System i

Praca w sieci
Protokół DHCP

Wersja 6 wydanie 1

System i

Praca w sieci
Protokół DHCP

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 53.

| To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także
| wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na
| wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Protokół DHCP (Dynamic Host Configuration Protocol)

Protokół DHCP jest standardem w ramach TCP/IP, który przewiduje używanie centralnego serwera do zarządzania adresami IP i innymi danymi konfiguracyjnymi na potrzeby całej sieci.

Serwer DHCP odpowiada na żądania klientów i dynamicznie przypisuje im odpowiednie parametry.

Plik PDF z informacjami dotyczącymi DHCP

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby przejrzeć lub pobrać dokument w formacie PDF, wybierz DHCP (około 1399 kB).

Zapisywanie plików PDF

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

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Odsyłacze pokrewne

“Informacje pokrewne dotyczące DHCP” na stronie 52
Informacje powiązane z kolekcją tematów dotyczących DHCP znajdują się w dokumentacji technicznej IBM (Redbooks) oraz w serwisach WWW. Wszystkie pliki PDF można wyświetlić lub wydrukować.

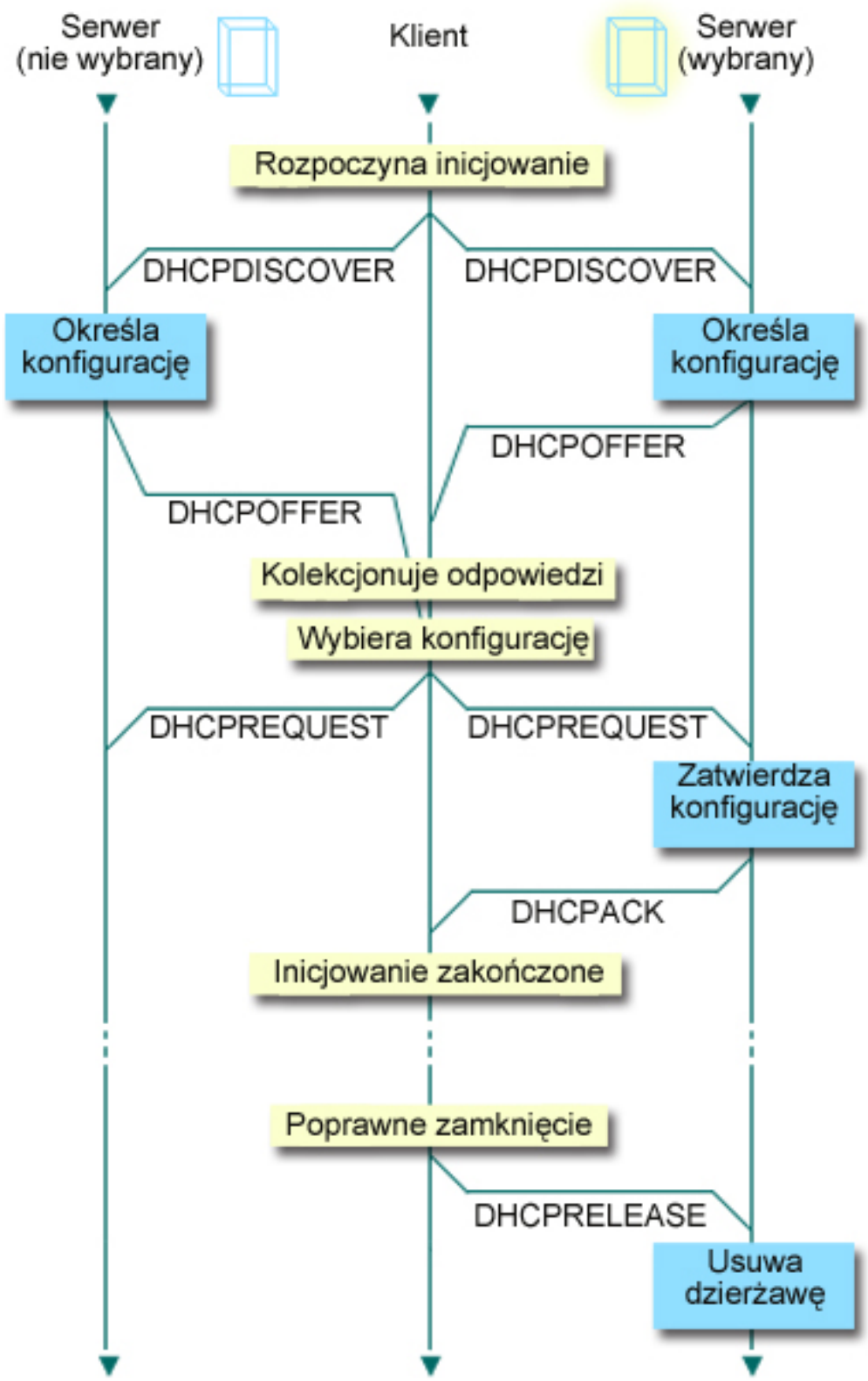
Zasada działania usług DHCP

Protokół DHCP (Dynamic Host Configuration Protocol) zapewnia automatyczne, dynamiczne konfigurowanie klientów. Zamieszczono tutaj kilka podstawowych pojęć dotyczących usług DHCP w celu wyjaśnienia ich działania.

Interakcja między klientem a serwerem DHCP

Interakcja między klientami a serwerami DHCP pozwala klientom na uzyskiwanie od serwera DHCP adresu IP i odpowiednich informacji o konfiguracji.

Proces ten odbywa się w kilku etapach przedstawionych na poniższym rysunku.



Rysunek 1. Interakcja między klientem a serwerem DHCP

Klient wysyła żądanie danych DHCP: DHCPDISCOVER

Najpierw klient wysyła komunikat DHCPDISCOVER z żądaniem adresu IP. Komunikat DHCPDISCOVER zawiera jednoznaczny identyfikator klienta (zazwyczaj jest to adres MAC). Komunikat może zawierać także

żądania dotyczące innych opcji, na przykład maski podsieci, serwera nazw domen, nazwy domeny lub trasy statycznej. Komunikat jest wysyłany w formie rozgłoszenia. Jeśli sieć zawiera routery, to ich konfiguracja może przewidywać przekazywanie pakietów DHCPDISCOVER serwerom DHCP w sąsiednich sieciach.

Serwer DHCP wysyła do klienta informacje: DHCPOFFER
Każdy serwer DHCP, który odbierze komunikat DHCPDISCOVER, może w odpowiedzi wysłać komunikat DHCPOFFER. Brak komunikatu DHCPOFFER z serwera DHCP może wynikać z różnych powodów; najczęściej są to: wyczerpanie puli adresów dostępnych do dzierżawy, brak konfiguracji podsieci lub brak obsługi danego klienta. Jeśli serwer DHCP wyśle w odpowiedzi komunikat DHCPOFFER, to będzie on zawierać dostępny adres IP oraz wszelkie inne dane konfiguracyjne, określone w konfiguracji DHCP.

Klient przyjmuje propozycję serwera DHCP: DHCPREQUEST
Klient odbiera komunikaty DHCPOFFER pochodzące z serwerów DHCP, które odpowiedziały na komunikat DHCPDISCOVER. Klient porównuje propozycje z ustawieniami, których dotyczyło pierwotne żądanie, po czym wybiera jeden z serwerów. Wysyła następnie komunikat DHCPREQUEST potwierdzający przyjęcie propozycji i wskazujący wybrany serwer. Komunikat jest rozgłaszany w całej sieci, aby wszystkie serwery DHCP otrzymały informację o tym, który serwer został wybrany.

Serwer DHCP potwierdza transakcję z klientem i dokonuje dzierżawy adresu IP: DHCPACK
Po otrzymaniu komunikatu DHCPREQUEST serwer oznacza dany adres jako wydzierżawiony. Na serwerach, które nie zostały wybrane, proponowane adresy powrócą do puli dostępnych adresów. Wybrany serwer wysyła klientowi potwierdzenie (DHCPACK), zawierające dodatkowe dane konfiguracyjne.

Klient może rozpocząć korzystanie z adresu IP i parametrów konfiguracyjnych. Będzie używać tych ustawień do chwili wygaśnięcia dzierżawy lub do wysłania przez klienta do serwera komunikatu DHCPRELEASE w celu zakończenia dzierżawy.

Klient próbuje odnowić dzierżawę: DHCPREQUEST, DHCPACK
Klient podejmuje próbę odnowienia dzierżawy po upływie połowy okresu jej ważności. Żądanie odnowienia przez klienta polega na wysłaniu do serwera komunikatu DHCPREQUEST. Jeśli serwer przyjmie żądanie, odpowie klientowi przez wysłanie komunikatu DHCPACK. W przypadku braku odpowiedzi od serwera klient może nadal korzystać z adresu IP i pozostałych danych konfiguracyjnych do czasu wygaśnięcia ważności dzierżawy. Dopóki dzierżawa jest aktywna, klient i serwer nie muszą powtarzać procedury wymiany komunikatów DHCPDISCOVER i DHCPREQUEST. Po upłynięciu terminu ważności dzierżawy klient musi na nowo zapoczątkować proces DHCPDISCOVER.

Klient zgłasza zakończenie dzierżawy: DHCPRELEASE
Klient zgłasza zakończenie dzierżawy, wysyłając serwerowi DHCP komunikat DHCPRELEASE. Serwer zwróci adres IP klienta do puli dostępnych adresów.

Pojęcia pokrewne

“Agenty przekazujące i routery” na stronie 5
Do skutecznego i bezpiecznego przesyłania danych w sieci można użyć zarówno agentów przekazujących DHCP, jak i routerów.

“Dzierżawa”
Kiedy serwer DHCP wysyła dane konfiguracyjne do klienta, dane te mają określony czas dzierżawy. Jest to czas korzystania z przypisanego użytkownikowi adresu IP. Czas trwania dzierżawy można zmienić zgodnie z konkretnymi wymaganiami.

Dzierżawa

Kiedy serwer DHCP wysyła dane konfiguracyjne do klienta, dane te mają określony czas dzierżawy. Jest to czas korzystania z przypisanego użytkownikowi adresu IP. Czas trwania dzierżawy można zmienić zgodnie z konkretnymi wymaganiami.

W trakcie dzierżawy serwer DHCP nie może przypisać tego samego adresu IP innemu klientowi. Podstawą koncepcji dzierżawy jest potrzeba ograniczenia czasu, przez który klient będzie używał adresu IP. Ograniczony czas dzierżawy uniemożliwia niepotrzebne zajmowanie adresów IP przez bezczynne klienty w sytuacji, gdy liczba klientów przekracza liczbę dostępnych adresów. Dodatkowo, administrator uzyskuje możliwość wprowadzania zmian w konfiguracji

wszystkich klientów w sieci w ograniczonym czasie. Po upływie terminu ważności dzierżawy klient zażąda odnowienia dzierżawy od serwera DHCP. W przypadku, gdy dane konfiguracyjne uległy zmianie, wraz z odnowieniem dzierżawy klient otrzyma już dane zaktualizowane.

Odnowienie dzierżawy

Klient podejmuje próbę odnowienia dzierżawy po upływie połowy okresu jej ważności. Na przykład, w przypadku dzierżawy na okres 24 godzin klient wyśle żądanie odnowienia dzierżawy po 12 godzinach. Żądanie odnowienia przez klienta polega na wysłaniu do serwera komunikatu DHCPREQUEST. Komunikat z żądaniem odnowienia dzierżawy zawiera informacje o bieżącym adresie IP i danych konfiguracyjnych klienta.

Jeśli serwer przyjmie żądanie, odpowie klientowi przez wysłanie komunikatu DHCPACK. W przypadku braku odpowiedzi z serwera, klient może nadal korzystać z adresu IP i pozostałych danych konfiguracyjnych do czasu wygaśnięcia ważności dzierżawy. Tak długo, jak dzierżawa jest aktywna, klient i serwer nie muszą powtarzać procedury wymiany komunikatów DHCPDISCOVER i DHCPREQUEST. Po upłynięciu terminu ważności dzierżawy klient musi na nowo zapoczątkować proces DHCPDISCOVER.

Jeśli serwer nie jest dostępny, klient może nadal korzystać z przypisanego mu adresu aż do wygaśnięcia dzierżawy. W poprzednim przykładzie klient może używać adresu przez 12 godzin po pierwszej próbie odnowienia dzierżawy. W trakcie 12-godzinnej przerwy w pracy serwera użytkownicy nie mogą uzyskiwać nowych dzierżaw, jednocześnie wszystkie dzierżawy wydane komputerom włączonym na początku przerwy w pracy, nie ulegną wygaśnięciu.

Określanie czasu trwania dzierżawy

Domyślny czas dzierżawy dla serwera DHCP wynosi 24 godziny. Przy ustawianiu czasu dzierżawy należy rozważyć cel, jaki ma zostać osiągnięty, sposób i harmonogram pracy danej sieci oraz zasady obsługi serwisowej danego serwera DHCP. Odpowiedź na poniższe pytania może pomóc w dobraniu odpowiedniego czasu dzierżawy w konkretnej sytuacji.

Czy w sieci jest więcej użytkowników niż adresów?
Jeśli tak, to czas dzierżawy powinien być krótki, aby zapewnić minimalny okres oczekiwania na zakończenie dzierżaw, które nie są używane.

Czy da się określić minimalny niezbędny czas dzierżawy?
Jeśli typowy użytkownik przebywa w sieci przynajmniej przez godzinę, czas dzierżawy powinien wynosić minimum godzinę.

Czy dana sieć pozwala obsłużyć intensywny ruch komunikatów DHCP?
Ruch w sieci przy przepływie pakietów DHCP może stanowić problem w przypadku sieci z dużą liczbą klientów lub sieci o niewielkiej przepustowości. Im krótszy czas dzierżawy, tym większe obciążenie dla serwera i dla łączy sieciowych, wynikające z częstszego zgłaszania żądań odnowienia dzierżawy.

Jak wygląda obsługa serwisowa urządzeń sieciowych i do jakiego stopnia sieć jest odporna na przerwy w pracy?
Należy rozważyć czas trwania rutynowych czynności konserwacyjnych oraz potencjalny wpływ przerwy w pracy serwera na działanie sieci. Jeśli czas dzierżawy jest przynajmniej dwukrotnie dłuższy niż przerwa konserwacyjna w pracy serwera, dzierżawy istniejące w chwili wyłączenia serwera nie zostaną utracone. Aby uniknąć problemów, należy ustalić, ile maksymalnie może trwać rutynowe wyłączenie serwera.

W jakiego typu środowisku sieciowym działa serwer DHCP? Do czego używany jest typowy klient?
Należy się zastanowić nad rodzajem prac wykonywanych zwykle przez klientów w sieci obsługiwanej przez serwer DHCP. Na przykład, w środowisku klientów o dużej mobilności, którzy łączą się z siecią o różnych porach dnia i sprawdzają swoją pocztę zwykle tylko raz lub dwa razy dziennie, wystarczający będzie krótki czas dzierżawy. W takim przypadku zazwyczaj nie jest konieczne rezerwowanie odrębnego adresu IP dla każdego klienta. Dzięki ograniczeniu czasu dzierżawy, można obsłużyć większą liczbę mobilnych klientów za pomocą mniejszej puli adresów IP.

Jako inny przykład można rozważyć środowisko biurowe, w którym większość pracowników korzysta ze stacjonarnych stacji roboczych. W tym przypadku bardziej stosowny będzie czas dzierżawy o długości 24 godzin. W takim środowisku może być konieczne utrzymanie adresów IP dla poszczególnych klientów tak

długo, aby umożliwić połączenie z siecią w godzinach pracy. Ponadto, zdefiniowanie krótszego czasu dzierżawy spowodowałoby znacznie częstsze negocjowanie odnowienia dzierżawy przez serwer DHCP i w konsekwencji niepotrzebne obciążenie sieci.

Na ile często konfiguracja sieci ulega zmianom?

Jeśli topologia sieci zmienia się często, należy unikać stosowania zbyt długich czasów dzierżawy. Długi czas dzierżawy stwarza problemy, gdy zachodzi potrzeba zmiany jakiegoś parametru konfiguracji. Źle dobrany czas dzierżawy może powodować, że zamiast odczekać pewien czas na odnowienie wszystkich dzierżaw, konieczne będzie ponowne uruchomienie każdego klienta, którego konfiguracja powinna ulec zmianie.

W sieciach, gdzie topologia raczej nie ulega zmianie, a pula adresów IP jest dostatecznie duża, można rozważyć skonfigurowanie dzierżawy DHCP na czas nieograniczony, czyli wprowadzenia dzierżawy bezterminowej. Jednak dzierżawy na czas nieograniczony nie są zalecane. Taka konfiguracja oznacza w praktyce trwałe przypisanie adresu IP do klienta. Po otrzymaniu adresu klient nie musi już starać się o odnowienie dzierżawy. Po przypisaniu klientowi dzierżawy bezterminowej, dany adres IP nie może już być przypisany innemu klientowi. Dlatego mogą wystąpić problemy, gdy trzeba będzie przypisać klientowi nowy adres IP lub przypisać adres IP klienta innemu klientowi.

W sieci mogą funkcjonować klienty, które zawsze powinny otrzymywać taki sam adres IP. Przykładem może być serwer plików. Zamiast stosowania dzierżawy bezterminowej, właściwym sposobem postępowania będzie przypisanie temu klientowi określonego adresu IP z długim czasem dzierżawy. Klient nadal korzysta z dzierżawy o ograniczonym czasie trwania i musi ją okresowo odnawiać, lecz serwer DHCP zarezerwuje na jego potrzeby jeden stały adres IP. W przypadku uruchomienia nowego serwera plików wystarczy zmienić identyfikator klienta (adres MAC), a serwer zacznie przypisywać ten sam adres nowemu serwerowi plików. Gdyby zastosowano dzierżawę bezterminową, serwer DHCP nie mógłby przypisać adresu innemu klientowi, chyba że dzierżawa zostałaby usunięta przez administratora.

Pojęcia pokrewne

“Informacje o topologii sieci” na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

Odsyłacze pokrewne

“Interakcja między klientem a serwerem DHCP” na stronie 1
Interakcja między klientami a serwerami DHCP pozwala klientom na uzyskiwanie od serwera DHCP adresu IP i odpowiednich informacji o konfiguracji.

Agenty przekazujące i routery

Do skutecznego i bezpiecznego przesyłania danych w sieci można użyć zarówno agentów przekazujących DHCP, jak i routerów.

Początkowo klienty DHCP rozgłaszają w sieci pakiety DHCPDISCOVER, ponieważ nie dysponują żadnymi informacjami na temat sieci, do której są podłączone. W niektórych sieciach serwer DHCP może nie znajdować się w obrębie tej samej sieci LAN, co klient. Dlatego niezbędne staje się przekazywanie rozgłoszonych pakietów DHCP do sieci, w której działa serwer DHCP. Niektóre routery mają konfigurację, która pozwala na przekazywanie pakietów DHCP. Jeśli dany router obsługuje przekazywanie pakietów DHCP, to przekazuje on pakiety DHCP do sieci LAN, w której działa serwer DHCP. Jednak wiele routerów nie przekazuje pakietów, których docelowy adres IP jest adresem rozgłoszeniowym (takich jak pakiety DHCP). W takim przypadku w sieci LAN musi działać agent przekazujący BOOTP/DHCP, odpowiedzialny za przekazywanie pakietów DHCP do sieci, w której działa serwer DHCP. Przykładowa sieć używająca agenta przekazywania i routera jest zamieszczona w sekcji “Przykład: profile DHCP i PPP na różnych serwerach System i” na stronie 36.

Ponieważ serwer DHCP znajduje się w odrębnej sieci, w obu sytuacjach klienty muszą mieć adres IP routera łączącego sieć klientów z siecią, w której działa serwer DHCP określony w opcji routera (opcja 3).

Jeśli agent przekazujący BOOTP/DHCP nie jest używany, obsługę klientów może zapewnić tylko dodatkowy serwer DHCP podłączony do tej samej sieci. W sekcji “Informacje o topologii sieci” na stronie 39 znajdują się informacje, które pomogą w ustaleniu wymaganej liczby serwerów DNS w sieci.

Pojęcia pokrewne

“Informacje o topologii sieci” na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

Zadania pokrewne

“Konfigurowanie serwera DHCP i agenta przekazującego BOOTP/DHCP” na stronie 42
Informacje z tej sekcji dotyczą konfigurowania, uruchamiania i zatrzymywania serwera DHCP oraz agenta przekazującego BOOTP/DHCP.

Odsyłacze pokrewne

“Interakcja między klientem a serwerem DHCP” na stronie 1
Interakcja między klientami a serwerami DHCP pozwala klientom na uzyskiwanie od serwera DHCP adresu IP i odpowiednich informacji o konfiguracji.

Obsługa klientów DHCP

Za pomocą serwera DHCP można zarządzać poszczególnymi klientami w sieci zamiast zarządzać wszystkimi klientami traktowanymi jak wielka grupa (podsieć).

Dzięki tej metodzie tylko klienty rozpoznawane przez serwer DHCP mogą otrzymać adres IP i dane konfiguracyjne.

Zazwyczaj usługa DHCP jest wdrażana z myślą o dysponowaniu pulą adresów IP i ich przypisywaniu klientom w podsieci. Gdy używana jest podsieć, każdy klient żądający od sieci danych DHCP może otrzymać adres IP pochodzący z puli adresów, chyba że klient ten zostanie jawnie wykluczony przez administratora DHCP. Jednak serwer DHCP może również ograniczyć zakres usług DHCP tylko do określonych klientów.

Serwer DHCP pozwala ograniczyć zakres usług zarówno na poziomie indywidualnych klientów, jak i w zależności od typu klienta (BOOTP lub DHCP).

Aby ograniczyć usługi na poziomie poszczególnych klientów, należy w konfiguracji DHCP określić dane każdego z klientów w sieci. Każdy klient jest rozpoznawany na podstawie identyfikatora (zwykle adresu MAC). Adresy IP i dodatkowe opcje konfiguracyjne będą przekazywane tylko klientom wprost wskazanym w konfiguracji serwera DHCP. Jeśli dany klient nie figuruje na liście konfiguracyjnej DHCP, serwer nie będzie obsługiwał jego żądań. Taka metoda postępowania uniemożliwia nieznanym hostom uzyskiwanie z serwera DHCP adresów IP i innych danych konfiguracyjnych.

W sytuacji gdy wymagany jest jeszcze wyższy poziom kontroli nad klientami w sieci oraz ich konfiguracją, usługę DHCP można skonfigurować w taki sposób, aby każdy klient miał przypisywany statyczny adres IP zamiast przypadkowych adresów pobieranych z puli. W takim przypadku powinno istnieć obustronnie jednoznaczne przyporządkowanie adresów statycznych do poszczególnych klientów, aby uniknąć sytuacji, w której dwa klienty otrzymają jednakowy adres IP. Dynamiczna alokacja adresów oznacza, że przypisywaniem adresów IP klientom steruje serwer DHCP.

Na poziomie bardziej ogólnym serwer DHCP może ograniczać swoje usługi na podstawie typu klienta (BOOTP lub DHCP). Serwer DHCP może odrzucać zgłoszenia klientów BOOTP.

Pojęcia pokrewne

“BOOTP” na stronie 7
Protokół BOOTP (Bootstrap Protocol) jest protokołem konfiguracji hosta, używanym przed wprowadzeniem protokołu DHCP. Obsługa protokołu BOOTP stanowi podzbiór obsługi protokołu DHCP.

“Informacje o topologii sieci” na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

BOOTP

Protokół BOOTP (Bootstrap Protocol) jest protokołem konfiguracji hosta, używanym przed wprowadzeniem protokołu DHCP. Obsługa protokołu BOOTP stanowi podzbiór obsługi protokołu DHCP.

Klient BOOTP jest identyfikowany na podstawie adresu MAC i otrzymuje określony adres IP. Zasadniczo każdy klient w sieci ma przypisany adres IP. Protokół BOOTP nie przewiduje dynamicznego przypisywania adresów -- w konfiguracji BOOTP musi być zapis identyfikujący każdego klienta w sieci. Ponadto zakres danych konfiguracyjnych otrzymywanych przez klienty z serwera BOOTP jest ograniczony.

Jako że protokół DHCP bazuje na protokole BOOTP, serwer DHCP może obsługiwać klienty BOOTP. Jeśli w sieci jest używany protokół BOOTP, to możliwe jest zainstalowanie i skonfigurowanie protokołu DHCP w sposób niezauważalny dla klientów BOOTP. Aby zapewnić obsługę klientów BOOTP, należy określić adres IP serwera startowego oraz opcję nazwy pliku startowego (opcja 67), a ponadto włączyć obsługę protokołu BOOTP dla całego serwera lub dla poszczególnych podsieci.

Obsługa klientów BOOTP przez serwer DHCP jest lepszym rozwiązaniem niż korzystanie z serwera BOOTP. Obsługa klientów BOOTP przez serwer DHCP polega zasadniczo na przypisaniu każdemu klientowi BOOTP określonego adresu IP, który przestaje być dostępny dla innych klientów. Użycie serwera DHCP ma jednak pewną zaletę: nie ma potrzeby konfigurowania jednoznacznego odwzorowania klientów BOOTP na adresy IP. Serwer DHCP nadal będzie dynamicznie przypisywał adresy IP z puli klientom BOOTP. Kiedy już adres IP zostanie przypisany klientowi BOOTP, adres ten pozostaje na stałe zarezerwowany dla tego klienta, chyba że rezerwacja zostanie usunięta przez administratora. Inną metodą postępowania jest konwersja klientów BOOTP na DHCP, co zapewnia większą kontrolę nad procesem konfiguracji hostów.

Pojęcia pokrewne

"Obsługa klientów DHCP" na stronie 6
Za pomocą serwera DHCP można zarządzać poszczególnymi klientami w sieci zamiast zarządzać wszystkimi klientami traktowanymi jak wielka grupa (podsieć).

BOOTP

"Informacje o topologii sieci" na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

Dynamiczne aktualizacje

Można skonfigurować serwer DHCP w taki sposób, aby pracował z serwerem DNS w celu dynamicznego aktualizowania danych DNS klientów po przypisaniu adresu IP przez DHCP.

DNS to system rozproszonej bazy danych służący do zarządzania nazwami hostów i przypisanymi im adresami protokołu IP. DNS pozwala użytkownikom na znajdowanie hostów za pomocą prostych nazw, takich jak www.przyklad.com, bez potrzeby stosowania adresów IP (xxx.xxx.xxx.xxx).

W przeszłości wszystkie dane DNS były przechowywane w statycznych bazach danych. Wszystkie rekordy zasobów DNS musiały być tworzone i modyfikowane przez administratora. Obecnie serwery DNS działające pod kontrolą programu BIND 8 mogą być konfigurowane w taki sposób, aby przyjmowały żądania dynamicznej aktualizacji danych strefy z innych źródeł.

Serwer DHCP można skonfigurować w taki sposób, aby wysyłał do serwera DNS żądania aktualizacji po każdym przypisaniu hostowi nowego adresu. Ten zautomatyzowany proces pozwala zmniejszyć pracochłonność administrowania serwerem DNS w szybko rozrastających się lub zmieniających sieciach TCP/IP oraz w sieciach, w których często zmieniają się położenia hostów. Gdy klient DHCP otrzyma adres IP, informacja o tym adresie jest natychmiast przekazywana do serwera DNS. Dzięki temu serwer DNS może prawidłowo odczytywać nazwy hostów, nawet jeśli ich adresy IP nie są stałe.

Konfiguracja serwera DHCP może przewidywać aktualizowanie w imieniu klienta rekordów odwzorowania adresów (A), rekordów wskaźników wyszukiwania zwrotnego (PTR) lub obu tych typów rekordów. Rekord typu A pozwala

odwzorować nazwę DNS klienta na jego adres IP. Rekord typu PTR odwzorowuje adres IP hosta na jego nazwę. Kiedy adres klienta ulega zmianie, serwer DHCP może automatycznie wysłać aktualizację do serwera DNS, dzięki czemu inne hosty w sieci będą mogły znaleźć klienta pod jego nowym adresem IP za pośrednictwem zapytań DNS. Dla każdego dynamicznie aktualizowanego rekordu zapisywany jest również powiązany rekord tekstowy (TXT), który wskazuje na aktualizację przez serwer DHCP.

Uwaga: Jeśli konfiguracja DHCP przewiduje aktualizowanie tylko rekordów PTR, konfiguracja serwera DNS powinna dopuszczać aktualizacje inicjowane przez klienty, aby każdy klient mógł zaktualizować odpowiadający mu rekord A.

Strefy dynamiczne są zabezpieczane za pośrednictwem listy źródeł upoważnionych do zgłaszania żądań aktualizacji rekordów. Przed wprowadzeniem zmian w rekordzie serwer DNS sprawdza, czy pakiet zgłoszenia nadszedł z uprawnionego źródła.

Dynamiczne aktualizacje między DNS a DHCP mogą być wykonywane w ramach pojedynczego serwera System i, między różnymi serwerami System i lub między serwerami innego typu, które obsługują dynamiczną aktualizację.

Pojęcia pokrewne

System DNS

"Informacje o topologii sieci" na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

"Problem: rekordy DNS nie są aktualizowane przez DHCP" na stronie 50
Serwer DHCP System i umożliwia dynamiczne aktualizowanie rekordów DNS. Podczas wybierania właściwego serwera DNS do aktualizacji serwer DHCP korzysta z interfejsów programistycznych i funkcji tłumaczenia nazw. Można użyć tych informacji podczas rozwiązywania problemów wynikających z dynamicznego aktualizowania.

Zadania pokrewne

"Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS" na stronie 46
Serwer DHCP można skonfigurować w taki sposób, aby wysyłał do serwera DNS żądania aktualizacji po każdym przypisaniu hostowi nowego adresu. Ten zautomatyzowany proces pozwala zmniejszyć pracochłonność administrowania serwerem DNS w szybko rozrastających się lub zmieniających sieciach TCP/IP oraz w sieciach, w których często zmieniają się położenia hostów.

Konfigurowanie odbierania dynamicznych aktualizacji przez serwer DNS

Odsyłacze pokrewne

Rekordy zasobu systemu DNS

Wyszukiwanie opcji DHCP

Protokół DHCP ma wiele opcji konfiguracji, które mogą być przesyłane z serwera DHCP do klientów w odpowiedzi na ich żądania. Do wyświetlenia wszystkich opcji DHCP można użyć narzędzia wyszukiwania.

Opcje DHCP określają dodatkowe dane konfiguracyjne, które serwer DHCP przekazuje klientom razem z adresem IP. Zwykle opcje te obejmują maskę podsieci, nazwę domeny, adres IP routera, adresy IP serwerów nazw domen oraz trasy statyczne.

W poniższej tabeli znajduje się opis standardowych opcji DHCP, zgodnych z treścią dokumentu RFC 2132: DHCP Options and BOOTP Vendor Extensions. Można także skonfigurować opcje dostosowane, używając ekranu opcji DHCP programu System i Navigator.

Tabela 1. Standardowe opcje DHCP

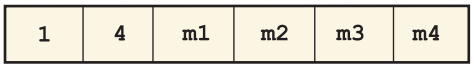
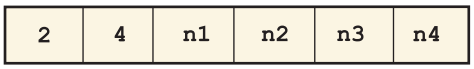
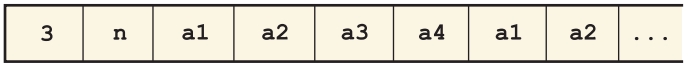
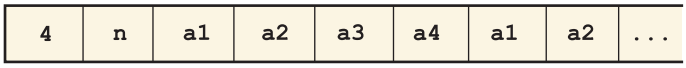
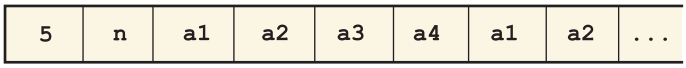
Numer opcji	Opcja	Opis
1	Maska podsieci	Opcja maski podsieci określa maskę podsieci klienta zgodnie z dokumentem RFC 950. Jeśli w odpowiedzi serwera DHCP zostały określone zarówno maska podsieci, jak i router, to maska podsieci musi występować pierwsza. Kod dla opcji maski podsieci to 1, a jej długość to 4 oktety. **Kod Dł. Maska podsieci**  RZAKG530-0
2	Przesunięcie czasu	Pole przesunięcia czasu określa w sekundach przesunięcie podsieci klienta względem czasu uniwersalnego. Przesunięcie jest wyrażane w postaci dwóch dopełniających się 32-bitowych liczb całkowitych. Przesunięcie dodatnie określa położenie na wschód względem południka zerowego, a przesunięcie ujemne określa położenie na zachód od południka zerowego. Kod dla opcji przesunięcia czasu to 2, a jej długość to 4 oktety. **Kod Dł. Przesunięcie czasu**  RZAKG531-0
3	Router	Opcja routera określa listę adresów IP dla routerów w podsieci klienta. Routery należy określić w preferowanym porządku. Kodem opcji routera jest 3. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  RZAKG511-0
4	Serwer czasu	Opcja serwera czasu określa listę serwerów czasu RFC 868 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera czasu jest 4. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  RZAKG512-0
5	Serwer nazw	Opcja serwera nazw określa listę serwerów nazw IEN 116 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera nazw jest 5. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  RZAKG513-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
6	Serwer DNS	Opcja serwera DNS określa listę serwerów DNS (STD 13, RFC 1035) dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera DNS jest 6. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 6 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG514-0
7	Serwer protokołu	Opcja serwera protokołu określa listę serwerów protokołu MIT-LCS UDP dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera protokołu jest 7. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 7 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG515-0
8	Serwer informacji cookie	Opcja serwera informacji cookie określa listę serwerów informacji cookie RFC 865 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera informacji cookie jest 8. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 8 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG516-0
9	Serwer LPR	Opcja serwera LPR określa listę serwerów LPR RFC 1179 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera LPR jest 9. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 9 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG517-0
10	Serwer Impress	Opcja serwera Impress określa listę serwerów Imagen Impress dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera Impress jest 10. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 10 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG518-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
11	Serwer wyszukiwania zasobów	Ta opcja określa listę serwerów wyszukiwania zasobów RFC 887 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem tej opcji jest 11. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 11 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG519-0
12	Nazwa hosta	Ta opcja określa nazwę klienta. Nazwa może, ale nie musi być kwalifikowana z nazwą domeny lokalnej (patrz sekcja 3.17, aby uzyskać informacje dotyczące preferowanego sposobu pobierania nazwy domeny). Informacje dotyczące ograniczeń znaków znajdują się w dokumencie RFC 1035. Kodem tej opcji jest 12, a jej minimalna długość to 1. **Kod Dł. Nazwa hosta** 12 | n | h1 | h2 | h3 | h4 | h5 | h6 | ... RZAKG520-0
13	Wielkość zbioru startowego	Ta opcja określa długość w blokach składających się z 512 oktetów domyślnego kodu startowego klienta. Długość zbioru jest określana jako 16-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 13, a jej długość to 2. **Kod Dł. Wielkość zbioru** 13 | 2 | 11 | 12 RZAKG541-0
14	Zbiór zrzutu	Ta opcja określa nazwę ścieżki zbioru, w którym jest umieszczany zrzut obrazu rdzenia klienta w przypadku awarii klienta. Ścieżką jest łańcuch składający się ze znaków z zestawu znaków ASCII NVT. Kodem tej opcji jest 14. Minimalna długość to 1. **Kod Dł. Ścieżka pliku zrzutu** 14 | n | n1 | n2 | n3 | n4 | ... RZAKG521-0
15	Nazwa domeny	Ta opcja określa nazwę domeny, której klient powinien używać podczas rozpoznawania nazw hostów za pośrednictwem DNS. Kodem tej opcji jest 15. Minimalna długość to 1. **Kod Dł. Nazwa domeny** 15 | n | d1 | d2 | d3 | d4 | ... RZAKG522-0
16	Serwer wymiany	Ta opcja określa adres IP serwera wymiany klienta. Kodem tej opcji jest 16, a jej długość to 4. **Kod Dł. Adres serwera wymiany** 16 | n | a1 | a2 | a3 | a4 RZAKG523-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
17	Ścieżka główna	Ta opcja określa nazwę ścieżki zawierającą główny dysk klienta. Ścieżką jest łańcuch składający się ze znaków z zestawu znaków ASCII NVT. Kodem tej opcji jest 17. Minimalna długość to 1. **Kod Dł. Ścieżka główna** 17 | n | n1 | n2 | n3 | n4 | ... RZAKG524-0
18	Ścieżka rozszerzeń	Łańcuch określający zbiór, do pobrania za pośrednictwem TFTP, zawierający informacje, które mogą być interpretowane w ten sam sposób, co 64-oktetowe pole rozszerzenia dostawcy w odpowiedzi BOOTP, z następującymi ograniczeniami: • Długość zbioru jest nieograniczona. • Wszystkie odniesienia do Tag 18 (instancje pola ścieżki rozszerzeń BOOTP) w zbiorze są ignorowane. Kodem tej opcji jest 18. Minimalna długość to 1. **Kod Dł. Ścieżka rozszerzeń** 18 | n | n1 | n2 | n3 | n4 | ... RZAKG525-0
19	Przekazywanie IP	Ta opcja określa, czy klient powinien konfigurować swoją warstwę IP do przekazywania pakietów. Wartość 0 oznacza wyłączenie przekazywania IP, a wartość 1 oznacza włączenie przekazywania IP. Kodem tej opcji jest 19, a jej długość to 1. **Kod Dł. Wartość** 19 | 1 | 0/1 RZAKG544-0
20	Nielokalny routing źródłowy	Ta opcja określa, czy klient powinien konfigurować swoją warstwę IP do przekazywania datagramów z nielokalnymi trasami źródłowymi. Wartość 0 oznacza uniemożliwienie przekazywania takich datagramów, a wartość 1 oznacza umożliwienie przekazywania takich datagramów. Kodem tej opcji jest 20, a jej długość to 1. **Kod Dł. Wartość** 20 | 1 | 0/1 RZAKG545-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
21	Filtr strategii	Ta opcja określa filtry strategii dla nielokalnego routingu źródłowego. Filtry zawierają listę adresów IP i masek określających pary adres docelowy/maska używane do filtrowania przychodzących tras źródłowych. Klient powinien usunąć wszystkie datagramy routingu źródłowego, których adres następnego przeskoku nie może zostać dopasowany do żadnego z filtrów. Kodem tej opcji jest 21. Minimalna długość tej opcji to 8 i zawsze musi być wielokrotnością liczby 8. **Kod Dł. Adres 1 Maska 1** 21 | n | a1 | a2 | a3 | a4 | m1 | m2 | m3 | m4 **Adres 2 Maska 2** a1 | a2 | a3 | a4 | m1 | m2 | m3 | m4 | ... RZAKG510-0
22	Maksymalna wielkość reasemblacji datagramu	Ta opcja określa maksymalną wielkość datagramu, który może być reasemblowany przez klienta. Wielkość jest określana jako 16-bitowa liczba całkowita bez znaku. Minimalna poprawna wartość to 576. Kodem tej opcji jest 22, a jej długość to 2. **Kod Dł. Wielkość** 22 | 2 | s1 | s2 RZAKG542-0
23	Domyślny czas życia datagramu IP	Ta opcja określa domyślny czas życia używany przez klienta dla wychodzących datagramów. Wartość TTL jest oktetem z zakresu od 1 do 255. Kodem tej opcji jest 23, a jej długość to 1. **Kod Dł. TTL** 23 | 1 | ttl RZAKG546-0
24	Limit czasu starzenia jednostki MTU dla ścieżki	Ta opcja określa limit czasu (w sekundach) starzenia wartości jednostek MTU wykrytych przez mechanizm zdefiniowany w dokumencie RFC 1191. Limit czasu jest określany jako 32-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 24, a jej długość to 4. **Kod Dł. Limit czasu** 24 | 4 | t1 | t2 | t3 | t4 RZAKG532-0
25	Tabela stałych jednostek MTU dla ścieżki	Ta opcja określa tabelę wielkości jednostek MTU używanych podczas wykrywania jednostek MTU ścieżki, jak zdefiniowano w dokumencie RFC 1191. Tabela ma postać listy 16-bitowych liczb całkowitych bez znaku ułożonych w porządku od najmniejszej do największej. Minimalna wartość jednostki MTU nie może być mniejsza niż 68. Kodem tej opcji jest 25. Minimalna długość to 2 i zawsze musi być wielokrotnością liczby 2. **Kod Dł. Wielkość 1 Wielkość 2** 25 | n | s1 | s2 | s1 | s2 | ... RZAKG526-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

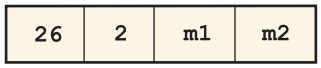
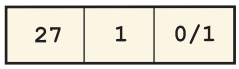
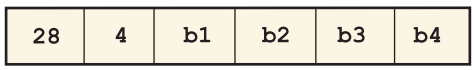
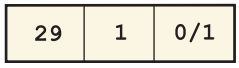
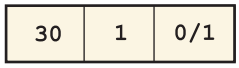
Numer opcji	Opcja	Opis
26	Jednostka MTU interfejsu	Ta opcja określa jednostkę MTU używaną dla tego interfejsu. Jednostka MTU jest określana jako 16-bitowa liczba całkowita bez znaku. Minimalna poprawna wartość jednostki MTU to 68. Kodem tej opcji jest 26, a jej długość to 2. **Kod Dł. MTU**  RZAKG543-0
27	Wszystkie podsieci są lokalne	Ta opcja określa, czy klient może przyjąć, że wszystkie podsieci sieci IP, z którymi klient jest połączony, używają tej samej jednostki MTU, co podsieć tej sieci, do której klient jest bezpośrednio podłączony. Wartość 1 wskazuje, że wszystkie podsieci współużytkują tę samą jednostkę MTU. Wartość 0 oznacza, że klient powinien przyjąć, że niektóre podsieci bezpośrednio podłączonej sieci mogą mieć mniejsze jednostki MTU. Kodem tej opcji jest 27, a jej długość to 1. **Kod Dł. Wartość**  RZAKG547-0
28	Adres rozgłaszania	Ta opcja określa adres rozgłaszania używany w podsieci klienta. Poprawne wartości dla adresów rozgłaszania są określone w sekcji 3.2.1.3 dokumentu RFC 2132. Kodem tej opcji jest 28, a jej długość to 4. **Kod Dł. Adres rozgłaszania**  RZAKG533-0
29	Wykrywanie routera	Ta opcja określa, czy klient powinien wykrywać maskę przy użyciu protokołu ICMP. Wartość 0 wskazuje, że klient nie powinien wykrywać maski. Wartość 1 oznacza, że klient powinien wykrywać maskę. Kodem tej opcji jest 29, a jej długość to 1. **Kod Dł. Wartość**  RZAKG548-0
30	Dostawca maski	Ta opcja określa, czy klient powinien odpowiadać na żądania maski podsieci przy użyciu protokołu ICMP. Wartość 0 wskazuje, że klient nie powinien odpowiadać. Wartość 1 oznacza, że klient powinien odpowiadać. Kodem tej opcji jest 30, a jej długość to 1. **Kod Dł. Wartość**  RZAKG549-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
31	Wykonaj wykrywanie routera	Ta opcja określa, czy klient powinien ubiegać się o routery przy użyciu mechanizmu wykrywania routerów zdefiniowanego w dokumencie RFC 1256. Wartość 0 wskazuje, że klient nie powinien wykrywać routerów. Wartość 1 oznacza, że klient powinien wykrywać routery. Kodem tej opcji jest 31, a jej długość to 1. **Kod Dł. Wartość** **31 1 0/1** RZAKG550-0
32	Adres wysyłania żądań ubiegania się o router	Ta opcja określa adres, pod który klient powinien przesyłać żądania ubiegania się o router. Kodem tej opcji jest 32, a jej długość to 4. **Kod Dł. Adres** **32 4 a1 a2 a3 a4** RZAKG534-0
33	Trasa statyczna	Ta opcja określa listę tras statycznych, które klient powinien zainstalować w swojej pamięci podręcznej routingu. Jeśli określono wiele tras do tego samego miejsca docelowego, te trasy są wyświetlone według ich priorytetu w porządku malejącym. Trasy składają się z listy par adresów IP. Pierwszy adres jest adresem docelowym, a drugi jest adresem routera kierującego do miejsca docelowego. Trasa domyślna (0.0.0.0) jest nieprawidłowym miejscem docelowym trasy statycznej. Kodem tej opcji jest 33. Minimalna długość tej opcji to 8 i zawsze musi być wielokrotnością liczby 8. **Kod Dł. Miejsce docelowe 1 Router 1** **33 n d1 d2 d3 d4 r1 r2 r3 r4** **Miejsce docelowe 2 Router 2** **d1 d2 d3 d4 r1 r2 r3 r4 ...** RZAKG509-0
34	Hermetyzacja końcówek	Ta opcja określa, czy klient powinien negocjować użycie końcówek (RFC 893) podczas używania protokołu ARP. Wartość 0 wskazuje, że klient nie powinien próbować używać końcówek. Wartość 1 wskazuje, że klient powinien próbować używać końcówek. Kodem tej opcji jest 34, a jej długość to 1. **Kod Dł. Wartość** **34 1 0/1** RZAKG573-0
35	Limit czasu pamięci podręcznej protokołu ARP	Ta opcja określa limit czasu w sekundach dla pozycji pamięci podręcznej ARP. Czas jest określany jako 32-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 35, a jej długość to 4. **Kod Dł. Czas** **35 4 t1 t2 t3 t4** RZAKG535-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

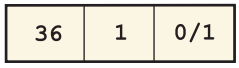
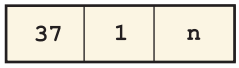
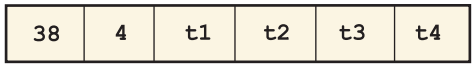
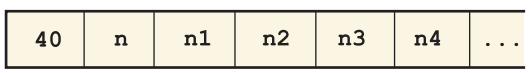
Numer opcji	Opcja	Opis
36	Hermetyzacja Ethernet	Ta opcja określa, czy klient powinien używać hermetyzacji Ethernet w wersji 2 (RFC 894) lub IEEE 802.3 (RFC 1042), jeśli interfejsem jest Ethernet. Wartość 0 wskazuje, że klient powinien używać hermetyzacji RFC 894. Wartość 1 wskazuje, że klient powinien używać hermetyzacji RFC 1042. Kodem tej opcji jest 36, a jej długość to 1. **Kod Dł. Wartość**  RZAKG551-0
37	Wartość domyślna TTL protokołu TCP	Ta opcja określa wartość domyślną TTL, której klient powinien używać podczas wysyłania segmentów TCP. Wartość jest reprezentowana jako 8-bitowa liczba całkowita bez znaku. Wartością minimalną jest 1. Kodem tej opcji jest 37, a jej długość to 1. **Kod Dł. TTL**  RZAKG552-0
38	Interwał utrzymania aktywności TCP	Ta opcja określa interwał (w sekundach) oczekiwania klienta TCP przed wysłaniem komunikatu o podtrzymaniu aktywności połączenia TCP. Czas jest określany jako 32-bitowa liczba całkowita bez znaku. Wartość 0 wskazuje, że klient nie powinien generować komunikatów podtrzymania aktywności połączeń, chyba, że zostanie to zażądane przez aplikację. Kodem tej opcji jest 38, a jej długość to 4. **Kod Dł. Czas**  RZAKG536-0
39	Bajt nieznaczący komunikatu podtrzymania TCP	Ta opcja określa, czy klient powinien wysyłać komunikaty podtrzymania TCP z oktetem bajtów nieznaczących w celu zapewnienia zgodności ze starszymi implementacjami. Wartość 0 wskazuje, że oktet bajtów nieznaczących nie powinien być wysyłany. Wartość 1 wskazuje, że oktet bajtów nieznaczących powinien być wysyłany. Kodem tej opcji jest 39, a jej długość to 1. **Kod Dł. Wartość**  RZAKG553-0
40	Domena systemu informacji sieciowej	Ta opcja określa nazwę domeny NIS klienta. Domeną jest łańcuch składający się ze znaków z zestawu znaków ASCII NVT. Kodem tej opcji jest 40. Minimalna długość to 1. **Kod Dł. Nazwa domeny NIS**  RZAKG540-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
41	Serwery NIS	Ta opcja określa listę adresów IP wskazujących serwery NIS dostępne dla klienta. Serwery należy określić w preferowanym porządku. Kodem tej opcji jest 41. Minimalna długość to 4 i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **41 n a1 a2 a3 a4 a1 a2 ...** RZAKG556-0
42	Opcja serwera Network Time Protocol	Ta opcja określa listę adresów IP wskazujących serwery NTP dostępne dla klienta. Serwery należy określić w preferowanym porządku. Kodem tej opcji jest 42. Minimalna długość to 4 i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **42 n a1 a2 a3 a4 a1 a2 ...** RZAKG557-0
44	Nazwa serwera NetBIOS przez TCP/IP	Opcja serwera nazw NetBIOS określa listę serwerów nazw NBNS RFC 1001/1002 NBNS określonych w preferowanym porządku. Kodem tej opcji jest 44. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **44 n a1 a2 a3 a4 b1 b2 b3 b4 ...** RZAKG558-0
45	Serwer dystrybucji datagramów NetBIOS przez TCP/IP	Opcja serwera dystrybucji datagramów NetBIOS (NBDD) określa listę serwerów NBDD RFC 1001/1002 określonych w preferowanym porządku. Kodem tej opcji jest 45. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **45 n a1 a2 a3 a4 b1 b2 b3 b4 ...** RZAKG559-0
46	Typ węzła NetBIOS przez TCP/IP	Opcja typu węzła NetBIOS umożliwia skonfigurowanie klientów NetBIOS przez TCP/IP, które mogą być konfigurowane, zgodnie z opisem w dokumencie RFC 1001/1002. Wartością jest pojedynczy oktet identyfikujący typ klienta w następujący sposób: **Wartość Typ węzła** **0x1 B-node** **0x2 P-node** **0x4 M-node** **0x8 H-node** RZAKG554-0 Zapis ’0x’ oznacza liczbę w systemie szesnastkowym. Kodem tej opcji jest 46. Długość tej opcji zawsze wynosi 1. **Kod Dł. Typ węzła** **46 1 Patrz niżej** RZAKG555-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
47	Zakres NetBIOS przez TCP/IP	Opcja zakresu NetBIOS określa parametr zakresu NetBIOS przez TCP/IP dla klienta, jak określono w dokumencie RFC 1001/1002. Kodem tej opcji jest 47. Minimalna długość tej wynosi 1. **Kod Dł. Zakres NetBIOS** **47 | n | s1 | s2 | s3 | s4 | ...** RZAKG528-0
48	Serwer czcionek systemu X Window	Ta opcja określa listę serwerów czcionek systemu X Window dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem tej opcji jest 48. Minimalna długość tej opcji to 4 oktety i musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **48 | n | a1 | a2 | a3 | a4 | a1 | a2 | ...** RZAKG560-0
49	Menedżer wyświetlania systemu X Window	Ta opcja określa listę adresów IP systemów z menedżerami wyświetlania systemu X Window dostępnych dla klienta. Adresy należy określić w preferowanym porządku. Kodem tej opcji jest 49. Minimalna długość tej opcji to 4 i musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** **49 | n | a1 | a2 | a3 | a4 | a1 | a2 | ...** RZAKG561-0
51	Czas dzierżawy adresu IP	Ta opcja jest używana w żądaniu klienta (DHCPDISCOVER lub DHCPREQUEST), aby umożliwić klientom żądanie czasu dzierżawy dla adresu IP. W odpowiedzi serwera (DHCPOFFER) opcja ta jest używana do określenia czasu dzierżawy, który serwer DHCP może udostępnić. Czas w sekundach jest określany jako 32-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 51, a jej długość to 4. **Kod Dł. Czas dzierżawy** **51 | 4 | t1 | t2 | t3 | t4** RZAKG537-0
58	Wartość czasu odnowienia (T1)	Ta opcja określa czas od przypisania adresu do momentu przejścia klienta w stan RENEWING. Czas w sekundach jest określany jako 32-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 58, a jej długość to 4. **Kod Dł. Czas odnowienia T1** **58 | 4 | t1 | t2 | t3 | t4** RZAKG538-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

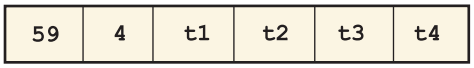
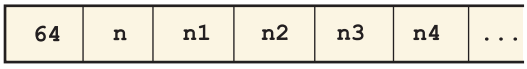
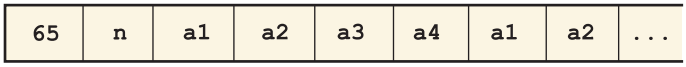
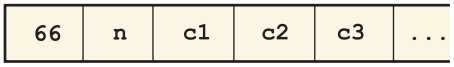
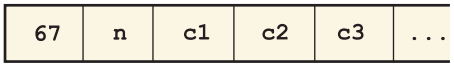
Numer opcji	Opcja	Opis
59	Czas ponownego wiązania (T2)	Ta opcja określa czas od przypisania adresu do momentu przejścia klienta w stan REBINDING. Czas w sekundach jest określany jako 32-bitowa liczba całkowita bez znaku. Kodem tej opcji jest 59, a jej długość to 4. **Kod Dł. Czas ponownego wiązania T2**  RZAKG539-0
62	Nazwa domeny NetWare/IP	Opcja ta określa nazwę domeny Netware/IP.
63	NetWare/IP	Opcja ta określa żądane podopcje NetWare. Zakres wartości od 1 do 255. Opcja 62 pozwala określić nazwę domeny NetWare/IP.
64	Nazwa domeny NIS	Ta opcja określa nazwę domeny NIS+ klienta. Domeną jest łańcuch składający się ze znaków z zestawu znaków ASCII NVT. Kodem tej opcji jest 64. Minimalna długość to 1. **Kod Dł. Nazwa domeny klienta NIS**  RZAKG527-0
65	Serwery NIS	Ta opcja określa listę adresów IP wskazujących serwery NIS+ dostępne dla klienta. Serwery należy określić w preferowanym porządku. Kodem tej opcji jest 65. Minimalna długość to 4 i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  RZAKG562-0
66	Nazwa serwera	Ta opcja służy do identyfikowania serwera TFTP, gdy pole ’sname’ w nagłówku DHCP zostało użyte dla opcji DHCP. Kodem tej opcji jest 66, a jej minimalna długość to 1. **Kod Dł. Serwer TFTP**  RZAKG571-0
67	Nazwa zbioru startowego	Ta opcja służy do identyfikowania serwera zbioru startowego, gdy pole ’file’ w nagłówku DHCP zostało użyte dla opcji DHCP. Kodem tej opcji jest 67, a jej minimalna długość to 1. **Kod Dł. Nazwa pliku startowego**  RZAKG572-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

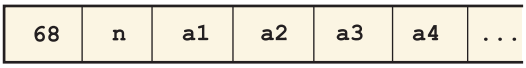
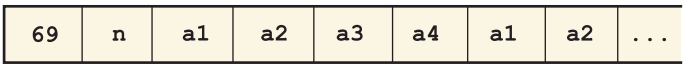
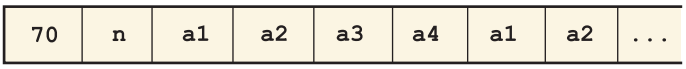
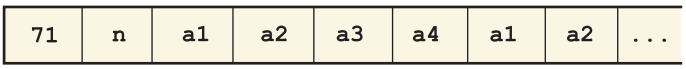
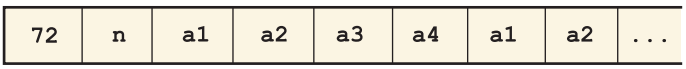
Numer opcji	Opcja	Opis
68	Adres podstawowy	Ta opcja określa listę adresów IP ruchomych agentów macierzystych IP dostępnych dla klienta. Agenty należy określić w preferowanym porządku. Kodem tej opcji jest 68. Minimalną długością jest 0 (co wskazuje, że żadne agenty podstawowe nie są dostępne); długość musi być wielokrotnością 4. Zwykle długość wynosi 4 oktety i zawiera pojedynczy adres agenta podstawowego. **Kod Dł. Liczba adresów agentów podstawowych(zero lub więcej)**  68 n a1 a2 a3 a4 ... RZAKG529-0
69	Serwery SMTP	Opcja serwera SMTP określa listę serwerów SMTP dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera SMTP jest 69. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  69 n a1 a2 a3 a4 a1 a2 ... RZAKG563-0
70	Serwer POP3	Opcja serwera POP3 określa listę serwerów POP3 dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera POP3 jest 70. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  70 n a1 a2 a3 a4 a1 a2 ... RZAKG564-0
71	Serwer NNTP	Opcja serwera NNTP określa listę serwerów NNTP dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera NNTP jest 71. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  71 n a1 a2 a3 a4 a1 a2 ... RZAKG565-0
72	Serwer WWW	Opcja serwera WWW określa listę serwerów WWW dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera WWW jest 72. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2**  72 n a1 a2 a3 a4 a1 a2 ... RZAKG566-0

Tabela 1. Standardowe opcje DHCP (kontynuacja)

Numer opcji	Opcja	Opis
73	Serwer Finger	Opcja serwera Finger określa listę serwerów Finger dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera Finger jest 73. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 73 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG567-0
74	Serwer IRC	Opcja serwera IRC określa listę serwerów IRC dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera IRC jest 74. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 74 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG568-0
75	Serwer StreetTalk	Opcja serwera StreetTalk określa listę serwerów StreetTalk dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera StreetTalk jest 75. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 75 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG569-0
76	Serwer STDA	Opcja serwera StreetTalk Directory Assistance określa listę serwerów STDA dostępnych dla klienta. Serwery należy określić w preferowanym porządku. Kodem opcji serwera STDA jest 76. Minimalna długość tej opcji to 4 oktety i zawsze musi być wielokrotnością liczby 4. **Kod Dł. Adres 1 Adres 2** 76 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG570-0
77	Klasa użytkownika	Opcja ta określa nazwę klasy, której podzbiorem jest host. Klasa ta musi zostać najpierw zdefiniowana podczas konfigurowania serwera DHCP.
78	Agent katalogów	Jeśli klient używa do obsługi komunikatów protokołu Service Location Protocol, to opcja ta określa adres IP agenta katalogów.
79	Zasięg usługi	Opcja ta określa zasięg agenta katalogów korzystającego z protokołu Service Location Protocol do odpowiedzi na komunikaty żądania usługi.
80	Ośrodek nadawania nazw	Opcja ta określa ośrodek nadawania nazw dla agenta katalogów, jeśli klient używa do obsługi komunikatów protokołu Service Location Protocol. Ośrodek nadawania nazw określa składnię dla konwencji używanej w adresach URL.

Informacje pokrewne

DHCP Options and BOOTP Vendor Extensions

Przykłady: DHCP

Najlepszą metodą na wybranie odpowiedniej instalacji sieci jest porównanie diagramów i przykładów różnych konfiguracji sieci.

Przeanalizowanie praktycznego zastosowania pewnej techniki w konkretnej sytuacji jest często najlepszym sposobem opanowania tej techniki. Przedstawiono tu przykłady ilustrujące sposób działania DHCP, sposób dopasowania usług DHCP do różnych konfiguracji sieci oraz metody wykorzystania niektórych nowych funkcji w wersji V5R4. Jest to znakomity punkt wyjścia zarówno dla początkujących użytkowników DHCP, jak i dla doświadczonych administratorów.

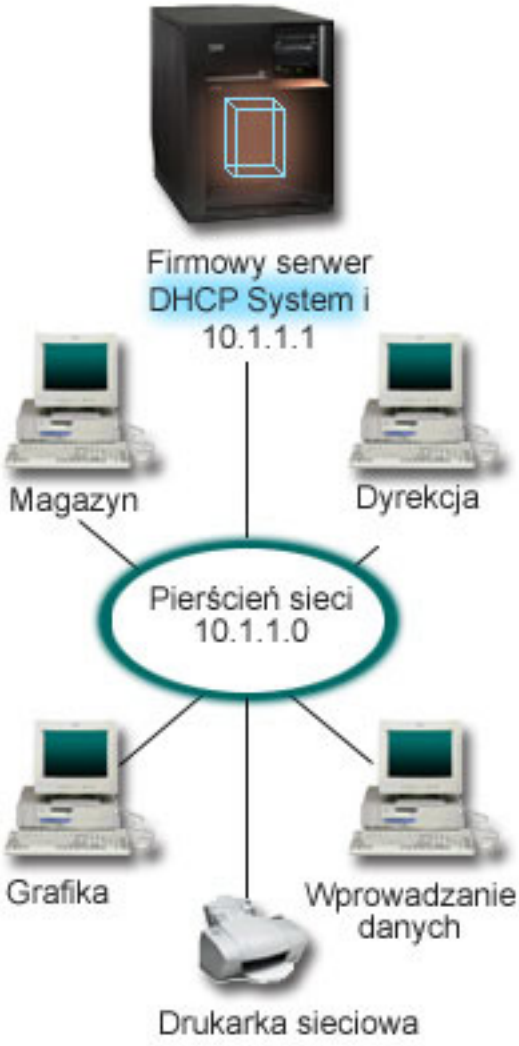
Pojęcia pokrewne

"Informacje o topologii sieci" na stronie 39
Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

Przykład: prosta podsieć DHCP

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby prostej sieci LAN z czterema klientami PC i drukarką sieciową.

W przykładzie tym serwer System i działa jako serwer DHCP dla podsieci IP 10.1.1.0. Serwer jest podłączony do sieci LAN za pośrednictwem interfejsu 10.1.1.1.



Rysunek 2. Konfiguracja serwera System i na potrzeby prostej sieci LAN

Przy tak niewielkiej liczbie klientów PC administratorzy mogą z łatwością wpisać i modyfikować informacje związane z adresami IP poszczególnych klientów. (W tym przypadku trzeba skonfigurować zaledwie cztery komputery). Wystarczy jednak sobie wyobrazić, że z początkowych czterech komputerów sieć rozrasta się do 200 stanowisk. Samodzielne konfigurowanie adresów IP każdego z nich z osobna stanie się czasochłonną operacją, która może również prowadzić do powstawania wielu błędów. DHCP zdecydowanie upraszcza proces przypisywania klientom adresów IP. Nawet jeśli podsieć 10.1.1.0 obejmuje setki klientów, wystarczy aby administrator jednorazowo zdefiniował strategię świadczenia usług DHCP w systemie. Serwer przydzieli adresy IP poszczególnym klientom zgodnie z tą strategią.

Po otrzymaniu od klientów sygnału DHCPDISCOVER serwer wyśle odpowiedź zawierającą wymagane dane IP. W tym przykładzie w sieci działa drukarka sieciowa, również konfigurowana poprzez DHCP. Ponieważ jednak zapewnienie prawidłowej komunikacji klientów z drukarką wymaga przypisania drukarce niezmiennego adresu IP, administrator sieci powinien uwzględnić tę okoliczność w konfiguracji DHCP. Jednym z rozwiązań byłoby przypisanie drukarce stałego adresu IP. Można użyć serwera DHCP do zdefiniowania w strategii DHCP klienta, takiego jak drukarka sieciowa, przez podanie jego adresu MAC. W definicji klienta DHCP można wybranemu klientowi przydzielić ściśle określone wartości parametrów, takich jak adres IP i adresy routerów.

Dla celów komunikacji klienta z siecią TCP/IP wymagany jest przynajmniej adres IP i maska podsieci. Z serwera DHCP klient może otrzymywać nie tylko adres IP, ale i dodatkowe dane konfiguracyjne (na przykład maskę podsieci), określane opcjami konfiguracyjnymi.

Planowanie konfiguracji DHCP dla prostej sieci LAN

Tabela 2. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Adresy podsieci nie przypisywane przez system		10.1.1.1 (serwer DNS)
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 3. Podsieć komputerów PC

Obiekt	**Wartość**
Nazwa podsieci	ProstaPodsieć
Zarządzane adresy	10.1.1.2 - 10.1.1.150
Czas dzierżawy	24 godziny (wartość domyślna)
Opcje konfiguracyjne Opcje dziedziczone	 Opcje z konfiguracji globalnej

Tabela 4. Klient drukarki

Obiekt	**Wartość**
Nazwa klienta	Drukarka LAN
Adres klienta	10.1.1.5
Opcje konfiguracyjne Opcje dziedziczone	 Opcje z konfiguracji globalnej

Odsyłacze pokrewne

“Przykład: wiele podsieci TCP/IP”
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby dwóch sieci LAN połączonych przez router z obsługą DHCP.

“Przykład: DHCP i serwery multihoming” na stronie 27
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby sieci LAN połączonej z Internetem za pośrednictwem routera internetowego.

Przykład: wiele podsieci TCP/IP

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby dwóch sieci LAN połączonych przez router z obsługą DHCP.

Ten przykład jest zbliżony do przykładu prostej podsieci DHCP, z tą różnicą, że do prostej podsieci DHCP wprowadzono dodatkową podsieć TCP/IP. Załóżmy, że komputery biurowe oraz stacje do wprowadzania danych znajdują się na różnych piętrach biurowca, oddzielone routerem. Jeśli administrator dojdzie do wniosku, że wszystkie

komputery powinny otrzymywać swoje adresy IP z serwera DHCP, stanie przed problemami, które nie występowały w przypadku prostej sieci DHCP. Poniższy rysunek przedstawia przykładowy układ sieci dla serwera DHCP System i podłączonego do dwóch sieci LAN z użyciem routera na granicy między sieciami. Na rysunku celowo umieszczono ograniczoną liczbę klientów, aby nie zaciemniać obrazu. W rzeczywistości w każdej podsieci może istnieć większa liczba klientów.

Rysunek 3. Sieci LAN połączone poprzez router

Router łączący obie sieci musi mieć konfigurację pozwalającą na przekazywanie pakietów DHCPDISCOVER. W przeciwnym razie stacje wprowadzania danych nie będą mogły odebrać swoich adresów IP i uzyskać dostępu do sieci. Ponadto w strategii DHCP należy określić dwie definicje podsieci, jedną dla podsieci stacji wprowadzania danych, a

drugą dla podsieci biurowej. Minimalną różnicą między konfiguracjami podsieci są adresy IP podsieci i adresy routerów. Podsieć stacji wprowadzania danych musi otrzymać adres routera 10.1.2.2, aby mogła komunikować się z podsiecią biurową.

Planowanie konfiguracji DHCP dla wielu sieci LAN

Tabela 5. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Adresy podsieci nie przypisywane przez system		10.1.1.1 (serwer DNS)
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 6. Podsieć klientów biurowych

Obiekt		**Wartość**
Nazwa podsieci		Biuro
Zarządzane adresy		10.1.1.3 - 10.1.1.150
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcja 3: router	10.1.1.2
	Opcje dziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.1.2 (router)

Tabela 7. Podsieć klientów wprowadzania danych

Obiekt		**Wartość**
Nazwa podsieci		WprowadzanieDanych
Zarządzane adresy		10.1.2.3 - 10.1.2.150
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcja 3: router	10.1.2.2
	Opcje dziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.2.2 (router)

Odsyłacze pokrewne

“Przykład: prosta podsieć DHCP” na stronie 22
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby prostej sieci LAN z czterema klientami PC i drukarką sieciową.

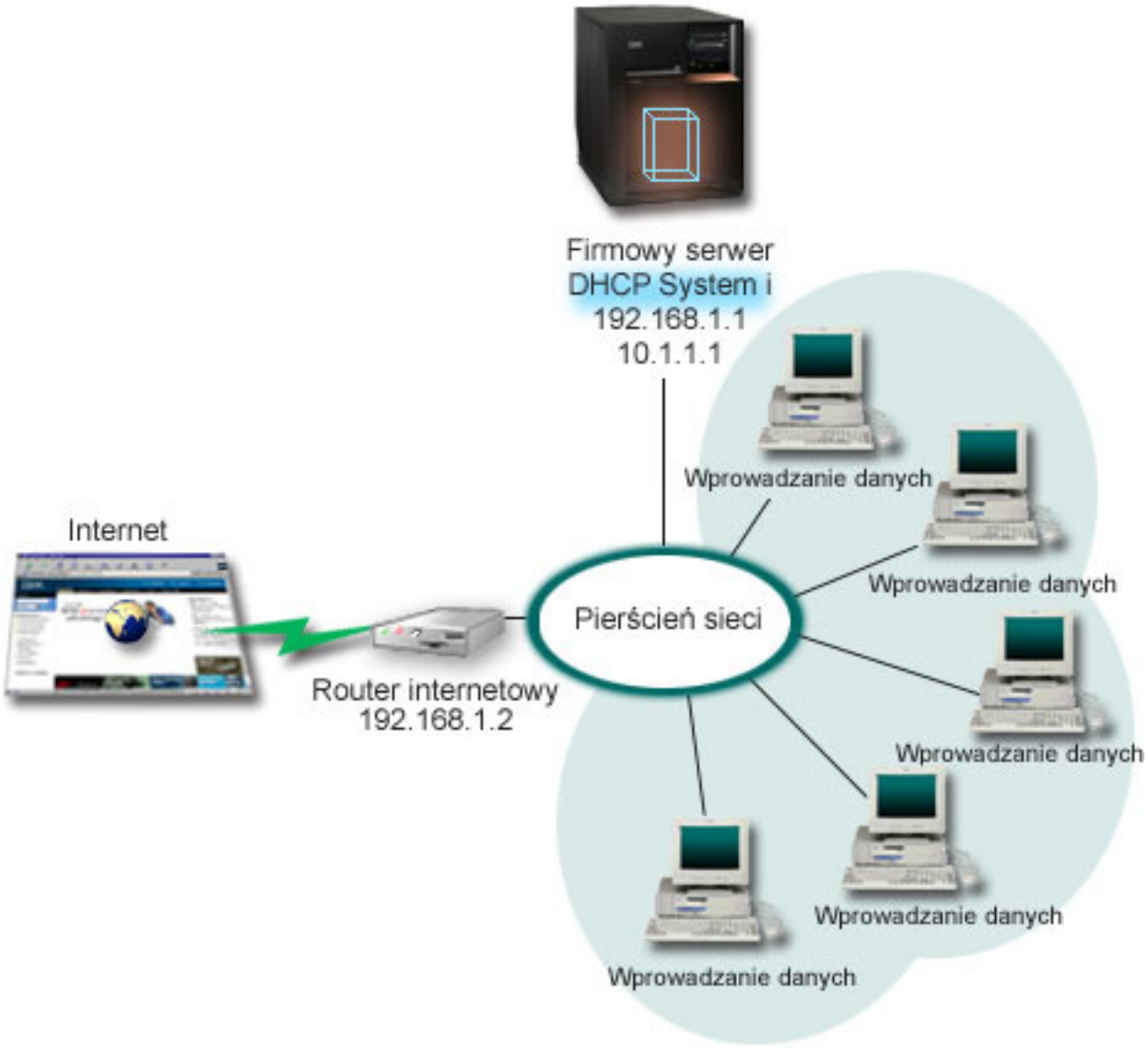
Przykład: DHCP i serwery multihoming

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby sieci LAN połączonej z Internetem za pośrednictwem routera internetowego.

Przykład ten jest podobny do przykładu z prostą podsiecią DHCP. W tym przykładzie komputery do wprowadzania danych komunikują się tylko między sobą i z serwerem System i. Swoje adresy IP otrzymują dynamicznie od serwera DHCP System i.

Jednak działająca na nich nowa wersja aplikacji do wprowadzania danych wymaga podłączenia do Internetu, toteż w firmie zdecydowano się zapewnić łącze z Internetem przez specjalny router, tak jak to pokazano na poniższym rysunku.

Oprócz routera administrator dodał jeszcze jeden interfejs z własnym adresem IP do komunikacji z Internetem. Konfiguracja, w której do jednego adaptera przypisanych jest kilka adresów IP, nosi nazwę jest multihoming.



Rysunek 4. Usługi DHCP w sieci, w której do jednego adaptera przypisanych jest wiele adresów IP

Uwaga: Opisywana metoda podłączenia sieci do Internetu jest wprawdzie możliwa, ale nie zapewnia wysokiego poziomu bezpieczeństwa. Konfiguracja taka sprawdza się jako przykład użycia DHCP, jednak w konkretnej sytuacji należy zawsze uwzględnić kwestie bezpieczeństwa sieci.

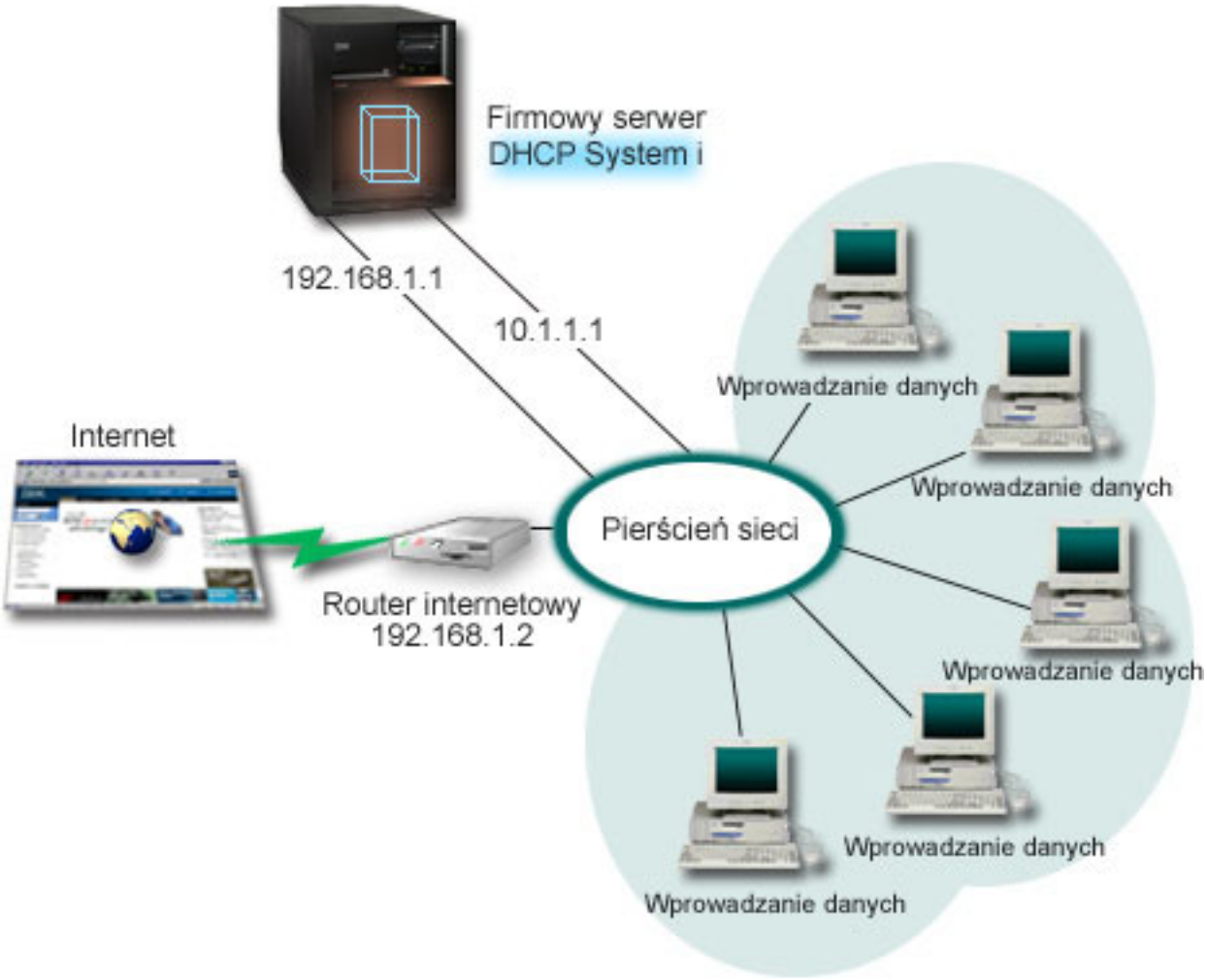
W konfiguracji DHCP musi być uwzględniony fakt, że serwer System i jest rozpoznawany pod dwoma różnymi adresami IP. Aby zrozumieć zasady właściwej konfiguracji DHCP w tym scenariuszu, wskazane jest przeanalizowanie procesów zachodzących po wysłaniu przez klienta pakietu DHCPDISCOVER.

Wysłany przez klienta pakiet DHCPDISCOVER zostaje rozgłoszony w całej sieci. Serwer DHCP System i nie jest w stanie ustalić, do którego z adresów IP dany pakiet jest skierowany. Jeśli pakiet będzie oznakowany adresem IP interfejsu używanego na potrzeby usług DHCP (10.1.1.1), klienty uzyskają informacje o adresie IP w przewidywany sposób. Istnieje też możliwość, że pakiet zostanie oznaczony adresem 192.168.1.1 (adres podłączenia do Internetu). Po wysłaniu pakietu skierowanego na adres interfejsu 192.168.1.1 klient nie otrzyma w odpowiedzi adresu IP.

Aby uwzględnić taką topologię sieci w konfiguracji DHCP, konieczne jest nie tylko zdefiniowanie osobnej podsieci dla zespołu klientów wprowadzania danych, lecz także podsieci odpowiadającej Internetowi. Konfiguracja dla podsieci Internetu obejmowałaby pustą pulę adresów. Najprostszą metodą realizacji takiej puli będzie zdefiniowanie podsieci z co najmniej jednym adresem IP (na przykład 192.168.1.1), a następnie wykluczenie tego adresu. Po zdefiniowaniu obu (lub większej liczby) podsieci należy je połączyć w grupę podsieci. Wówczas nawet jeśli pakiet DHCPDISCOVER zostanie oznakowany interfejsem 192.168.1.1, podsieć wprowadzania danych i tak otrzyma poprawne dane IP.

Aby scenariusz ten sprawdził się w praktyce, podsieć wprowadzania danych musi przekazywać klientom adres routera dającego dostęp do Internetu. W tym przypadku adresem routera jest interfejs 10.1.1.1 serwera System i. Aby zapewnić przepływ pakietów między podsieciami, należy w obu interfejsach włączyć opcję przekazywania datagramów IP. W przykładzie tym zarówno zewnętrzne, jak i wewnętrzne adresy IP są reprezentowane jako adresy zarezerwowane. W sieciach pasujących do tego schematu należałoby jeszcze użyć translacji adresu sieciowego (NAT), aby zapewnić klientom możliwość komunikowania się z Internetem.

Zakres zastosowania techniki grup podsieci jako sposobu wyeliminowania problemów z oznakowaniem pakietów nie ogranicza się do konfiguracji multihoming. Podobny typ problemu występuje zawsze, ilekroć do pojedynczej sieci podłączonych jest wiele interfejsów. Poniższy rysunek ilustruje serwer System i mający dwa fizyczne połączenia z siecią wprowadzania danych. Taka konfiguracja sieci będzie wymagać podobnej strategii grup DHCP, co konfiguracja multihoming, ponieważ pakiety DHCPDISCOVER mogłyby otrzymywać odpowiedź z interfejsu 192.168.1.1.



Rysunek 5. Korzystanie z DHCP w systemie z kilkoma interfejsami podłączonymi do tej samej sieci

Planowanie konfiguracji DHCP dla serwera multihoming

Tabela 8. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt	Wartość
Czy system wykonuje aktualizacje DNS?	Nie
Czy system obsługuje klientów BOOTP?	Nie

Tabela 9. Podsieć klientów wprowadzania danych

Obiekt		Wartość
Nazwa podsieci		Wprowadzanie danych
Zarządzane adresy		10.1.1.2 - 10.1.1.150
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 3: router	10.1.1.1
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Adresy w podsieci nie przypisywane przez serwer		10.1.1.1 (router, serwer DNS)

Tabela 10. Podsieć dla klientów internetowych (podsieć pusta)

Obiekt	Wartość
Nazwa podsieci	Internet
Zarządzane adresy	192.168.1.1 - 192.168.1.1
Adresy w podsieci nie przypisywane przez serwer	192.168.1.1 (wszystkie dostępne adresy IP)

Tabela 11. Grupa podsieci dla wszystkich przychodzących pakietów DHCPDISCOVER

Obiekt	Wartość
Nazwa grupy podsieci	Multihomed
Podsieci należące do grupy	Podsieć Internet Podsieć WprowadzanieDanych

Pozostałe opcje konfiguracji

- Na obu interfejsach należy włączyć opcję przekazywania datagramów IP.
- Należy skonfigurować usługę NAT dla stacji wprowadzania danych.

Odsyłacze pokrewne

"Przykład: prosta podsieć DHCP" na stronie 22
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP na potrzeby prostej sieci LAN z czterema klientami PC i drukarką sieciową.

Przykład: serwery DNS i DHCP na tym samym serwerze System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i jako serwer DHCP z dynamicznymi aktualizacjami usług DNS w prostej sieci LAN.

Poniższy rysunek ilustruje, w jaki sposób serwer System i może pełnić funkcję serwera DHCP i DNS w prostej podsieci. W przykładowej sieci klienty w magazynie, stacje wprowadzania danych oraz komputery dyrekcji służą do tworzenia dokumentów zawierających grafiki pobierane z serwera plików graficznych. Łączenie się z serwerem plików

graficznych odbywa się przez odwołania do dysku sieciowego rozpoznawanego przez nazwę hosta.

Rysunek 6. Dynamiczne usługi DNS i DHCP

Poprzednie wersje serwerów DHCP i DNS działały niezależnie od siebie. Jeśli serwer DHCP przypisał klientowi nowy adres IP, administrator musiał samodzielnie zmodyfikować odpowiednie rekordy DNS. W tym przykładzie, jeśli adres IP serwera plików graficznych ulegnie zmianie po przypisaniu innego adresu przez DHCP, klienty nie będą w stanie przypisać dysku sieciowego do nazwy hosta, ponieważ w rekordach DNS będzie figurował poprzedni adres IP.

Bieżąca wersja serwera DNS pozwala na dynamiczną aktualizację rekordów DNS związaną ze zmianami adresów IP w wyniku działania DHCP. Na przykład, rekordy DNS serwera plików zostaną dynamicznie zaktualizowane po tym, jak serwer ten odnowi dzierżawę i otrzyma nowy adres IP 10.1.1.250. Dzięki temu pozostałe komputery będą mogły dalej bez przeszkód odwoływać się do serwera plików graficznych poprzez nazwę hosta, interpretowaną prawidłowo przez serwer DNS.

Konfiguracja serwera DHCP może przewidywać aktualizowanie w imieniu klienta rekordów odwzorowania adresów (A) lub rekordów wskaźników wyszukiwania zwrotnego (PTR). Rekord typu A pozwala odwzorować nazwę hosta klienta na jego adres IP. Rekord typu PTR odwzorowuje adres IP klienta na jego nazwę. Dla każdego dynamicznie aktualizowanego rekordu zapisywany jest również powiązany rekord tekstowy (TXT), który wskazuje na aktualizację przez serwer DHCP. Serwer DHCP może aktualizować jednocześnie rekordy A i PTR lub tylko rekordy PTR. Więcej informacji na temat konfigurowania usług DNS na potrzeby dynamicznej aktualizacji zawiera sekcja Przykład: DNS i DHCP na tym samym serwerze System i w kolekcji tematów dotyczących DNS.

Uwaga: Jeśli konfiguracja DHCP przewiduje aktualizowanie tylko rekordów PTR, konfiguracja serwera DNS powinna dopuszczać aktualizacje inicjowane przez klienty, aby każdy klient mógł zaktualizować odpowiadający mu rekord A. Nie każdy klient DHCP jest w stanie wysyłać zgłoszenia aktualizacji własnego rekordu A. Dlatego przed zdecydowaniem się na tę metodę należy dokładnie zapoznać się z dokumentacją platformy klienta.

Aby włączyć aktualizacje DNS, należy utworzyć klucz DNS dla serwera DHCP. Klucz DNS nadaje serwerowi DHCP uprawnienie do modyfikowania rekordów DNS w oparciu o przydzielone przezeń adresy IP. Następnie w konfiguracji DHCP należy określić zakres wykonywania aktualizacji DNS. Na przykład, jeśli aktualizacje mają być wykonywane dla wszystkich podsieci, należy odpowiednie parametry ustawić na poziomie globalnym. Jeśli aktualizacje mają dotyczyć tylko jednej podsieci, konfiguracja powinna dotyczyć tylko jej.

Planowanie konfiguracji DHCP z dynamicznym aktualizowaniem DNS

Tabela 12. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.10
	Opcja 15: nazwa domeny	moja_firma.com
Czy system wykonuje aktualizacje DNS?		Tak -- rekordy A i PTR
Czy system obsługuje klientów BOOTP?		Nie

Tabela 13. Podsieć dla sieci pierścieniowej

Obiekt		**Wartość**
Nazwa podsieci		PodsiećSieci
Zarządzane adresy		10.1.1.250 - 10.1.1.254
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcje dziedziczone	Opcje z konfiguracji globalnej

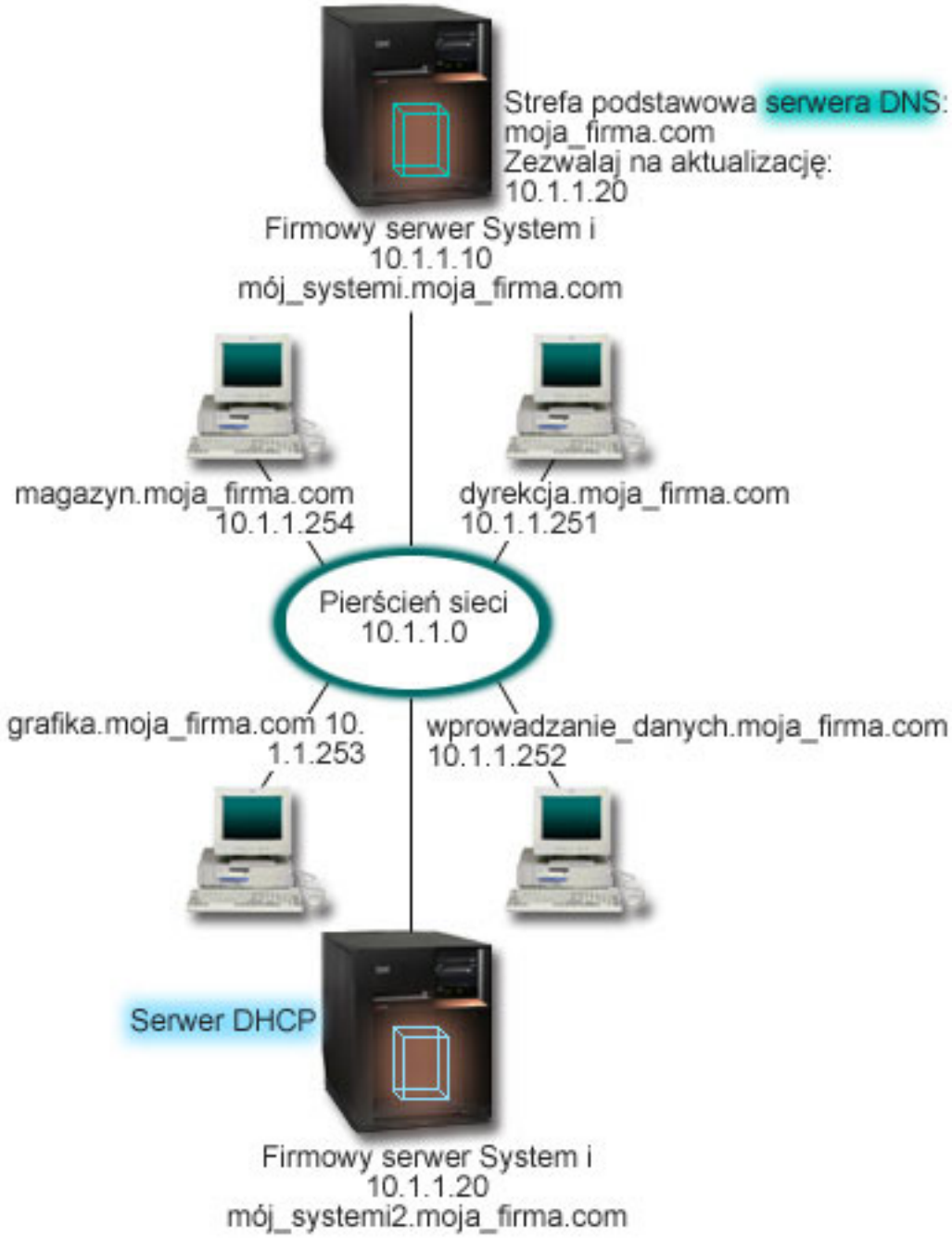
Pozostałe opcje konfiguracyjne:

Uprawnienie serwera DHCP do wysyłania wpisów do DNS. Informacje na ten temat zawiera sekcja Przykład: DNS i DHCP na tym samym serwerze System i w kolekcji tematów dotyczących DNS.

Przykład: DNS i DHCP na różnych serwerach System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować usługi DHCP i DNS na dwóch różnych serwerach System i, aby zapewnić dynamiczne aktualizowanie rekordów DNS w prostej sieci LAN.

Poniższy rysunek przedstawia niewielką podsieć z usługami DNS i DHCP uruchomionymi na osobnych serwerach System i. System, w którym uruchomiony jest DNS, będzie skonfigurowany dokładnie tak samo jak wtedy, gdy DNS i DHCP działa na jednym serwerze System i. Wymagane są jednak dodatkowe czynności w celu skonfigurowania serwera DHCP pod kątem dynamicznej aktualizacji wpisów.



Rysunek 7. DNS i DHCP na różnych serwerach System i

Planowanie konfiguracji DHCP z dynamicznym aktualizowaniem DNS

Więcej przykładów konfiguracji globalnych i ustawień podsieci można znaleźć w “Przykład: serwery DNS i DHCP na tym samym serwerze System i” na stronie 30.

Pozostałe opcje konfiguracyjne:

Instalowanie systemu nazw domen (Opcja 31) w systemie i5/OS.

Należy zainstalować system nazw domen (Opcja 31) w systemie i5/OS na serwerze System i, na którym będzie uruchomiony DHCP. Opcja ta zawiera funkcje API dynamicznej aktualizacji zarządzające procesem modyfikacji rekordów zasobów. Instrukcje dotyczące instalacji można znaleźć w sekcji Wymagania systemu DNS.

Nadawanie serwerowi DHCP uprawnień do wysyłania aktualizacji do DNS

Serwer DHCP musi dysponować uprawnieniem do wysyłania aktualizacji do serwera DNS. Można w tym celu powtórzyć procedurę definiowania klucza dynamicznej aktualizacji lub wysłać odpowiedni plik i umieścić go w odpowiedniej ścieżce do katalogu.

Aby utworzyć klucz dynamicznej wymiany na obu serwerach System i, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **DNS**.
2. W lewym panelu kliknij prawym przyciskiem myszy pozycję **DNS** i wybierz opcję **Zarządzaj kluczami dynamicznej aktualizacji** (Manage Dynamic Update Keys).
3. Na stronie Zarządzaj kluczami dynamicznej aktualizacji kliknij przycisk **Dodaj**
4. Na stronie Dodaj klucze aktualizacji dynamicznej wypełnij poniższe pola:
   - **Nazwa klucza**: Określ nazwę dla klucza, na przykład mojafirma.key. Nazwa klucza musi kończyć się kropką.
   - **Dynamicznie aktualizowane strefy**: Określ nazwy stref, dla których tworzony klucz będzie poprawny. Można podać nazwę więcej niż jednej strefy.
   - **Wygeneruj klucz**: Wybierz metodę, za pomocą której zostanie wygenerowany tajny klucz.
5. Powtórz powyższe czynności, aby ten sam klucz był zdefiniowany na serwerze System i obsługującym DNS i na serwerze System i obsługującym DHCP.

Pojęcia pokrewne

Wymagania systemu DNS

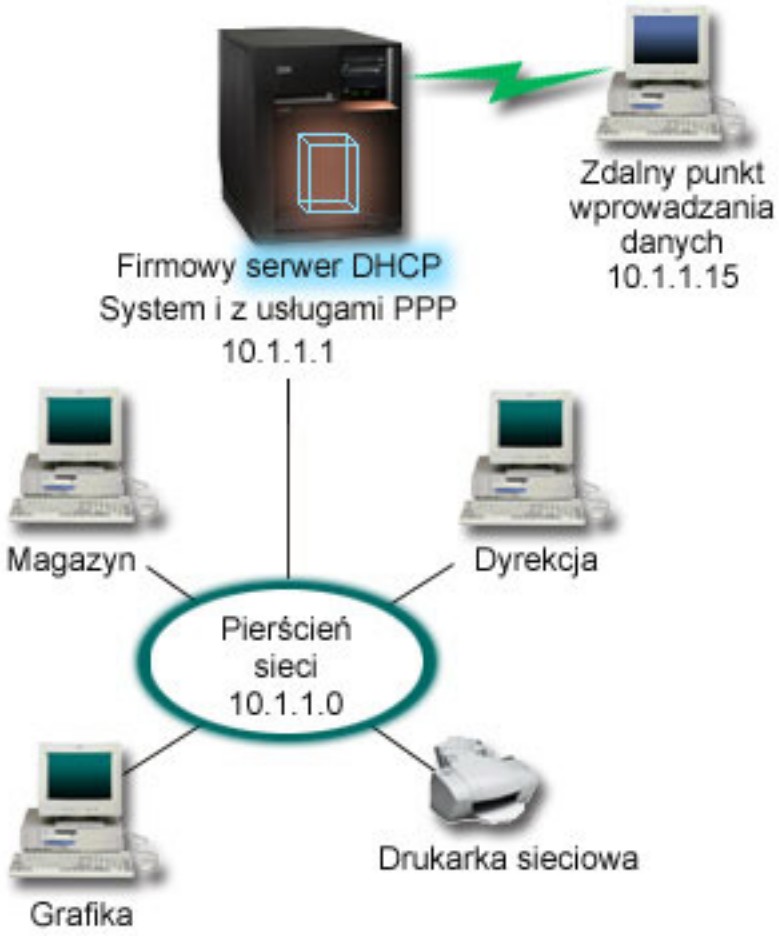
Informacje pokrewne

Update DNS API

Przykład: PPP i DHCP na jednym serwerze System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i na potrzeby sieci LAN i zdalnych klientów z połączeniem modemowym.

Często zachodzi potrzeba dopuszczania do firmowej sieci LAN klientów łączących się zdalnie, na przykład za pośrednictwem łączy telefonicznych. Klienty z połączeniem modemowym mogą uzyskać dostęp do serwera System i za pomocą protokołu PPP. Aby uzyskać dostęp do sieci, klient z połączeniem modemowym wymaga informacji IP, tak samo jak klient podłączony bezpośrednio do sieci. Serwer DHCP System i może przekazywać adresy IP klientom z połączeniem modemowym za pośrednictwem protokołu PPP na takiej samej zasadzie, jak w przypadku innych klientów, podłączonych bezpośrednio. Poniższy rysunek przedstawia sytuację, w której klient zdalny musi uzyskać dostęp do sieci firmowej, aby wykonać pewne czynności.



Rysunek 8. PPP i DHCP na jednym serwerze System i

Aby zdalny pracownik mógł podłączyć się do firmowej sieci, serwer System i musi skorzystać z usługi zdalnego dostępu RAS (Remote Access Service) i DHCP. Funkcja RAS umożliwia modemowy dostęp do serwera System i. Jeśli połączenie modemowe jest prawidłowo skonfigurowane, to bezpośrednio po jego nawiązaniu przez klienta serwer PPP wysyła do serwera DHCP żądanie dystrybucji danych TCP/IP do klienta zdalnego.

W tym przykładzie obsługa klientów w sieci LAN, jak i zdalnych klientów modemowych odbywa się według spójnej strategii dla jednej podsieci.

Parametry zlecające serwerowi DHCP dystrybucję danych IP dla klienta zdalnego są konfigurowane w profilu PPP. W ustawieniach TCP/IP profilu połączenia odbiorcy należy zmienić metodę przypisania zdalnego adresu IP z wartości Stały (Fixed) na DHCP. Aby umożliwić klientom modemowym komunikację z innymi klientami w sieci, na przykład z drukarką, należy również włączyć przekazywanie IP w ustawieniach TCP/IP profilu oraz we właściwościach konfiguracji (stosu) TCP/IP. Jeśli przekazywanie IP zostanie skonfigurowane tylko w profilu PPP, serwer System i nie będzie przekazywał pakietów IP. Konieczne jest włączenie przekazywania IP jednocześnie w profilu i w stosie.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP należącym do definicji podsieci serwera DHCP. W tym przykładzie adres lokalnego interfejsu w profilu PPP to 10.1.1.1. Adres ten powinien zostać wykluczony z puli zarządzanej przez serwer DHCP, aby nie został przypisany klientowi DHCP.

Planowanie konfiguracji DHCP dla klientów lokalnych i klientów PPP

Tabela 14. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 15. Podsieć dla klientów lokalnych i modemowych

Obiekt		**Wartość**
Nazwa podsieci		SiećGłówna
Zarządzane adresy		10.1.1.3 - 10.1.1.150
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcje dziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.1.1 (lokalny adres interfejsu, podany w ustawieniach TCP/IP we właściwościach profilu połączenia odbiorcy w programie System i Navigator)

Pozostałe opcje konfiguracji

- W profilu połączenia PPP odbiorcy należy podać DHCP jako metodę określania zdalnego adresu IP.
  1. Należy włączyć możliwość połączenia z serwerem DHCP klientów sieci WAN lub połączenia przekazywanego, używając pozycji menu **Usługi** menu Usługi zdalnego dostępu w programie System i Navigator.
  2. We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator jako metodę przypisywania adresów IP należy wybrać DHCP.
- We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator należy umożliwić zdalnemu komputerowi dostęp z innych sieci (przekazywanie IP).
- We właściwościach ustawień TCP/IP w programie System i Navigator należy włączyć przekazywanie datagramów IP.

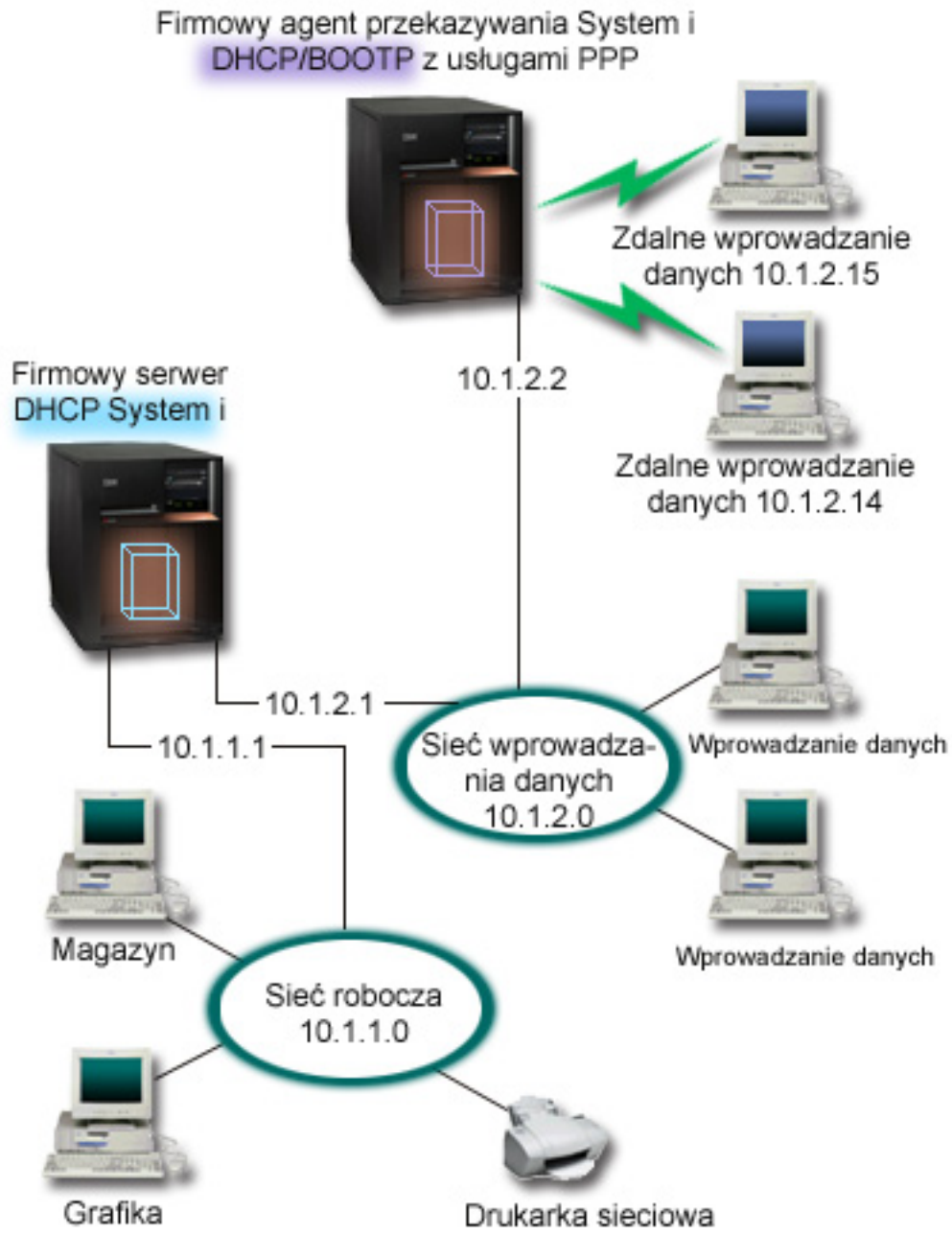
Odsyłacze pokrewne

"Przykład: profile DHCP i PPP na różnych serwerach System i"
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować dwa serwery System i, aby pełniły rolę serwera DHCP i agenta przekazującego BOOTP/DHCP na potrzeby dwóch sieci LAN i zdalnych klientów z połączeniem modemowym.

Przykład: profile DHCP i PPP na różnych serwerach System i

W tym przykładzie wyjaśniono, w jaki sposób skonfigurować dwa serwery System i, aby pełniły rolę serwera DHCP i agenta przekazującego BOOTP/DHCP na potrzeby dwóch sieci LAN i zdalnych klientów z połączeniem modemowym.

W przykładzie dotyczącym PPP i DHCP na jednym serwerze System i przedstawiono sposób korzystania z DHCP i PPP w jednym systemie w celu umożliwienia łączenia się z siecią klientom z połączeniem modemowym. Jednak z uwagi na fizyczną budowę sieci i ze względów bezpieczeństwa, lepszym rozwiązaniem może być rozdzielenie serwerów PPP i DHCP lub zainstalowanie dedykowanego serwera PPP bez usług DHCP. Poniższy rysunek przedstawia sieć, w której klientów z połączeniem modemowym obsługują serwery PPP i DHCP umieszczone na różnych maszynach.



Rysunek 9. Profile DHCP i PPP na różnych serwerach System i

Zdalne klienty wprowadzania danych wybierają połączenie z serwerem PPP System i. Profil PPP na tym serwerze musi określać przypisywanie zdalnych adresów IP poprzez DHCP, jak w przykładzie dotyczącym PPP i DHCP na jednym serwerze System i. Profil PPP oraz właściwości stosu TCP/IP serwera PPP muszą mieć ustawione przekazywanie IP. Ponadto, ponieważ ten serwer działa w charakterze agenta przekazującego pakiety DHCP, musi być włączony agent przekazujący BOOTP/DHCP. Dzięki temu serwer zdalnego dostępu System i będzie mógł przekazywać pakiety DHCPDISCOVER do serwera DHCP. Serwer DHCP w odpowiedzi na te pakiety będzie udostępniał klientom modemowym dane konfiguracyjne TCP/IP za pośrednictwem serwera PPP.

Serwer DHCP jest odpowiedzialny za dystrybucję adresów IP w obu sieciach: 10.1.1.0 i 10.1.2.0. W sieci wprowadzania danych adresy z zakresu od 10.1.2.10 do 10.1.2.40 będą przypisywane przez serwer DHCP zarówno klientom z połączeniem modemowym, jak i klientom podłączonym bezpośrednio do sieci. Klientom z podsieci

wprowadzania danych potrzebny będzie jeszcze adres routera (opcja 3) 10.1.2.1, pozwalający nawiązać połączenie z siecią roboczą, przy czym serwer DHCP System i musi mieć także włączone przekazywanie IP.

Ponadto adres IP interfejsu lokalnego w profilu PPP musi być adresem IP należącym do definicji podsieci serwera DHCP. W tym przykładzie adres lokalnego interfejsu w profilu PPP to 10.1.2.2. Adres ten powinien zostać wykluczony z puli zarządzanej przez serwer DHCP, aby nie został przypisany klientowi DHCP. Adres IP lokalnego interfejsu musi być adresem, pod który serwer DHCP może przesyłać pakiety odpowiedzi.

Planowanie konfiguracji DHCP dla serwera z agentem przekazującym DHCP

Tabela 16. Globalne opcje konfiguracyjne (odnoszą się do wszystkich klientów obsługiwanych przez serwer DHCP)

Obiekt		**Wartość**
Opcje konfiguracyjne	Opcja 1: maska podsieci	255.255.255.0
	Opcja 6: serwer DNS	10.1.1.1
	Opcja 15: nazwa domeny	moja_firma.com
Czy system wykonuje aktualizacje DNS?		Nie
Czy system obsługuje klientów BOOTP?		Nie

Tabela 17. Podsieć dla sieci roboczej

Obiekt		**Wartość**
Nazwa podsieci		SiećRobocza
Zarządzane adresy		10.1.1.3 - 10.1.1.150
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcje dziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		brak

Tabela 18. Podsieć sieci wprowadzania danych

Obiekt		**Wartość**
Nazwa podsieci		WprowadzanieDanych
Zarządzane adresy		10.1.2.10 - 10.1.2.40
Czas dzierżawy		24 godziny (wartość domyślna)
Opcje konfiguracyjne	Opcja 3: router	10.1.2.1
	Opcje dziedziczone	Opcje z konfiguracji globalnej
Adresy w podsieci nie przypisywane przez serwer		10.1.2.1 (router) 10.1.2.15 (adres IP lokalnego interfejsu dla zdalnego klienta wprowadzania danych) 10.1.2.14 (adres IP lokalnego interfejsu dla zdalnego klienta wprowadzania danych)

Inne ustawienia na platformie System i z usługą PPP

- Konfiguracja serwera TCP/IP agenta przekazującego BOOTP/DHCP

Obiekt	**Wartość**
Adres interfejsu	10.1.2.2
Przekazywanie pakietów pod adres IP serwera	10.1.2.1

- W profilu połączenia PPP odbiorcy należy podać DHCP jako metodę określania zdalnego adresu IP.

1. Należy włączyć możliwość połączenia z serwerem DHCP klientów sieci WAN lub połączenia przekazywanego, używając pozycji menu Usługi w Usługach zdalnego dostępu w programie System i Navigator.
2. We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator jako metodę przypisywania adresów IP należy wybrać DHCP.

- We właściwościach ustawień TCP/IP w profilu połączenia odbiorcy w programie System i Navigator należy umożliwić zdalnemu komputerowi dostęp do innych sieci (przekazywanie IP). Chodzi tu o umożliwienie zdalnym klientom komunikowania się z siecią wprowadzania danych.
- We właściwościach ustawień TCP/IP w programie System i Navigator należy włączyć przekazywanie datagramów IP. Chodzi tu o umożliwienie zdalnym klientom komunikowania się z siecią wprowadzania danych.

Odsyłacze pokrewne

"Przykład: PPP i DHCP na jednym serwerze System i" na stronie 34
W tym przykładzie wyjaśniono, w jaki sposób skonfigurować serwer System i na potrzeby sieci LAN i zdalnych klientów z połączeniem modemowym.

Planowanie usług DHCP

Konfigurowanie usług DHCP może być procesem czasochłonnym i podatnym na wiele błędów, dlatego niezwykle istotne jest wcześniejsze zaplanowanie konfiguracji serwera DHCP. Aby konfiguracja serwera DHCP przebiegła efektywniej, należy wcześniej rozważyć konfigurację sieci i zagadnienia dotyczące bezpieczeństwa.

Odsyłacze pokrewne

"Konfigurowanie usług DHCP" na stronie 42
Ta sekcja zawiera instrukcje dotyczące konfigurowania serwera i klientów DHCP oraz konfigurowania dynamicznej aktualizacji rekordów DNS.

Kwestie związane z bezpieczeństwem

Protokół DHCP nie zapewnia mechanizmów pozwalających sprawdzić, czy klient żądający adresu IP ma do tego prawo.

Z uwagi na istotny wpływ usług DHCP na działanie sieci, duże znaczenie ma zabezpieczenie serwera System i przed pakietami klientów zewnętrznych. Jeśli serwer DHCP jest uruchomiony na serwerze System i, który należy do zaufanej sieci wewnętrznej, można użyć filtrowania IP oraz translacji adresu sieciowego, aby zapewnić dodatkową ochronę serwera przed dostępem bez uprawnień. Jeśli serwer DHCP jest uruchomiony na serwerze System i, który jest podłączony do sieci niezaufanej, takiej jak Internet, można skorzystać z informacji zawartych w temacie System i a bezpieczeństwo internetowe.

Pojęcia pokrewne

Filtrowanie IP i translacja adresów sieciowych

Bezpieczeństwo

Informacje o topologii sieci

Przy planowaniu konfiguracji DHCP należy uwzględnić różne czynniki, takie jak topologia sieci, urządzenia obecne w sieci (na przykład routery) oraz przewidywany sposób obsługi klientów DHCP.

Podstawy topologii sieci

Jednym z najważniejszych elementów planowania implementacji usług DHCP jest prawidłowe uwzględnienie topologii sieci. Po przeanalizowaniu budowy sieci możliwe będzie szybkie określenie zakresu adresów IP, jakie można oddać do dyspozycji serwerowi DHCP, parametrów konfiguracyjnych potrzebnych każdemu klientowi, urządzeń, jakie należy skonfigurować w celu przekazywania komunikatów DHCP oraz zasad współpracy serwera DHCP z serwerami DNS i PPP. W zależności od stopnia złożoności sieci może być nawet wskazane narysowanie schematu topologii na kartce papieru. Na schemacie należy uwzględnić wszystkie sieci lokalne, urządzenia łączące sieci lokalne ze sobą oraz adresy IP urządzeń i klientów (na przykład drukarki), które wymagają przydziału stałego adresu. Podczas sporządzania diagramu topologii sieci, pomocne może być przeanalizowanie kilku przykładów konfiguracji DHCP.

Określanie liczby serwerów DHCP

Nawet w przypadku bardzo złożonych sieci możliwe jest obsłużenie wszystkich klientów za pomocą pojedynczego serwera DHCP. W zależności od topologii sieci, może to wymagać skonfigurowania kilku agentów przekazujących DHCP/BOOTP lub umożliwienia przekazywania pakietów DHCP przez routery.

Zastosowanie tylko jednego serwera DHCP na potrzeby całej sieci pozwoli scentralizować funkcje konfiguracji hosta dla wszystkich klientów. Są jednak sytuacje, w których warto się zastanowić nad uruchomieniem w sieci więcej niż jednego serwera DHCP.

Aby uniknąć sytuacji, gdy awaria jednego systemu powoduje przestój całej sieci, można uruchomić dwa lub nawet więcej serwerów DHCP obsługujących tę samą podsieć. Gdy jeden z serwerów ulegnie awarii, pozostałe będą dalej świadczyć usługi dla podsieci. Każdy z serwerów DHCP musi być podłączony do podsieci bezpośrednio albo za pośrednictwem agenta przekazującego DHCP/BOOTP.

Jako że dwa serwery DHCP nie mogą przypisywać jednakowych adresów, każdy z serwerów działających w jednej podsieci musi mieć do dyspozycji osobną pulę adresów. Dlatego, gdy określona podsieć ma być obsługiwana przez więcej niż jeden serwer DHCP, należy ogólną pulę adresów dostępnych w danej podsieci podzielić na mniejsze i rozłączne pule, pozostające w dyspozycji poszczególnych serwerów. Na przykład, jeden serwer może otrzymać pulę obejmującą 70% adresów dostępnych dla podsieci, a drugi serwer zarządzać będzie pozostałymi 30% dostępnych adresów.

Jednoczesne korzystanie z wielu serwerów DHCP zmniejsza ryzyko przestoju sieci spowodowanego awarią takiego serwera, chociaż nie pozwala takiego ryzyka całkiem wyeliminować. Jeśli wystąpi awaria serwera DHCP w określonej podsieci, inny serwer DHCP może nie obsłużyć wszystkich żądań nowych klientów, które mogą przykładowo spowodować zajęcie dostępnej puli adresów serwera.

W przypadku konfiguracji wieloserwerowej należy pamiętać, że żadne dwa serwery DHCP nie mogą zarządzać tymi samymi adresami. Każdy z serwerów DHCP działających w tej samej podsieci musi mieć do dyspozycji własny, unikalny zakres adresów IP.

Określenie adresów IP, które powinny być zarządzane przez serwer DHCP

Opierając się na schemacie topologii sieci, należy sporządzić zestawienie zakresów adresów sieciowych, które mają być zarządzane przez serwer DHCP. Należy określić, które urządzenia powinny mieć ręcznie skonfigurowane adresy IP (na przykład adres IP routera). Adresy te muszą zostać wyłączone z puli serwera DHCP.

Dodatkowo trzeba rozważyć, czy adresy będą przypisywane przez serwer DHCP w sposób dynamiczny, czy też dla niektórych klientów wymagana jest rezerwacja określonych adresów IP. Rezerwacja określonego adresu i parametrów konfiguracyjnych dla niektórych klientów w podsieci może być potrzebna, na przykład dla klienta będącego serwerem plików. Można także wszystkim klientom przydzielić z góry zadane adresy IP. Omówienie różnic między dynamicznym a statycznym przypisywaniem adresów IP znajduje się w sekcji Obsługa klientów DHCP.

Określanie czasu dzierżawy adresów IP

Domyślny czas dzierżawy dla serwera DHCP wynosi 24 godziny. Optymalny czas dzierżawy dla określonego serwera DHCP zależy od kilku czynników. Należy rozważyć cel, jaki chcemy osiągnąć, sposób i harmonogram pracy danej sieci oraz zasady obsługi serwisowej danego serwera DHCP. Więcej informacji pomocnych w określaniu czasu dzierżawy dla klientów DHCP można znaleźć w sekcji Dzierżawa.

Obsługa klientów BOOTP

Jeśli aktualnie w sieci działa serwer BOOTP, warto wiedzieć, że serwer DHCP może bez trudu zastąpić serwer BOOTP, przy czym odbędzie się to praktycznie w sposób niezauważalny dla klientów BOOTP. Możliwe są trzy sposoby postępowania z obecnymi w sieci klientami BOOTP.

Najłatwiejszym sposobem jest skonfigurowanie serwera DHCP na potrzeby obsługi klientów BOOTP. Obsługa klientów BOOTP przez serwer DHCP polega zasadniczo na przypisaniu każdemu klientowi BOOTP określonego adresu IP, który przestaje być dostępny dla innych klientów. Użycie serwera DHCP ma jednak pewną zaletę: nie ma potrzeby konfigurowania jednoznacznego odwzorowania klientów BOOTP na adresy IP. Serwer DHCP nadal będzie dynamicznie przypisywał adresy IP z puli klientom BOOTP. Kiedy już adres IP zostanie przypisany klientowi BOOTP, adres ten pozostaje na stałe zarezerwowany dla tego klienta, chyba że rezerwacja zostanie usunięta przez administratora. Takie rozwiązanie jest dobre, jeśli w sieci jest duża liczba klientów BOOTP.

Inna możliwość polega na przeprowadzeniu migracji konfiguracji serwera BOOTP do serwera DHCP. W miejsce każdego klienta BOOTP zapisanego w konfiguracji serwera zostanie utworzony klient DHCP. Przy takim trybie postępowania wskazane jest skonfigurowanie klientów jako klientów DHCP. Po zrealizowaniu migracji konfiguracji BOOTP do serwera DHCP mechanizm przypisywania adresów DHCP będzie działał prawidłowo zarówno dla klientów DHCP, jak i dla klientów BOOTP. Jest to nieoceniona zaleta w okresie przejściowym, w trakcie migrowania klientów BOOTP do standardu DHCP. Nawet jeśli rekonfiguracja klientów BOOTP na DHCP będzie się rozciągnięta w czasie, komputery będą mogły bez przeszkód pracować w sieci.

Jako ostatnią opcję można wykonać zamianę wszystkich klientów BOOTP na DHCP i skonfigurowanie serwera DHCP na dynamiczne przypisywanie adresów. Jest to praktycznie równoznaczne z usunięciem usług BOOTP z sieci.

Określanie danych konfiguracyjnych na potrzeby klientów

Na podstawie diagramu topologii sieci łatwo jest wskazać urządzenia (na przykład routery), które muszą być wyróżnione w konfiguracji DHCP. Ponadto należy zidentyfikować inne serwery w sieci, o których informacje powinny być przekazywane klientom, na przykład serwer DNS. Odpowiednie dane można określić dla całej sieci, dla wybranej podsieci lub dla określonego klienta bez względu na podsieć.

W przypadku urządzeń mających znaczenie dla wielu klientów, ich deklaracja powinna być wykonana na najwyższym możliwym poziomie (na przykład, na poziomie globalnym dla całej sieci lub na poziomie wybranej podsieci). Pozwoli to ograniczyć zakres wymaganych zmian w konfiguracji DHCP po zmianie urządzenia. Na przykład, gdyby ten sam router został określony niezależnie dla każdego klienta w sieci, to po zmianie routera konieczne byłoby odpowiednie zaktualizowanie konfiguracji każdego klienta z osobna. Jeśli natomiast router zostanie określony na poziomie globalnym (dane konfiguracyjne routera będą przekazywane centralnie wszystkim klientom), wystarczy zmienić parametry routera w jednym miejscu, a zmiana zostanie uwzględniona przez wszystkich klientów.

W przypadku niektórych klientów może być wymagane indywidualne określenie parametrów konfiguracji TCP/IP na poziomie klienta. Serwer DHCP może rozpoznawać te komputery i przekazywać im specjalnie dobrane dane konfiguracyjne. Dotyczy to nie tylko opcji konfiguracyjnych, lecz także czasu dzierżawy i adresu IP. Na przykład, jeden z klientów może wymagać dłuższego czasu dzierżawy niż obowiązujący dla innych klientów. Innym przykładem może być klient będący serwerem plików, który musi mieć stały, wydzielony adres IP. Zidentyfikowanie tych nietypowych klientów i określenie potrzebnych im danych konfiguracyjnych będzie pomocne przy konfigurowaniu serwera DHCP.

Krótki opis wszystkich opcji konfiguracyjnych można znaleźć w sekcji “Wyszukiwanie opcji DHCP” na stronie 8.

Dynamiczne aktualizowanie rekordów DNS przez serwer DHCP

Jeśli serwer DNS służy do zarządzania wszystkimi nazwami i adresami IP klientów, z pewnością godne polecenia jest zrekonfigurowanie serwera DNS w taki sposób, aby akceptował on dynamiczne aktualizacje z serwera DHCP. Podczas korzystania z funkcji dynamicznego aktualizowania rekordów DNS jakiekolwiek zmiany w adresowaniu klientów przez DHCP stają się niezauważalne z punktu widzenia działania DNS. Więcej informacji dotyczących korzystania z serwera DHCP w połączeniu z serwerem DNS można znaleźć w sekcji Dynamiczne aktualizacje.

Jeśli obecnie w sieci nie jest uruchomiony serwer DNS, warto zastanowić się nad jego wprowadzeniem wraz z serwerem DHCP. Więcej informacji na temat zalet i wymagań związanych z usługami DNS można znaleźć w odpowiedniej sekcji Centrum informacyjnego.

Korzystanie z DHCP na potrzeby klientów zdalnych

Jeśli do sieci należą komputery łączące się z nią zdalnie za pomocą protokołu PPP, możliwe jest skonfigurowanie serwera DHCP w taki sposób, aby dynamicznie przypisywał tym zdalnym klientom adresy IP w chwili podłączenia do sieci. Przykłady sieci, w których taka możliwość została wykorzystana, znajdują się w sekcjach “Przykład: PPP i DHCP na jednym serwerze System i” na stronie 34 i “Przykład: profile DHCP i PPP na różnych serwerach System i” na stronie 36. W przykładach tych opisano także sposób konfiguracji sieci pod kątem łącznego stosowania protokołów PPP i DHCP dla klientów zdalnych.

Pojęcia pokrewne

“Przykłady: DHCP” na stronie 22
Najlepszą metodą na wybranie odpowiedniej instalacji sieci jest porównanie diagramów i przykładów różnych konfiguracji sieci.

“Agenty przekazujące i routery” na stronie 5
Do skutecznego i bezpiecznego przesyłania danych w sieci można użyć zarówno agentów przekazujących DHCP, jak i routerów.

“Obsługa klientów DHCP” na stronie 6
Za pomocą serwera DHCP można zarządzać poszczególnymi klientami w sieci zamiast zarządzać wszystkimi klientami traktowanymi jak wielka grupa (podsieć).

“Dzierżawa” na stronie 3
Kiedy serwer DHCP wysyła dane konfiguracyjne do klienta, dane te mają określony czas dzierżawy. Jest to czas korzystania z przypisanego użytkownikowi adresu IP. Czas trwania dzierżawy można zmienić zgodnie z konkretnymi wymaganiami.

“BOOTP” na stronie 7
Protokół BOOTP (Bootstrap Protocol) jest protokołem konfiguracji hosta, używanym przed wprowadzeniem protokołu DHCP. Obsługa protokołu BOOTP stanowi podzbiór obsługi protokołu DHCP.

“Dynamiczne aktualizacje” na stronie 7
Można skonfigurować serwer DHCP w taki sposób, aby pracował z serwerem DNS w celu dynamicznego aktualizowania danych DNS klientów po przypisaniu adresu IP przez DHCP.

System DNS

Konfigurowanie usług DHCP

Ta sekcja zawiera instrukcje dotyczące konfigurowania serwera i klientów DHCP oraz konfigurowania dynamicznej aktualizacji rekordów DNS.

Odsyłacze pokrewne

“Planowanie usług DHCP” na stronie 39
Konfigurowanie usług DHCP może być procesem czasochłonnym i podatnym na wiele błędów, dlatego niezwykle istotne jest wcześniejsze zaplanowanie konfiguracji serwera DHCP. Aby konfiguracja serwera DHCP przebiegła efektywniej, należy wcześniej rozważyć konfigurację sieci i zagadnienia dotyczące bezpieczeństwa.

Konfigurowanie serwera DHCP i agenta przekazującego BOOTP/DHCP

Informacje z tej sekcji dotyczą konfigurowania, uruchamiania i zatrzymywania serwera DHCP oraz agenta przekazującego BOOTP/DHCP.

Pojęcia pokrewne

“Agenty przekazujące i routery” na stronie 5
Do skutecznego i bezpiecznego przesyłania danych w sieci można użyć zarówno agentów przekazujących DHCP, jak i routerów.

Konfigurowanie serwera DHCP lub przeglądanie jego konfiguracji

Do utworzenia nowej lub przejrzenia istniejącej konfiguracji DHCP można użyć funkcji konfiguracji serwera DHCP.

Aby uzyskać dostęp do konfiguracji serwera DHCP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz polecenie **Konfiguracja**.

W przypadku tworzenia nowej konfiguracji wyświetlany jest ekran kreatora pomagającego w skonfigurowaniu serwera DHCP. W oknie kreatora wyświetlane są podstawowe pytania na temat parametrów konfiguracyjnych w celu uproszczenia procesu tworzenia podsieci. Po zakończeniu pracy kreatora utworzoną konfigurację można modyfikować i ulepszać, dopasowując ją do wymagań danej sieci.

Jeśli serwer DHCP jest już skonfigurowany, wywołanie funkcji konfiguracji serwera DHCP spowoduje wyświetlenie bieżącej konfiguracji z uwzględnieniem wszystkich podsieci i klientów, które mogą być zarządzane poprzez dany serwer, oraz z podaniem informacji, które zostaną wysłane klientom.

Tworzenie skrótu do okna konfiguracji DHCP

Wykonaj następujące czynności, jeśli często przeglądasz konfigurację DHCP i chcesz utworzyć na pulpicie skrót do okna konfiguracyjnego DHCP.

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz **Utwórz skrót**.

Zatrzymywanie i uruchamianie serwera DHCP

Kiedy serwer DHCP jest już skonfigurowany, można go uruchomić lub zatrzymać, wykonując następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy **DHCP**, a następnie wybierz pozycję **Uruchom** lub **Zatrzymaj**.

Konfigurowanie automatycznego uruchamiania serwera DHCP

Aby skonfigurować serwer DHCP tak, aby był on uruchamiany automatycznie, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz polecenie **Konfiguracja**.
3. Kliknij prawym przyciskiem myszy pozycję **Serwer DHCP** i wybierz polecenie **Właściwości**.
4. Zaznacz pole wyboru **Uruchom wraz z TCP/IP**.
5. Kliknij przycisk **OK**.

Dostęp do monitora serwera DHCP

Monitor serwera DHCP umożliwia monitorowanie informacji o aktywnych dzierżawach dla serwera DHCP IBM System i. Ten interfejs graficzny pozwala na wyświetlanie dzierżawionych adresów IP, czasu ich dzierżawienia i dostępności do ponownej dzierżawy.

Aby uzyskać dostęp do monitora serwera DHCP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz polecenie **Monitor**.

Konfigurowanie agenta przekazującego BOOTP/DHCP

W systemie i5/OS jest dostępny agent przekazujący DHCP/BOOTP, który może służyć do przekazywania pakietów DHCP do serwera DHCP znajdującego się w innej sieci.

Aby skonfigurować agenta przekazującego BOOTP/DHCP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **BOOTP/DHCP**.
2. Kliknij prawym przyciskiem myszy **Agent przekazujący BOOTP/DHCP**, a następnie wybierz **Konfigurowanie**.
3. Określ interfejs, poprzez który agent przekazujący będzie odbierał pakiety DHCP, oraz kierunek, w którym pakiety mają być przekazywane, i kliknij przycisk **OK**.

Uruchamianie i zatrzymywanie agenta przekazującego BOOTP/DHCP

Kiedy agent przekazujący DHCP/BOOTP jest już skonfigurowany, można go uruchomić albo zatrzymać, wykonując następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP → BOOTP/DHCP**.
2. Kliknij prawym przyciskiem myszy **Agent przekazujący BOOTP/DHCP**, a następnie wybierz **Uruchom** lub **Zatrzymaj**.

Konfigurowanie automatycznego uruchamiania agenta przekazującego BOOTP/DHCP

Aby skonfigurować automatyczne uruchamianie agenta przekazującego BOOTP/DHCP przy uruchamianiu TCP/IP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP → BOOTP/DHCP**.
2. Kliknij prawym przyciskiem **Agent przekazujący BOOTP/DHCP**, a następnie wybierz **Właściwości**.
3. Zaznacz pole wyboru **Uruchom wraz z TCP/IP** i kliknij przycisk **OK**.

Konfigurowanie klientów do korzystania z DHCP

Po skonfigurowaniu serwera DHCP, należy również skonfigurować klienty, aby mogły na żądanie uzyskiwać od serwera DHCP informacje o konfiguracji.

Poniżej opisano kolejne czynności konfigurowania klientów w systemie Windows w taki sposób, aby pobierały dane o swojej konfiguracji z serwera DHCP. Ponadto zawarto tutaj informacje, jak z poziomu klienta odczytać informacje o dzierżawie danego klienta.

Włączenie DHCP dla klientów systemów Windows Me

Funkcję DHCP dla klientów systemów Windows Me można włączyć lub wyłączyć za pomocą interfejsu graficznego udostępnianego przez system operacyjny Windows Me.

Aby włączyć DHCP, wykonaj następujące czynności:

1. W menu **Start** kliknij opcję **Ustawienia → Panel sterowania**.
2. Kliknij dwukrotnie ikonę **Sieć** i wybierz zakładkę **Protokoły**.
3. Wybierz opcję **Protokół TCP/IP**, a następnie kliknij pozycję **Właściwości**.
4. Na karcie **Adres IP** kliknij opcję **Uzyskaj adres IP z serwera DHCP** i kliknij przycisk **OK**.

Sprawdzanie danych o dzierżawie DHCP dla klientów Windows Me:

Klienty Windows Me zawierają narzędzie wyświetlające adres MAC klienta oraz informacje o dzierżawie DHCP. Pozwala ono również zwalniać i odnawiać dzierżawy DHCP.

Aby sprawdzić dane o dzierżawie DHCP danego klienta, wykonaj następujące czynności:

1. Otwórz okno *Tryb MS-DOS*.
2. Uruchom program **WINIPCFG**.

Uwaga: Narzędzie to nie aktualizuje wyświetlanych informacji dynamicznie, dlatego w celu wyświetlenia efektu modyfikacji ustawień wymagane jest ponowne uruchomienie programu.

Włączenie DHCP dla klientów systemów Windows 2000

Funkcję DHCP dla klientów systemów Windows 2000 można włączyć lub wyłączyć za pomocą interfejsu graficznego udostępnianego przez system operacyjny Windows 2000.

Aby włączyć DHCP, wykonaj następujące czynności:

1. W menu **Start** wybierz pozycję **Ustawienia → Połączenia sieciowe i telefoniczne**.
2. Kliknij prawym przyciskiem myszy odpowiednią nazwę połączenia i wybierz polecenie **Właściwości**.

3. Wybierz pozycję **Protokół TCP/IP**, a następnie wybierz pozycję **Właściwości**.
4. Na karcie **Ogólne** zaznacz opcję **Uzyskaj adres IP z serwera DHCP**.
5. Kliknij przycisk **OK**.

Sprawdzanie adresu MAC i danych o dzierżawie DHCP:

Klienty Windows 2000 i Windows XP zawierają narzędzie wyświetlające adres MAC klienta oraz informacje o dzierżawie DHCP. Pozwala ono również zwalniać i odnawiać dzierżawy DHCP.

Aby sprawdzić dane o dzierżawie DHCP klienta Windows 2000 lub Windows XP, wykonaj następujące czynności:

1. Otwórz okno wiersza poleceń.
2. Uruchom program **IPCONFIG /ALL**.

Uwaga: Narzędzie to nie aktualizuje wyświetlanych informacji dynamicznie, dlatego w celu wyświetlenia efektu modyfikacji ustawień wymagane jest ponowne uruchomienie programu. Ten sam program można wywoływać z użyciem różnych parametrów, co pozwala zwolnić i odnowić dzierżawę (odpowiednio IPCONFIG /RELEASE i IPCONFIG /RENEW). Aby wyświetlić informacje o wszystkich możliwych parametrach, w wierszu poleceń MS-DOS należy wydać polecenie IPCONFIG /?.

Jeśli serwer DHCP ma w imieniu klienta aktualizować rekordy DNS typu A, wymagana jest dodatkowa konfiguracja klientów Microsoft Windows 2000 i Windows XP. Taka konfiguracja może uprościć administrowanie serwerem DNS, ponieważ aktualizacje dla wszystkich klientów będą wykonywane centralnie przez serwer DHCP, a nie indywidualnie przez niektóre klienty.

Aktualizowanie rekordów DNS typu A:

Aby umożliwić systemowi Windows 2000 lub Windows XP używanie serwera DHCP do aktualizowania w imieniu klienta rekordów DNS typu A, wykonaj następujące czynności:

1. W menu **Start** wykonaj jedną z następujących czynności, zależnie od środowiska systemu Windows.
   - W systemie Windows XP: wybierz opcję **Panel sterowania → Połączenia sieciowe**.
   - W systemie Windows 2000: wybierz opcję**Ustawienia → Połączenia sieciowe i telefoniczne**.
2. Kliknij prawym przyciskiem myszy odpowiednią nazwę połączenia i wybierz polecenie **Właściwości**.
3. Wybierz pozycję **Protokół TCP/IP**, a następnie wybierz pozycję **Właściwości**.
4. Kliknij **Zaawansowane**. Na karcie **DNS** upewnij się, że opcja **Zarejestruj adresy tego połączenia w DNS** nie jest zaznaczona.
5. Kliknij przycisk **OK** w panelu Zaawansowane ustawienia TCP/IP.
6. Kliknij przycisk **OK** w panelu Właściwości: Protokół internetowy (TCP/IP).
7. Kliknij przycisk **OK**.

Włączenie DHCP dla klientów systemów Windows XP

Funkcję DHCP dla klientów systemów Windows XP można włączyć lub wyłączyć za pomocą interfejsu graficznego udostępnianego przez system operacyjny Windows XP.

Aby włączyć DHCP, wykonaj następujące czynności:

1. W menu **Start** wybierz opcję **Panel sterowania → Połączenia sieciowe**.
2. Kliknij prawym przyciskiem myszy odpowiednią nazwę połączenia i wybierz polecenie **Właściwości**.
3. Wybierz pozycję **Protokół TCP/IP**, a następnie wybierz pozycję **Właściwości**.
4. Na karcie **Ogólne** wybierz opcję **Uzyskaj adres IP automatycznie**.
5. Kliknij przycisk **OK**.

Sprawdzanie adresu MAC i danych o dzierżawie DHCP:

Klienty Windows 2000 i Windows XP zawierają narzędzie wyświetlające adres MAC klienta oraz informacje o dzierżawie DHCP. Pozwala ono również zwalniać i odnawiać dzierżawy DHCP.

Aby sprawdzić dane o dzierżawie DHCP klienta Windows 2000 lub Windows XP, wykonaj następujące czynności:

1. Otwórz okno wiersza poleceń.
2. Uruchom program **IPCONFIG /ALL**.

Uwaga: Narzędzie to nie aktualizuje wyświetlanych informacji dynamicznie, dlatego w celu wyświetlenia efektu modyfikacji ustawień wymagane jest ponowne uruchomienie programu. Ten sam program można wywoływać z użyciem różnych parametrów, co pozwala zwolnić i odnowić dzierżawę (odpowiednio IPCONFIG /RELEASE i IPCONFIG /RENEW). Aby wyświetlić informacje o wszystkich możliwych parametrach, w wierszu poleceń MS-DOS należy wydać polecenie IPCONFIG /?.

Jeśli serwer DHCP ma w imieniu klienta aktualizować rekordy DNS typu A, wymagana jest dodatkowa konfiguracja klientów Microsoft Windows 2000 i Windows XP. Taka konfiguracja może uprościć administrowanie serwerem DNS, ponieważ aktualizacje dla wszystkich klientów będą wykonywane centralnie przez serwer DHCP, a nie indywidualnie przez niektóre klienty.

Aktualizowanie rekordów DNS typu A:

Aby umożliwić systemowi Windows 2000 lub Windows XP używanie serwera DHCP do aktualizowania w imieniu klienta rekordów DNS typu A, wykonaj następujące czynności:

1. W menu **Start** wykonaj jedną z następujących czynności, zależnie od środowiska systemu Windows.
   - W systemie Windows XP: wybierz opcję **Panel sterowania → Połączenia sieciowe**.
   - W systemie Windows 2000: wybierz opcję**Ustawienia → Połączenia sieciowe i telefoniczne**.
2. Kliknij prawym przyciskiem myszy odpowiednią nazwę połączenia i wybierz polecenie **Właściwości**.
3. Wybierz pozycję **Protokół TCP/IP**, a następnie wybierz pozycję **Właściwości**.
4. Kliknij **Zaawansowane**. Na karcie **DNS** upewnij się, że opcja **Zarejestruj adresy tego połączenia w DNS** nie jest zaznaczona.
5. Kliknij przycisk **OK** w panelu Zaawansowane ustawienia TCP/IP.
6. Kliknij przycisk **OK** w panelu Właściwości: Protokół internetowy (TCP/IP).
7. Kliknij przycisk **OK**.

Konfigurowanie serwera DHCP pod kątem wysyłania dynamicznych aktualizacji DNS

Serwer DHCP można skonfigurować w taki sposób, aby wysyłał do serwera DNS żądania aktualizacji po każdym przypisaniu hostowi nowego adresu. Ten zautomatyzowany proces pozwala zmniejszyć pracochłonność administrowania serwerem DNS w szybko rozrastających się lub zmieniających sieciach TCP/IP oraz w sieciach, w których często zmieniają się położenia hostów.

Gdy klient DHCP otrzyma adres IP, informacja o tym adresie jest natychmiast przekazywana do serwera DNS. Dzięki temu serwer DNS może prawidłowo odczytywać nazwy hostów, nawet jeśli ich adresy IP nie są stałe.

Aby zostały wykonane aktualizacje rekordów, na serwerze musi być zainstalowany serwer DNS (Opcja 31 systemu i5/OS). Interfejsy programistyczne instalowane z Opcją 31 są niezbędne podczas wykonywania dynamicznych aktualizacji przez serwer DHCP. Serwer DNS może działać na odrębnym modelu serwera System i, który umożliwia dynamiczne aktualizowanie adresów. Więcej informacji dotyczących sprawdzania, czy Opcja 31 jest zainstalowana, można znaleźć w sekcji Wymagania systemu DNS.

Aby skonfigurować właściwości DHCP w sposób, który umożliwi serwerowi DHCP wykonywanie dynamicznych aktualizacji DNS, wykonaj poniższe czynności:

1. Rozwiń pozycję **Sieć → Usługa → TCP/IP**.

2. W prawym panelu kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz polecenie **Konfiguracja**.
3. W lewym panelu okna Konfiguracja serwera DHCP kliknij prawym przyciskiem myszy pozycję **Globalne** i wybierz polecenie **Właściwości**.
4. Wybierz zakładkę **Opcje**.
5. Na liście **Wybrane opcje** zaznacz pozycję **opcja 15: Nazwa domeny**. Jeśli opcja 15 nie jest widoczna na liście **Wybrane opcje**, wybierz pozycję 15: Nazwa domeny z listy **Dostępne opcje** i kliknij przycisk **Dodaj**.
6. W polu **Nazwa domeny** określ nazwę domeny, której ma używać klient podczas translacji nazwy hosta za pomocą DNS.
7. Wybierz zakładkę **Dynamiczny DNS**.
8. Zaznacz opcję **Serwer DHCP aktualizuje zarówno rekordy A, jak i PTR** lub **Serwer DHCP aktualizuje tylko rekordy PTR**.
9. Ustaw opcję **Dodaj nazwę domeny do nazwy hosta** na **Tak**.
10. Kliknij przycisk **OK**, aby zamknąć stronę Właściwości globalne.

Pojęcia pokrewne

"Dynamiczne aktualizacje" na stronie 7
Można skonfigurować serwer DHCP w taki sposób, aby pracował z serwerem DNS w celu dynamicznego aktualizowania danych DNS klientów po przypisaniu adresu IP przez DHCP.

Wyłączenie dynamicznego aktualizowania DNS

Wyłączenie funkcji dynamicznego aktualizowania DNS powoduje przywrócenie administratorowi odpowiedzialności za zarządzanie serwerem DNS. Wyłączenie dynamicznego aktualizowania DNS może być dogodne w sieciach, w których zmiana położenia hostów zdarza się rzadko, rozwój i zmiany są sporadyczne, bądź konieczne jest ścisłe administrowanie serwerem DNS.

Aby wyłączyć dynamiczne aktualizowanie DNS z poziomu klienta, wykonaj następujące czynności:

1. W menu **Start** wybierz pozycję **Ustawienia → Połączenia sieciowe i telefoniczne**.
2. Kliknij prawym przyciskiem myszy odpowiednią nazwę połączenia i wybierz polecenie **Właściwości**.
3. Wybierz pozycję **Protokół TCP/IP**, a następnie wybierz pozycję **Właściwości**.
4. Kliknij przycisk **Zaawansowane**.
5. Na karcie **DNS** usuń zaznaczenie opcji ″Zarejestruj adresy tego połączenia w DNS″ i ″Użyj sufiksu DNS tego połączenia do rejestracji w DNS″.
6. Kliknij przycisk **OK**.

Powyższe czynności należy wykonać dla wszystkich połączeń, dla których aktualizacje rekordów DNS mają być przekazane do serwera DHCP.

Zarządzanie dzierżawionymi adresami IP

Do określenia puli adresów IP zarządzanych przez serwer DHCP oraz obowiązującego dla nich czasu dzierżawy można użyć narzędzia konfiguracji DHCP. Aby wyświetlić aktualnie dzierżawione adresy IP, można użyć monitora serwera DHCP.

Monitor serwera DHCP umożliwia monitorowanie informacji o aktywnych dzierżawach dla serwera DHCP System i. Ten interfejs graficzny pozwala na wyświetlanie dzierżawionych adresów IP, czasu ich dzierżawienia i dostępności do ponownej dzierżawy.

Monitor serwera DHCP pozwala także odzyskać adresy IP, które nie są już używane. Jeśli pula adresów DHCP została wyczerpana, można przejrzeć informacje o aktywnej dzierżawie. Uzyskane w ten sposób informacje można wykorzystać do określenia, czy istnieją jakieś dzierżawy, które można usunąć, aby udostępnić adres IP innym klientom. Na przykład może to dotyczyć klienta, który nie jest już podłączony do sieci, a mimo to nadal dysponuje aktywną dzierżawą adresu. Dzierżawę dla takiego klienta można bezpiecznie usunąć. Przed wykonaniem tej operacji należy się jednak upewnić, że klient nie będzie już próbował korzystać z adresu. Serwer DHCP nie powiadamia klientów o

usunięciu ich aktywnych dzierżaw adresów IP. Samodzielne usunięcie aktywnej dzierżawy należącej do klienta, który nadal jest podłączony do sieci, bez zwolnienia adresu ze strony klienta, może prowadzić do ponownego przypisania adresu IP w sieci.

Pojęcia pokrewne

“Problem: podwójne przydziały adresów IP w tej samej sieci” na stronie 49
Adres IP musi być unikalny w obrębie całej sieci. Serwer DHCP nie może przypisać jednego adresu IP więcej niż jednemu klientowi.

Rozwiązywanie problemów z DHCP

Przy rozwiązywaniu problemów z DHCP należy postępować zgodnie z poniższymi wskazówkami.

Jeśli napotkany problem nie został tu opisany, zalecane jest zapoznanie się z tematem “Planowanie usług DHCP” na stronie 39 i upewnić się, że podczas konfigurowania serwera i klientów DHCP zostały uwzględnione wszystkie istotne czynniki.

Należy wybrać opis problemu z poniższej listy lub przeczytać sekcję Gromadzenie szczegółowych informacji o błędzie DHCP, gdzie opisano sposób korzystania z danych protokołu serwera i zapisów śledzenia operacji.

Odsyłacze pokrewne

Używanie śledzenia komunikacji do rozwiązywania problemów z komunikacją

Gromadzenie szczegółowych informacji o błędzie DHCP

Jest kilka sposobów na odszukanie szczegółowych informacji o błędzie, który spowodował problem.

Po pierwsze, należy przejrzeć zawartość protokołu zadania serwera DHCP, wykonując następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP**, a następnie wybierz **Zadania serwera**.

Jeśli protokół zadania serwera DHCP nie zawiera żadnych komunikatów, może być konieczne odczytanie danych zebranych przez funkcję śledzenia komunikacji serwera System i lub wewnętrzną funkcję śledzenia programu serwera DHCP. Śledzenie komunikacji pozwala ustalić, czy żądania klienta docierają do serwera DHCP oraz czy serwer DHCP odpowiada klientowi. Jeśli żądania klienta docierają do celu, ale nie wywołują oczekiwanej reakcji serwera, należy użyć wewnętrznej funkcji śledzenia programu serwera DHCP.

Śledzenie serwera DHCP

Plik protokołu DHCP jest używany do zapisywania informacji protokołowania serwera DHCP. Przeglądanie pliku protokołu DHCP może być pomocne w lokalizowaniu problemu i przyczyn jego wystąpienia.

Aby śledzić pracę serwera, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** → **DHCP**.
2. Kliknij prawym przyciskiem myszy pozycję **DHCP** i wybierz polecenie **Konfiguracja**.
3. Kliknij prawym przyciskiem myszy pozycję **Serwer DHCP** i wybierz polecenie **Właściwości**.
4. Wybierz zakładkę **Protokołowanie**.
5. Zaznacz pole wyboru **Włącz protokołowanie**.
6. Sprawdź, czy w polu **Nazwa** znajduje się wpis **dhcpsd.log**.
7. Zaznacz wszystkie kategorie na liście **Protokołuj** z wyjątkiem pozycji Komunikaty śledzenia i Statystyki (protokoły śledzenia i statystyki są wykorzystywane tylko przez pracowników pomocy technicznej).
8. Kliknij przycisk **OK**.
9. Jeśli serwer DHCP został już uruchomiony, kliknij prawym przyciskiem myszy pozycję **Serwer DHCP** i wybierz polecenie **Aktualizuj serwer**, aby go zrestartować.
10. Odtwórz sytuację, w której problem daje się zaobserwować.

11. Kliknij prawym przyciskiem myszy pozycję **Serwer DHCP** i wybierz pozycję **Właściwości → Protokołowanie**.
12. Usuń zaznaczenie opcji **Włącz protokołowanie**, aby wyłączyć zapisywanie do protokołu.
13. Kliknij przycisk **OK**.
14. Kliknij prawym przyciskiem myszy pozycję **Serwer DHCP**, a następnie wybierz pozycję **Aktualizuj serwer**, aby ponownie uruchomić serwer DHCP.
15. Wyświetl zawartość pliku protokołu DHCP o nazwie QIBM/UserData/OS400/DHCP/dhcpsd.log. Wykonaj jedną z poniższych czynności:
    - W programie System i Navigator rozwiń pozycję ***system*** **→ Systemy plików → Zintegrowany system plików → Root →** ***katalog plików***.
    - W interfejsie znakowym wpisz komendę Praca z dowiązaniami obiektów (Work with Object Links - WRKLNK) i wybierz opcję 5 (Wyświetl).

Problem: klient nie otrzymuje adresu IP ani danych konfiguracyjnych

Jeśli klient nie może uzyskać adresu IP lub danych o konfiguracji, to jest to oznaką wystąpienia problemów. Wydzierżawienie adresu IP klientowi jest czteroetapowym procesem interakcji między klientem a serwerem DHCP.

Aby klient uzyskał adres IP, wszystkie cztery etapy muszą zostać zakończone. Szczegółowe informacje na temat czterech etapów procesu znajdują się w sekcji “Interakcja między klientem a serwerem DHCP” na stronie 1.

Poniżej znajduje się kilka najczęściej spotykanych przyczyn wystąpienia takiego problemu.

Klient jest podłączony do podsieci, która nie została uwzględniona w konfiguracji serwera DHCP.
Należy sprawdzić konfigurację DHCP i ustalić, czy obejmuje ona wszystkie podsieci zarządzane przez serwer DHCP. W przypadku wątpliwości, które podsieci powinny być zarządzane przez serwer DHCP, można skorzystać ze wskazówek w sekcji “Informacje o topologii sieci” na stronie 39.

Komunikat DHCPDISCOVER od klienta nie dociera do serwera DHCP.
Jeśli serwer DHCP nie należy do tej samej podsieci co klient, musi działać router lub agent przekazujący DHCP/BOOTP, odpowiedzialny za przekazywanie wysyłanych przez klienta komunikatów DHCPDISCOVER do serwera DHCP. Więcej informacji zawiera sekcja “Agenty przekazujące i routery” na stronie 5. Serwer musi mieć możliwość nie tylko odebrania rozgłaszanego komunikatu, ale i wysłania pakietów z odpowiedzią z powrotem do podsieci klienta.

Jeśli serwer System i jest systemem multihomed, to może być konieczne dodanie grupy podsieci do konfiguracji DHCP. Szczegółowe informacje na temat konfigurowania DHCP w systemach multihomed znajdują się w sekcji “Przykład: DHCP i serwery multihoming” na stronie 27. W przykładzie tym opisano zmiany, jakie należy wprowadzić w konfiguracji DHCP, aby umożliwić systemowi odebranie rozgłaszanego komunikatu klienta.

Serwer DHCP nie dysponuje już wolnymi adresami, które mógłby przydzielić klientowi.
Monitor serwera DHCP pozwala także wyświetlić adresy, które są aktualnie używane przez serwer DHCP. W sekcji “Zarządzanie dzierżawionymi adresami IP” na stronie 47 znajdują się szczegółowe informacje na temat używania monitora serwera DHCP. Jeśli pula dostępnych adresów serwera DHCP została wyczerpana, rozwiązaniem może być dodanie do puli nowych adresów, skrócenie czasu dzierżawy lub usunięcie niepotrzebnych dzierżaw trwałych.

Problem: podwójne przydziały adresów IP w tej samej sieci

Adres IP musi być unikalny w obrębie całej sieci. Serwer DHCP nie może przypisać jednego adresu IP więcej niż jednemu klientowi.

W określonych warunkach serwer DHCP podejmuje próby ustalenia, czy adres, który ma zostać przypisany klientowi, nie znajduje się właśnie w użyciu. Jeśli serwer DHCP wykryje, że adres, który nie powinien być używany, jest w istocie zajęty, adres ten zostanie tymczasowo oznakowany jako zajęty i nie będzie on przypisywany innym klientom.

Monitora serwera DHCP można użyć do sprawdzenia, które z wykrytych adresów IP są używane, ale nie zostały przypisane przez serwer DHCP. Adresy te będą wyróżnione statusem USED i identyfikatorem klienta UNKNOWN_TO_IBMDHCP.

Poniżej znajduje się kilka najczęściej spotykanych przyczyn wystąpienia takiego problemu.

Więcej niż jeden serwer DHCP ma prawo przypisywać te same adresy IP.
Jeśli konfiguracja dwóch różnych serwerów DHCP pozwala na przypisywanie tych samych adresów IP, to możliwa się staje sytuacja, w której jeden adres IP zostanie przypisany dwóm różnym klientom. Jeden klient otrzyma adres IP z jednego serwera, a drugi klient otrzyma ten sam adres z drugiego serwera. W obrębie jednej podsieci lub sieci może działać wiele serwerów DHCP, lecz pozostające w ich dyspozycji pule adresów nie mogą być takie same ani nie mogą się na siebie nakładać.

Klient został ręcznie skonfigurowany przez nadanie mu adresu IP, który należy do puli zarządzanej w ramach DHCP.
Przed przypisaniem adresu IP klientowi serwer DHCP zazwyczaj próbuje ustalić, czy adres ten nie znajduje się już w użyciu. Nigdy nie ma jednak gwarancji, że ręcznie skonfigurowany klient jest w tym momencie podłączony do sieci oraz że może odpowiedzieć na wysłany przez serwer komunikat sprawdzający zajętość adresu IP. Gdy taka sytuacja wystąpi, adres może zostać przypisany przez DHCP innemu klientowi. Kiedy następnie ręcznie skonfigurowany klient podłączy się do sieci, wystąpi powielenie adresu IP. Adresy IP, które należą do puli zarządzanej przez serwer DHCP, nie powinny być stosowane podczas ręcznego konfigurowania klientów. Jeśli klient wymaga ręcznego przypisania adresu IP, adres ten należy wykluczyć z puli adresów pozostających do dyspozycji serwera.

Pojęcia pokrewne

“Zarządzanie dzierżawionymi adresami IP” na stronie 47
Do określenia puli adresów IP zarządzanych przez serwer DHCP oraz obowiązującego dla nich czasu dzierżawy można użyć narzędzia konfiguracji DHCP. Aby wyświetlić aktualnie dzierżawione adresy IP, można użyć monitora serwera DHCP.

Problem: rekordy DNS nie są aktualizowane przez DHCP

Serwer DHCP System i umożliwia dynamiczne aktualizowanie rekordów DNS. Podczas wybierania właściwego serwera DNS do aktualizacji serwer DHCP korzysta z interfejsów programistycznych i funkcji tłumaczenia nazw. Można użyć tych informacji podczas rozwiązywania problemów wynikających z dynamicznego aktualizowania.

W przypadku, gdy rekordy DNS nie są dynamicznie aktualizowane, należy sprawdzić następujące elementy konfiguracji:

Których podsieci dotyczy aktualizacja oraz jakiego rodzaju rekordy (A, PTR albo obydwa jednocześnie) jej podlegają.
Należy sprawdzić konfigurację DHCP i ustalić, czy faktycznie włączona jest aktualizacja wpisów DNS dla podsieci klientów oraz jakiego typu rekordów aktualizacje dotyczą.

Należy sprawdzić, czy system nazw domen (Opcja 31 systemu i5/OS) jest zainstalowany na serwerze System i, na którym uruchomiony jest DHCP.
Serwer DHCP korzysta z interfejsów programistycznych udostępnianych przez funkcję DNS i5/OS (Opcja 31). Serwer DNS, do którego kierowane są zgłoszenia aktualizacji, nie musi rezydować w tym samym systemie, co serwer DHCP.

Serwer DHCP musi mieć uprawnienia do wysyłania aktualizacji do serwera DNS.
Należy sprawdzić, czy konfiguracja strefy DNS dopuszcza dynamiczne aktualizacje oraz czy serwer DHCP jest uwzględniony na liście kontroli dostępu.

Serwery DNS muszą być zdolne do tłumaczenia nazw hostów w domenie klientów.
Za pomocą komendy CHGTCPDMN należy wyświetlić listę serwerów DNS na serwerze System i, na którym działa DHCP. Wymienione serwery DNS muszą być zdolne do tłumaczenia nazw w domenie, której dotyczą aktualizacje. W tym celu można na serwerze System i obsługującym DHCP uruchomić komendę NSLOOKUP (Name Server Lookup) w celu przetłumaczenia nazwy (lub adresu IP) należącej do domeny stwarzającej problemy podczas aktualizacji. Serwer DHCP musi być w stanie określić pełną nazwę domeny klienta, którego rekord ma zostać zaktualizowany. Serwer DHCP nie podejmie próby dynamicznej aktualizacji DNS,

jeśli nie będzie dysponował pełną nazwą domeny, obejmującą nazwę hosta i nazwę domeny klienta. Serwer DHCP uzyskuje pełną nazwę domeny klienta w następującej kolejności:

1. Opcja 81 (pełna nazwa domeny klienta) w otrzymanym od klienta komunikacie DHCPREQUEST.
2. Opcja 12 (nazwa hosta), Opcja 15 (nazwa domeny) lub obydwie te opcje w otrzymanym od klienta komunikacie DHCPREQUEST.
3. Opcja 12 (nazwa hosta) w komunikacie DHCPREQUEST od klienta, Opcja 15 (nazwa domeny) zapisana w konfiguracji serwera DHCP lub obydwie te opcje. W tym przypadku w celu uzyskania pełnej nazwy domenowej (FQDN), konfiguracja serwera DHCP musi umożliwiać dodanie nazwy domeny do nazwy hosta (opcja określona na zakładce **Właściwości → Dynamiczny DNS** dla poziomu globalnego, podsieci, klasy lub klienta).

Rekord TXT może nie być zgodny z odpowiadającym mu rekordem DNS.

Konfiguracja serwera DHCP może nakazywać sprawdzanie istniejących rekordów DNS w celu ustalenia, z którym klientem DHCP są one skojarzone. Serwer DHCP realizuje tę funkcję, zapisując rekord TXT odpowiadający każdemu aktualizowanemu rekordowi A i PTR. Jeśli system jest skonfigurowany tak, że przed wykonaniem aktualizacji DNS sprawdza identyfikator klienta, to dane w rekordzie TXT muszą być zgodne z identyfikatorem klienta, który otrzymał przydział adresu od serwera DHCP. Jeśli dane te nie są zgodne, serwer DHCP nie wprowadzi aktualizacji rekordu DNS typu A. Taka procedura uniemożliwia nadpisanie istniejących rekordów. Jednak konfiguracja serwera DHCP może nakazywać ignorowanie istniejących rekordów i wykonywanie aktualizacji DNS bez względu na treść rekordu TXT (opcja określona na zakładce **Właściwości → Dynamiczny DNS** dla poziomu globalnego, podsieci, klasy lub klienta).

Pojęcia pokrewne

“Dynamiczne aktualizacje” na stronie 7
Można skonfigurować serwer DHCP w taki sposób, aby pracował z serwerem DNS w celu dynamicznego aktualizowania danych DNS klientów po przypisaniu adresu IP przez DHCP.

Problem: protokół zadania DHCP zawiera komunikaty DNS030B z kodem błędu 3447

Kod błędu 3447 oznacza, że nastąpiło przekroczenie limitu czasu oczekiwania przez serwer DHCP na odpowiedź z serwera DNS. Powodem takiej sytuacji mogą być zakłócenia w pracy sieci lub błąd połączenia między serwerem DHCP System i a serwerem DNS.

Komunikatowi temu będzie towarzyszył komunikat TCP5763, zawierający informację o typie rekordu zasobu DNS oraz szczegółowe dane, jakie serwer DHCP próbował zaktualizować.

Ponieważ serwer DHCP podejmuje próby aktualizacji rekordów zasobów DNS podczas każdego odnowienia dzierżawy, plik konfiguracyjny strefy może już zawierać odpowiedni rekord zasobu, utworzony przy okazji pierwszego przypisania adresu IP lub przy poprzednim odnowieniu dzierżawy. Do sprawdzania danych konfiguracji strefy DNS służy narzędzie NSLOOKUP. Może się okazać, że rekord zasobu jest już obecny i zawiera poprawne dane, przez co nie są wymagane żadne czynności.

Jeśli plik konfiguracyjny strefy DNS nie zawiera odpowiedniego rekordu zasobu, to jest kilka sposobów na jego zaktualizowanie. Serwer DHCP będzie próbował zaktualizować rekord zasobu po otrzymaniu następnego żądania odnowienia dzierżawy. W tym przypadku wystarczy więc zaczekać, aż to nastąpi. Poza tym wiele klientów usiłuje odnowić lub uzyskać adres IP bezpośrednio po włączeniu. W związku z tym można wyłączyć i ponownie uruchomić klienta, co sprawi, że serwer DHCP powtórzy próbę zapisu danych w rekordzie DNS.

Jeśli żadna z tych możliwości nie wchodzi w grę, można ręcznie zaktualizować odpowiedni rekord zasobu DNS. Ta metoda nie jest zalecana, ponieważ podczas dokonywania ręcznych poprawek nie może być uruchomiony mechanizm dynamicznego zarządzania strefą. W trakcie tego przestoju może więc nastąpić utrata innych dynamicznych aktualizacji z DHCP. Do zaktualizowania rekordu zasobu można jednak użyć narzędzi dynamicznej aktualizacji, dostarczanych w niektórych implementacjach klientów i serwera DNS BIND. Chociaż procedura ta przypomina ręczne aktualizowanie danych strefy (administrator musi samodzielnie wpisać dane rekordu zasobu), narzędzie pozwala dokonać aktualizacji bez wyłączania dynamicznego zarządzania strefą.

Informacje pokrewne dotyczące DHCP

Informacje powiązane z kolekcją tematów dotyczących DHCP znajdują się w dokumentacji technicznej IBM (Redbooks) oraz w serwisach WWW. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Dokumentacja techniczna IBM (Redbooks)

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

Ta publikacja IBM Redbooks zawiera informacje na temat obsługi serwerów DNS (Domain Name System) i DHCP (Dynamic Host Configuration Protocol) wchodzących w skład systemu i5/OS. Informacje i przykłady zawarte w tej publikacji Redbooks pomagają zainstalować, dostosować i skonfigurować obsługę DNS i DHCP, a także rozwiązywać ewentualne problemy.

Dokumenty RFC dotyczące DHCP

Dokumenty RFC (Requests for Comments) są to spisane definicje protokołów, które obowiązują lub są proponowane jako standardy dla Internetu. Poniższe dokumenty RFC mogą być pomocne w pełniejszym zrozumieniu DHCP i pokrewnych funkcji:

- RFC 2131: Dynamic Host Configuration Protocol (zastępuje 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)

Odsyłacze pokrewne

“Plik PDF z informacjami dotyczącymi DHCP” na stronie 1
Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Dodatek. Uwagi

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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

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

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

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

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

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

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

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

Licencjonowany program opisany w niniejszym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

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

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje dotyczące interfejsu programistycznego

Niniejsza publikacja opisuje planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu operacyjnego IBM i5/OS.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

AS/400
i5/OS
IBM
IBM (logo)
Redbooks
System i

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

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

Warunki

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

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

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

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

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

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

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

HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Drukowane w USA