

Laboratorium - Wdrożenie DHCPv4

Topologia sieci

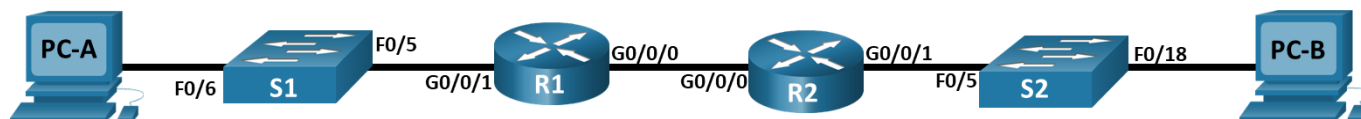


Tabela adresowania

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/0	10.0.0.1	255.255.255.252	nd.
	G0/0/1	nd.	nd.	
	G0/0/1.100			
	G0/0/1.200			
	G0/0/1.1000	nd.	nd.	
R2	G0/0/0	10.0.0.2	255.255.255.252	nd.
	G0/0/1			
S1	VLAN 200			
S2	VLAN 1			
PC-A	karta sieciowa	DHCP	DHCP	DHCP
PC-B	karta sieciowa	DHCP	DHCP	DHCP

Tabela VLAN

VLAN	Nazwa	Przypisany interfejs
1	nd.	S2: F0/18
100	Clients	S1: F0/6
200	Management	S1: VLAN 200
999	Parking_Lot	S1: F0/1-4, F0/7-24, G0/1-2
1000	Native	nd.

Cele

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Część 2: Konfigurowanie i weryfikacja dwóch serwerów DHCPv4 na R1

Część 3: Konfigurowanie i weryfikacja agenta przekazywania DHCP na R2

Wprowadzenie

Protokół DHCP (Dynamic Host Configuration Protocol) to protokół sieciowy, który pozwala administratorom sieci zarządzać i zautomatyzować przypisywanie adresów IP. Bez protokołu DHCP dla protokołu IPv4 administrator musi ręcznie przypisywać i konfigurować adresy IP, preferowane serwery DNS i bramy domyślne. Wraz z rozwojem sieci staje się to problemem administracyjnym, gdy urządzenia są przenoszone z jednej sieci wewnętrznej do drugiej.

W tym scenariuszu firma rozbudowała się, a administratorzy sieci nie mogą już przypisywać adresów IP do urządzeń ręcznie. Twoim zadaniem jest skonfigurowanie routera R1 do przypisywania adresów IPv4 w dwóch różnych podsięciach.

Uwaga: Routery używane w praktycznych laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.4 (obraz universalk9). Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.2 (2) (obraz lanbasek9). Można użyć również innych routerów i przełączników Cisco z różnymi wersjami Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przeglądź tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, że konfiguracje startowe routerów i przełączników zostały wykasowane. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane zasoby

- 2 routery (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalnym)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.2(2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzeń

W części 1 utworzysz topologię sieciową i skonfigurujesz podstawowe ustawienia komputerów i przełączników.

Krok 1: Przygotuj schemat adresowania

Podziel sieć 192.168.1.0/24, aby spełnić następujące wymagania:

- a. Jedna podsieć, „Podsieć A”, obsługująca 58 hostów (VLAN Client w R1).

Podsieć A:

Zapisz pierwszy adres IP w tabeli adresowania dla R1 G0/0/1.100. Zapisz drugi adres IP w tabeli adresów dla sieci VLAN 200 S1 i wprowadź skojarzoną bramę domyślną.

- b. Jedna podsieć, „Podsieć B”, obsługująca 28 hostów (VLAN Management w R1).

Podsieć B:

Zapisz pierwszy adres IP w tabeli adresowania dla R1 G0/0/1.200. Zapisz drugi adres IP w tabeli adresów dla sieci VLAN 1 i wprowadź skojarzoną bramę domyślną.

- c. Jedna podsieć, „Podsieć C”, obsługująca 12 hostów (sieć kliencka w R2).

Podsieć C:

Zapisz pierwszy adres IP w tabeli adresowania dla R2 G0/0/1.

Krok 2: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable tak, jak pokazano na schemacie topologii.

Krok 3: Skonfiguruj podstawowe ustawienia dla każdego routera.

- a. Przypisz routerowi nazwę.
- b. Wyłącz DNS lookup, aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych komend, jako nazw hostów.
- c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.
- d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.
- e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.
- f. Zasyfruj hasła zapisane jawnym tekstem.
- g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.
- h. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).
- i. Ustaw zegar na routerze na dzisiejszą godzinę i datę.

Uwaga: Użyj znaku zapytania (?) aby uzyskać informację pomocniczą o kolejności parametrów potrzebnych do wykonania tego polecenia.

Krok 4: Skonfiguruj routing między sieciami VLAN na R1.

- a. Aktywuj interfejs G0/0/1 na routerze.
- b. Skonfiguruj podinterfejsy dla każdej sieci VLAN zgodnie z tabelą adresowania IP. Wszystkie podinterfejsy używają enkapsulacji 802.1Q i są przypisywane pierwszy adres użytkowy z puli adresów IP, którą obliczono. Upewnij się, że podinterfejs dla natywnej sieci VLAN nie ma przypisanego adresu IP. Dołącz opis dla każdego podinterfejsu.
- c. Sprawdź, czy podinterfejsy działają

Krok 5: Skonfiguruj G0/0/1 na R2, następnie G0/0/0 i routing statyczny dla obu routerów

- a. Skonfiguruj G0/1 na R2 przy użyciu pierwszego adresu IP podsieci C obliczonej wcześniej.
- b. Skonfiguruj interfejs G0/0/0 dla każdego routera na podstawie powyższej tabeli adresowania IP.
- c. Skonfiguruj domyślną trasę na każdym routerze wskazującą na adres IP G0/0/0 na drugim routerze.
- d. Sprawdź, czy routing statyczny działa, wysyłając pakiety ping na adres G0/0/1 routera R2 z routera R1.
- e. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Krok 6: Wykonaj podstawową konfigurację przełączników.

- a. Przypisz nazwę urządzenia do przełącznika.
- b. Wyłącz DNS lookup, aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych komend, jako nazw hostów.

- c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.
- d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.
- e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.
- f. Zaszzyfruj hasła zapisane jawnym tekstem.
- g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.
- h. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).
- i. Ustaw zegar na przełączniku na dzisiejszy czas i datę.

Uwaga: Użyj znaku zapytania (?) aby uzyskać informację pomocniczą o kolejności parametrów potrzebnych do wykonania tego polecenia.

- j. Skopiuj bieżącą konfigurację do startowego pliku konfiguracyjnego.

Krok 7: Utwórz sieci VLAN w S1.

Uwaga: S2 jest skonfigurowany tylko z ustawieniami podstawowymi.

- a. Utwórz i nazwij wymagane sieci VLAN na przełączniku 1 z powyższej tabeli.
- b. Skonfiguruj i aktywuj interfejs zarządzania na S1 (VLAN 200) przy użyciu drugiego adresu IP z podsieci obliczonej wcześniej. Dodatkowo ustaw domyślną bramę dla S1.
- c. Skonfiguruj i aktywuj interfejs zarządzania na S2 (VLAN 1) przy użyciu drugiego adresu IP z podsieci obliczonej wcześniej. Dodatkowo ustaw domyślną bramę dla S2.
- d. Przypisz wszystkie nieużywane porty S1 do sieci VLAN Parking_Lot, skonfiguruj je w trybie dostępu statycznego i dezaktywuj je administracyjnie. Na S2 administracyjnie dezaktywuj wszystkie nieużywane porty.

Uwaga: Polecenie interface range jest pomocne, aby wykonać to zadanie z minimalną koniecznych poleceń.

Krok 8: Przypisz sieci VLAN do odpowiednich interfejsów przełącznika.

- a. Przypisz używane porty do odpowiedniej sieci VLAN (określonej w powyższej tabeli VLAN) i skonfiguruj je w trybie dostępu statycznego.
- b. Sprawdź, czy sieci VLAN są przypisane do odpowiednich interfejsów.

Dlaczego interfejs F0/5 jest wymieniony w VLAN 1?

Krok 9: Ręcznie skonfiguruj interfejs S1 F0/5 jako trunk 802.1Q.

- a. Zmień switchport mode na interfejsie, aby wymusić trunk.
- b. W ramach konfiguracji łącza trunk ustaw natywną sieć jako VLAN 1000.
- c. W ramach innej części konfiguracji łącza trunk określ, że tylko sieci VLAN 100, 200 i 1000 mogą korzystać z łącza.
- d. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.
- e. Zweryfikuj status łącza trunk.

W tym momencie jaki adres IP miałby komputer, gdyby były podłączone do sieci za pomocą DHCP?

Część 2: Konfigurowanie i weryfikacja dwóch serwerów DHCPv4 na R1

W części 2 skonfigurujesz i weryfikujesz serwer DHCPv4 na R1. Serwer DHCPv4 będzie obsługiwał dwie podsieci: podsieć A i podsieć C.

Krok 1: Skonfiguruj R1 z pulami DHCPv4 dla dwóch obsługiwanych podsieci. Tylko pula DHCP dla podsieci A jest podana poniżej

- Wyklucz pierwsze pięć użytecznych adresów z każdej puli adresów.
- Utwórz pulę DHCP (użyj unikatowej nazwy dla każdej puli).
- Określ sieć obsługiwaną przez ten serwer DHCP.
- Ustaw nazwę domeny jako ccna-lab.com
- Skonfiguruj odpowiednią bramę domyślną dla każdej puli DHCP.
- Skonfiguruj czas dzierżawy na 2 dni 12 godzin i 30 minut.
- Następnie skonfiguruj drugą pulę DHCPv4 używając nazwy puli R2_Client_LAN i obliczonej sieci, domyślnego routera i użyj tej samej nazwy domeny i czasu dzierżawy z poprzedniej puli DHCP.

Krok 2: Zapisz konfigurację

Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Krok 3: Sprawdź konfigurację serwera DHCPv4

- Wydadź polecenie **show ip dhcp pool**, aby sprawdzić szczegóły puli.
- Wydadź polecenie **show ip dhcp bindings**, aby sprawdzić ustalone przypisania adresów DHCP.
- Wydadź polecenie **show ip dhcp server statistics**, aby sprawdzić komunikaty DHCP.

Krok 4: Spróbuj uzyskać adres IP z DHCP na komputerze PC-A

- Otwórz wiersz poleceń na PC-A i wydaj polecenie **ipconfig /renew**.
- Po zakończeniu procesu odnawiania wydaj polecenie **ipconfig**, aby wyświetlić nowe informacje IP.
- Przetestuj łączność wydając ping na adres IP interfejsu G0/0/1 routera R1.

Część 3: Konfigurowanie i weryfikacja agenta przekazywania DHCP na R2

W części 3 zostanie skonfigurowany R2 do przekazywania żądań DHCP z sieci lokalnej na interfejsie G0/0/1 do serwera DHCP (R1).

Krok 1: Skonfiguruj R2 jako agenta przekazywania DHCP dla sieci LAN na G0/0/1

- Skonfiguruj polecenie **ip helper-address** na G0/0/1, określając adres IP G0/0/0 routera R1.
- Zapisz konfigurację.

Krok 2: Spróbuj uzyskać adres IP z DHCP na komputerze PC-B

- Otwórz wiersz poleceń na PC-B i wydaj polecenie **ipconfig /renew**.
- Po zakończeniu procesu odnawiania wydaj polecenie **ipconfig**, aby wyświetlić nowe informacje IP.
- Przetestuj łączność wydając ping na adres IP interfejsu G0/0/1 routera R1.
- Wydadź polecenie **show ip dhcp binding** na R1, aby zweryfikować powiązania DHCP.

- e. Wyдай polecenie **show ip dhcp server statistics** na R1 i R2, aby zweryfikować komunikaty DHCP.