t1	t2	t3	t4			
51	4	t1	t2	t3	t4						
58	Hodnota času obnovy (T1)	<p>Tato volba uvádí časový interval mezi přiřazením adresy a přechodem klienta do stavu RENEWING (OBNOVENÍ).</p> <p>Hodnota je uvedena ve vteřinách a je zadána ve tvaru 32bitového celého čísla bez uvedení znaménka.</p> <p>Kód této volby je 58 a její délka je 4.</p> <p>Code Len T1 Interval</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">58</td> <td style="text-align: center;">4</td> <td style="text-align: center;">t1</td> <td style="text-align: center;">t2</td> <td style="text-align: center;">t3</td> <td style="text-align: center;">t4</td> </tr> </table> <p style="text-align: right;">RZAKG538-0</p>	58	4	t1	t2	t3	t4			
58	4	t1	t2	t3	t4						
59	Volba Hodnota času znovusvázání (T2)	<p>Tato volba uvádí časový interval mezi přiřazením adresy a přechodem klienta do stavu REBINDING (ZNOVUSVÁZÁNÍ).</p> <p>Hodnota je uvedena ve vteřinách a je zadána ve tvaru 32bitového celého čísla bez uvedení znaménka.</p> <p>Kód této volby je 59 a její délka je 4.</p> <p>Code Len T2 Interval</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">59</td> <td style="text-align: center;">4</td> <td style="text-align: center;">t1</td> <td style="text-align: center;">t2</td> <td style="text-align: center;">t3</td> <td style="text-align: center;">t4</td> </tr> </table> <p style="text-align: right;">RZAKG539-0</p>	59	4	t1	t2	t3	t4			
59	4	t1	t2	t3	t4						
62	Jméno domény NetWare/IP	Uvádí jméno domény Netware/IP.									
63	NetWare/IP	Uvádí podvolby NetWare, které potřebujete. Rozsah je 1 až 255. K zadání jména domény NetWare/IP použijte volbu 62.									
64	Jméno domény NIS	<p>Tato volba uvádí jméno domény NIS+ klienta. Doména je naformátována jako znakový řetězec obsahující znaky ze znakové sady NVT ASCII.</p> <p>Kód této volby je 64. Její minimální délka je 1.</p> <p>Code Len NIS Client domain name</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">64</td> <td style="text-align: center;">n</td> <td style="text-align: center;">n1</td> <td style="text-align: center;">n2</td> <td style="text-align: center;">n3</td> <td style="text-align: center;">n4</td> <td style="text-align: center;">...</td> </tr> </table> <p style="text-align: right;">RZAKG527-0</p>	64	n	n1	n2	n3	n4	...		
64	n	n1	n2	n3	n4	...					
65	Servery NIS	<p>Tato volba uvádí seznam IP adres, určujících servery NIS+, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód této volby je 65. Její minimální délka je 4 a délka musí být násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">65</td> <td style="text-align: center;">n</td> <td style="text-align: center;">a1</td> <td style="text-align: center;">a2</td> <td style="text-align: center;">a3</td> <td style="text-align: center;">a4</td> <td style="text-align: center;">a1</td> <td style="text-align: center;">a2</td> <td style="text-align: center;">...</td> </tr> </table> <p style="text-align: right;">RZAKG562-0</p>	65	n	a1	a2	a3	a4	a1	a2	...
65	n	a1	a2	a3	a4	a1	a2	...			

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis									
66	Jméno serveru	<p>Tato volba se používá k identifikaci serveru TFTP, pokud se pole 'sname' v záhlaví DHCP používá pro volby DHCP.</p> <p>Kód této volby je 66 a její minimální délka je 1.</p> <p>Code Len TFTP Server</p> <table border="1"> <tr> <td>66</td> <td>n</td> <td>c1</td> <td>c2</td> <td>c3</td> <td>...</td> </tr> </table> <p>RZAKG571-0</p>	66	n	c1	c2	c3	...			
66	n	c1	c2	c3	...						
67	Jméno zaváděcího souboru	<p>Tato volba se používá k identifikaci zaváděcího souboru, pokud se pole 'file' v záhlaví DHCP používá pro volby DHCP.</p> <p>Kód této volby je 67 a její minimální délka je 1.</p> <p>Code Len Bootfile name</p> <table border="1"> <tr> <td>67</td> <td>n</td> <td>c1</td> <td>c2</td> <td>c3</td> <td>...</td> </tr> </table> <p>RZAKG572-0</p>	67	n	c1	c2	c3	...			
67	n	c1	c2	c3	...						
68	Domovská adresa	<p>Tato volba uvádí seznam IP adres, které určují mobilní domovské IP agenty, které jsou klientovi k dispozici. Agenti by měli být vypsáni v pořadí podle preferencí.</p> <p>Kód této volby je 68. Její minimální délka je 0 (což znamená, že žádní domovští agenti nejsou k dispozici) a délka musí být násobkem 4. Předpokládá se, že obvyklá délka je 4 oktety a obsahuje jednu adresu domovského agenta.</p> <p>Home agent addresses (zero or more)</p> <p>Code Len</p> <table border="1"> <tr> <td>68</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>...</td> </tr> </table> <p>RZAKG529-0</p>	68	n	a1	a2	a3	a4	...		
68	n	a1	a2	a3	a4	...					
69	Servery SMTP	<p>Volba serverů SMTP uvádí seznam serverů SMTP, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server SMTP je 69. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>69</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG563-0</p>	69	n	a1	a2	a3	a4	a1	a2	...
69	n	a1	a2	a3	a4	a1	a2	...			
70	Server POP3	<p>Volba serveru POP3 uvádí seznam serverů POP3, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server POP3 je 70. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>70</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG564-0</p>	70	n	a1	a2	a3	a4	a1	a2	...
70	n	a1	a2	a3	a4	a1	a2	...			

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis									
71	Server NNTP	<p>Volba serveru NNTP uvádí seznam serverů NNTP, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server NNTP je 71. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>71</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG565-0</p>	71	n	a1	a2	a3	a4	a1	a2	...
71	n	a1	a2	a3	a4	a1	a2	...			
72	Server WWW	<p>Volba serveru WWW uvádí seznam serverů WWW, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server WWW je 72. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>72</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG566-0</p>	72	n	a1	a2	a3	a4	a1	a2	...
72	n	a1	a2	a3	a4	a1	a2	...			
73	Server Finger	<p>Volba serveru Finger uvádí seznam serverů Finger, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server Finger je 73. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>73</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG567-0</p>	73	n	a1	a2	a3	a4	a1	a2	...
73	n	a1	a2	a3	a4	a1	a2	...			
74	Server IRC	<p>Volba serveru IRC uvádí seznam serverů IRC, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server IRC je 74. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>74</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG568-0</p>	74	n	a1	a2	a3	a4	a1	a2	...
74	n	a1	a2	a3	a4	a1	a2	...			
75	Server StreetTalk	<p>Volba serverů StreetTalk uvádí seznam serverů StreetTalk, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server StreetTalk je 75. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <p>Code Len Address 1 Address 2</p> <table border="1"> <tr> <td>75</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </table> <p>RZAKG569-0</p>	75	n	a1	a2	a3	a4	a1	a2	...
75	n	a1	a2	a3	a4	a1	a2	...			

Tabulka 1. (pokračování)

Číslo volby	Volba	Popis																		
76	Server STDA	<p>Volba serverů STDA (StreetTalk Directory Assistance) uvádí seznam serverů STDA, které jsou klientovi k dispozici. Servery by měly být vypsány v pořadí podle preferencí.</p> <p>Kód volby pro server StreetTalk Directory Assistance je 76. Minimální délka této volby je 4 oktety a délka musí být vždy násobkem 4.</p> <table border="1"> <thead> <tr> <th>Code</th> <th>Len</th> <th colspan="4">Address 1</th> <th colspan="3">Address 2</th> </tr> </thead> <tbody> <tr> <td>76</td> <td>n</td> <td>a1</td> <td>a2</td> <td>a3</td> <td>a4</td> <td>a1</td> <td>a2</td> <td>...</td> </tr> </tbody> </table> <p style="text-align: right;">RZAKG570-0</p>	Code	Len	Address 1				Address 2			76	n	a1	a2	a3	a4	a1	a2	...
Code	Len	Address 1				Address 2														
76	n	a1	a2	a3	a4	a1	a2	...												
77	Třída uživatele	Uvádí jméno třídy, jejímž členem je hostitelský systém. Tuto třídu jste již dříve museli serveru DHCP definovat během konfigurace serveru DHCP.																		
78	Agent adresáře	Určuje IP adresu agenta adresáře, pokud klienti používají k přenosu zpráv protokol SLP (Service Location Protocol).																		
79	Rozsah služeb	Uvádí rozsah agenta adresáře, který používá pro odpovědi na zprávy vzniklé při zpracování servisních požadavků protokol SLP (Service Location Protocol).																		
80	Oprávnění k pojmenování	Určuje oprávnění k pojmenování agenta adresáře, pokud klienti používají k přenosu zpráv protokol SLP (Service Location Protocol). Tato služba určuje syntaxi schémat, která se používají v URL.																		

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Související informace

<http://www.rfc-editor.org/rfc/rfc2132.txt>

Příklady DHCP

Když si prohlédnete schémata a příklady toho, jak jsou uspořádány různé sítě, budete moci zjistit nejlepší volbu pro svou instalaci.

Sledování toho, jak někdo jiný používá určitou technologii, je často tím nejlepším způsobem, jak se o této technologii dovědět co nejvíce. Následující příklady ukazují, jak DHCP pracuje, jak je včleněn do nastavení jiných sítí, a jak je možné připojit něco z nové funkce V5R4. Je to skvělé místo, kde začít, ať už jste v práci s DHCP začátečníkem, nebo zkušeným administrátorem.

Související pojmy

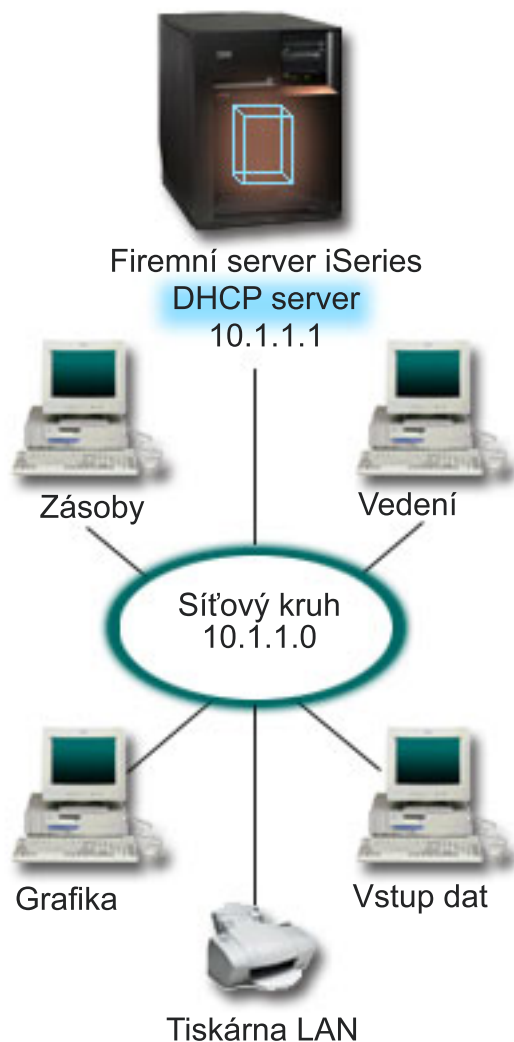
“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Příklad: Jednoduchá podsít DHCP

Zde se dozvíte, jak nastavit server iSeries jako server DHCP v jednoduché síti LAN se čtyřmi PC klienty a tiskárnou na síti LAN.

Následující obrázek ukazuje jednoduchou síť LAN se serverem iSeries, čtyřmi PC klienty a tiskárnou na síti LAN. V tomto případě funguje server iSeries jako server DHCP pro IP podsít 10.1.1.0. Je připojen k síti LAN rozhraním 10.1.1.1.



Obrázek 2. Nastavení jednoduché sítě LAN pro server iSeries

Když je v síti tak málo PC klientů, mohou administrátoři snadno psát staticky informace pro každé PC. V tomto případě musejí navštívit jen čtyři PC. Nyní si představte, že ze čtyř PC je 200 PC. Nastavení IP informací pro každý PC by se stalo zdoluhavou úlohou, která by mohla navíc vést k chybám v přesnosti. DHCP může proces přiřpisování IP informací klientům zjednodušit. I kdyby měla podsít 10.1.1.0 stovky klientů, administrátorovi by stačilo vytvořit na serveru iSeries jednu strategii DHCP. Tato strategie by distribuovala IP informace každému klientovi.

Když budou PC klienti odesílat signály DHCP DISCOVER, server iSeries pošle odpovídající IP informace. V tomto případě má společnost také LAN tiskárnu, která rovněž dostává IP informace od DHCP. Protože však závislost PC klientů na IP adrese tiskárny zůstává stejná, síťový administrátor by to měl vzít v úvahu při vytváření strategie DHCP. Jedním z řešení je přiřadit tiskárně stálou IP adresu. Server DHCP umožňuje definovat klienta DHCP, jako je LAN tiskárna, ve strategii DHCP pomocí MAC adresy. V definici klienta DHCP můžete klientovi přiřadit určité hodnoty, jako jsou IP adresy a adresy směrovačů.

Aby mohl klient komunikovat se sítí TCP/IP, musí mít alespoň IP adresu a masku podsítě. Klienti obdrží IP adresu od serveru DHCP a server DHCP pošle pomocí voleb konfigurace další informace o konfiguraci (například masku podsítě).

Plánování nastavení DHCP pro jednoduchou síť LAN

Tabulka 2. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt	Hodnota
Volby konfigurace volba 1: Masky podsítě volba 6: Server DNS volba 15: Jméno domény	255.255.255.0 10.1.1.1 mycompany.com
Adresy podsítě nejsou přiřazeny serverem	10.1.1.1 (Server jmen domény)
Provádí server aktualizace DNS?	Ne
Podporuje server klienty BOOTP?	Ne

Tabulka 3. Podsítě pro PC

Objekt	Hodnota
Jméno podsítě	SimpleSubnet
Spravované adresy	10.1.1.2 - 10.1.1.150
Doba pronájmu	24 hodin (předvolená)
Volby konfigurace	Volby z globální konfigurace
Zděděné volby	

Tabulka 4. Klient pro tiskárnu

Objekt	Hodnota
Jméno klienta	LANPrinter
Adresa klienta	10.1.1.5
Volby konfigurace	Volby z globální konfigurace
Zděděné volby	

Související odkazy

“Příklad: Vícenásobné podsítě TCP/IP”

Zde se dozvíte, jak nastavit server iSeries jako server DHCP se dvěma sítěmi LAN připojenými směrovačem s povoleným DHCP.

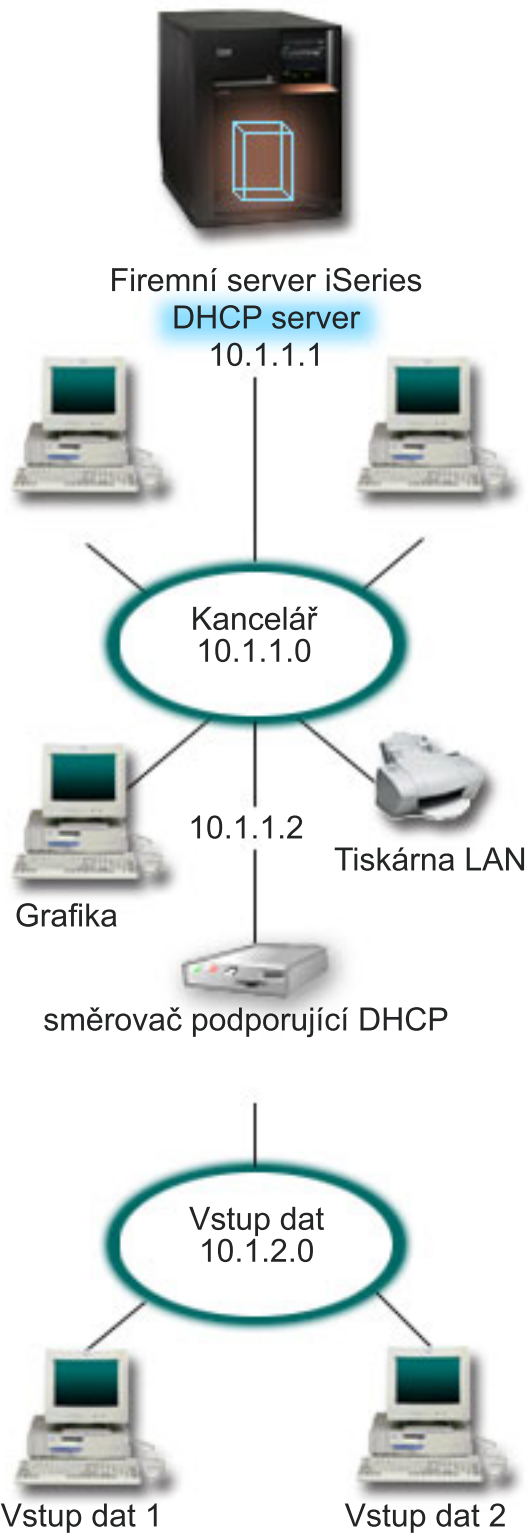
“Příklad: DHCP a multihoming” na stránce 25

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN, která je připojena k Internetu pomocí internetového směrovače.

Příklad: Vícenásobné podsítě TCP/IP

Zde se dozvíte, jak nastavit server iSeries jako server DHCP se dvěma sítěmi LAN připojenými směrovačem s povoleným DHCP.

Tento příklad je podobný předchozímu příkladu jednoduché podsítě DHCP s výjimkou toho, že nyní již existuje další podsítě TCP/IP. Předpokládáme, že klienti Office a klienti Data Entry jsou na různých podlažích budovy a jsou odděleni směrovačem. Když administrátor chce, aby všichni klienti dostali IP informace prostřednictvím DHCP, musí řešit některé otázky, které se liší od otázek jednoduché podsítě DHCP. Následující obrázek ukazuje příklad uspořádání sítě se serverem iSeries DHCP připojeným ke dvěma sítím LAN, které používají mezi sítěmi směrovač. Na obrázku je v zájmu přehlednosti omezený počet klientů. Ve skutečném prostředí by bylo v podsíti klientů daleko víc.



Obrázek 3. Vícenásobné sítě LAN spojené prostřednictvím směrovače

Směrovač, který spojuje obě sítě, musí být schopen přenášet pakety DHCP DISCOVER. Pokud toho není schopen, nebudou klienti Data Entry moci obdržet IP informace a vstupovat do sítě. Ve strategii DHCP je také potřeba mít dvě

definice podsítě - jednu pro podsít Data Entry a jednu pro podsít Office. Podsítě se budou lišit minimálně ve svých IP adresách a adresách směrovače. Podsít Data Entry musí při komunikaci s podsítí Office obdržet adresu směrovače 10.1.2.2.

Plánování nastavení DHCP pro více sítí LAN

Tabulka 5. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt		Hodnota
Volby konfigurace	volba 1: Maska podsítě	255.255.255.0
	volba 6: Server DNS	10.1.1.1
	volba 15: Jméno domény	mycompany.com
Adresy podsítě nejsou přiřazeny serverem		10.1.1.1 (Server jmen domény)
Provádí server aktualizace DNS?		Ne
Podporuje server klienty BOOTP?		Ne

Tabulka 6. Podsít pro klienty Office

Objekt		Hodnota
Jméno podsítě		Office
Spravované adresy		10.1.1.3 - 10.1.1.150
Doba pronájmu		24 hodin (předvolená)
Volby konfigurace	volba 3: Směrovač	10.1.1.2
	Zděděné volby	Volby z globální konfigurace
Adresy podsítě nejsou přiřazeny serverem		10.1.1.2 (Směrovač)

Tabulka 7. Podsít pro klienty Data Entry

Objekt		Hodnota
Jméno podsítě		DataEntry
Spravované adresy		10.1.2.3 - 10.1.2.150
Doba pronájmu		24 hodin (předvolená)
Volby konfigurace	volba 3: Směrovač	10.1.2.2
	Zděděné volby	Volby z globální konfigurace
Adresy podsítě nejsou přiřazeny serverem		10.1.2.2 (Směrovač)

Související odkazy

“Příklad: Jednoduchá podsít DHCP” na stránce 21

Zde se dozvíte, jak nastavit server iSeries jako server DHCP v jednoduché síti LAN se čtyřmi PC klienty a tiskárnou na síti LAN.

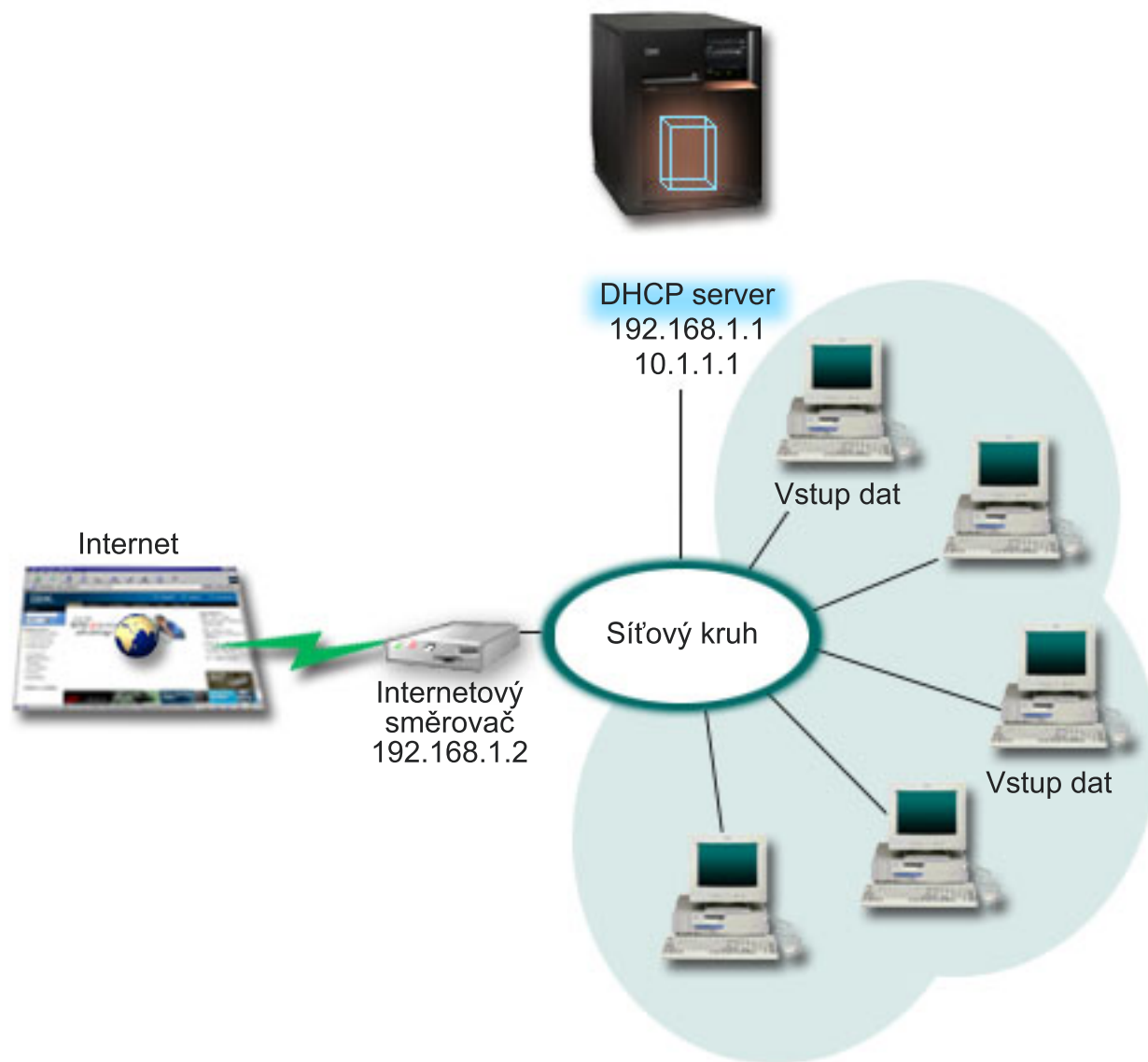
Příklad: DHCP a multihoming

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN, která je připojena k Internetu pomocí internetového směrovače.

Tento příklad se velmi podobá prvnímu příkladu jednoduché podsítě DHCP. V tomto příkladu klienti Data Entry komunikují pouze mezi sebou a serverem iSeries. Získávají IP informace dynamicky od serveru iSeries DHCP.

Nová verze aplikace Data Entry však vyžaduje, aby síť komunikovala s Internetem, a společnost se proto rozhodla poskytovat přístup k Internetu prostřednictvím internetového směrovače, jak je zobrazeno na obrázku 4-1. Kromě

směrovače přidal administrátor také další rozhraní s IP adresou kvůli komunikaci s Internetem. Když je ke stejnému adaptéru přiřazeno více IP adres, jedná se o server iSeries připojený k více sítím (multihoming).



Obrázek 4. Použití DHCP s několika IP adresami přiřazenými ke stejnému adaptéru

Poznámka: Přestože je tento způsob připojení k Internetu možný, není nejbezpečnější. Vyhovuje účelům tohoto příkladu DHCP, ale při konfiguraci vlastního serveru byste měli vzít v úvahu také otázky zabezpečení.

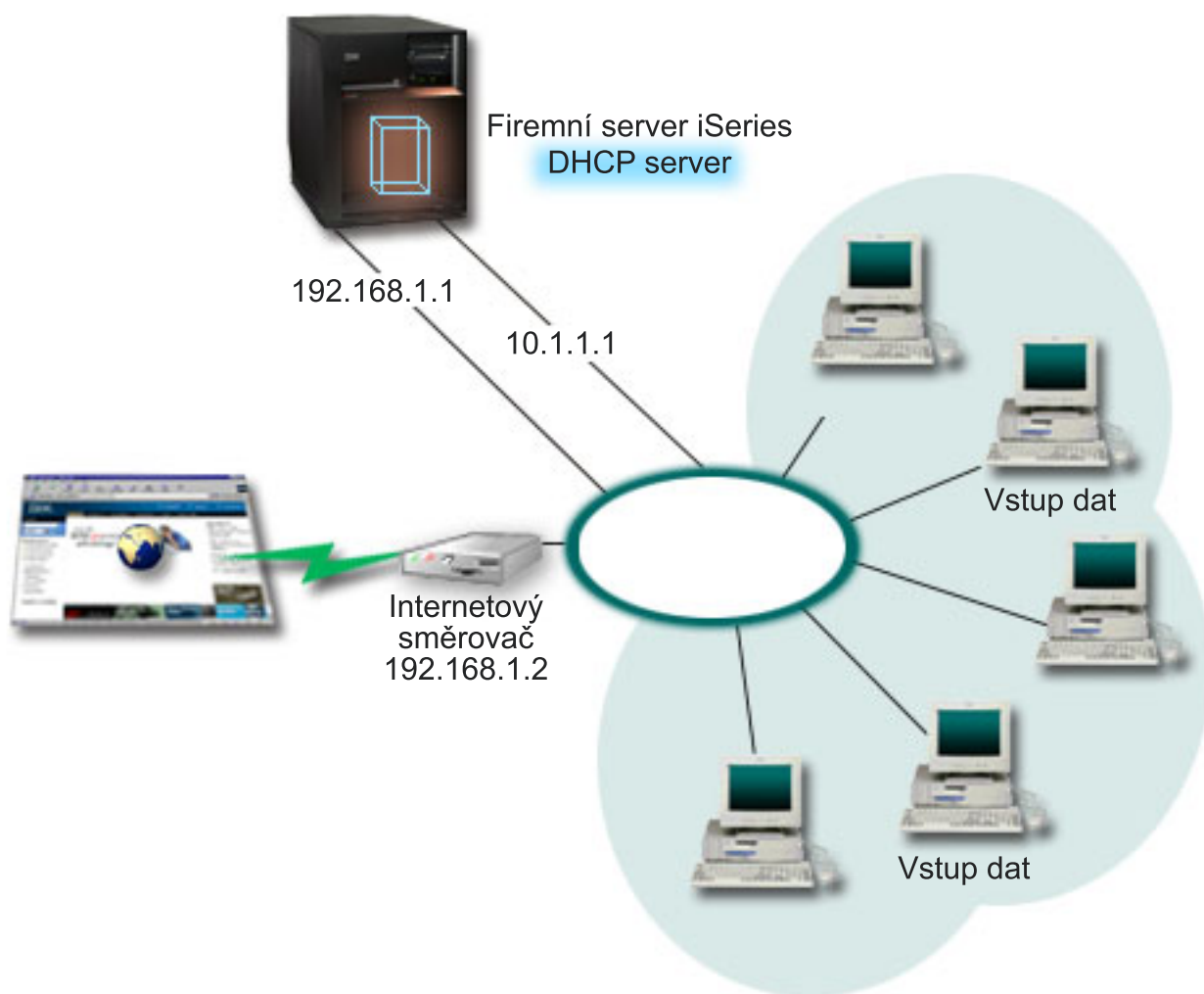
Při nastavení DHCP je třeba také počítat s tím, že server iSeries je rozpoznatelný podle dvou různých IP adres. Abyste pochopili, jak nastavit DHCP správně pro tento případ, je třeba pochopit, co se děje, když klient odesílá paket DHCP DISCOVER.

Když klient odešle paket DHCP DISCOVER, je paket vyslán do okruhu. Server iSeries proto nemůže stanovit, pro které IP adresy byl paket určen. Pokud by byl tento paket označen IP rozhraním 10.1.1.1 (používaným pro DHCP), klienti obdrží IP informace podle předpokladu. Je ale možné, že paket byl označen adresou 192.168.1.1 (připojenou k Internetu). Pokud by paket byl přijat na rozhraní 192.168.1.1, klient Data Entry by nedostal žádné IP informace.

Při nastavování DHCP v této situaci musíte vytvořit nejen podsít DHCP Data Entry, ale také jednu podsít pro Internet. Internetová strategie se skládá z podsít bez dostupných adres. Nejjednodušším způsobem je definovat podsít alespoň s jednou IP adresou (například 192.168.1.1) a potom tuto IP adresu vyjmout. Když máte definovány dvě podsítě, spojíte nyní obě podsítě (nebo více podsítí) do skupiny podsítí. Pokud je paket DISCOVER označen rozhraním 192.168.1.1, podsít Data Entry bude stále vydávat platné IP informace.

Aby tento scénář fungoval, musí strategie pro podsít Data Entry poslat klientům adresu směrovače, aby měli přístup k Internetu. V tomto případě je adresa směrovače rozhraním iSeries 10.1.1.1. Pro obě rozhraní musíte také nastavit volbu Postoupit datagram pomocí IP na "zapnuto", aby si mohla určovat cestu pro sebe navzájem. Tento příklad využívá při označování jak interních, tak externích IP adres vyhrazené IP adresy. Pokud se na vaši síť hodí tento scénář, budete muset pro klienty Data Entry použít také NAT, aby mohli tito klienti komunikovat s Internetem.

Použití skupin podsítí při problému s označováním není omezeno jen na příklady týkající se vícenásobného připojení. S tímto problémem se můžete setkat vždy, když se vícenásobná rozhraní připojují ke stejné síti. Obrázek ukazuje, jak může mít server iSeries dvě fyzická připojení k síti Data Entry. Konfigurace této sítě vyžaduje podobnou strategii DHCP skupin jako nastavení týkající se vícenásobného připojení, protože pakety DHCP DISCOVER mohou obdržet odpověď od rozhraní 192.168.1.1.



Obrázek 5. Použití DHCP s několika rozhraními připojenými ke stejné síti

Plánování nastavení DHCP pro multihoming

Tabulka 8. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt	Hodnota
Provádí server aktualizace DNS?	Ne
Podporuje server klienty BOOTP?	Ne

Tabulka 9. Podsítě pro klienty Data Entry

Objekt	Hodnota	
Jméno podsítě	Data Entry	
Spravované adresy	10.1.1.2 - 10.1.1.150	
Doba pronájmu	24 hodin (předvolená)	
Volby konfigurace	volba 1: Maska podsítě	255.255.255.0
	volba 3: Směrovač	10.1.1.1
	volba 6: Server DNS	10.1.1.1
	volba 15: Jméno domény	mycompany.com
Adresy podsítě nejsou přiřazeny serverem	10.1.1.1 (Směrovač, server DNS)	

Tabulka 10. Podsítě pro klienty Internetu (prázdná podsítě)

Objekt	Hodnota
Jméno podsítě	Internet
Spravované adresy	192.168.1.1 - 192.168.1.1
Adresy podsítě nejsou přiřazeny serverem	192.168.1.1 (Všechny dostupné IP adresy)

Tabulka 11. Skupina podsítí pro všechny příchozí pakety DISCOVER

Objekt	Hodnota
Jméno skupiny podsítí	Multihomed
Podsítě zahrnuté ve skupině	Podsítě Internet Podsítě DataEntry

Další nastavení

- Nastavit volbu Postoupit datagram pomocí IP na "zapnuto" pro obě rozhraní.
- Nastavit NAT pro klienty Data Entry.

Související pojmy

“Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci” na stránce 47

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

Související odkazy

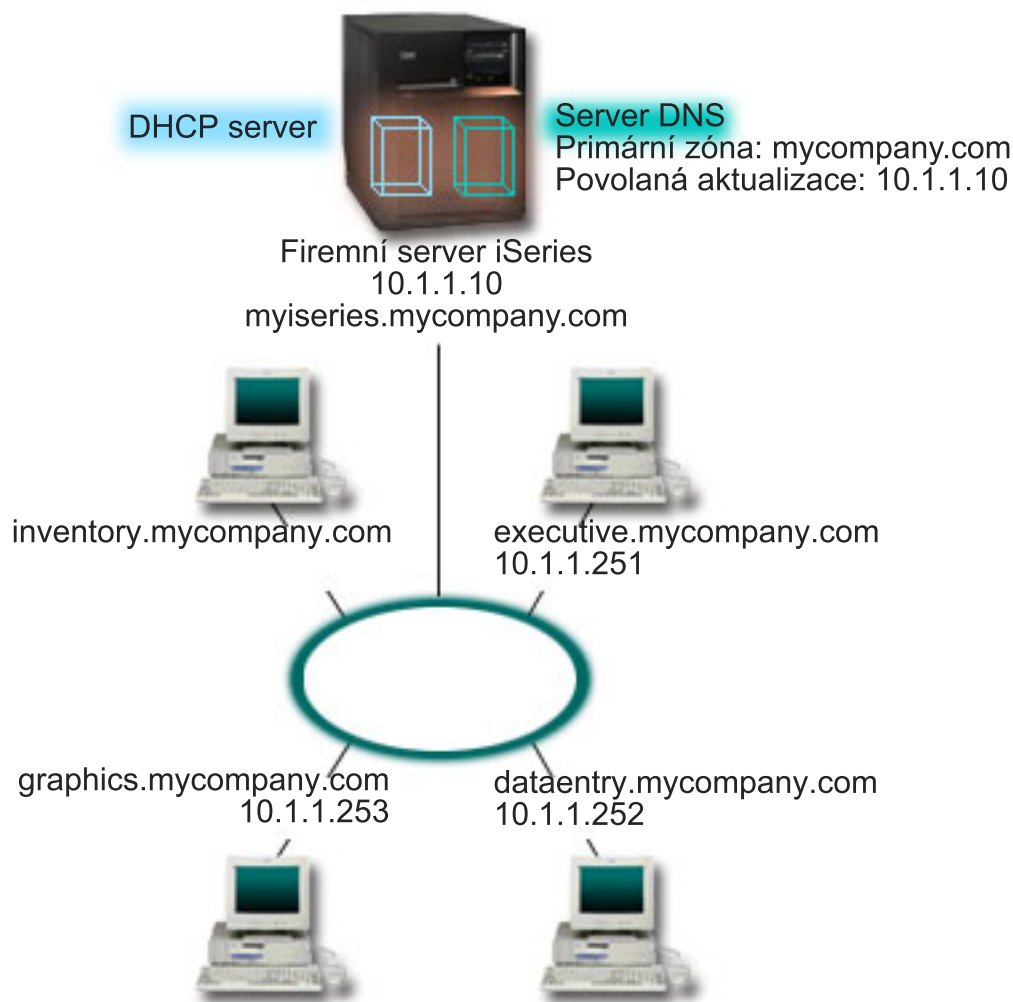
“Příklad: Jednoduchá podsítě DHCP” na stránce 21

Zde se dozvíte, jak nastavit server iSeries jako server DHCP v jednoduché síti LAN se čtyřmi PC klienty a tiskárnou na síti LAN.

Příklad: DNS a DHCP na stejném serveru iSeries

Zde se dozvíte, jak nastavit server iSeries jako server DHCP s dynamickými aktualizacemi DNS pro jednoduchou síť LAN.

Obrázek 6 ukazuje, jak může server iSeries pracovat pro jednoduchou podsíť jako server DHCP a DNS. Předpokládáme, že v tomto pracovním prostředí vytvářejí inventární klienti, klienti Data Entry a aktivní klienti dokumenty obsahující grafiku z grafického souborového serveru. Připojují se ke grafickému souborovému serveru pomocí síťové jednotky k jeho jménu hostitele.



Obrázek 6. Dynamický server DNS a DHCP

Předchozí verze DHCP a DNS byly na sobě nezávislé. Když server DHCP přiřadil klientovi novou IP adresu, musel administrátor ručně aktualizovat záznamy DNS. Kdyby se v tomto případě změnila IP adresa grafického souborového serveru, protože by byla přiřazena serverem DHCP, potom by závislí klienti nemohli mapovat síťovou jednotku na hostitelské jméno, protože záznamy DNS by obsahovaly předchozí IP adresu souborového serveru.

U nového serveru DNS dodávaného ve verzi V5R1 můžete dynamicky aktualizovat záznamy DNS společně s tím, jak se v DHCP mění adresa. Když například grafický souborový server obnoví pronájem a server DHCP mu přiřadí IP adresu 10.1.1.250, přiřazené záznamy DNS se aktualizují dynamicky. To umožní ostatním klientům dotazovat se serveru DNS na grafický souborový server podle hostitelského jména bez přerušení.

Můžete konfigurovat DHCP tak, aby aktualizoval zdrojové záznamy v záznamech (A) a záznamech PTR namísto klienta. Záznam A mapuje klientovo hostitelské jméno na IP adresu. Záznam PTR mapuje klientovu IP adresu na hostitelské jméno. U každého záznamu, který je dynamicky aktualizován, bude napsán přiřazený záznam TXT uvádějící, že záznam byl zapsán serverem DHCP. Můžete si vybrat, zda má DHCP aktualizovat záznamy A i PTR nebo

pouze záznamy PTR. Více informací o konfiguraci serveru DNS, aby přijímal dynamické aktualizace, najdete pod tématem Příklad: DNS a DHCP na stejném serveru iSeries v tématu DNS.

Poznámka: Pokud nastavíte DHCP tak, aby aktualizoval pouze záznamy PTR, musíte konfigurovat DNS a umožnit klientům aktualizaci, aby každý klient mohl aktualizovat svůj záznam A. Ne všichni klienti DHCP podporují vytváření vlastních požadavků na aktualizaci záznamu typu A. Před tím, než zvolíte tuto metodu, prostudujte si dokumentaci pro platformu klienta.

Pokud chcete umožnit aktualizace DNS, musíte pro server DHCP vytvořit klíč DNS. Klíč DNS poskytuje oprávnění serveru DHCP k aktualizaci záznamů DNS vycházející z IP adresy, kterou distribuoval. Potom v konfiguraci serveru DHCP zvolte úroveň, kde se mají aktualizace DNS provádět. Pokud například chcete, aby aktualizace DNS prováděly všechny podsítě, nastavte aktualizace na globální úrovni. Pokud chcete, aby aktualizace prováděla pouze jedna podsít, potom nastavte pro aktualizaci jen tuto podsít.

Plánování nastavení DHCP při použití dynamického DNS

Tabulka 12. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt	Hodnota	
Volby konfigurace	volba 1: Maska podsítě	255.255.255.0
	volba 6: Server DNS	10.1.1.10
	volba 15: Jméno domény	mycompany.com
Provádí server aktualizace DNS?	Ano -- záznamy A i PTR	
Podporuje server klienty BOOTP?	Ne	

Tabulka 13. Podsít pro síťový kruh

Objekt	Hodnota	
Jméno podsítě	NetworkSubnet	
Spravované adresy	10.1.1.250 - 10.1.1.254	
Doba pronájmu	24 hodin (předvolená)	
Volby konfigurace	Zděděné volby	Volby z globální konfigurace

Další nastavení:

Poskytnout DHCP oprávnění k odesílání aktualizací na server DNS. Viz Příklad: DNS a DHCP na stejném serveru iSeries v tématu DNS.

Související odkazy

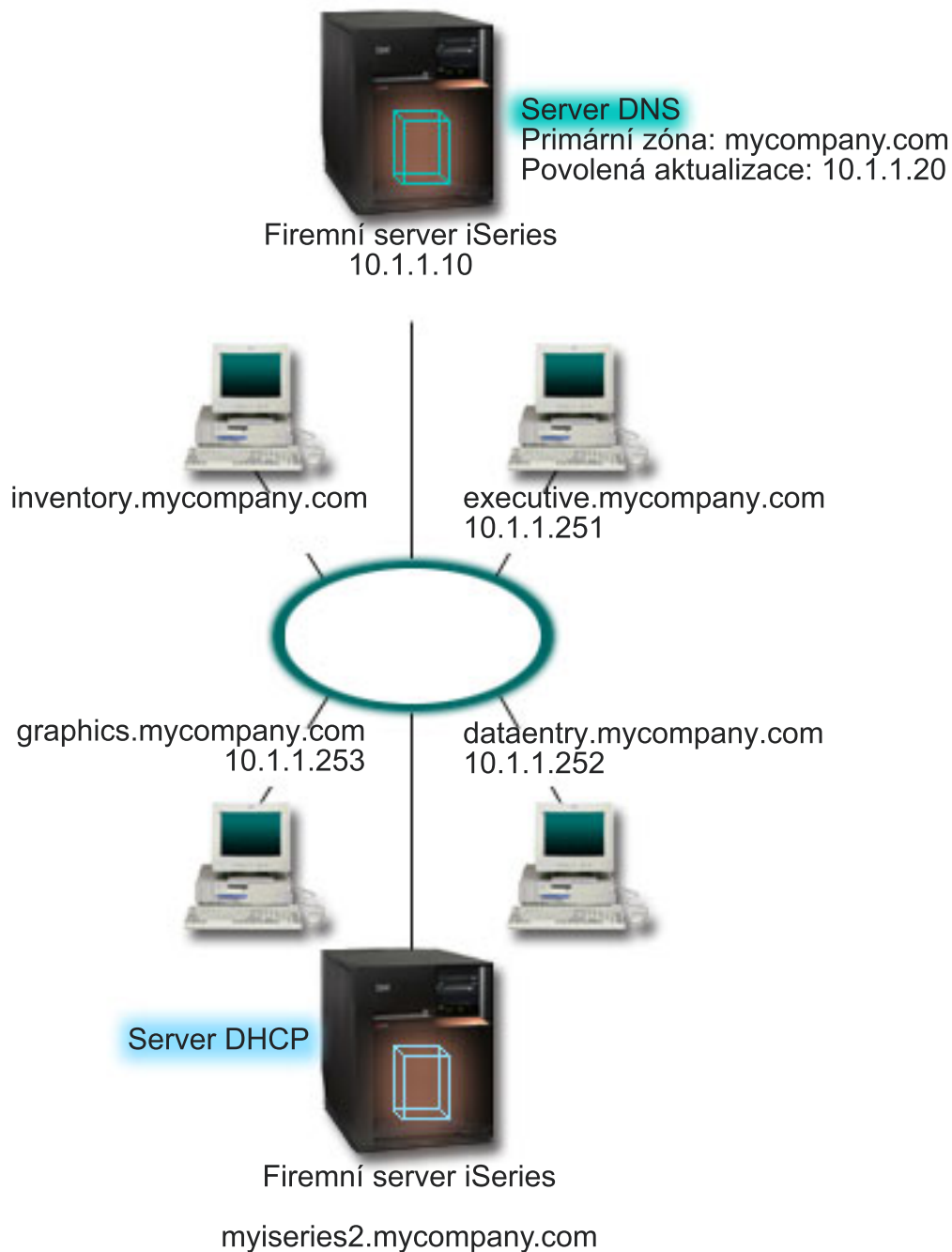
“Příklad: DNS a DHCP na různých serverech iSeries”

Zde se dozvíte, jak nastavit DHCP a DNS na různých serverech iSeries, aby bylo možné provádět dynamické aktualizace po jednoduché síti LAN.

Příklad: DNS a DHCP na různých serverech iSeries

Zde se dozvíte, jak nastavit DHCP a DNS na různých serverech iSeries, aby bylo možné provádět dynamické aktualizace po jednoduché síti LAN.

Obrázek ukazuje malou podsít s DNS a DHCP spuštěnou na různých serverech iSeries. Server iSeries, na kterém je spuštěn DNS, bude konfigurován stejným způsobem, jako když byly DNS a DHCP na stejném serveru iSeries. Je však třeba provést několik dalších kroků a konfigurovat server DHCP tak, aby odesílal dynamické aktualizace.



Obrázek 7. DNS a DHCP na různých serverech iSeries

Plánování nastavení DHCP při použití dynamického DNS

Příklady globálních voleb konfigurace a nastavení podsítě naleznete v "Příklad: DNS a DHCP na stejném serveru iSeries" na stránce 28.

Další nastavení:

Instalace i5/OS (volba 31) (Domain Name System)

Nainstalujte i5/OS (volba 31) na server iSeries, na kterém bude provozován DHCP, v tomto případě myiseries2. Tato volba obsahuje dynamickou aktualizaci API, která řídí proces aktualizace zdrojového záznamu. Pokyny pro instalaci najdete pod tématem Systémové požadavky DNS.

Autorizace DHCP, aby odesílal aktualizace na server DNS

Musíte udělit oprávnění serveru DHCP, aby odesílal aktualizace do serveru DNS. Můžete buď opakovat proces definice klíče dynamické aktualizace (Dynamic Update Key), nebo můžete soubor odeslat a umístit ho do správné cesty k adresáři.

Pokud chcete vytvořit klíč dynamické aktualizace na obou serverech iSeries, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries** → **Síť** → **Servery** → **DNS**.
2. V levém podokně klepněte pravým tlačítkem myši na **DNS** a vyberte **Správa klíčů dynamické aktualizace...**
3. Na stránce **Správa klíčů dynamické aktualizace** vyberte **Přidat...**
4. Na stránce **Přidat klíč dynamické aktualizace** vyplňte tato pole:
 - **Jméno klíče:** Zadejte jméno klíče, například `mycompany.key`. Jméno klíče musí být ukončeno tečkou.
 - **Zóny dynamické aktualizace:** Zadejte jména zón, pro které bude tento klíč platný. Můžete zadat více zón.
 - **Generovat klíč:** Vyberte metodu, kterou chcete použít při vytvoření tajného klíče.
5. Opakujte výše uvedené kroky, aby byl stejný klíč definován jak na serveru iSeries s DNS a serveru iSeries s DHCP.

Související úlohy

Systémové požadavky DNS

Související odkazy

“Příklad: DNS a DHCP na stejném serveru iSeries” na stránce 28

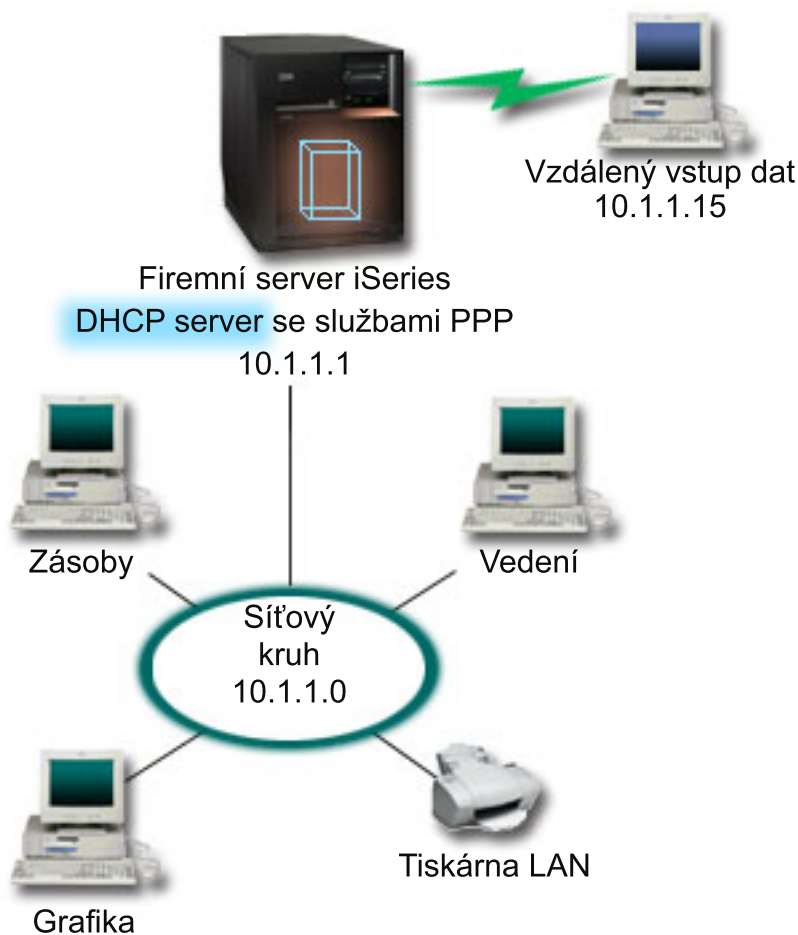
Zde se dozvíte, jak nastavit server iSeries jako server DHCP s dynamickými aktualizacemi DNS pro jednoduchou síť LAN.

API dynamické aktualizace

Příklad: PPP a DHCP na jednom serveru iSeries

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN a vzdáleného klienta připojeného přes komutovanou linku.

Vzdálení klienti, jako například klienti s připojením přes komutovanou linku, často požadují přístup do sítě společnosti. Klienti s připojením přes komutovanou linku mohou získat přístup do serveru iSeries s PPP. Aby měl takový klient přístup k síti, potřebuje stejné IP informace jako jakýkoliv klient s přímým připojením. Server iSeries DHCP může distribuovat informace o IP adrese tomuto klientovi PPP s připojením přes komutovanou linku, stejně jako jakémukoliv jinému klientovi s přímým připojením. Obrázek ukazuje vzdáleného zaměstnance, který se potřebuje připojit k síti společnosti, aby provedl nějakou práci.



Obrázek 8. PPP a DHCP na jednom serveru iSeries

Aby se vzdálený zaměstnanec úspěšně připojil k síti společnosti, musí server iSeries použít kombinaci služeb RAS (Remote Access Services) a DHCP. Funkce RAS umožní serveru iSeries připojit klienta s připojením přes komutovanou linku. Pokud je server PPP správně nastaven, sdělí serveru DHCP v okamžiku, kdy pracovník vytvoří spojení přes komutovanou linku, aby distribuoval zaměstnanci TCP/IP informace.

V tomto příkladu pokryje zásada jedné podsítě DHCP jak klienty připojující se k síti přímo, tak klienty připojující se přes komutovanou linku.

Pokud chcete, aby váš profil PPP byl odložen na DHCP za účelem distribuce IP, musíte tak učinit v profilu PPP. V nastavení TCP/IP v profilu připojení příjemce musíte nastavit metodu přiřazování vzdálených IP adres z "Pevná" na "DHCP". Aby klienti s připojením přes komutovanou linku mohli komunikovat s ostatními síťovými klienty, jako například s tiskárnou LAN, musíte rovněž umožnit přesměrování IP v nastavení TCP/IP profilu a ve vlastnostech konfigurace TCP/IP (zásobníku). Pokud nastavíte přesměrování IP pouze v profilu PPP, server iSeries nepřesměruje IP pakety. Musíte nastavit směrování IP v profilu i v zásobníku.

IP adresa lokálního rozhraní v profilu PPP musí být IP adresou, která spadá pod definici podsítě na serveru DHCP. V tomto případě je adresa profilu PPP lokálního rozhraní 10.1.1.1. Tato adresa by měla být vyjmuta ze společné oblasti adres serveru DHCP, aby nebyla přiřazena klientovi DHCP.

Plánování nastavení DHCP pro klienty s přímým připojením a PPP klienty

Tabulka 14. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt	Hodnota	
Volby konfigurace	volba 1: Maska podsítě	255.255.255.0
	volba 6: Server DNS	10.1.1.1
	volba 15: Jméno domény	mycompany.com
Provádí server aktualizace DNS?	Ne	
Podporuje server klienty BOOTP?	Ne	

Tabulka 15. Podsít pro klienty s přímým připojením a klienty s připojením přes komutovanou linku

Objekt	Hodnota
Jméno podsítě	MainNetwork
Spravované adresy	10.1.1.3 - 10.1.1.150
Doba pronájmu	24 hodin (předvolená)
Volby konfigurace	Zděděné volby Volby z globální konfigurace
Adresy podsítě nejsou přiřazeny serverem	10.1.1.1 (Adresa lokálního rozhraní specifikována v Nastavení TCP/IP ve vlastnostech Profilu připojení příjemců v rámci produktu iSeries Navigator)

Další nastavení

- Nastavte metodu vzdálené IP adresy v profilu připojení příjemců PPP na DHCP.
 1. Aktivujte připojení klienta DHCP WAN k serveru DHCP nebo připojení pro přenos rámce. To učiníte pomocí položky menu Služby pro služby RAS (Remote Access Services) v rámci produktu iSeries Navigator.
 2. V prostředí produktu iSeries Navigator vyberte volbu Profil připojení příjemců, Nastavení TCP/IP - Vlastnosti a pro metodu přiřazení IP adres vyberte Použít DHCP.
- V prostředí produktu iSeries Navigator vyberte volbu Profil připojení příjemců, Nastavení TCP/IP - Vlastnosti a povolte vzdálenému systému přístup k jiným sítím (směrování pomocí IP).
- V prostředí produktu iSeries Navigator vyberte volbu Konfigurace TCP/IP a v nastavení vlastností TCP/IP vyberte volbu Postoupit datagram pomocí IP.

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Související odkazy

“Příklad: Profil DHCP a PPP na různých serverech iSeries”

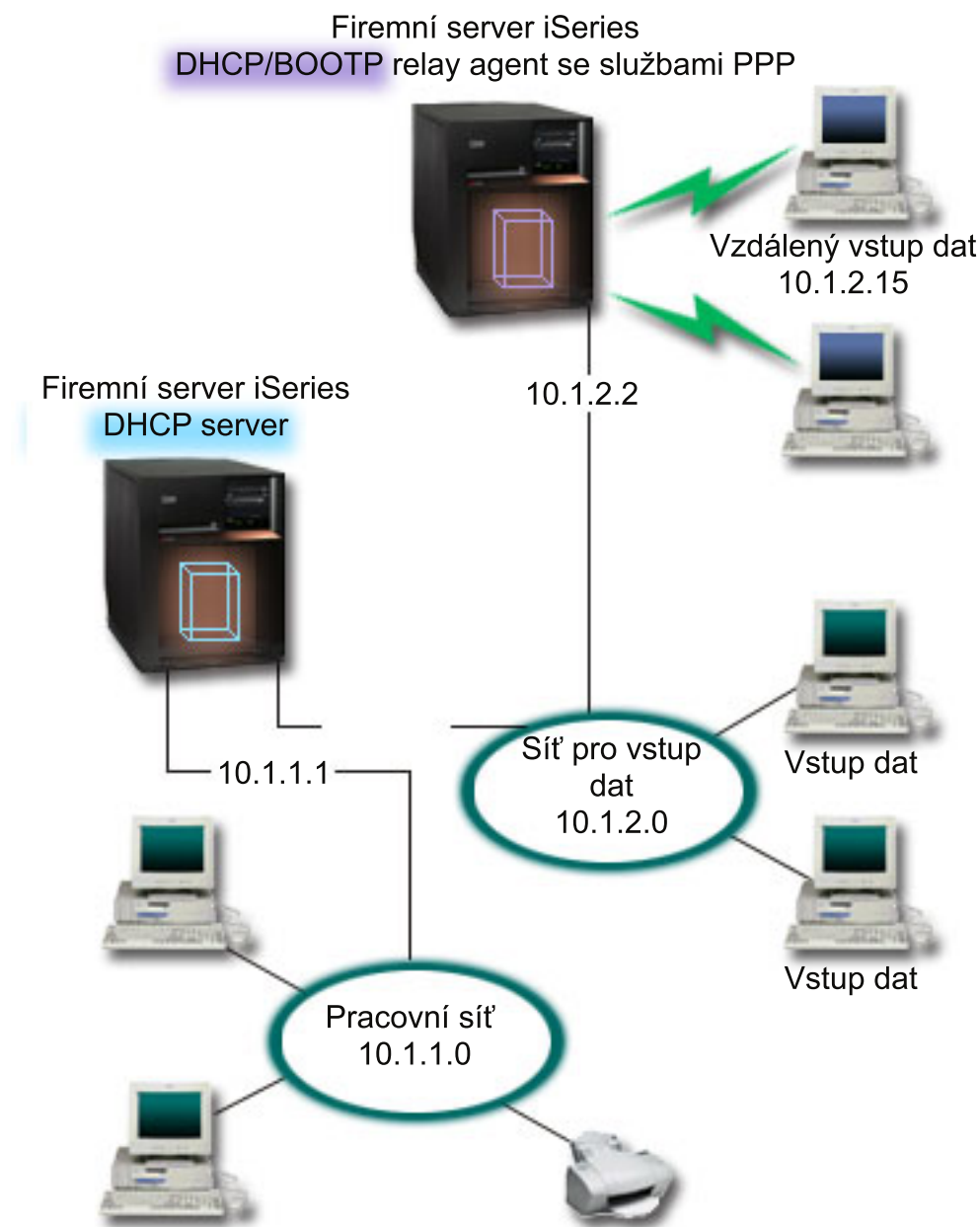
Zde se dozvíte, jak nastavit dva servery iSeries jako síťový server DHCP a agenta přenosu DHCP/BOOTP pro dvě sítě LAN a vzdálené klienty připojené přes komutovanou linku.

Příklad: Profil DHCP a PPP na různých serverech iSeries

Zde se dozvíte, jak nastavit dva servery iSeries jako síťový server DHCP a agenta přenosu DHCP/BOOTP pro dvě sítě LAN a vzdálené klienty připojené přes komutovanou linku.

Předchozí příklad PPP a DHCP na jednom serveru iSeries ukázal, jak použít PPP a DHCP na jednom serveru iSeries, aby se klienti s připojením přes komutovanou linku mohli připojit k síti. Ať už se jedná o fyzické uspořádání sítě nebo otázky bezpečnosti, mohlo by být vhodnější mít servery PPP a DHCP odděleny nebo mít vyhrazený PPP server bez

služeb PPP. Obrázek představuje síť, která má klienty s připojením přes komutovanou linku, ale zásady PPP a DHCP jsou na různých serverech.



Obrázek 9. Profil DHCP a PPP na různých serverech iSeries

Vzdálení klienti Data Entry se připojují k serveru iSeries PPP. Profil PPP na tomto serveru musí mít aktivní jak metodu vzdálené IP adresy "DHCP", jako tomu bylo v předchozím příkladu, tak funkci Směrování pomocí IP v profilu PPP a ve vlastnostech zásobníku TCP/IP. Vzhledem k tomu, že se tento server chová jako agent přenosu DHCP, musí být navíc spuštěn server BOOTP/DHCP relay agent TCP/IP. To umožní serveru iSeries Remote Access předat pakety DHCP DISCOVER serveru DHCP. Server DHCP potom odpoví a doručí klientovi s připojením přes komutovanou linku prostřednictvím serveru PPP informace TCP/IP.

Server DHCP je odpovědný za distribuci IP adres v síti 10.1.1.0 i v síti 10.1.2.0. V síti Data Entry vydá IP adresy od 10.1.2.10 do 10.1.2.40 klientovi s připojením přes komutovanou linku nebo klientovi s přímým připojením k síti.

Klienti Data Entry potřebují také adresu směrovače (volba 3) 10.1.2.1, aby mohli komunikovat s pracovní sítí (Work network), a server iSeries DHCP musí podporovat směrování pomocí IP.

IP adresa lokálního rozhraní v profilu PPP musí být IP adresou, která spadá pod definici podsítě na serveru DHCP. V tomto případě by byla adresa profilu PPP lokálního rozhraní 10.1.2.2. Tato adresa by měla být vyjmuta ze společné oblasti adres serveru DHCP, aby nebyla přiřazena klientovi DHCP. IP adresa lokálního rozhraní musí být adresou, na kterou může server DHCP odesílat pakety s odpověďmi.

Plánování nastavení DHCP pro DHCP s agentem přenosu DHCP

Tabulka 16. Volby globální konfigurace (týká se všech klientů, které obsluhuje server DHCP)

Objekt		Hodnota
Volby konfigurace	volba 1: Maska podsítě	255.255.255.0
	volba 6: Server DNS	10.1.1.1
	volba 15: Jméno domény	mycompany.com
Provádí server aktualizace DNS?		Ne
Podporuje server klienty BOOTP?		Ne

Tabulka 17. Podsítě pro pracovní síť

Objekt		Hodnota
Jméno podsítě		WorkNetwork
Spravované adresy		10.1.1.3 - 10.1.1.150
Doba pronájmu		24 hodin (předvolená)
Volby konfigurace	Zděděné volby	Volby z globální konfigurace
Adresy podsítě nejsou přiřazeny serverem		žádné

Tabulka 18. Podsítě pro síť datového vstupu

Objekt		Hodnota
Jméno podsítě		DataEntry
Spravované adresy		10.1.2.10 - 10.1.2.40
Doba pronájmu		24 hodin (předvolená)
Volby konfigurace	volba 3: Směrovač	10.1.2.1
	Zděděné volby	Volby z globální konfigurace
Adresy podsítě nejsou přiřazeny serverem		10.1.2.1 (Směrovač) 10.1.2.15 (IP adresa lokálního rozhraní vzdáleného klienta Data Entry) 10.1.2.14 (IP adresa lokálního rozhraní vzdáleného klienta Data Entry)

Další nastavení na serveru iSeries provádějícím PPP

- Nastavte server BOOTP/DHCP relay agent TCP/IP.

Objekt	Hodnota
Adresa rozhraní	10.1.2.2
Předat pakety do IP adresy serveru	10.1.2.1

- Nastavte metodu vzdálené IP adresy v profilu připojení příjemců PPP na DHCP.

1. Aktivujte připojení klienta DHCP WAN k serveru DHCP nebo připojení pro přenos rámce. To učiníte pomocí položky menu Služby pro služby RAS (Remote Access Services) v rámci produktu iSeries Navigator.
 2. V prostředí produktu iSeries Navigator vyberte volbu Profil připojení příjemců, Nastavení TCP/IP - Vlastnosti a pro metodu přiřazení IP adres vyberte Použít DHCP.
- V prostředí produktu iSeries Navigator vyberte volbu Profil připojení příjemců, Nastavení TCP/IP - Vlastnosti a povolte vzdálenému systému přístup k jiným sítím (směrování pomocí IP). Tím umožníte vzdáleným klientům komunikaci se sítí Data Entry.
 - V prostředí produktu iSeries Navigator vyberte volbu Konfigurace TCP/IP a v nastavení vlastností TCP/IP vyberte Postoupit datagram pomocí IP (čímž umožníte vzdáleným klientům komunikovat se sítí Data Entry).

Související pojmy

“Agenti přenosu a směrovače” na stránce 5

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Související odkazy

“Příklad: PPP a DHCP na jednom serveru iSeries” na stránce 32

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN a vzdáleného klienta připojeného přes komutovanou linku.

Plánování DHCP

Je několik kroků, které musíte provést, chcete-li naplánovat, jak by měl být server DHCP nastaven pro vaši síť.

Pokud si neuděláte čas pro plánování toho, jak by měl být nakonfigurován server DHCP, může být nastavování serveru DHCP zdoluhavým a obtížným procesem. Pokud si předem promyslíte nastavení sítě a bezpečnostní otázky, můžete server DHCP konfigurovat mnohem účelněji. Následující témata poukazují na některé důležité otázky, které byste si měli před zahájením konfigurace DHCP v síti promyslet.

Otázky týkající se topologie sítě

Většinu nastavení DHCP si můžete promyslet při pouhém pohledu na topologii sítě, zařízení v síti (například směrovače) a na to, jak chcete v DHCP podporovat klienty.

Otázky týkající se zabezpečení

Protokol DHCP není schopen ověřit, zda jsou klienti požadující IP adresy k této činnosti oprávněni. Vzhledem k charakteru vzájemného působení DHCP a sítě je důležité, abyste zabezpečili server iSeries před vnějšími klienty. Jestliže je server DHCP na serveru iSeries, který je součástí důvěryhodné vnitřní sítě, můžete použít Pravidla paketu (filtrování a NAT) a tím ještě zvýšit zabezpečení sítě před neoprávněnými stranami. Jestliže váš server DHCP je na serveru iSeries, který je připojen k nedůvěryhodné síti, jako je Internet, přečtěte si téma iSeries a bezpečnost na internetu. Další odkazy na zabezpečení naleznete v tématu Zabezpečení v aplikaci Information Center.

Související pojmy

Pravidla paketů (filtrování a NAT)

iSeries a zabezpečení Internetu

Zabezpečení

Související úlohy

“Odstraňování problémů se serverem DHCP” na stránce 46

Můžete prohlížet protokol úloh a trasovat data - také můžete použít seznamy k odstraňování běžných problémů.

Související odkazy

“Konfigurace DHCP” na stránce 40

Toto téma poskytuje pokyny pro nastavení klientů a serveru DHCP a pro konfigurování serveru DHCP, aby mohl odesílat dynamické aktualizace do serveru DNS.

Otázky týkající se topologie sítě

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

Pochopení topologie sítě

Jedním z nejdůležitějších aspektů při plánování implementace DHCP je pochopení uspořádání sítě neboli topologie sítě. Když pochopíte topologii sítě, budete moci rychle určit rozsah IP adres pro DHCP, informace o konfiguraci, které potřebuje každý klient, typ zařízení, která musí být konfigurována, aby mohla přeměrovat zprávy DHCP, a zda DHCP může pracovat se servery DNS nebo PPP. Podle složitosti sítě si můžete dokonce načrtnout topologii vaší sítě na kus papíru. Měli byste zahrnout všechny sítě LAN, zařízení, která spojují sítě LAN, a IP adresy zařízení a klientů (například tiskárny), kteří potřebují definovanou IP adresu. Můžete se podívat na některé příklady DHCP, které vám pomohou při návrhu topologie vaší sítě.

Určení počtu serverů DHCP

Dokonce i ve složitých sítích je možné spravovat všechny síťové klienty pouze s jedním serverem DHCP. V závislosti na topologii sítě můžete instalovat několik agentů přenosu DHCP/BOOTP nebo umožnit směrovačům, aby přeměrovaly pakety DHCP.

Použití pouze jednoho serveru DHCP pro celou síť centralizuje správu konfigurace hostitele pro všechny klienty. Existují však případy, kdy můžete uvažovat o použití více serverů DHCP.

Můžete nakonfigurovat dva nebo více serverů DHCP, aby obsluhovaly stejnou podsít, a vyhnete se tak jakékoliv chybě. Pokud jeden server selže, druhý bude pokračovat v obsluze sítě. Každý ze serverů DHCP musí být dostupný buď přímým připojením k síti, nebo pomocí agenta přenosu DHCP/BOOTP.

Jelikož dva servery DHCP nemohou obsluhovat stejné adresy, musí být společné oblasti adres jedinečné pro každý server DHCP. Proto, když při obsluze určité podsítě používáte dva nebo více serverů DHCP, musíte úplný seznam adres pro podsít rozdělit mezi servery. Jeden server můžete například nakonfigurovat tak, aby používal společnou oblast adres sestávající ze 70 % všech dostupných adres podsítě, a druhý server by používal společnou oblast adres sestávající ze zbývajících 30 % dostupných adres.

Použití několika serverů DHCP snižuje pravděpodobnost chyby přístupu k síti se vztahem k DHCP, nemůže však tuto chybu zcela vyloučit. Pokud server DHCP pro určitou podsít selže, druhý server DHCP nemusí být schopen vyřídít všechny požadavky nových klientů, což může například vyčerpat omezenou společnou oblast dostupných adres serveru.

Pokud uvažujete o použití více serverů, pamatujte si, že více serverů nemůže sdílet stejné adresy. Pokud v síti používáte více než jeden server DHCP, každý server musí mít konfigurovan vlastní jedinečný rozsah IP adres.

Určení IP adres, které by měl server DHCP spravovat

Pomocí topologie sítě byste měli začít dokumentovat, jaký rozsah adres by měl server DHCP spravovat. Měli byste určit, jaká zařízení mají ručně konfigurovanou IP adresu (například IP adresa směrovačů), kterou můžete vyjmout ze společné oblasti adres serveru DHCP.

Navíc můžete zvážit, zda by server DHCP měl tyto adresy přiřazovat dynamicky nebo zda chcete určitým klientům přiřadit specifickou IP adresu. Určitému klientovi, jako například souborovému serveru, můžete vyhradit specifickou adresu a parametry konfigurace. Nebo můžete mapovat všechny klienty na určitou IP adresu. Více informací o dynamickém a statickém přiřazování IP adres naleznete pod tématem Podpora klienta DHCP.

Určení doby pronájmu pro IP adresy

Předvolená doba pronájmu u serveru DHCP je 24 hodin. Doba, na kterou nastavíte pronájem, závisí na několika faktorech. Budete muset zvážit své cíle, modely využití uzlu a uspořádání služeb pro server DHCP. Více informací, které vám pomohou určit dobu pronájmu pro klienty DHCP, získáte pod tématem Pronájemy.

Podpora klientů BOOTP

Pokud nyní používáte server BOOTP, uvědomte si, že server DHCP může v síti nahradit server BOOTP jen s malým nebo žádným dopadem na klienty BOOTP. Pokud jsou ve vaší síti klienti BOOTP, máte tři možnosti.

Nejjednodušší možností je konfigurovat server DHCP tak, aby podporoval klienty BOOTP. Když při podpoře klientů BOOTP používáte DHCP, je každý klient BOOTP v podstatě mapován na jednu IP adresu, a tuto adresu proto nemůže znovu použít jiný klient. V tomto případě je však výhodou používání DHCP to, že není třeba konfigurovat prosté mapování klientů BOOTP na IP adresy. Server DHCP bude stále dynamicky přiřazovat IP adresy klientovi BOOTP ze společné oblasti adres. Jakmile je klientovi BOOTP přiřazena IP adresa, pak je tato adresa trvale vyhrazena tomuto klientovi, dokud vyhrazenou adresu explicitně nevymažete. Tato volba je dobrá, pokud máte v síti velký počet klientů BOOTP.

Další možností je migrovat konfiguraci serveru iSeries BOOTP na serveru DHCP. Pro každého klienta BOOTP uvedeného v konfiguraci serveru BOOTP bude vytvořen klient DHCP. V tomto případě vám doporučujeme konfigurovat vaše klienty na klienty DHCP. Když však migrujete konfiguraci BOOTP na DHCP, bude přiřazování adres DHCP fungovat buď pro klienty BOOTP, nebo DHCP. To by mohla být dobrá možnost při převodu BOOTP klientů na DHCP. Klienti BOOTP budou během konfigurace na DHCP stále podporováni.

Nakonec byste si mohli vybrat třetí možnost, tj. změnit každého klienta BOOTP na DHCP a konfigurovat server DHCP tak, aby jim dynamicky přiřazoval adresy. Tato volba v podstatě zcela odstraní BOOTP ze sítě.

Určení informací o konfiguraci síťových klientů

Pomocí uspořádání topologie sítě můžete jasně vidět zařízení (například směrovač), která musí být identifikována v konfiguraci DHCP. Navíc byste měli určit ostatní servery v síti, jako je server DNS (Domain Name System), o kterých mohou chtít vaši klienti vědět. Tuto informaci můžete zadat pro celou síť, určitou podsít' nebo pro určitého klienta bez ohledu na podsít'.

Pokud máte zařízení používaná mnoha klienty, můžete je specifikovat na nejvyšší možné úrovni (například na globální úrovni pro celou síť nebo na úrovni podsít' pro určitou podsít'). Tím minimalizujete počet změn, které budete muset provést v konfiguraci DHCP při změně zařízení. Pokud například specifikujete stejný směrovač pro každého klienta v síti, budete muset po změně směrovače změnit konfiguraci každého klienta. Pokud jste však určili směrovač na globální úrovni (všichni klienti zdědí tyto informace o konfiguraci), budete muset změnit tuto informaci pouze jednou a informace se změní pro všechny klienty.

Někteří z klientů mohou mít zvláštní požadavky na konfiguraci TCP/IP, které vyžadují, aby informace byly konfigurovány na úrovni klienta. DHCP může takové klienty rozpoznat a poskytnout jim jedinečná konfigurační data. To neplatí pouze pro volby konfigurace, ale také pro dobu pronájmu a IP adresu. Klient může například potřebovat delší dobu pronájmu než všichni ostatní klienti. Nebo jeden klient, jako například souborový server, potřebuje vyhrazenou IP adresu. Když si předem určíte tyto klienty a jedinečné informace, které vyžadují, pomůže vám to při konfiguraci serveru DHCP.

Rychlý přehled všech voleb konfigurace najdete v tématu "Vyhledávání voleb DHCP" na stránce 8.

Použití dynamického serveru DNS se serverem DHCP

Pokud v současné době používáte při správě všech hostitelských jmen klientů a IP adres server DNS, určitě budete chtít konfigurovat server DNS tak, aby přijímal dynamické aktualizace ze serveru DHCP. Pokud používáte dynamický

server DNS, klienti si při přechodu na DHCP nepovšimnou žádných přerušení nebo změn ve službě serveru DNS. Více informací o použití DHCP se serverem DNS najdete pod tématem Dynamické aktualizace.

Pokud v současné době nepoužíváte server DNS, možná budete při přidávání serveru DHCP uvažovat také o přidání serveru DNS. V aplikaci Information Center si pod tématem DNS můžete přečíst další informace o výhodách a požadavcích serveru DNS.

Použití DHCP pro vzdálené klienty

Pokud máte vzdálené klienty, kteří se připojují k síti pomocí PPP, můžete nastavit DHCP tak, aby jim při připojení k síti dynamicky přiřazoval IP adresu. Příklad sítě, kde může být tato volba užitečná, najdete pod tématem Příklad: PPP a DHCP na jednom serveru iSeries nebo Příklad: Profil DHCP a PPP na různých serverech iSeries. Tyto příklady také vysvětlují, jak nastavit síť, aby mohla používat PPP a DHCP společně pro vzdálené klienty.

Související pojmy

“Agenti přenosu a směrovače” na stránce 5

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

“Příklady DHCP” na stránce 21

Když si prohlédnete schémata a příklady toho, jak jsou uspořádány různé sítě, budete moci zjistit nejlepší volbu pro svou instalaci.

“Podpora klienta DHCP” na stránce 6

Pomocí DHCP můžete spravovat každého klienta v síti namísto správy všech klientů jako velké skupiny (podsíť).

“Pronájmy” na stránce 3

Zde naleznete informace o tom, jaké jsou DHCP pronájmy, a některé otázky, které je třeba zvážit při určování doby pronájmu pro klienty DHCP.

“BOOTP” na stránce 6

Toto téma popisuje, co je BOOTP, a uvádí určitou historii o BOOTP a DHCP.

“Dynamické aktualizace” na stránce 7

Můžete používat server DHCP společně se serverem DNS při dynamické aktualizaci informací o klientovi v DNS, když DHCP přiřazuje klientovi IP adresu.

DNS

“Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci” na stránce 47

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

Související odkazy

“Vyhledávání voleb DHCP” na stránce 8

DHCP má mnoho konfiguračních voleb, které mohou být odeslány klientovi v případě požadavků na informace od serveru DHCP. Můžete použít nástroj pro vyhledávání, který popisuje všechny volby DHCP.

“Příklad: PPP a DHCP na jednom serveru iSeries” na stránce 32

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN a vzdáleného klienta připojeného přes komutovanou linku.

“Příklad: Profil DHCP a PPP na různých serverech iSeries” na stránce 34

Zde se dozvíte, jak nastavit dva servery iSeries jako síťový server DHCP a agenta přenosu DHCP/BOOTP pro dvě sítě LAN a vzdálené klienty připojené přes komutovanou linku.

Konfigurace DHCP

Toto téma poskytuje pokyny pro nastavení klientů a serveru DHCP a pro konfigurování serveru DHCP, aby mohl odesílat dynamické aktualizace do serveru DNS.

Související odkazy

“Plánování DHCP” na stránce 37

Je několik kroků, které musíte provést, chcete-li naplánovat, jak by měl být server DHCP nastaven pro vaši síť.

Konfigurace serveru DHCP a agenta přenosu BOOTP/DHCP

Toto téma vysvětluje, jaký software potřebujete, abyste mohli konfigurovat server iSeries DHCP. Také obsahuje instrukce popisující jak pracovat s konfigurací DHCP, jak používat nástroj pro administraci serveru DHCP (DHCP Server Monitor Program) a jak nastavit agenta přenosu DHCP/BOOTP.

Související pojmy

“Agenti přenosu a směrovače” na stránce 5

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

Konfigurování nebo zobrazení serveru DHCP

K tomu, abyste mohli vytvořit novou konfiguraci DHCP nebo abyste si mohli prohlédnout stávající konfiguraci, potřebujete funkci konfigurace serveru. Chcete-li přistoupit ke konfiguraci serveru DHCP, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Konfigurace**.

Pokud vytváříte novou konfiguraci DHCP, použijte průvodce, který vám pomůže nastavit server DHCP. Tento průvodce vám položí některé základní otázky týkající se konfigurace a provede vás procesem vytváření podsítě. Jakmile dokončíte průvodce, můžete měnit a zlepšovat konfiguraci podle potřeb sítě.

Pokud je server DHCP nakonfigurován, funkce konfigurace serveru DHCP zobrazí aktuální konfiguraci, včetně všech podsítí a klientů, kteří mohou být spravováni ze serveru DHCP, a to včetně informací o konfiguraci, které budou odeslány klientům.

Vytvoření zástupce konfiguračního okna DHCP

Pokud se díváte na konfiguraci DHCP často a chcete vytvořit zástupce konfiguračního okna DHCP, postupujte takto.

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Vytvořit zástupce**.

Spuštění nebo zastavení serveru DHCP

Jakmile je server DHCP nakonfigurován, můžete ho spustit nebo zastavit takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Spustit** nebo **Zastavit**.

Konfigurace serveru DHCP, který se má spouštět automaticky

Proveďte následující kroky, chcete-li konfigurovat server DHCP, aby se spouštěl automaticky:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Konfigurace**.
3. Klepněte pravým tlačítkem myši na **server DHCP** a vyberte **Vlastnosti**.
4. Zaškrtněte políčko **Spustit při spuštění TCP/IP**.
5. Klepněte na **OK**.

Přístup k DHCP Server Monitor

Nástroj DHCP Server Monitor slouží k monitorování aktivních informací o pronájmu serveru IBM iSeries DHCP. Toto grafické rozhraní vám umožní sledovat, které IP adresy jsou pronajaty, jak dlouho jsou pronajaty a kdy budou k dispozici pro další pronájem. Chcete-li získat přístup k nástroji administrace serveru DHCP, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Monitor**.

Konfigurace agenta přenosu BOOTP/DHCP

Server iSeries poskytuje agenta přenosu DHCP/BOOTP, který může být použit při směrování paketů DHCP na server DHCP v jiné síti.

Při nastavení agenta přenosu iSeries DHCP/BOOTP postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **agent přenosu BOOTP/DHCP**.
2. Klepněte pravým tlačítkem myši na **Agent přenosu BOOTP/DHCP** a pak vyberte **Konfigurace**.
3. Zadejte rozhraní, ze kterého agent přenosu obdrží paket DHCP a místo určení, kam má být paket přeměrován.
4. Klepněte na **OK**.

Spuštění nebo zastavení agenta přenosu BOOTP/DHCP

Jakmile bude agent přenosu DHCP/BOOTP konfigurován, můžete jej spustit nebo zastavit:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **agent přenosu BOOTP/DHCP**.
2. Klepněte pravým tlačítkem myši na **Agent přenosu BOOTP/DHCP** a pak vyberte **Spustit** nebo **Zastavit**.

Konfigurace agenta přenosu BOOTP/DHCP pro automatické spuštění

Navíc můžete nakonfigurovat agenta přenosu BOOTP/DHCP tak, aby ho automaticky spustil server iSeries při spuštění TCP/IP. Postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **agent přenosu BOOTP/DHCP**.
2. Klepněte pravým tlačítkem myši na **Agent přenosu BOOTP/DHCP** a pak vyberte **Vlastnosti**.
3. Zaškrtněte políčko **Spustit při spuštění TCP/IP**.
4. Klepněte na **OK**.

Konfigurování klientů, aby mohli používat DHCP

V tomto tématu se dozvíte, jak konfigurovat klienty Microsoft Windows a OS/2, aby si informace o konfiguraci vyžádali od serveru DHCP.

Jakmile bude server DHCP nakonfigurován, musí být nakonfigurován také každý klient, aby mohl používat DHCP. Následující informace popisují kroky při konfiguraci klientů s operačními systémy Windows and OS/2, aby tito klienti mohli ze serveru DHCP požadovat informace o konfiguraci. Navíc popisují, jak si klienti mohou prohlédnout vlastní informace DHCP o pronájmu.

Povolte DHCP pro klienty s operačním systémem Windows 95, Windows 98 nebo Windows.

Chcete-li povolit DHCP, proveďte následující kroky:

1. V menu **Start** vyberte **Nastavení** → **Ovládací panely**.
2. Dvakrát klepněte na **Síť** a pak vyberte kartu **Protokoly**.
3. Vyberte **Protokol TCP/IP** a pak vyberte tlačítko **Vlastnosti**.
4. Na kartě **Adresa IP** vyberte přepínač **Získat IP adresu ze serveru DHCP**.
5. Klepněte na **OK**.

Kontrola pronájmu klienta DHCP pro klienty:

Také klienti s operačním systémem Windows 95, Windows 98 nebo Windows mají k dispozici obslužný program, který zobrazí klientovu IP adresu a informace DHCP o pronájmu. Tento program také umožňuje ukončit nebo obnovit pronájem DHCP. Při kontrole pronájmu klienta DHCP postupujte takto:

1. Otevřete *příkazovou řádku MS-DOS*.
2. Spusťte **WINIPCFG**.

Poznámka: Tento obslužný program neprovádí dynamickou aktualizaci zobrazených informací, takže pokud si chcete prohlédnout aktualizovaný stav, je nutné spustit ho ještě jednou.

Povolte DHCP pro klienty Windows NT

Chcete-li povolit DHCP, proveďte následující kroky:

1. V menu **Start** vyberte **Nastavení** → **Ovládací panely**.
2. Dvakrát klepněte na **Síť** a pak vyberte kartu **Protokoly**.
3. Vyberte **Protokol TCP/IP** a pak vyberte **Vlastnosti**.
4. Na kartě **IP Adresa** vyberte **Získat IP adresu ze serveru DHCP**.
5. Klepněte na **OK**.

Kontrola adresy MAC a pronájem DHCP:

Také klienti s operačním systémem Windows NT a Windows mají k dispozici obslužný program, který zobrazí klientovu IP adresu a informace DHCP o pronájmu. Při kontrole DHCP pronájmu klienta s operačním systémem Windows NT nebo Windows 2000 postupujte takto:

1. Otevřete okno příkazového řádky.
2. Spusťte **IPCONFIG /ALL**.

Poznámka: Tento obslužný program neprovádí dynamickou aktualizaci zobrazených informací, takže pokud si chcete prohlédnout aktualizovaný stav, bude nutné spustit ho ještě jednou. Při zrušení nebo obnově pronájmu můžete použít stejný obslužný program s jinými parametry (**IPCONFIG /RELEASE** a **IPCONFIG /RENEW**). Pokud si chcete prohlédnout všechny možné parametry příkazu, spusťte z příkazového řádku MS-DOS příkaz **IPCONFIG /?**.

Pokud u klientů DHCP s operačním systémem Microsoft Windows 2000 chcete, aby server DHCP aktualizoval záznamy DNS typu A namísto klienta, je třeba změnit konfiguraci klienta. Můžete také pověřit aktualizací server DHCP, pokud má vaše síť standardní klienty s operačním systémem Windows, jako např. Windows 95 a NT, protože tito klienti momentálně neprovádějí aktualizaci záznamů DNS typu A. To může zjednodušit administraci DNS, protože ze serveru DHCP budou pocházet aktualizace DNS pro všechny klienty namísto toho, aby někteří klienti sami aktualizovali své záznamy.

Klienti s operačním systémem Windows 2000

Chcete-li povolit DHCP, proveďte následující kroky:

1. V menu **Start** vyberte **Nastavení** → **Síťová a komutovaná připojení**.
2. Klepněte pravým tlačítkem myši na odpovídající jméno připojení a vyberte **Vlastnosti**.
3. Vyberte **Protokol TCP/IP** a pak vyberte **Vlastnosti**.
4. Na kartě **Obecné** vyberte **Získat IP adresu ze serveru DHCP**.
5. Klepněte na **OK**.

Kontrola adresy MAC a pronájem DHCP:

Také klienti s operačním systémem Windows NT a Windows mají k dispozici obslužný program, který zobrazí klientovu IP adresu a informace DHCP o pronájmu. Při kontrole DHCP pronájmu klienta s operačním systémem Windows NT nebo Windows 2000 postupujte takto:

1. Otevřete okno příkazového řádky.
2. Spusíte **IPCONFIG /ALL**.

Poznámka: Tento obslužný program neprovádí dynamickou aktualizaci zobrazených informací, takže pokud si chcete prohlédnout aktualizovaný stav, bude nutné spustit ho ještě jednou. Při zrušení nebo obnově pronájmu můžete použít stejný obslužný program s jinými parametry (IPCONFIG /RELEASE a IPCONFIG /RENEW). Pokud si chcete prohlédnout všechny možné parametry příkazu, spusíte z příkazového řádku MS-DOS příkaz IPCONFIG /?.

Pokud u klientů DHCP s operačním systémem Microsoft Windows 2000 chcete, aby server DHCP aktualizoval záznamy DNS typu A namísto klienta, je třeba změnit konfiguraci klienta. Můžete také pověřit aktualizací server DHCP, pokud má vaše síť standardní klienty s operačním systémem Windows, jako např. Windows 95 a NT, protože tito klienti momentálně neprovádějí aktualizaci záznamů DNS typu A. To může zjednodušit administraci DNS, protože ze serveru DHCP budou pocházet aktualizace DNS pro všechny klienty namísto toho, aby někteří klienti sami aktualizovali své záznamy.

Povolte DHCP pro klienty s operačním systémem OS/2 Warp 4

Chcete-li povolit DHCP, proveďte následující kroky:

1. Vyberte **Konfigurace TCP/IP**.
2. Vyberte přepínač **Získat IP adresu automaticky**.
3. Klepněte na **OK**.

Klienta můžete spustit ručně z okna OS/2 zadáním DHCPDCD. Můžete také aktualizovat konfigurační soubor klienta (mptn\etc\dhcpcd.cfg) a umožnit mu požadovat volby DHCP.

Warp má také k dispozici obslužný program pro sledování pronájmů. V okně OS/2 zadejte příkaz DHCPMON nebo vyberte na monitoru ikonu DHCP ve složce TCP/IP. Klienta můžete ukončit zadáním DHCPMON -t.

Poznámka: Tento příkaz neprovede ukončení DHCP, ale ukončí klienta DHCP tak, že již neobnoví pronájem.

Můžete si také prohlédnout klientův soubor protokolu DHCP a prozkoumat vzájemné působení mezi klientem a serverem a volby odeslané serverem. Jméno souboru je možné konfigurovat v klientově konfiguračním souboru. Některé systémy mají protokol v kořenovém adresáři se jménem souboru dhcpcd.log. Navíc předešlý získaný pronájem a informace o volbách jsou uloženy klientem v souboru mptn\etc\dhcpc.db. Pokud budete někdy potřebovat restartovat klienta "od nuly", měli byste vymazat soubor mptn\etc\dhcpc.db.

Zakázání dynamických aktualizací DNS

Chcete-li zablokovat dynamické aktualizace ze strany klienta, postupujte takto:

1. V menu **Start** vyberte **Nastavení** → **Síťová a komutovaná připojení**.
2. Klepněte pravým tlačítkem myši na odpovídající jméno připojení a vyberte **Vlastnosti**.
3. Vyberte **Protokol TCP/IP** a pak vyberte **Vlastnosti**.
4. Vyberte **Rozšířené**.
5. Na kartě **DNS** zrušte volby "Registrovat adresy tohoto připojení v DNS" a "Použít přípony DNS těchto připojení v registraci DNS".
6. Klepněte na **OK**.

Tyto kroky proveďte u všech připojení, u kterých chcete, aby aktualizaci záznamů DNS převzal server DHCP.

Konfigurování serveru DHCP, aby mohl odesílat dynamické aktualizace na server DNS

Můžete konfigurovat servery DHCP a DNS, aby bylo možné dynamicky aktualizovat zdrojové záznamy DNS, když server DHCP pronajímá klientovi IP adresu.

Server DHCP můžete konfigurovat tak, aby odesílal aktualizované požadavky na server DNS pokaždé, když přiřazuje novou adresu hostiteli. Tento automatizovaný proces snižuje náročnost správy serveru DNS v rychle rostoucích nebo měnících se sítích TCP/IP a v sítích, kde hostitelé často mění umístění. Když klient, který používá DHCP, obdrží IP adresu, jsou tato data ihned odeslána serveru DNS. Pomocí této metody může DNS pokračovat v úspěšném řešení dotazů pro hostitele, dokonce i když se jejich IP adresy mění.

Pokud chcete, aby docházelo k aktualizacím záznamů, musíte na serveru iSeries nainstalovat volbu 31. Server DHCP používá při provádění dynamických aktualizací programovací prostředí poskytované volbou 31. Server DNS může být spuštěn na nezávislém serveru iSeries, který je schopný provádět dynamické aktualizace. Informace o tom, jak zjistit, zda je nainstalována volba 31, najdete pod tématem Požadavky systému DNS.

Při konfiguraci vlastností DHCP s cílem umožnit serveru DHCP provádění dynamických aktualizací postupujte takto:

1. Rozbalte **Síť** → **Servery** → **TCP/IP**.
2. V pravém podokně klepněte pravým tlačítkem myši na **DHCP** a vyberte **Konfigurace**.
3. V levém podokně okna **Konfigurace serveru DHCP** klepněte pravým tlačítkem myši na **Globální** a vyberte **Vlastnosti**.
4. Vyberte kartu **Volby**.
5. Vyberte **Volbu 15: Jméno domény** ze seznamu **Vybrané volby**. Pokud se volba 15 neobjeví v seznamu **Vybrané volby**, vyberte 15: Jméno domény ze seznamu **Dostupné volby** a klepněte na **Přidat**.
6. V poli **Jméno domény** zadejte jméno domény, které klient používá, když pomocí DNS rozlišuje hostitelská jména.
7. Vyberte kartu **Dynamická aktualizace DNS**.
8. Vyberte **Server DHCP aktualizuje záznamy A i záznamy PTR** nebo **Server DHCP aktualizuje pouze záznamy PTR**.
9. Nastavte **Přidat ke jménu hostitele jméno domény** na **Ano**.
10. Klepněte na **OK** a uzavřete stránku **Globální vlastnosti**.

Související pojmy

“Dynamické aktualizace” na stránce 7

Můžete používat server DHCP společně se serverem DNS při dynamické aktualizaci informací o klientovi v DNS, když DHCP přiřazuje klientovi IP adresu.

Související odkazy

Systémové požadavky DNS

Správa pronajatých IP adres

Při monitorování a správě pronájmů vám může pomoci DHCP Server Monitor.

Nástroj pro konfiguraci DHCP vám pomůže nastavit server DHCP, klienty, které bude obsluhovat, a informace, které jsou odesílány klientům. V nástroji pro konfiguraci DHCP určíte společnou oblast IP, kterou bude DHCP spravovat, a dobu pronájmu pro tyto společné oblasti adres. Pokud si chcete prohlédnout, které IP adresy jsou aktuálně pronajaty, musíte použít nástroj pro administraci serveru DHCP (DHCP Server Monitor Program).

Nástroj DHCP Server Monitor slouží k monitorování aktivních informací o pronájmu serveru IBM iSeries DHCP. Toto grafické rozhraní vám umožní sledovat, které IP adresy jsou pronajaty, jak dlouho jsou pronajaty a kdy budou k dispozici pro další pronájem.

Nástroj administrace serveru DHCP můžete použít také při získávání IP adres, které již nejsou používány. Pokud byla společná oblast adres vyčerpána, můžete si projit aktivní informace o pronájmu a určit, zda existují pronájmy, které můžete vymazat, a učinit tak IP adresu dostupnou pro jiné klienty. Můžete mít například klienta, který již není v síti, ale stále má aktivní pronájem IP adresy. Takový aktivní pronájem IP adresy můžete vymazat. Tuto operaci byste měli provádět jen tehdy, když jste si jisti, že se klient už nepokusí adresu použít. Když vymažete aktivní pronájem IP adresy, server DHCP na to klienty neupozorní. Pokud vymažete aktivní pronájem u klienta, který je stále v síti, aniž byste z tohoto klienta uvolnili IP adresu, může v síti dojít k duplicitnímu přiřazování IP adres.

Související pojmy

“Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci” na stránce 47

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

“Problém: Přiřazování duplicitních IP adres ve stejné síti” na stránce 48

IP adresa by měla být v síti jedinečná. Server DHCP nepřihadí jednu adresu více než jednomu klientovi.

Odstraňování problémů se serverem DHCP

Můžete prohlížet protokol úloh a trasovat data - také můžete použít seznamy k odstraňování běžných problémů.

Následující informace vám pomohou s odstraňováním problémů, které se mohou vyskytnout u serveru DHCP. Pokud váš problém není v tomto tématu popsán, podívejte se znovu na téma Plánování DHCP a ověřte, zda jste při zvažování konfigurace DHCP vzali v úvahu všechny eventuality.

Z níže uvedeného seznamu vyberte popis problému nebo si přečtete téma Shromažďování podrobných informací o chybách DHCP, kde najdete směrnice pro přístup k datům protokolu serveru a k informacím o sledování.

Související pojmy

Trasování komunikace iSeries

Související odkazy

“Plánování DHCP” na stránce 37

Je několik kroků, které musíte provést, chcete-li naplánovat, jak by měl být server DHCP nastaven pro vaši síť.

Shromažďování podrobných informací o chybách DHCP

Existuje několik způsobů, jak zjistit podrobnosti o chybě, která souvisí s vaším problémem.

Nejdříve se podívejte na protokol úloh serveru DHCP, a to následovně:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Úlohy serveru**.

Pokud v protokolu úloh serveru DHCP nejsou žádné zprávy, bude možná nutné získat tyto informace od monitorovacího programu (iSeries Communication Trace) nebo od interního sledovacího programu serveru DHCP. Program iSeries Communication Trace vám pomůže určit, zda jsou klientovy požadavky přijímány serverem DHCP a zda server DHCP klientovi odpovídá. Pokud server DHCP přijímá klientovy požadavky, ale server neodpovídá, použijte funkci interního sledovacího programu serveru DHCP.

Trasování serveru DHCP

Chcete-li trasovat server DHCP, postupujte takto:

1. V prostředí produktu **iSeries Navigator** rozbalte **server iSeries** → **Síť** → **Servery** → **TCP/IP** → **DHCP**.
2. Klepněte pravým tlačítkem myši na **DHCP** a pak vyberte **Konfigurace**.
3. Klepněte pravým tlačítkem myši na **server DHCP** a vyberte **Vlastnosti**.
4. Vyberte kartu vlastností **Protokolování**.
5. Zaškrtněte políčko **Umožnit protokolování**.

6. Ověřte, že **Jméno souboru protokolu** je **dhcpcsd.log**.
7. Zkontrolujte všechny kategorie **Protokol** kromě Sledování a Statistika (protokoly sledování a statistiky používá pouze linka podpory).
8. Klepněte na **OK**.
9. Klepněte pravým tlačítkem myši na **DHCP Server**, vyberte **Aktualizovat server** a restartujte server DHCP, pokud již byl spuštěn.
10. Znovu vytvořte problémovou situaci.
11. Klepněte pravým tlačítkem myši na **Server DHCP** a pak vyberte **Vlastnosti** → **Protokolování**.
12. Zrušte zaškrtnutí **Umožnit protokolování**, čímž vypnete protokolování.
13. Klepněte na **OK**.
14. Klepněte pravým tlačítkem myši na **server DHCP** a pak vyberte **Aktualizovat server**. Pak server DHCP restartujte.
15. V 'QIBM/UserData/OS400/DHCP/dhcpcsd.log' si prohlédněte soubor protokolu DHCP. V prostředí produktu **iSeries Navigator** rozbalte **Server iSeries** → **Systému souborů** → **Integrovaný systém souborů** → **Root** → **adresář souboru**. Nebo ve znakově orientovaném rozhraní použijte příkaz **wrklnc** a vyberte volbu **5=Display**.

Problém: Klienti nedostávají IP adresu nebo informace o konfiguraci

Mohou se objevit problémy, pokud klienti nemohou přijímat informace o IP adrese nebo informace o konfiguraci. IP adresa je klientovi pronajata během procesu probíhajícího mezi klientem a serverem DHCP, který se skládá ze čtyř kroků.

Všechny čtyři kroky musí proběhnout předtím, než klient obdrží IP adresu. Více podrobností o tomto procesu najdete pod tématem **Vzájemné působení klienta a serveru DHCP**.

Toto jsou některé běžné příčiny tohoto problému.

Klient je připojen k podsíti, která není konfigurována na serveru DHCP.

Zkontrolujte konfiguraci DHCP a ověřte, zda jsou všechny podsítě spravované serverem DHCP uvedeny v konfiguraci. Pokud si nejste jisti tím, které podsítě by měly být spravovány serverem DHCP, prostudujte si téma **Otázky topologie sítě**.

Zpráva DHCP DISCOVER od klienta nemůže dorazit do serveru DHCP.

Pokud server DHCP nemá v podsíti klienta IP adresu, je třeba použít směrovač nebo agenta přenosu DHCP/BOOTP, kteří mohou přesměrovat klientovu zprávu DHCP DISCOVER na server DHCP. Více informací najdete pod tématem **Agenti přenosu a směrovače**. Server musí umět kromě přijímání vysílané zprávy také odesílat pakety s odpovědí do podsítě klienta.

Pokud je server iSeries připojen k více sítím (multihoming), budete možná muset ke konfiguraci DHCP přidat skupinu podsítě. Více podrobností o konfiguraci DHCP pro vícenásobně připojený server najdete pod tématem **Příklad: DHCP a multihoming**. Tento příklad popisuje, co je třeba udělat v konfiguraci DHCP, aby server obdržel klientem vyslanou zprávu.

Server DHCP nemá pro klienta žádné dostupné adresy ve společné oblasti adres.

Pomocí nástroje pro administraci serveru DHCP (DHCP Server Monitor) se můžete podívat, které adresy server DHCP právě používá. Správa pronajatých IP adres je téma, které vám poskytne více informací o použití nástroje administrace serveru DHCP. Pokud server DHCP vyčerpá všechny dostupné adresy, budete možná muset přidat nové adresy do společné oblasti adres, zkrátit dobu pronájmu nebo vymazat trvalé pronájmy, které již nejsou využívány.

Související pojmy

“Otázky týkající se topologie sítě” na stránce 38

Většinu nastavení DHCP si můžete promyslet při prohlédnutí topologie sítě, zařízení v síti (například směrovače) a toho, jak chcete v DHCP podporovat klienty.

“Agenti přenosu a směrovače” na stránce 5

Možná budete muset použít agenta přenosu DHCP ve své síti; někdy stačí směrovač. Můžete také používat agenta přenosu DHCP a směrovač k účinnému a bezpečnému přenosu dat po síti.

“Správa pronajatých IP adres” na stránce 45

Při monitorování a správě pronájmů vám může pomoci DHCP Server Monitor.

Související odkazy

“Vzájemné působení klienta a serveru DHCP” na stránce 1

Klient získává informace o DHCP ze serveru a odesílají se určité zprávy mezi klientem a serverem. DHCP získává a vrací pronájmy.

“Příklad: DHCP a multihoming” na stránce 25

Zde se dozvíte, jak nastavit server iSeries jako server DHCP pro síť LAN, která je připojena k Internetu pomocí internetového směrovače.

Problém: Přiřazování duplicitních IP adres ve stejné síti

IP adresa by měla být v síti jedinečná. Server DHCP nepřihradí jednu adresu více než jednomu klientovi.

Za určitých podmínek se server DHCP předtím, než přiřadí adresu klientovi, pokusí ověřit, zda adresa již není používána. Když server DHCP zaznamená, že adresa je používána, i když by neměla být, dočasně adresu označí jako použitou a nepřihradí ji žádnému klientovi. Můžete použít nástroj pro administraci serveru DHCP (DHCP Server Monitor Program) a podívat se, které IP adresy, jež server zaznamenal, jsou používány, ale nebyly přiřazeny serverem DHCP. Tyto adresy budou mít stav USED a identifikátor klienta UNKNOWN_TO_IBMDHCP.

Toto jsou některé běžné příčiny tohoto problému.

Několik serverů DHCP je konfigurováno tak, aby přiřazovaly stejnou IP adresu.

Pokud jsou dva servery DHCP konfigurovány tak, aby přiřazovaly klientovi stejnou IP adresu, potom mohou dva různí klienti obdržet stejnou IP adresu. Jeden z klientů obdrží IP adresu z jednoho serveru DHCP a druhý klient obdrží stejnou IP adresu z druhého serveru DHCP. Podsíť nebo síť může být obsluhována několika servery DHCP, které by však neměly konfigurovány se stejnou společnou oblastí adres nebo překrývajícími se společnými oblastmi adres.

Klientova IP adresa, která je spravována serverem DHCP, byla konfigurována ručně.

Před přiřazením IP adresy klientovi se server DHCP obvykle pokusí ověřit, zda adresa není používána. Neexistuje však žádná záruka, že ručně konfigurovaný klient není v okamžiku ověřování IP adresy serverem DHCP připojen k síti nebo dostupný pro odpověď. Server DHCP tak může přiřadit tuto IP adresu klientovi DHCP. Když se ručně konfigurovaný klient připojí k síti, budete mít v síti duplicitní IP adresy. IP adresy, které jsou spravovány serverem DHCP, by neměly být používány při ruční konfiguraci klientova síťového nastavení. Pokud klient potřebuje, aby jeho IP adresa byla konfigurována ručně, měla by být tato adresa vyřazena se společné oblasti adres serveru DHCP.

Související pojmy

“Správa pronajatých IP adres” na stránce 45

Při monitorování a správě pronájmů vám může pomoci DHCP Server Monitor.

Problém: DHCP neaktualizuje záznamy DNS

Server iSeries DHCP je schopen dynamicky aktualizovat zdrojové záznamy DNS. Chyby dynamické aktualizace mohou být způsobeny selháním aktualizace záznamů DNS.

Více se o této schopnosti dozvíte pod tématem “Dynamické aktualizace” na stránce 7. Server DHCP používá při určování odpovídajícího dynamického serveru, který má aktualizovat, programovací prostředí a funkce pro rozlišení jména. Toho můžete využít ve svůj prospěch při určování zdroje chyb dynamické aktualizace.

Když se záznamy DNS neaktualizují dynamicky, zkontrolujte následující body.

Ověřte, které podsítě a který typ zdrojových záznamů (záznamy A a/nebo PTR) jsou aktualizovány.

Zkontrolujte konfiguraci DHCP a ověřte, zda je klientova podsít nastavena pro dynamickou aktualizaci zdrojových záznamů, a ověřte, který typ záznamu je aktualizován.

Ověřte, že na serveru iSeries, na kterém je spuštěno DHCP, je instalována volba 31 (Domain Name System) operačního systému i5/OS.

Server DHCP používá programovací prostředí poskytované volbou 31 operačního systému i5/OS. Server DNS, který je dynamicky aktualizován, nemusí být umístěn na stejném serveru iSeries jako server DHCP.

Ověřte, zda je server DHCP oprávněn k odesílání aktualizací na server DNS.

Zkontrolujte konfiguraci DNS a ověřte, zda je zóna DNS konfigurována tak, aby umožňovala dynamické aktualizace, a zda je server DHCP zahrnut na přístupovém seznamu (ACS).

Ověřte, zda servery DNS mohou rozlišit klientovu doménu.

Pomocí příkazu CHGTCPDMN zobrazte seznam serverů DNS na serveru iSeries, na kterém je umístěn server DHCP. Ověřte, zda tyto servery DNS mohou rozlišit aktualizovanou doménu. Provedete to pomocí příkazu NSLOOKUP ze serveru iSeries, kde se spouští DHCP při rozlišování jména (nebo IP adresy), které existuje v doméně, jež při aktualizaci selže. Server DHCP musí být schopen odvodit FQDN (fully qualified domain name) klienta, aby mohl aktualizovat jeho záznamy DNS. Server DHCP se nepokusí aktualizovat dynamický server DNS bez FQDN (klientovo hostitelské jméno a jméno domény). Server DHCP odvodí klientovo FQDN pomocí tohoto pořadí:

1. Volba 81 (Klient FQDN) ve zprávě DHCPREQUEST od klienta.
2. Volba 12 (Host Name) a/nebo volba 15 (Domain Name) ve zprávě DHCPREQUEST od klienta.
3. Volba 12 (Host Name) ve zprávě DHCPREQUEST od klienta a/nebo volba 15 (Domain Name) nakonfigurovaná na serveru DHCP. V tomto případě musí být server DHCP při odvozování FQDN konfigurován tak, aby přidal jméno domény k hostitelskému jménu (zadáno ve **Vlastnosti** → , **karta Dynamické aktualizace DNS** pro globální úroveň, podsít, třídu nebo klienta).

Záznam TXT nemusí vyhovovat odpovídajícímu záznamu DNS.

Server DHCP může být konfigurován tak, aby zkontroloval stávající zdrojové záznamy DNS a tak určil, se kterými klienty DHCP jsou spojeny. Server DHCP toho dosáhne tím, že napíše odpovídající TXT záznam pro každý záznam A nebo PTR, který je aktualizován v DNS. Pokud je server konfigurován tak, aby ověřil ID klienta ještě před provedením aktualizace DNS, potom musí data záznamu TXT vyhovovat ID klienta, který obdržel adresu ze serveru DHCP. Pokud nevyhovují, server DHCP nebude aktualizovat zdrojový záznam DNS typu A. Je to proto, aby se zabránilo přepsání stávajících záznamů. Server DHCP však může být konfigurován tak, aby ignoroval stávající záznamy a aby provedl aktualizaci DNS bez ohledu na data v záznamu TXT (zadáno ve **Vlastnosti** → , **karta Dynamické aktualizace DNS** pro globální úroveň, podsít, třídu nebo klienta).

Související pojmy

“Dynamické aktualizace” na stránce 7

Můžete používat server DHCP společně se serverem DNS při dynamické aktualizaci informací o klientovi v DNS, když DHCP přiřazuje klientovi IP adresu.

Problém: Protokol úloh DHCP uvádí zprávy DNS030B s chybou č. 1 ze 3447

Chybový kód 3447 znamená, že server DHCP ukončil čekání na odpověď ze serveru DNS. Tato situace může nastat z důvodu problémů v síti nebo ve spojení mezi serverem iSeries DHCP a serverem DNS.

Tato zpráva bude doprovázena zprávou TCP5763, která obsahuje typ zdrojového záznamu DNS a podrobná data pro zdrojový záznam, který se server DHCP pokusil aktualizovat.

Protože se server iSeries s DHCP pokouší aktualizovat zdrojové záznamy DNS pokaždé, když se obnovuje pronájem, zdrojové záznamy mohou být již obsaženy v zónovém konfiguračním souboru z původní IP adresy nebo z předešlé obnovy pronájmu. Zkontrolujte zónová konfigurační data DNS, např. pomocí nástroje NSLOOKUP. Možná zjistíte, že zdrojový záznam již obsahuje správná data a není nutné nic měnit.


Pokud zdrojový záznam není obsažen v DNS, existuje několik způsobů, jak zdrojový záznam aktualizovat. Server iSeries DHCP se pokusí aktualizovat zdrojový záznam při dalším požadavku na obnovu pronájmu. Můžete tedy počkat na další obnovu pronájmu. Mnozí klienti se také pokoušejí obnovit nebo znovu získat IP adresu při spuštění. Můžete zkusit restartovat klienta, což by mohlo přinutit server DHCP, aby se pokusil opět aktualizovat zdrojové záznamy DNS.







Pokud žádná z těchto možností nefunguje, můžete aktualizovat zdrojové záznamy DNS ručně. Tento způsob však nedoporučujeme, protože při aktualizaci nesmí být spuštěna dynamická zóna. Ostatní dynamické aktualizace ze serveru DHCP tak budou během tohoto prostoje ztraceny. Existují však obslužné programy pro dynamickou aktualizaci, které jsou poskytovány některými implementacemi klienta nebo serveru DNS založeného na BIND. Při aktualizaci zdrojového záznamu můžete tento obslužný program pro dynamickou aktualizaci použít. Obslužné programy pro dynamickou aktualizaci jsou podobné jako v procesu ruční aktualizace zóny (administrátor musí zadat data zdrojového záznamu, který má být aktualizován), ale umožňují aktualizaci zóny, i když je zóna aktivní.

Související informace o DHCP

Zde jsou uvedeny červené knihy IBM Redbooks (ve formátu PDF) a dokumenty RFC k tématu DHCP. Všechny tyto soubory ve formátu PDF můžete prohlížet a tisknout.

Dokumenty DHCP RFC

RFC (Requests for Comments)  jsou písemné definice standardů pro protokoly a navržených standardů používaných pro Internet. Níže uvedené definice RFC vám mohou pomoci pochopit DHCP a související funkce:

- RFC 2131: Dynamic Host Configuration Protocol (starý RFC 1541) 
- RFC 2132: DHCP Options and BOOTP Vendor Extensions 
- RFC 951: The Bootstrap Protocol (BOOTP) 
- RFC 1534: Interoperation Between DHCP and BOOTP 
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol 
- RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE) 

IBM Redbooks

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

Tato publikace popisuje podporu pro server DNS (Domain Name System) server a server DHCP (Dynamic Host Configuration Protocol), která je součástí i5/OS. Informace v této knize vám prostřednictvím obrázků pomohou instalovat, přizpůsobit, konfigurovat a řešit problémy týkající se podpory DNS a DHCP.


Poznámka: Tato kniha nebyla aktualizována a neobsahuje nové funkce BIND 8, včetně dynamických aktualizací, které jsou k dispozici pro verzi V5R1. Pomůže vám ale s celkovou koncepcí DNS a DHCP.

Uložení souborů ve formátu PDF

Pokud chcete uložit soubor PDF na pracovní stanici, abyste si ho mohli prohlédnout nebo vytisknout, postupujte takto:

1. Klepněte pravým tlačítkem myši na soubor ve formátu PDF (klepněte pravým tlačítkem myši na výše uvedený řádek).
2. Klepněte na volbu pro lokální uložení souboru ve formátu PDF.
3. Zadejte cestu do adresáře, ve kterém chcete soubor ve formátu PDF uložit.
4. Klepněte na **Save (Uložit)**.

Stážení aplikace Adobe Reader

- | Chcete-li zobrazit nebo tisknout tyto soubory ve formátu PDF, potřebujete program Adobe Reader. Jeho bezplatnou
- | kopii si můžete stáhnout z webové stránky společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabídnout 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. Použit lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

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

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

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), obraťte se na zastoupení IBM ve Vaší zemi, nebo písemně kontaktujte 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", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řady některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk 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.

Jakékoli 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 jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoli 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 Corporation

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

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

- | IBM poskytuje licencovaný program popsany v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Informace, týkající se produktů jiných firem než IBM, byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy, které se týkají vlastností produktů od jiných dodavatelů, musí být adresovány příslušným dodavatelům.

Veškerá prohlášení týkající se budoucích trendů nebo strategií IBM podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

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.

LICENCE:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které ilustrují programovací techniky na různých operačních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto příklady nebyly důkladně testovány za všech podmínek. IBM proto nezaručuje ani nevyvozuje spolehlivost, obsluhovatelost nebo funkčnost těchto programů.

Každá kopie nebo část těchto vzorových programů nebo odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů od IBM Corporation. © 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

Tato publikace DHCP je určena pro programovací rozhraní umožňující zákazníkovi psát programy za účelem získání služeb operačního systému IBM i5/OS.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA a případně v dalších jiných zemích:

AS/400
e(server)server
eServer
i5/OS
IBM
IBM (logo)
iSeries
OS/2
Redbooks

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

Další jména společností, produktů nebo služeb mohou být ochrannými známkami jiných společností.

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 jakékoli 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 jakékoli 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 NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.



Vytištěno v Dánsku společností IBM Danmark A/S.