

T: Konfiguracja router NAT w Windows Server 2019.

Cel ogólny lekcji: Nauczenie uczniów konfiguracji routera NAT w Windows Server 2019 z wykorzystaniem usługi Routing i dostęp zdalny (RRAS).

Cele szczegółowe

- Prawidłowa identyfikacja i nazwanie interfejsów LAN oraz WAN.
- Konfiguracja adresacji interfejsu LAN.
- Instalacja roli „Dostęp zdalny” oraz funkcji „Trasowanie”.
- Konfiguracja RRAS jako router NAT.
- Wykonanie testów poprawności działania NAT.
- Udokumentowanie wyników (wnioski).

1. Przygotowanie środowiska

Przed przystąpieniem do ćwiczenia

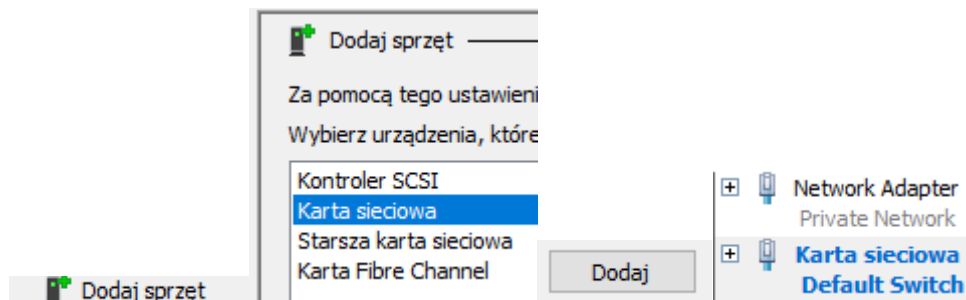
a. Przywróć właściwy punkt kontrolny przed rozpoczęciem konfiguracji. W Hyper-V wykonaj:

Wybierz *nazwa twojej grupy_2019* → Punkty kontrolne → wybierz punkt kontrolny → Prawoklik → Zastosuj → Zastosuj.

b. Upewnij się, że pracujesz na punkcie kontrolnym, w którym serwer **NIE pełni funkcji kontrolera domeny (DC)**. W tym ćwiczeniu Windows Server 2019 musi działać jako serwer standalone, ponieważ konfiguracja NAT w RRAS nie jest wykonywana na kontrolerze domeny.

c. Upewnij się, że serwer dysponuje dwoma interfejsami sieciowymi: LAN i WAN. Interfejs WAN musi mieć dostęp do Internetu, a interfejs LAN będzie służył do obsługi klientów.

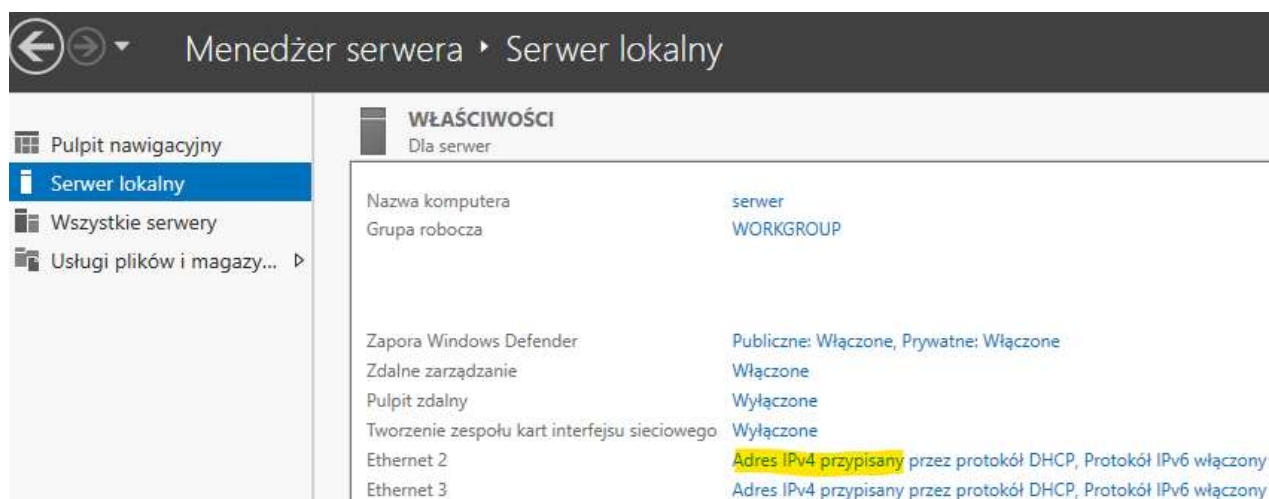
Aby dodać interfejsy sieciowe dla serwera wybierz, odpowiednią maszynę > Ustawienia >



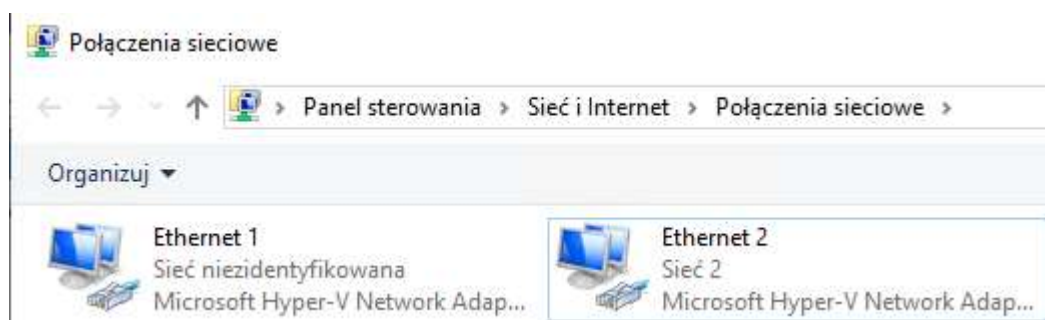
Uruchom maszynę właściwego serwera Windows 2019 > Ctrl+Delete > Administrator > zaq1@WSX

Po uruchomieniu pojawi się komunikat dotyczący sieci wybierz **Tak**.

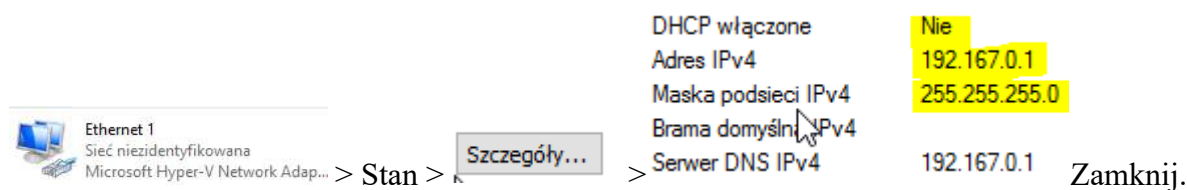
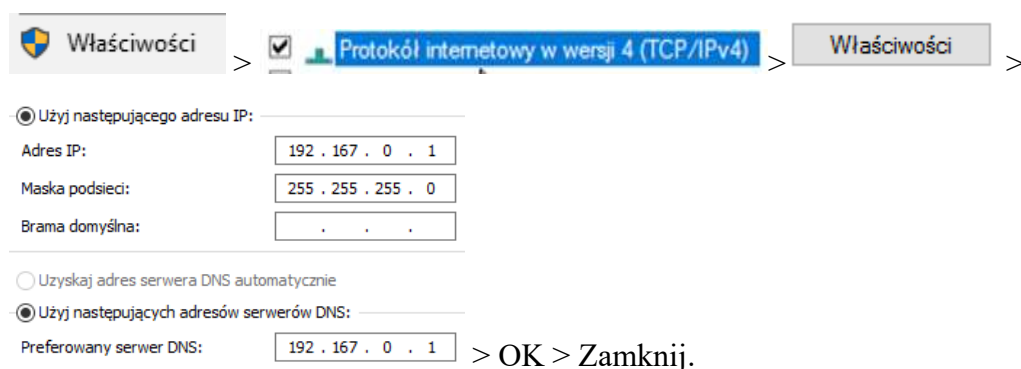
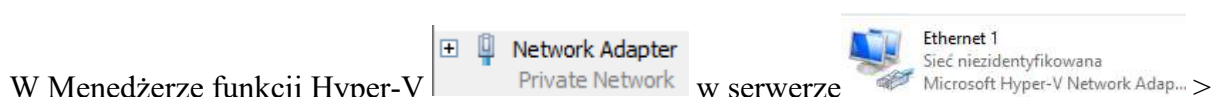
Wybierz **Adres IPv4 przypisany ...** jak poniżej



Otworzy się okno podobne do tego poniżej



Wykonaj konfigurację interfejsów sieciowych serwera jak poniżej:



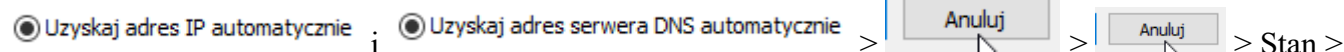
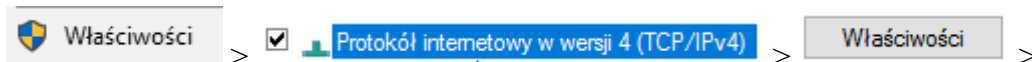
W Menedżerze funkcji Hyper-V

Karta sieciowa
Default Switch

w serwerze



>



> Stan >

Opis	Microsoft Hyper-V 1
Adres fizyczny	00-15-5D-07-2E-36
DHCP włączone	Tak
Adres IPv4	172.27.131.227
Maska podsieci IPv4	255.255.240.0
Dzierżawa uzyskana	wtorek, 3 stycznia :
Dzierżawa wygasa	środa, 4 stycznia 2l
Brama domyślna IPv4	172.27.128.1
Serwer DHCP IPv4	172.27.128.1
Serwer DNS IPv4	172.27.128.1

Szczegóły...

(przykładowe dane konfiguracyjne mogą się różnić).

Pozostaw włączony serwer.

Następnie przywróć punkt kontrolny klienta Windows 11.

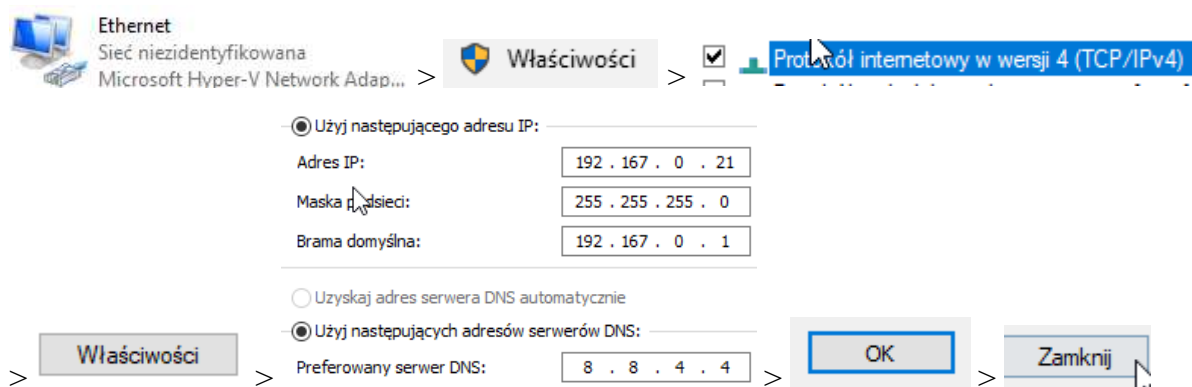
Przygotuj klienta Windows 11 jak poniżej:

W Hyper-V wybierz Ustawienia

Karta sieciowa
Private Network

Uruchom klienta Windows 11 Podaj login: admin > i hasło: zaq1@WSX

Panel sterowania > Sieć i Internet > Połączenia sieciowe



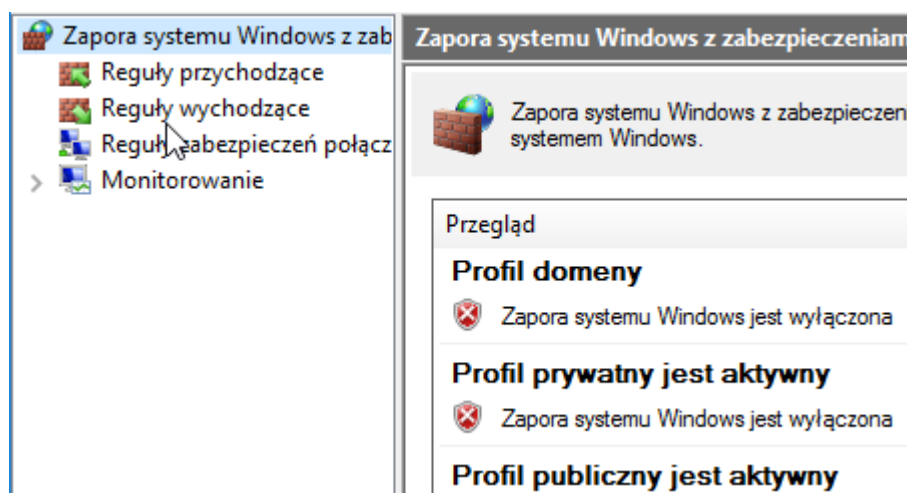
Ethernet Sieć 2 Microsoft Hyper-V Network Adap...	DHCP włączone	Nie
	Adres IPv4	192.167.0.21
	Maska podsieci IPv4	255.255.255.0
	Brama domyślna IPv4	192.167.0.1
	Serwer DNS IPv4	8.8.4.4

Na kliencie i serwerze wyłącz całą zaporę (na czas konfiguracji RRAS NAT)

Serwer i klient → PowerShell (uruchom jako Administrator):

Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False

lub w środowisku graficznym



W zeszycie opisz krok po kroku konfigurację: interfejsy, instalacja roli, RRAS NAT, testy, statystyki, wnioski.

Uwaga – adresacja 192.167.x.x (laboratorium)

W praktyce produkcyjnej używamy prywatnych zakresów RFC1918: **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16**. Adres **192.167.x.x** **nie jest prywatny** – należy do przestrzeni traktowanej jako publiczna, więc **nie wolno** go stosować w realnych sieciach LAN (ryzyko konfliktu z Internetem).

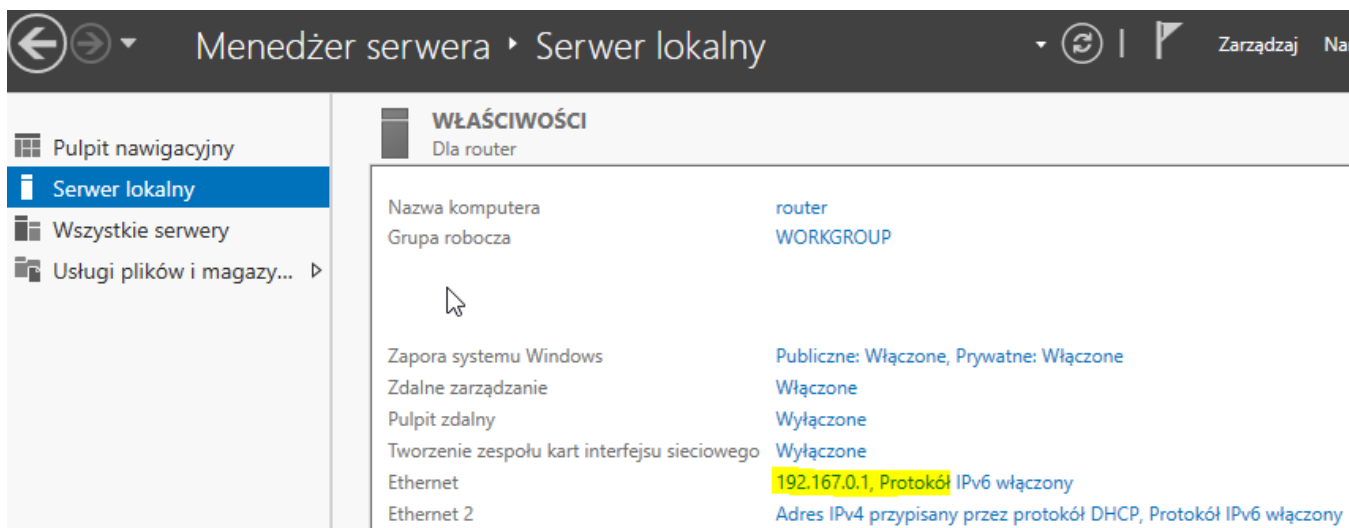
W tych ćwiczeniach używamy **192.167.x.x celowo**, wyłącznie w **odizolowanym środowisku wirtualnym** (Hyper-V), aby **wyraźnie odróżnić sieć laboratoryjną** od fizycznej i uniknąć kolizji z typowym 192.168.x.x. W projektach i w pracy zawodowej **zawsze** stosuj adresację prywatną z RFC1918. *(Ta notatka ma charakter dydaktyczny i dotyczy tylko środowiska lab.)*

Pozostaw włączony serwer Windows 2019

Wykonaj:

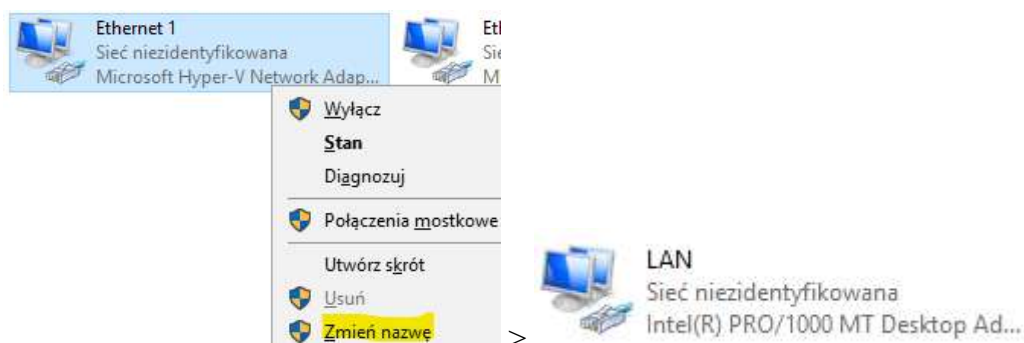
1. **Mapowanie interfejsów i nadanie nazw (Hyper-V ↔ Windows)**, aby lepiej je zidentyfikować. Serwer musi mieć dwie karty sieciowe, jedną skonfigurowaną dla sieci wewnętrznej o nazwie LAN), a drugą skonfigurowaną do dostępu do Internetu o nazwie WAN.

Skonfiguruj interfejsy serwera, w tym celu w menedżerze serwera wybierz (kliknij) **192.167.0.1, ...**



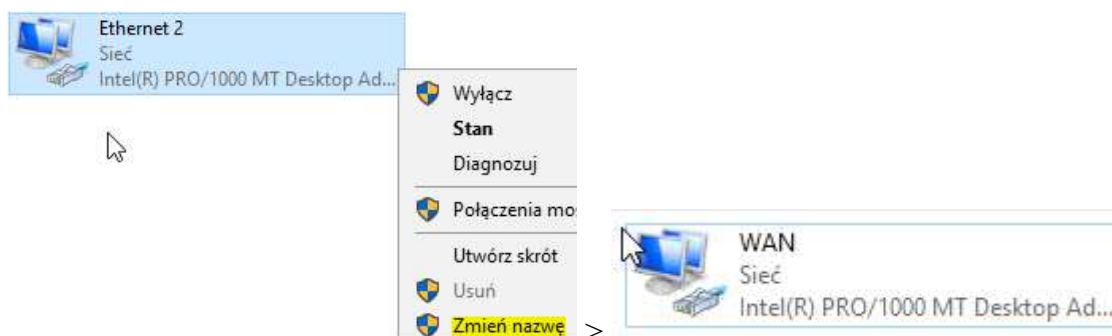
LAN (Private Network → LAN)

- Sprawdź MAC adaptera VM podłączonego w Hyper-V do przełącznika **Private Network**.
- W Windows otwórz **Połączenia sieciowe**, znajdź kartę z **tym samym adresem MAC** i nazwij ją.
- W oknie **Połączenia sieciowe**: wybierz kartę → **Zmień nazwę** → wpisz **LAN**:



WAN (Default Switch → WAN)

- Sprawdź MAC adaptera VM podłączonego w Hyper-V do przełącznika **Default Switch**.
- W Windows znajdź kartę z **tym samym adresem MAC** i nazwij ją.
- W oknie **Połączenia sieciowe**: wybierz kartę → **Zmień nazwę** → wpisz **WAN**:



To powinno wyglądać tak:



Uwaga: Porównujesz MAC w Hyper-V z MAC w Windows, aby mieć pewność, że **to ten sam interfejs**. Nie ustawiaj identycznego MAC na dwóch różnych kartach (LAN i WAN).

Powinno wyglądać tak:

- LAN – połączony z **Private Network** (ten sam MAC w Hyper-V i Windows).
- WAN – połączony z **Default Switch** (ten sam MAC w Hyper-V i Windows).

Adapter LAN musi być skonfigurowany ze statycznym adresem, adapter WAN powinien być ustawiony na DHCP.

Adres skonfigurowany na karcie LAN to adres, którego komputery klienckie będą używać jako bramy.

LAN	192.167.0.1, Protokół IPv6 włączony
WAN	Adres IPv4 przypisany przez protokół DHCP, Protokół IPv6 włączony

2. Dodanie roli serwera „Dostęp zdalny”

Zainstaluj rolę serwera „Dostęp zdalny”. Otwórz Menedżer serwera i wybierz „Dodaj role i funkcje”.



Naciskaj „Dalej”, aż dojdiesz do poniższego ekranu. Wybierz rolę „Dostęp zdalny” i naciśnij „Dalej”.

Wybieranie ról serwera

SERWER DOCELOWY
router

Zanim rozpoczniesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Dostęp zdalny

Usługi ról

Potwierdzenie

Wyniki

Wybierz jedną lub więcej ról do zainstalowania na wybranym serwerze.

Role

- ☒ Dostęp zdalny
- ☐ Hyper-V
- ☐ Serwer DHCP
- ☐ Serwer DNS
- ☐ Serwer faksów
- ☐ Serwer sieci Web (IIS)
- ☐ Środowisko systemu Windows Server Essentials
- ☐ Usługa Ochrona hosta
- ☐ Usługi aktywacji zbiorczej
- ☐ Usługi certyfikatów Active Directory
- ☐ Usługi domenowe Active Directory
- ☐ Usługi drukowania i zarządzania dokumentami
- ☐ Usługi federacyjne Active Directory (AD FS)
- ☐ Usługi LDS w usłudze Active Directory
- ☐ Usługi MultiPoint
- ☒ Usługi plików i magazynowania (Zainstalowano 1 z 2)
- ☐ Usługi pulpitu zdalnego
- ☐ Usługi wdrażania systemu Windows
- ☐ Usługi zarządzania prawami dostępu w usłudze Active Directory

Opis

Funkcja DirectAccess zapewnia zawsze działające i zarządzane połączenie. Serwer zdalnego dostępu zapewnia tradycyjne usługi wirtualnej sieci prywatnej, w tym łączność między lokalnymi (w oddziałach firmy lub chmurze). Serwer proxy aplikacji sieci Web umożliwia publikowanie wybranych aplikacji opartych na protokołach HTTP i HTTPS z sieci firmowej na urządzeniach klienckich znajdujących się poza nią. Routing zapewnia tradycyjne możliwości, w tym translację adresów sieciowych i inne opcje łączności. Serwer dostępu zdalnego i routing można wdrożyć w trybie wielodostępnym lub z pojedynczym dostępem.

< Wstecz

Dalej >

Zainstaluj

Anuluj

Naciśnij „Dalej” na następnym ekranie.

Wybieranie funkcji

SERWER DOCELOWY
router

Zanim rozpoczniesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Dostęp zdalny

Usługi ról

Potwierdzenie

Wyniki

Wybierz jedną lub więcej funkcji do zainstalowania na wybranym serwerze.

Funkcje

- ☐ Serwer zarządzania adresami IP (IPAM)
- ☐ SMB Bandwidth Limit
- ☐ Struktura biometryczna systemu Windows
- ☐ Szyfrowanie dysków funkcją BitLocker
- ☒ Usługa aktywacji procesów systemu Windows
- ☐ Usługa bezprzewodowej sieci LAN
- ☒ Usługa inteligentnego transferu w tle (BITS)
- ☐ Usługa serwera iSNS
- ☒ Usługa SNMP
- ☐ Usługa Windows Search
- ☐ Usługi Simple TCP/IP
- ☐ Wewnętrzna baza danych systemu Windows
- ☐ Wielościeżkowe We/Wy
- ☐ Windows Identity Foundation 3.5
- ☒ Windows PowerShell (Zainstalowano 2 z 5)
- ☐ Zarządzanie magazynami systemu Windows opartymi na plikach
- ☐ Zarządzanie zasadami grupy
- ☐ Zdalne wywoływanie procedur za pośrednictwem WMI
- ☐ Zestaw administracyjny menedżera połączeń RAS

Opis

Usługa BranchCache instaluje usługi wymagane do skonfigurowania tego komputera jako serwera hostowanej pamięci podręcznej lub serwera zawartości z włączoną usługą BranchCache. W przypadku wdrażania serwera zawartości należy go również skonfigurować jako serwer sieci Web HTTP (Hypertext Transfer Protocol) lub serwer aplikacji oparty na usłudze inteligentnego transferu w tle (BITS, Background Intelligent Transfer Service). Aby wdrożyć serwer plików z włączoną usługą BranchCache, użyj Kreatora dodawania ról w celu zainstalowania roli serwera usług plików z usługą serwera plików i usługą BranchCache dla plików sieciowych.

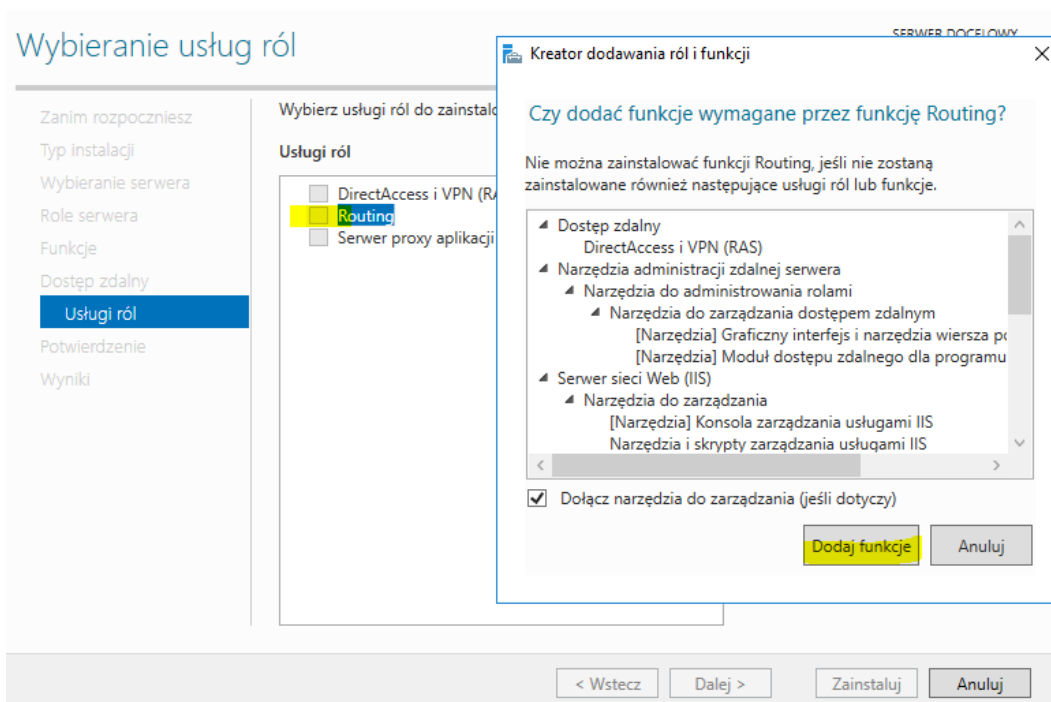
< Wstecz

Dalej >

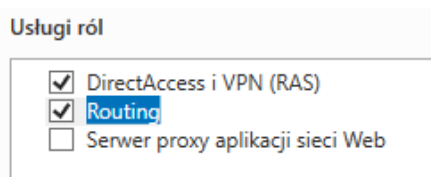
Zainstaluj

Anuluj

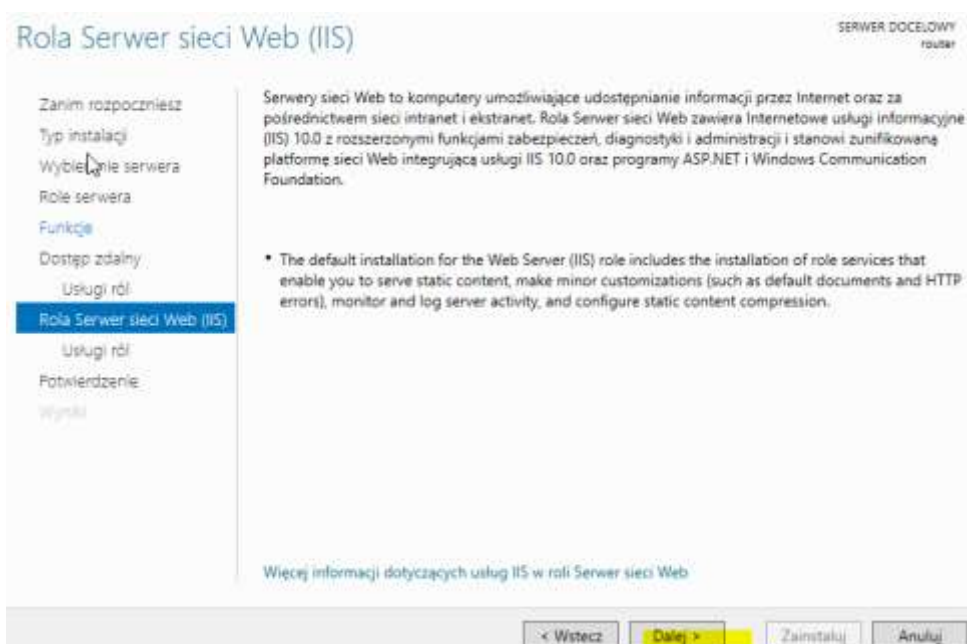
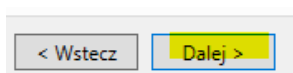
Naciśnij „Dalej”, a następnie wybierz „Trasowanie”, jak pokazano poniżej:



Kliknij „Dodaj funkcje”.



Idź do końca kreatora, naciskając „Dalej”. Naciśnij „Zainstaluj” na ekranie potwierdzenia.



Wybieranie usług ról

SEKWER DOCELOWY
router

Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Rola serwera
Funkcje
Dostęp zdalny
Usługi ról
Rola Serwer sieci Web (IIS)
Usługi ról
Potwierdzenie
Wyniki

Wybierz usługi ról do zainstalowania dla roli Serwer sieci Web (IIS).

Usługi ról

- ☒ Serwer sieci Web
 - ☒ Kondycja i diagnostyka
 - ☒ Rejestrowanie HTTP
 - ☐ Monitor żądań
 - ☐ Narzędzia rejestrowania
 - ☐ Rejestrowanie niestandardowe
 - ☐ Rejestrowanie ODBC
 - ☐ Śledzenie
 - ☒ Wspólne funkcje HTTP
 - ☒ Błędy HTTP
 - ☒ Dokument domyślny
 - ☒ Przeglądanie katalogów
 - ☒ Zawartość statyczna
 - ☐ Przekierowywanie HTTP
 - ☐ Publikowanie WebDAV
 - ☒ Wydajność
 - ☒ Kompresja zawartości statycznej
 - ☐ Kompresja zawartości dynamicznej
 - ☒ Zabezpieczenia

Opis

Funkcja Serwer sieci Web oferuje obsługę witryn sieci Web w formacie HTML i opcjonalną obsługę programów ASP.NET i ASP oraz rozszerzeń serwera sieci Web. Serwera sieci Web można używać do obsługi wewnętrznej lub zewnętrznej witryny sieci Web albo w celu dostarczenia środowiska deweloperom, którzy tworzą aplikacje sieci Web.

< Wstecz Dalej > Zainstaluj Anuluj

Kreator dodawania ról i funkcji

Potwierdzanie opcji instalacji

SEKWER DOCELOWY
router

Zanim rozpoczniesz
Typ instalacji
Wybieranie serwera
Rola serwera
Funkcje
Dostęp zdalny
Usługi ról
Rola Serwer sieci Web (IIS)
Usługi ról
Potwierdzenie
Wyniki

Aby zainstalować następujące role, usługi ról lub funkcje na wybranym serwerze, kliknij przycisk Zainstaluj.

☒ Automatycznie uruchom ponownie serwer docelowy, jeśli będzie to potrzebne

Kreator dodawania ról i funkcji

Jeśli jest wymagane ponowne uruchomienie, ten serwer zostanie automatycznie ponownie uruchomiony bez dodatkowych powiadomień. Czy chcesz zezwolić na automatyczne ponowne uruchamianie?

Tak Nie

Graficzny interfejs i narzędzia wiersza polecenia dostępu zdalnego
Moduł dostępu zdalnego dla programu Windows PowerShell

Serwer sieci Web (IIS)

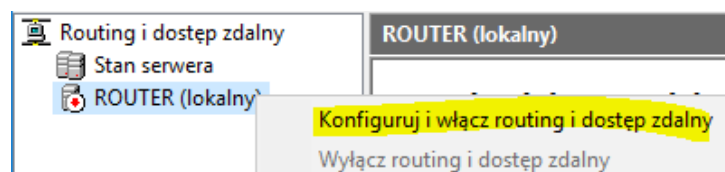
Eksportuj ustawienia konfiguracji
Określanie alternatywnej ścieżki źródłowej

< Wstecz Dalej > Zainstaluj Anuluj

3. Konfigurowanie „routera NAT”

Po zakończeniu instalacji otwórz „Routing i dostęp zdalny”. W „Narzędziach” znajdź „Routing i dostęp zdalny”.

Kliknij prawym przyciskiem myszy nazwę serwera i wybierz „Konfiguruj i włącz routing i dostęp zdalny”.



Naciśnij „Dalej” na ekranie powitalnym kreatora. Wybierz „Translacja adresów sieciowych (NAT)” i naciśnij „Dalej”.

Kreator instalacji serwera routingu i dostępu zdalnego

Konfiguracja

Możesz włączyć dowolną kombinację usług lub dostosować ten serwer.

☐ Dostęp zdalny (połączenie telefoniczne lub sieć VPN)
Zezwalaj klientom zdalnym na łączenie się z tym serwerem poprzez połączenie telefoniczne lub bezpieczne połączenie internetowe wirtualnej sieci prywatnej VPN.

☒ **Translator adresów sieciowych**
Zezwalaj klientom wewnętrznym na łączenie się z Internetem przy użyciu jednego publicznego adresu IP.

Wybierz adapter WAN i naciśnij „Dalej”.

Kreator instalacji serwera routingu i dostępu zdalnego

Połączenie internetowe NAT

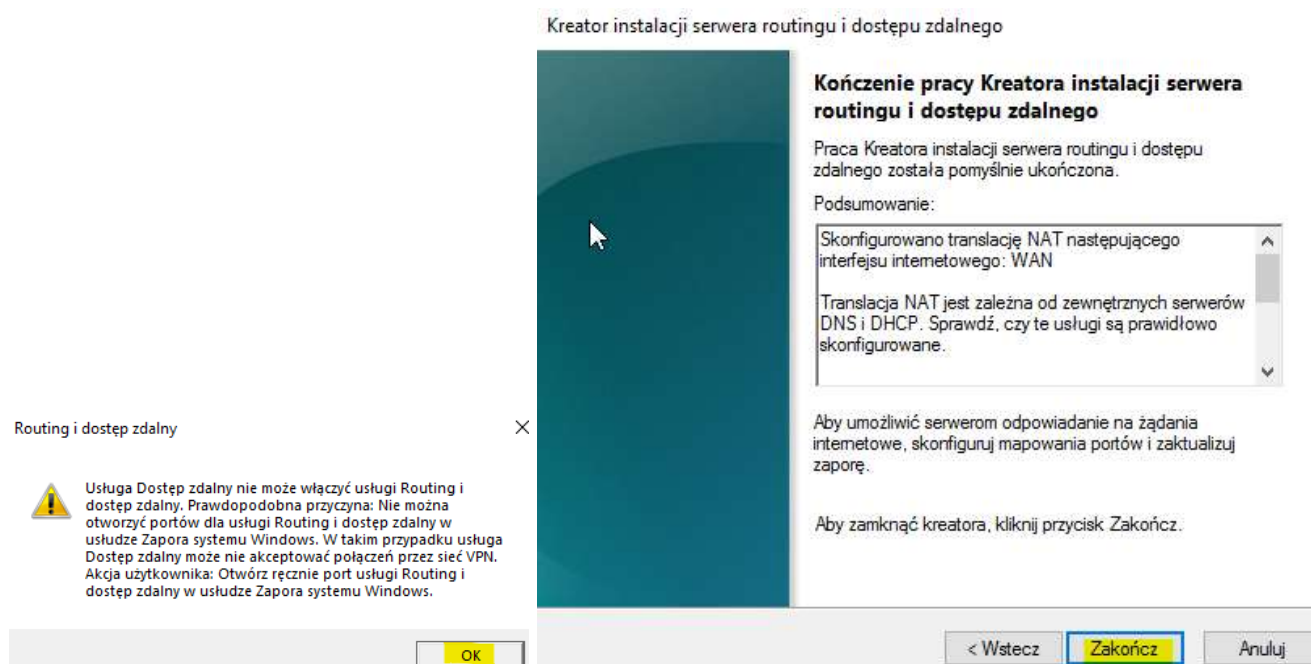
Można zaznaczyć istniejący interfejs albo utworzyć nowy interfejs wybierania numeru na żądanie połączenia komputerów klienckich z Internetem.

☒ Użyj tego interfejsu publicznego do łączenia się z Internetem:
Interfejsy sieciowe:

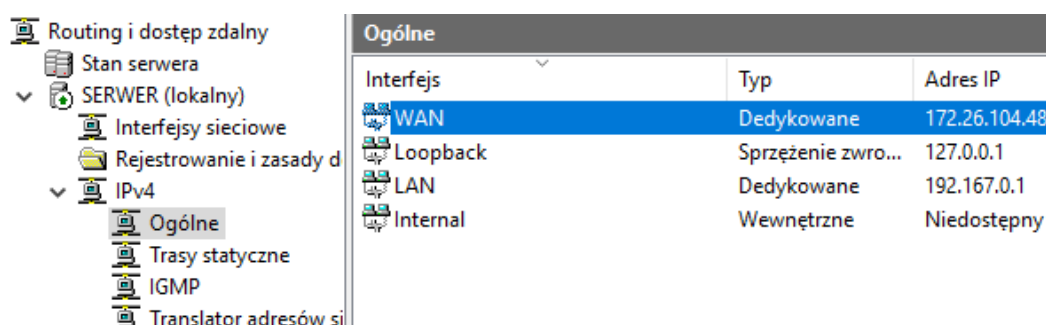
Nazwa	Opis	Adres IP
LAN	Intel(R) PRO/1000 MT...	192.167.0.1
WAN	Intel(R) PRO/1000 MT...	10.0.3.15 (DHCP)

☐ Utwórz nowy interfejs wybierania numeru na żądanie do Internetu
Interfejs wybierania numeru na żądanie jest aktywowany, gdy klient używa Internetu. Wybierz tę opcję, jeśli ten serwer łączy się za pomocą modemu lub przy użyciu protokołu Point-to-Point Protocol w sieci Ethernet. Kreator interfejsu wybierania numeru na żądanie zostanie uruchomiony po zakończeniu pracy tego kreatora.

< Wstecz **Dalej >** Anuluj



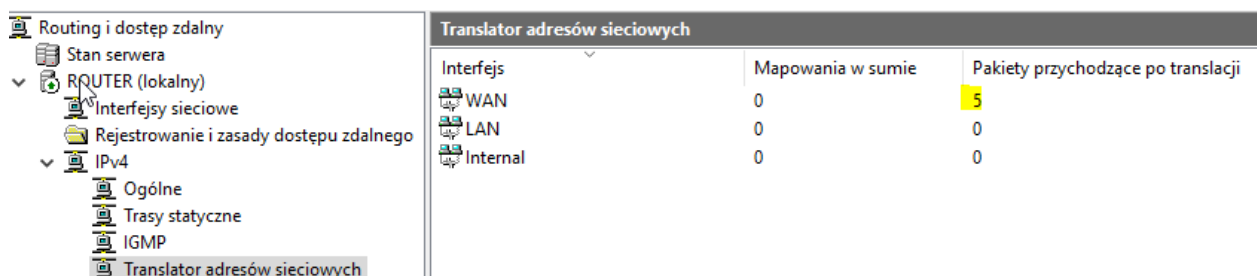
Naciśnij „Zakończ”, poczekaj na zakończenie konfiguracji i sprawdź, czy router NAT działa poprawnie.



4. Testy „routera NAT”

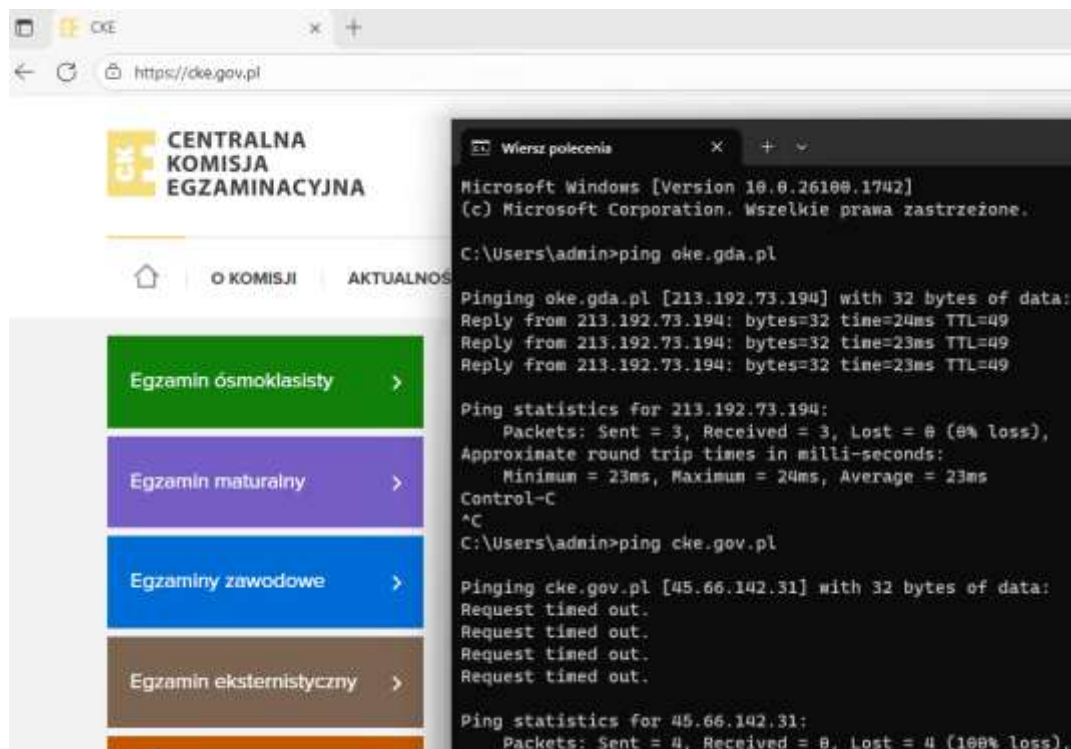
- a) Na serwerze wykonaj **ping zakończony sukcesem** do 192.167.0.21, oke.gda.pl, 1.1.1.1 oraz ping do cke.gov.pl **nie odpowiada** (pozostaw do sprawdzenia).

Rozwiń węzeł IPv4, wybierz „NAT” i powinieneś zobaczyć, że pakiety zostały przetłumaczone.



- b) Na kliencie (Windows 11) wykonaj **ping zakończony sukcesem** do 192.167.0.1, oke.gda.pl, 1.1.1.1 oraz ping do cke.gov.pl **nie odpowiada** (pozostaw do sprawdzenia).

c) Na kliencie (Windows 11) otwórz w przeglądarce **stronę cke.gov.pl z sukcesem** (pozostaw do sprawdzenia).



W czasie testów po konfiguracji NAT może się zdarzyć, że:

- ping do niektórych stron działa, np. ping oke.gda.pl
- ping do innych stron nie działa, np. ping cke.gov.pl

To zachowanie **nie oznacza błędu w Twojej konfiguracji NAT**.

Dlaczego tak się dzieje? Niektóre serwery w Internecie **blokuja ruch ICMP (ping)**, aby zwiększyć bezpieczeństwo. Mimo że ping jest zablokowany, **strona WWW działa prawidłowo**, co widać na ekranie - przeglądarka bez problemu otwiera stronę CKE, chociaż ping cke.gov.pl nie odpowiada.

Wniosek dla ucznia: Jeśli strona WWW otwiera się poprawnie, a ping nie działa, oznacza to, że **NAT działa prawidłowo**, a brak odpowiedzi ping wynika tylko z konfiguracji zdalnego serwera, a nie z Twojego błędu.

d) Na serwerze pozostaw do sprawdzenia poniższe konsole (wynik podobny, ale nie identyczny):

Translator adresów sieciowych

Interfejs	Mapowania w sumie	Pakiety przychodzące
WAN	102	185 335
LAN	0	0
Internal	0	0

Ogólne

Interfejs	Typ	Adres IP	Bajty przychodzące	Bajty wychodzące
WAN	Dedykowane	10.0.3.15	359 762 660	6 730 402
Loopback	Sprzężenie zwro...	127.0.0.1	0	0
LAN	Dedykowane	192.167.0.1	5 828 765	355 168 847
Internal	Wewnętrzne	Niedostępny	-	-

Poniżej wyjaśnienie do instrukcji dla ucznia, odnoszące się do tego, co widać powyżej z **RRAS → IPv4 → Translator adresów sieciowych** oraz z **Interfejsy sieciowe → Ogólne**.

Po wykonaniu konfiguracji NAT w RRAS należy sprawdzić, czy ruch sieciowy klientów jest poprawnie tłumaczony. W tym celu:

1. Przejdź do: **Routing i dostęp zdalny → IPv4 → Translator adresów sieciowych**

2. Co powinno być widoczne?

- **Interfejs WAN** – powinien mieć **rosnące wartości** w kolumnach: **Mapowania w sumie** oraz **Pakiety przychodzące**. Oznacza to, że serwer wykonuje translację adresów dla ruchu wychodzącego klientów.
- **Interfejs LAN** – zwykle pokazuje **0 pakietów przychodzących**, ponieważ nie wykonuje translacji. Jest to normalne, bo NAT działa tylko na interfejsie zewnętrznym (WAN).

3. Dodatkowe potwierdzenie działania NAT

W sekcji: **Routing i dostęp zdalny → IPv4 → Interfejsy sieciowe → Ogólne**

- Interfejs **WAN** powinien pokazywać duże wartości w kolumnie **Bajty przychodzące** oraz **Bajty wychodzące** – oznacza to, że ruch przechodzi przez router.
- Interfejs **LAN** będzie miał ruch tylko od strony klientów.

Wniosek dla ucznia: Jeśli podczas testu (ping, otwieranie stron WWW) liczby przy interfejsie **WAN** **rosną**, oznacza to, że **NAT działa prawidłowo**, a ruch z sieci LAN jest tłumaczony i przekazywany do Internetu.

e) Ponowny test po zakończeniu konfiguracji NAT i włączeniu zapory systemu Windows

Po wykonaniu wszystkich kroków konfiguracji routera NAT (RRAS) należy **przywrócić pełną ochronę systemu** poprzez ponowne włączenie zapory. Uruchom **PowerShell jako Administrator** na serwerze i na kliencie:

```
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
```

Wykonaj kolejny test połączenia (po włączeniu zapory)

Na serwerze: ping 192.167.0.21, ping oke.gda.pl, ping cke.gov.pl, ping 1.1.1.1

Na kliencie Windows 11: ping 192.167.0.1, ping oke.gda.pl, ping cke.gov.pl, ping 1.1.1.1

Strony WWW powinny nadal otwierać się poprawnie (jednocześnie pamiętaj: nie wszystkie serwery odpowiadają na **ping**, i to jest normalne - patrzymy na działanie stron WWW).

Notatki i wnioski:

Przedstaw notatki w zeszycie opisujące procedurę wykonywania konfiguracji router NAT w Windows Server 2019. Wszystkie czynności konfiguracyjne zostały zapisane w zeszycie. Oraz przedstaw wnioski z zadania dostępne tu i w pliku cw29 Wnioski.pdf.

Zgłoszenie 1

Przywróć pierwszy punkt kontrolny

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.