

## T: Konfiguracja sieci wirtualnych.

Przykład konfiguracji sieci VLAN w przełącznikach CISCO:

```
Switch>enable
Switch#conf t
Switch(config)#hostname sw
sw(config)#vlan 101
sw(config-vlan)#name users
sw(config-vlan)#exit
sw(config)#vlan 102
sw(config-vlan)#name teachers
sw(config-vlan)#exit
sw(config)#interface range fastEthernet 0/1 - 14
sw(config-if-range)#switchport mode access
sw(config-if-range)#switchport access vlan 101
sw(config-if-range)#exit
sw(config)#interface fastEthernet 0/23
sw(config-if)#switchport mode access
sw(config-if)#switchport access vlan 102
sw(config-if)#exit
sw(config)#int F 0/24
sw(config-if)#sw mode trunk
sw(config-if)#sw trunk allowed vlan add 101
sw(config-if)#sw trunk allowed vlan remove 102
sw(config-if)#sw trunk allowed vlan all
sw(config-if)#exit
sw(config)#exit
sw#show vlan
sw#show interfaces trunk
sw#exit
sw>
```

### Zadanie1:

Wykorzystując program Cisco Packet Tracer połącz dwa komputery do dwóch przełączników. Następnie skonfiguruj łącze trunkowe pomiędzy tymi przełącznikami i sprawdź możliwość komunikacji pomiędzy komputerami należącymi do tej samej jak i do różnych sieci VLAN.

Przykłady konfiguracji sieci wirtualnych za pomocą poleceń konsoli tekstowej:

```
vlanserver# configure terminal
vlanserver(config)# interface fastEthernet 0/1
vlanserver(config-if)# switchport mode trunk
vlanserver(config)# vtp mode server
vlanserver(config)# vtp domain elektronik #nadanie nazwy domenie VTP
vlanserver# show vtp status #sprawdzenie nazwy domeny
vlanserver(config)#vlan 10
vlanserver(config-vlan)#name vlan10
vlanserver(config)#vlan 20
vlanserver(config-vlan)#name vlan20

vlanclient(config)#vtp mode client #ustawienie trybu klienta VTP
vlanclient#show vtp status
vlanclient#show vlan
```

## Konfiguracja połączenia VPN w systemie Windows



**Połączenia sieciowe**

Wstecz Wyszukaj Foldery Przejdź

**Zadania sieciowe**

- Utwórz nowe połączenie
- Zmień ustawienia Zapory systemu
- Uruchamia Kreatora nowego połączenia, który pomaga utworzyć połączenie z Internetem

**Zobacz też**

- Rozwiązywanie problemów z siecią

**Inne miejsca**

- Panel sterowania

**Sieć LAN lub szybki Internet**

lan  
Połączono, z zapora Realtek RTL8139/810x Family...

---

**Kreator nowego połączenia**

**Kreator nowego połączenia - Zapraszamy!**

Ten kreator pomoże Ci:

- Połączyć się z Internetem.
- Połączyć się z siecią prywatną, taką jak sieć w Twoim miejscu pracy.
- Skonfigurować sieć w domu lub w małej firmie.

Aby połączyć z siecią bezprzewodową, wyświetl [sieć bezprzewodowe w zasiegu!](#)

Aby kontynuować, kliknij przycisk Dalej.

< Wstecz Dalej > Anuluj

---

**Kreator nowego połączenia**

**Typ połączenia sieciowego**  
Co chcesz zrobić?

- Połącz z Internetem**  
Połącz się z Internetem, aby móc przeglądać sieć Web i czytać wiadomości e-mail.
- Połącz z siecią w miejscu pracy**  
Połącz się z siecią firmową (za pomocą połączenia telefonicznego lub sieci VPN), aby móc pracować z domu, biura w terenie lub innej lokalizacji.
- Konfiguruj sieć w domu lub w małej firmie**  
Połącz się z istniejącą siecią w domu lub w małej firmie lub skonfiguruj nową.
- Konfiguruj połączenie zaawansowane**  
Połącz się bezpośrednio z innym komputerem używając portu szeregowego, równoległego lub portu podczepieni, lub skonfiguruj ten komputer tak, aby inne komputery mogły się z nim połączyć.

< Wstecz Dalej > Anuluj

---

**Kreator nowego połączenia**

**Połączenie sieciowe**  
Jak chcesz połączyć się z siecią w swoim miejscu pracy?

Utwórz następujące połączenie:

- Połączenie telefoniczne**  
Łączy używając modemu i zwykłej linii telefonicznej lub linii telefonicznej sieci cyfrowej zintegrowanych usług ISDN.
- Połączenie wirtualnej sieci prywatnej**  
Łączy z siecią używając połączenia wirtualnej sieci prywatnej (VPN) przez Internet.

< Wstecz Dalej > Anuluj

---

**Kreator nowego połączenia**

**Nazwa połączenia**  
Podaj nazwę tego połączenia do swojego miejsca pracy.

W poniższym polu wpisz nazwę tego połączenia.

Nazwa firmy

zs9elektronik.pl

Na przykład możesz wpisać nazwę swojego miejsca pracy lub nazwę serwera, z którym się łączysz.

< Wstecz Dalej > Anuluj

---

**Kreator nowego połączenia**

**Wybór serwera sieci VPN**  
Jaka jest nazwa lub adres serwera sieci VPN?

Podaj nazwę hosta lub adres protokołu internetowego (IP) komputera, z którym się łączysz.

Nazwa hosta lub adres IP (np. microsoft.com lub 157.54.0.1):

zs9elektronik.pl

< Wstecz Dalej > Anuluj

**Kreator nowego połączenia**

**Dostępność połączeń**  
Możesz utworzyć nowe połączenie dostępne dla każdego użytkownika lub tylko dla siebie.

Połączenie utworzone tylko do Twojego użytku jest zapisywane w Twoim koncie użytkownika i jest dostępne tylko po Twoim zalogowaniu.

Utwórz to połączenie:

Do użytku dla wszystkich

Tylko do mojego użytku

< Wstecz Dalej > Anuluj

**Kreator nowego połączenia**

**Kończenie pracy Kreatora nowego połączenia**

Pomyślnie ukończono czynności potrzebne do utworzenia następującego połączenia:

**zs9elektronik.pl**


Połączenie zostanie zapisane w folderze Połączenia sieciowe.

Dodaj skrót do tego połączenia na moim pulpicie

Aby utworzyć połączenie i zamknąć kreatora, kliknij przycisk Zakończ.

< Wstecz Zakończ Anuluj

**Łączenie z zs9elektronik.pl**



Nazwa użytkownika: greszata

Hasło: ●●●●●●

Zapisz tę nazwę użytkownika i hasło dla następujących użytkowników:

Tylko ja

Dowolny użytkownik tego komputera

Połącz Anuluj Właściwości Pomoc

**zs9elektronik.pl Właściwości**

Ogólne Opcje Zabezpieczenia Sieć

Nazwa hosta lub adres IP miejsca docelowego (np. microsoft.com lub 157.54.0.1):

zs9elektronik.pl

Łączenie najpierw

System Windows może najpierw połączyć z siecią publiczną, taką jak Internet, przed próbą ustanowienia połączenia wirtualnego.

Wybierz najpierw numer innego połączenia:

Pokaż ikonę w obszarze powiadomień podczas połączenia

OK Anuluj

**zs9elektronik.pl Właściwości**

Ogólne Opcje Zabezpieczenia Sieć

Opcje wybierania numeru

Wyświetl wskaźnik postępu w trakcie łączenia

Monitoruj o nazwę użytkownika, hasło, certyfikat itp.

Dołącz domenę logowania systemu Windows

Opcje ponownego wybierania numeru

Próby ponownego wybrania numeru: 3

Czas pomiędzy kolejnymi próbami ponownego wybrania numeru: 1 minuta

Czas bezczynności przed rozłączeniem: Nigdy

Wybierz numer ponownie po przerwaniu połączenia

OK Anuluj

**zs9elektronik.pl Właściwości**

Ogólne Opcje Zabezpieczenia Sieć

Opcje zabezpieczeń

Typowe (ustawienia zalecane)

Weryfikuj moją tożsamość jako:

Wymagaj bezpiecznego hasła

Automatycznie użyj mojej nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows

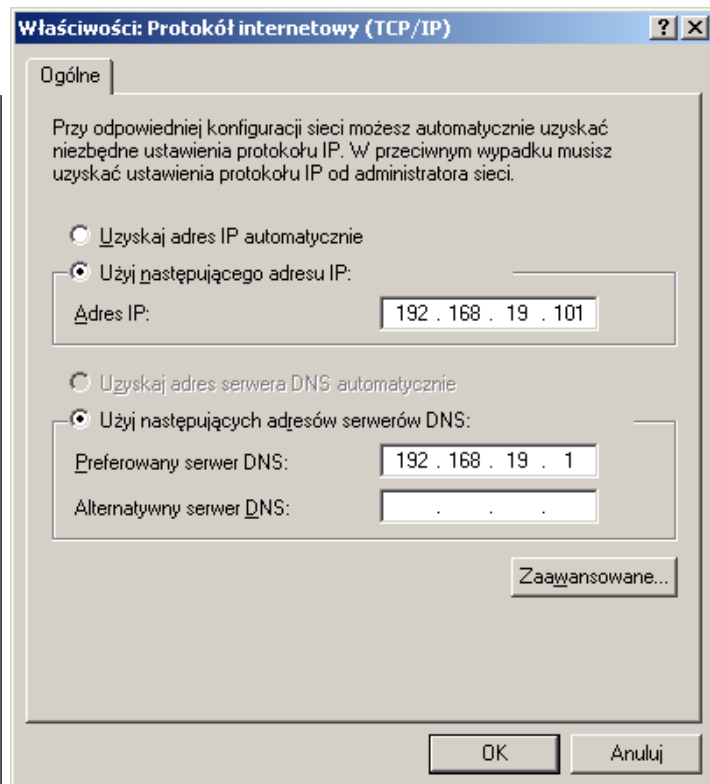
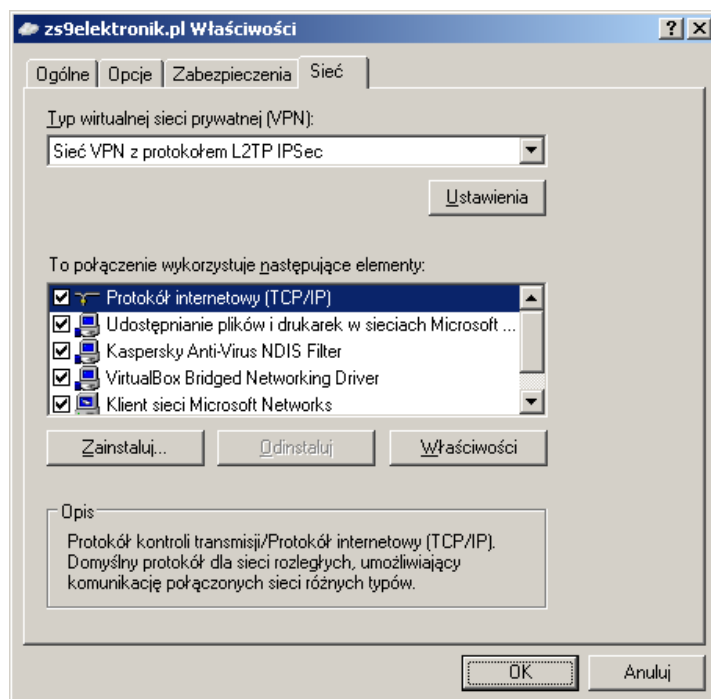
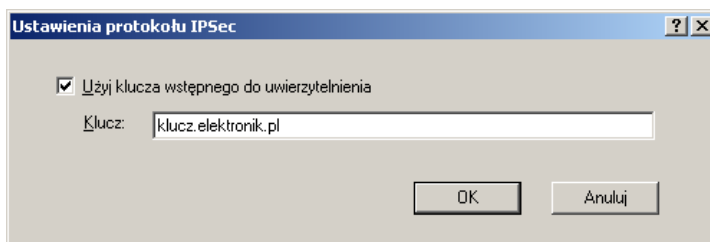
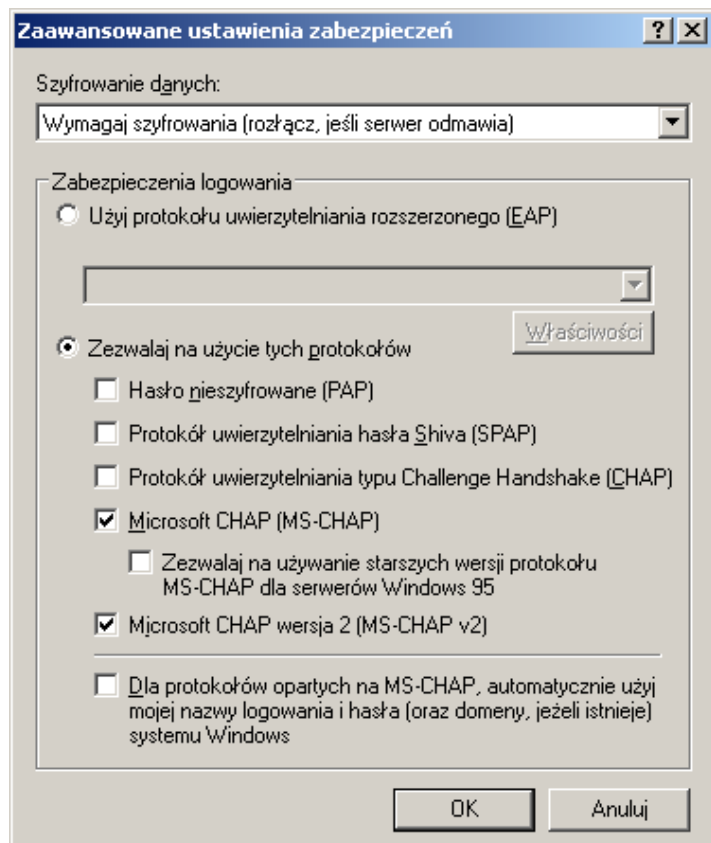
Wymagaj szyfrowania danych (przerwywaj połączenia nie obsługujące szyfrowania)

Zaawansowane (ustawienia niestandardowe)

Zmiana tych ustawień wymaga znajomości protokołów zabezpieczeń. Ustawienia...

Ustawienia protokołu IPsec...

OK Anuluj

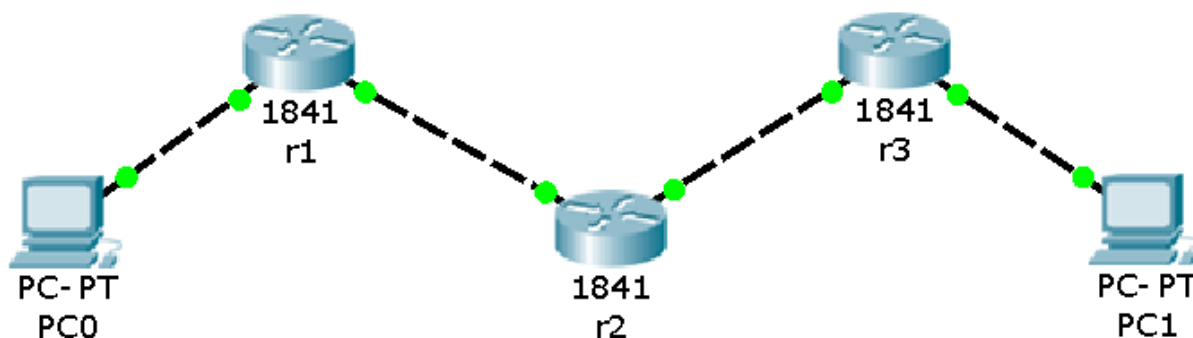


## Zadanie2:

Utwórz projekt sieci VPN w programie Cisco Packet Tracer według następujących wytycznych:

- w sieci występują dwa odrębne punkty dostępowe VPN odpowiednio w sali 27 oraz w sali 32,
- w każdej z sal komputery podłączone są przewodowo do jednego przełącznika,
- wszystkie komputery pracujące w danej pracowni posiadają statyczne adresy IP,
- adresy sieci komputerowych w salach są różne,
- w każdej pracowni znajdują się dwa komputery stacjonarne z kartami sieciowymi Ethernet,
- wszystkie komputery w sieci mają być wzajemnie widoczne.

Pracę zachowaj w pliku pod nazwą **\$nazwisko\_\$klasa\_\$gr\_vpn.pkt** i prześlij plik pocztą elektroniczną do nauczyciela w postaci załącznika na adres [greszata@zs9elektronik.pl](mailto:greszata@zs9elektronik.pl). Do wykonania zadania posłuż się instrukcją dostępną na końcu dokumentu.

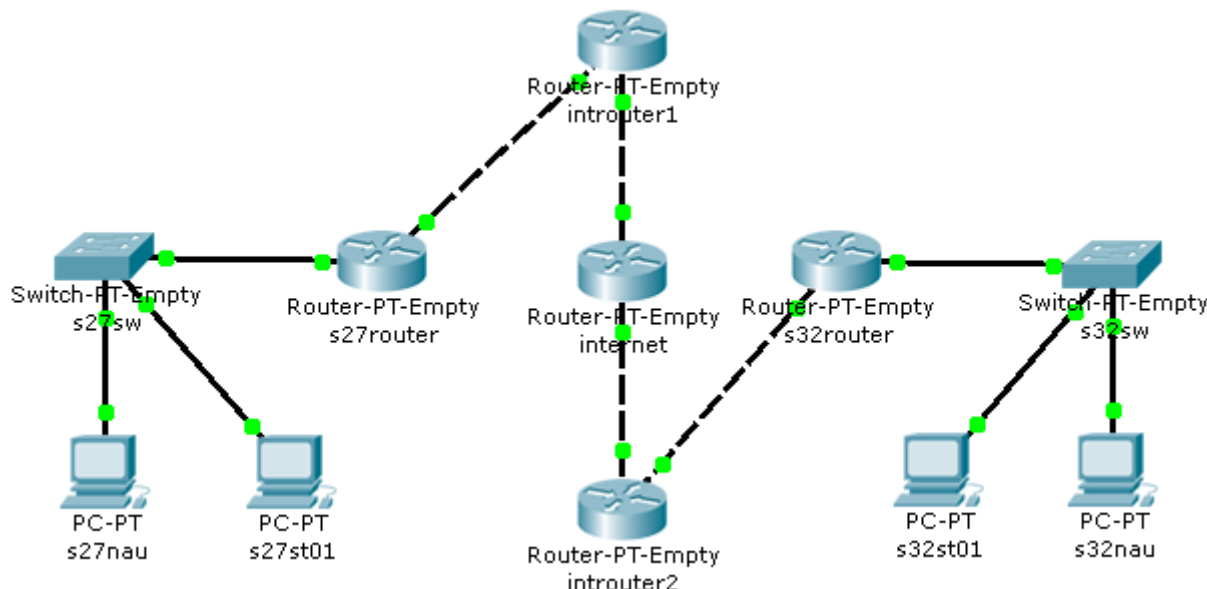


### Zadanie3:

Utwórz projekt sieci VPN w programie Cisco Packet Tracer według następujących wytycznych:

- w sieci występuje pięć odrębnych punktów dostępowych VPN,
- w dwóch salach komputerowych nr 27 i 32 znajdują się routery udostępniające połączenie z sieciami rozległymi,
- w każdej z sal komputery podłączone są przewodowo do jednego przełącznika,
- wszystkie komputery pracujące w danej pracowni posiadają statyczne adresy IP,
- adresy sieci komputerowych w salach są różne,
- w każdej pracowni znajdują się dwa komputery stacjonarne z kartami sieciowymi Ethernet,
- wszystkie komputery w sieci mają być wzajemnie widoczne.

Pracę zachowaj w pliku pod nazwą **\$nazwisko\_\$klasa\_\$gr\_vpn\_lab.pkt** i prześlij plik pocztą elektroniczną do nauczyciela w postaci załącznika na adres [greszata@zs9elektronik.pl](mailto:greszata@zs9elektronik.pl). Do wykonania zadania posłuż się instrukcją dostępną w pliku **lab\_vpn.pdf**.



Materiały pomocnicze:

<http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default.html>

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf\\_gd/ike.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ike.html)

### Rozwiązanie zadania

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **s27router**:

```
s27router>enable
s27router#?
s27router#configure terminal
s27router(config)#interface GigabitEthernet0/0
s27router(config-if)#ip address 192.168.19.1 255.255.255.0
```

```
s27router(config-if)#no shutdown
s27router(config-if)#exit
s27router(config)# interface GigabitEthernet1/1
s27router(config-if)#ip address 10.0.27.254 255.255.255.0
s27router(config-if)#no shutdown
s27router(config-if)#exit
s27router(config)#ip route 0.0.0.0 0.0.0.0 10.0.27.1
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **s32router**:

```
s32router>en
s32router#conf t
s32router(config)#int g0/1
s32router(config-if)#ip address 192.168.18.1 255.255.255.0
s32router(config-if)#no shutdown
s32router(config-if)#exit
s32router(config)#int g1/1
s32router(config-if)#ip address 10.0.32.254 255.255.255.0
s32router(config-if)#no shutdown
s32router(config-if)#exit
s32router(config)#ip route 0.0.0.0 0.0.0.0 10.0.32.1
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **introuter1**:

```
introuter1>en
introuter1#config terminal
introuter1(config)#int g0/1
introuter1(config-if)#ip address 10.0.27.1 255.255.255.0
introuter1(config-if)#no shutdown
introuter1(config-if)#exit
introuter1(config)#int g1/1
introuter1(config-if)#ip address 27.27.27.27 255.255.255.0
introuter1(config-if)#no shutdown
introuter1(config-if)#exit
introuter1(config)#ip route 0.0.0.0 0.0.0.0 27.27.27.1
introuter1(config)#ip route 192.168.19.0 255.255.255.0 10.0.27.254
introuter1(config)#no ip route 192.168.19.0 255.255.255.0 10.0.27.254
introuter1(config)#exit
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **introuter2**:

```
introuter2>en
introuter2#configure terminal
introuter2(config)#int g0/1
introuter2(config-if)#ip address 10.0.32.1 255.255.255.0
introuter2(config-if)#no shutdown
introuter2(config-if)#exit
introuter2(config)#int g1/1
introuter2(config-if)#ip address 32.32.32.32 255.255.255.0
introuter2(config-if)#no shutdown
introuter2(config-if)#exit
introuter2(config)#ip route 0.0.0.0 0.0.0.0 32.32.32.1
introuter1(config)#ip route 192.168.18.0 255.255.255.0 10.0.32.254
introuter1(config)#no ip route 192.168.18.0 255.255.255.0 10.0.32.254
introuter2(config)#exit
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **internet**:

```
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
```

```
Router(config-if)#ip address 27.27.27.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet1/0
Router(config-if)#ip address 32.32.32.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#hostname internet
internet(config)#ip route 27.27.27.0 255.255.255.0 27.27.27.27
internet(config)#ip route 32.32.32.0 255.255.255.0 32.32.32.32
internet(config)#ip route 10.0.27.0 255.255.255.0 27.27.27.27
internet(config)#ip route 10.0.32.0 255.255.255.0 32.32.32.32
#internet(config)#ip route 192.168.19.0 255.255.255.0 27.27.27.27
#internet(config)#no ip route 192.168.19.0 255.255.255.0 27.27.27.27
#internet(config)#ip route 192.168.18.0 255.255.255.0 32.32.32.32
#internet(config)#no ip route 192.168.18.0 255.255.255.0 32.32.32.32
internet(config)#exit
internet#
```

Ustawienia polityki ISAKMP/IKE (niezbędne do nawiązania połączenia tunelowego) wydawane w zakładce Command Line Interface (CLI) na routerze **introuter1**:

```
introuter1>enable
introuter1#configure terminal
introuter1(config)#crypto isakmp policy 5
introuter1(config-isakmp)#encryption 3des
introuter1(config-isakmp)#group 2
introuter1(config-isakmp)#hash sha
introuter1(config-isakmp)#lifetime 28800
introuter1(config-isakmp)#authentication pre-share
introuter1(config-isakmp)#exit
introuter1(config)#crypto isakmp key hr5xb8416aa9r6 address
32.32.32.32
introuter1(config)#access-list 101 permit ip 10.0.27.0 0.255.255.255
10.0.32.0 0.255.255.255
introuter1(config)#ip route 0.0.0.0 0.0.0.0 27.27.27.1
introuter1(config)#ip route 10.0.32.0 255.255.255.0 27.27.27.1
introuter1(config)#crypto ipsec transform-set STRONG esp-3des esp-
sha-hmac
introuter1(config)#crypto map CISCO 10 ipsec-isakmp
introuter1(config-crypto-map)#set security-association life seconds
3600
introuter1(config-crypto-map)#set transform-set STRONG
introuter1(config-crypto-map)#set pfs group2
introuter1(config-crypto-map)#set peer 32.32.32.32
introuter1(config-crypto-map)#match address 101
introuter1(config-crypto-map)#exit
introuter1(config)#int g1/1
introuter1(config-if)#crypto map CISCO
introuter1(config-if)#exit
```

Ustawienia polityki ISAKMP/IKE (niezbędne do nawiązania połączenia tunelowego) wydawane w zakładce Command Line Interface (CLI) na routerze **introuter2**:

```
introuter2>en
introuter2#configure terminal
introuter2(config)#crypto isakmp policy 5
introuter2(config-isakmp)#encryption 3des
```



```
introuter2(config-isakmp)#group 2
introuter2(config-isakmp)#hash sha
introuter2(config-isakmp)#lifetime 28800
introuter2(config-isakmp)#authentication pre-share
introuter2(config-isakmp)#exit
introuter2(config)#crypto isakmp key hr5xb8416aa9r6 address
27.27.27.27
introuter2(config)#access-list 101 permit ip 10.0.32.0 0.255.255.255
10.0.27.0 0.255.255.255
introuter2(config)#ip route 0.0.0.0 0.0.0.0 32.32.32.1
introuter2(config)#ip route 10.0.27.0 255.255.255.0 32.32.32.1
introuter2(config)#crypto ipsec transform-set STRONG esp-3des esp-
sha-hmac
introuter2(config)#crypto map CISCO 10 ipsec-isakmp
introuter2(config-crypto-map)#set security-association life seconds
3600
introuter2(config-crypto-map)#set transform-set STRONG
introuter2(config-crypto-map)#set pfs group2
introuter2(config-crypto-map)#set peer 27.27.27.27
introuter2(config-crypto-map)#match address 101
introuter2(config-crypto-map)#exit
introuter2(config)#int g1/1
introuter2(config-if)#crypto map CISCO
introuter2(config-if)#exit
```

## Konfiguracja VPN w systemie Linux OpenSUSE

### Instalacja OpenVPN

```
zipper install openvpn
```

### Sprawdzenie, czy posiadamy sterownik wirtualnego interfejsu TUN/TAP

```
modprobe tun #nic nie powinno zostać wyświetlone
dmesg | grep tun
```

### Generowanie klucza wykorzystywanego do szyfrowania i uwierzytelniania transmisji

```
openvpn --genkey --secret /etc/openvpn/static.key
```

### Zezwolenie na przekazywanie pakietów, dokonujemy zmiany wpisu w pliku /etc/sysctl.conf

```
net.ipv4.ip_forward=1
```

### Utworzenie grupy oraz użytkownika na potrzeby połączenia tunelowego

```
groupadd openvpn
useradd -g openvpn -d /usr/local/etc/openvpn -s /bin/false -f 1
openvpn
```

### Tworzenie pliku konfiguracyjnego dla połączenia tunelowego /etc/openvpn/openvpn.conf o następującej treści:

```
dev tun #określenie interfejsu
local 192.168.19.21 #adres IP serwera
proto udp #protokół transmisji danych
port 17997 #port transmisji danych, należy odblokować w
zaporce sieciowej

user openvpn
group openvpn
secret static.key #klucz prywatny serwera
ifconfig 10.0.0.0 255.255.255.0 #adres sieci, z której przydzielane
zostaną adresy IP klientom
comp-lzo #algorytm kompresji
```

### Uruchomienie serwera VPN

```
/etc/init.d/openvpn start
```

### Sprawdzenie interfejsu połączenia tunelowego

```
ifconfig | grep tun
```

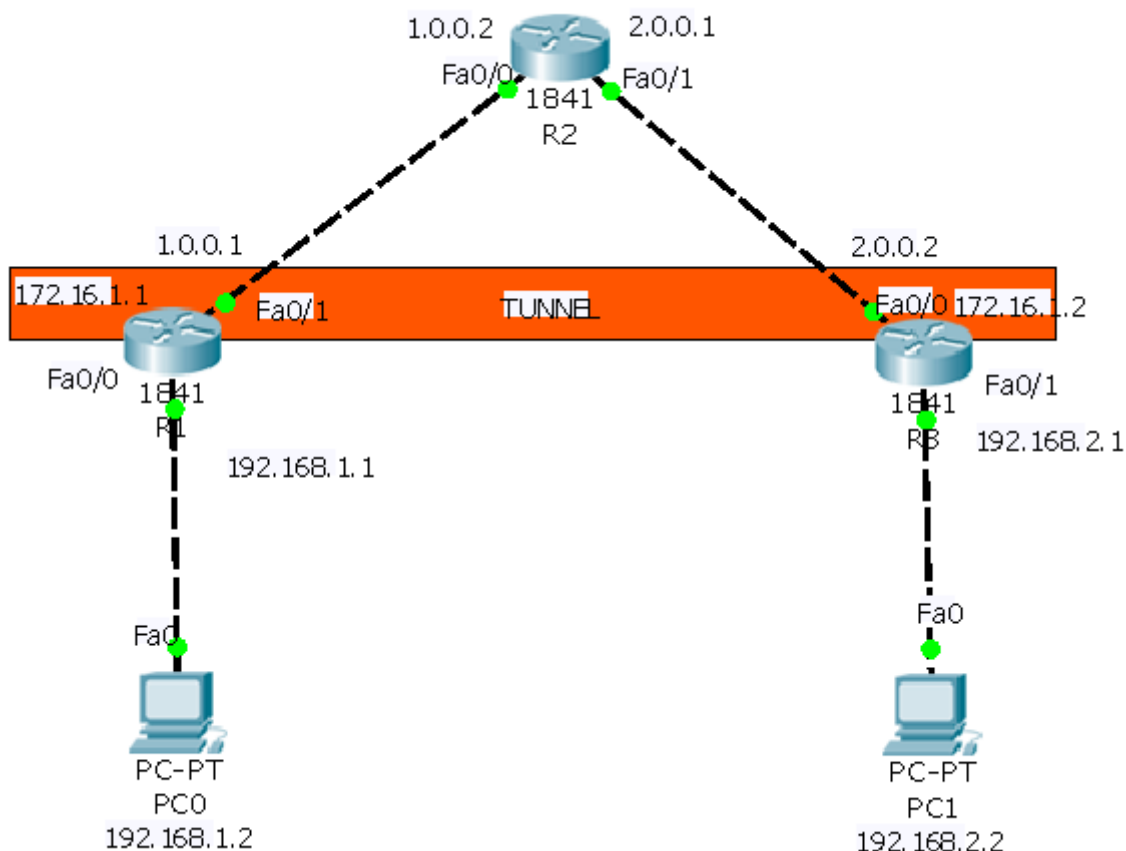


**Zadanie4:**

Zainstaluj i skonfiguruj usługę VPN w systemie Linux OpenSUSE.

**Zadanie5:**

Zapoznaj się z informacjami na temat oprogramowanie VPNonline, Cyber GhostVPN, BartVPN lub OpenVPN.

**Instrukcje rozwiązania do zadania 2:****CONFIGURATION ON ROUTER R1:**

```
Router>enable
Router#config t
Router(config)#host r1
r1(config)#int fa0/0
r1(config-if)#ip add 192.168.1.1 255.255.255.0
r1(config-if)#no shut
r1(config-if)#exit
r1(config)#int fa0/1
r1(config-if)#ip address 1.0.0.1 255.0.0.0
r1(config-if)#no shut
```

**CONFIGURATION ON ROUTER R2:**

```
Router>enable
Router#config t
Router(config)#host r2
r2(config)#int fa0/0
r2(config-if)#ip add 1.0.0.2 255.0.0.0
r2(config-if)#no shut
r2(config-if)#exit
r2(config)#int fa0/1
r2(config-if)#ip add 2.0.0.1 255.0.0.0
r2(config-if)#no shut
```

**CONFIGURATION ON ROUTER R3:**

```
Router>enable
Router#config t
Router(config)#host r3
r3(config)#int fa0/0
r3(config-if)#ip add 2.0.0.2 255.0.0.0
r3(config-if)#no shut
r3(config-if)#exit
r3(config)#int fa0/1
r3(config-if)#ip add 192.168.2.1 255.255.255.0
r3(config-if)#no shut
```

**DEFAULT ROUTING CONFIGURATION ON ROUTER R1:**

```
r1>enable
r1#config t
Enter configuration commands, one per line. End with CNTL/Z.
r1(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.2
r1(config)#
```

**DEFAULT ROUTING CONFIGURATION ON ROUTER r3:**

```
r3>enable
r3#config t
Enter configuration commands, one per line. End with CNTL/Z.
r3(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1
r3(config)#
```

**FIRST CREATE A VPN TUNNEL ON ROUTER R1:**

```
r1#config t
r1(config)#interface tunnel 10
r1(config-if)#ip address 172.16.1.1 255.255.0.0
r1(config-if)#tunnel source fa0/1
r1(config-if)#tunnel destination 2.0.0.2
r1(config-if)#no shut
```

**NOW CREATE A VPN TUNNEL ON ROUTER R3:**

```
r3#config t
r3(config)#interface tunnel 100
r3(config-if)#ip address 172.16.1.2 255.255.0.0
r3(config-if)#tunnel source fa0/0
r3(config-if)#tunnel destination 1.0.0.1
r3(config-if)#no shut
```

**Now Do routing for created VPN Tunnel on Both Router R and R3:**

```
r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2
r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

**Now i am going to router R1 and R3 and test whether tunnel is created or not.**

```
r1#show interfaces Tunnel 10
r3#show interfaces Tunnel 100
```

```
PC0>tracert 192.168.2.2
PC1>tracert 192.168.1.2
```