

## Instalacja i konfiguracja serwera DHCP.

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia, które użyjesz, aby:

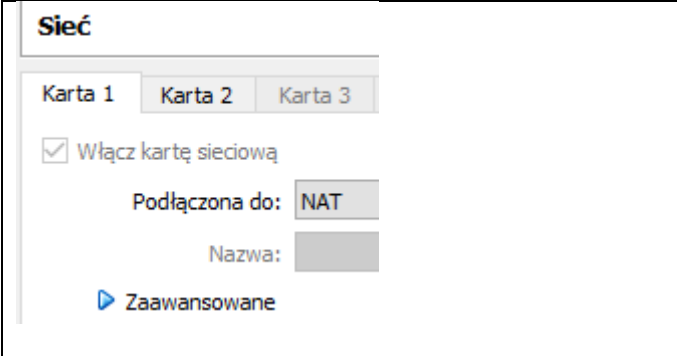
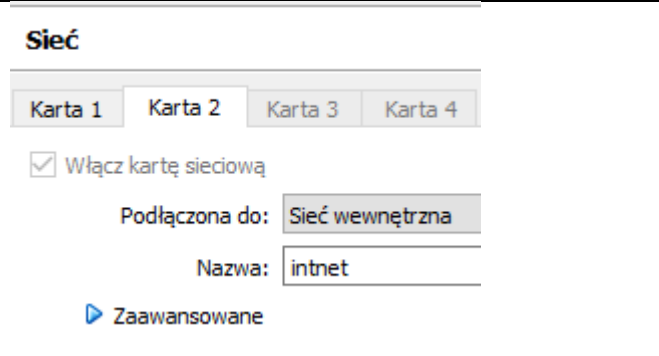
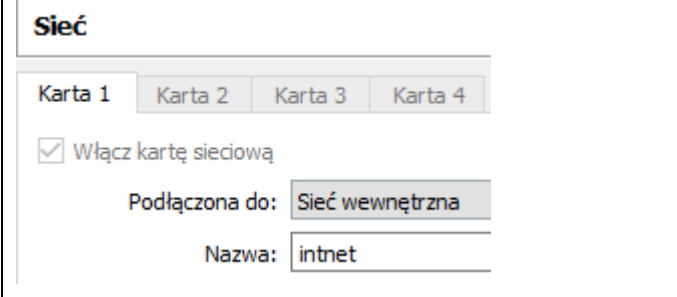
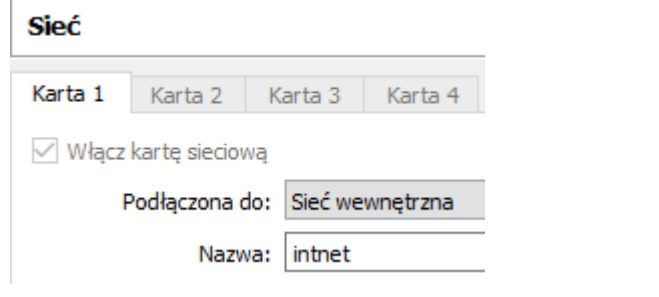
- wyjaśnić pojęcia związane z dhcp,
- zainstalować serwer dhcp,
- uruchomić lub zatrzymać usługi sieciowe,
- konfigurować serwer dhcp,
- korzystać z dhcp.

2. podaj odpowiedzi na pytania zadane w treści zadań.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Ubuntu serwer i klient. Przygotuj Ubuntu.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Windows. Przygotuj Windows.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu.

<p>Ubuntu serwer Adapter 1</p> 	<p>Ubuntu serwer Adapter 2</p> 
<p>Windows Adapter 1</p> 	<p>Ubuntu desktop Adapter 1</p> 

Po uruchomieniu Ubuntu podaj login: **ubuntu** Password: **ubuntu**

Wis **sudo -s** Password: **buntu**

Lub dla login root hasło 1234

```
ubuntu@dlp:~$ sudo -s
[sudo] password for ubuntu:
```

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Za pomocą polecenia `ifconfig -a` ustal dostępne interfejsy sieciowe.

```
root@dlp:~# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe68:a08 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:68:0a:08 txqueuelen 1000 (Ethernet)
    RX packets 2712 bytes 2450820 (2.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1142 bytes 77401 (77.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

Plik `/etc/netplan/00-installer-config.yaml` - opisuje interfejsy sieciowe dostępne w systemie i jak je aktywować.

2. Zmień adres IP dla Ubuntu na enp0s8 (Adapter 2) na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe `nano /etc/netplan/0` tabulator `*.yaml`

Pozostaw zalecane wpisy w tym pliku

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s17:
      dhcp4: true
    enp0s8:
      dhcp4: no
      addresses: [10.0.0.30/24]
```

3. Zastosuj ustawienia

```
root@dlp:~# netplan apply
```

```
root@dlp:~# netplan apply
```

4. Wyświetl domyślną bramę (adres routera) dla interfejsów sieciowych serwera

```
root@dlp:~# ip route show default
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
```

## Podsystemy Dnsmasq (odrobina teorii)

Dnsmasq ma trzy główne podsystemy, a mianowicie:

- **Podsystem DNS** : zapewnia buforowanie rekordów A, AAAA, CNAME i PTR, a także rekordów DNSKEY i DS.
- **Podsystem DHCP** : Zapewnij obsługę DHCPv4, DHCPv6, BOOTP i PXE. Można używać zarówno statycznych, jak i dynamicznych dzierżaw DHCP, wbudowanego serwera TFTP tylko do odczytu do obsługi rozruchu sieciowego.
- **Podsystem reklam routera** : zapewnia podstawową automatyczną konfigurację hosta IPv6

Ubuntu 18.04+ jest dostarczany z systemd-resolve, który należy wyłączyć, ponieważ wiąże się z portem **53**, który będzie powodował konflikt z portem Dnsmasq.

Uruchom następujące polecenia, aby wyłączyć rozwiązana usługę:

```
systemctl disable systemd-resolved
systemctl stop systemd-resolved
```

Usuń `resolv.conf` plik z dowiązaniem symbolicznym

```
ls -lh /etc/resolv.conf
rm /etc/resolv.conf
echo nameserver 8.8.8.8 | tee /etc/resolv.conf
```

Teraz można przejść do zadania.

Zapisz w zeszycie co się stało po wykonaniu poleceń. Wpisz kolejno polecenia.

## Część 1 - Instalacja i konfiguracja serwera DHCP dla Ubuntu serwer.

### 1.1 Instalacja Dnsmasq

1. Zainstaluj Dnsmasq, który jest forwardera DNS, czyli pełni rolę cache dla wywołań DNS od hostów naszej sieć i jest oprogramowaniem serwera DHCP.

```
root@dlp:~# apt -y install dnsmasq
```

```
root@dlp:~# apt -y install dnsmasq
```

2. Skonfiguruj Dnsmasq.

```
root@dlp:~# nano /etc/dnsmasq.conf
```

```
root@dlp:~# nano /etc/dnsmasq.conf lub root@dlp:~# vi /etc/dnsmasq.conf
```

linia 19: odkomentuj (nigdy nie przesyłaj zwykłych nazw)

**domain-needed**

linia 21: odkomentuj (nigdy nie przesyłaj dalej adresów w nie routowanych przestrzeniach adresowych)

**bogus-priv**

linia 53: odkomentuj (zapytanie z każdym serwerem ściśle w kolejności w resolv.conf)

**strict-order**

linia 67: dodaj, jeśli potrzebujesz

zapytaj konkretną nazwę domeny do określonego serwera DNS

poniższy przykład oznacza domenę zapytania [server.education] na serwer [10.0.0.30]

**server=/server.education/10.0.0.30**

# linia 135: odkomentuj (dodaj nazwę domeny automatycznie)

**expand-hosts**

# linia 145: dodaj (określ nazwę domeny)

**domain=srv.world**

**esc > wq!** – w celu zapisania – jeśli używasz vi

```
root@dlp:~# systemctl restart dnsmasq
```

```
root@dlp:~# systemctl restart dnsmasq
```

3. Dodaj rekordy DNS w /etc/hosts. Następnie Dnsmasq odpowie na zapytania od klientów.

```
root@dlp:~# nano /etc/hosts
```

dodaj rekord

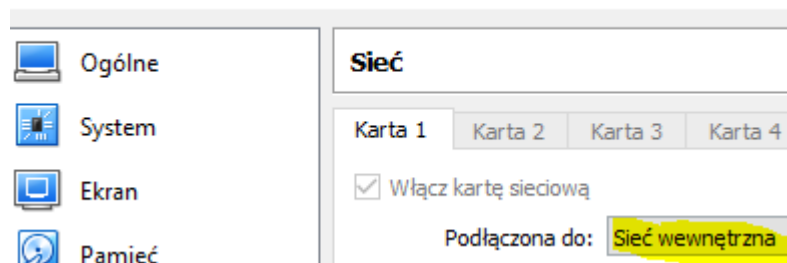
```
10.0.0.30    dlp.srv.world dlp
```

```
10.0.0.30 dlp.srv.world dlp
```

```
root@dlp:~# systemctl restart dnsmasq
```

4. Sprawdź, czy nazwa lub adres IP jest rozpoznawany przez klienta (ubuntu desktop) znajdującego się w sieci wewnętrznej.

ubuntu desktop - Ustawienia



```
root@bolek-VirtualBox:~# nano /etc/netplan/01-network-manager-all.yaml
```

zmień ustawienia DNS na Dnsmasq Server

**nameservers:**

addresses: [10.0.0.30]

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.0.51/24]
      nameservers:
        addresses: [10.0.0.30]
```

root@desktop:~# netplan apply

root@desktop:~# systemd-resolve --status --no-pager | tail -7

```
root@bolek-VirtualBox:~# systemd-resolve --status --no-pager | tail -7
Link 2 (enp0s3)
  Current Scopes: DNS
    LLMNR setting: yes
  MulticastDNS setting: no
  DNSSEC setting: no
  DNSSEC supported: no
  DNS Servers: 10.0.0.30
```

root@bolek-VirtualBox:~# dig dlp.srv.world.

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:

dlp.srv.world. 0 IN A 10.0.0.30

root@bolek-VirtualBox:~# dig -x 10.0.0.30

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:

30.0.0.10.in-addr.arpa. 0 IN PTR dlp.srv.world.

5. Włącz na serwerze zintegrowaną funkcję DHCP w Dnsmasq i skonfiguruj serwer DHCP.

Skonfiguruj Dnsmasq.

root@dlp:~# vi /etc/dnsmasq.conf

linia 158: dodaj (zakres adresu IP do dzierżawy i okres dzierżawy)

dhcp-range=10.0.0.50,10.0.0.150,12h

wiersz 335: dodaj (określ domyślną bramkę)

dhcp-option=option:router,10.0.2.15

wiersz 344: dodaj (zdefiniuj NTP, DNS, serwer i podsieć maski)

dhcp-option=option:ntp-server,10.0.2.15

dhcp-option=option:dns-server,10.0.2.15

dhcp-option=option:netmask,255.255.255.0

esc > : wq! – aby zapisać

```
root@dlp:~# systemctl restart dnsmasq
```

**Przejdź do klienta (ubuntu desktop)**

```
root@bolek-vbox:~# nano /etc/netplan/01-netcfg.yaml
```

```
root@bolek-VirtualBox:~# nano /etc/netplan/01-network-manager-all.yaml
```

6. Włącz dhcp4 i komentuje statyczne ustawienia związane z IP

network:

version: 2

renderer: networkd

ethernets:

enp0s3:

dhcp4: yes

#addresses: [10.0.0.51/24]

#gateway4: 10.0.0.1

#nameservers:

# addresses: [10.0.0.30]

```
renderer: networkd
ethernets:
  enp0s3:
    dhcp4: yes
    #addresses: [10.0.0.51/24]
    #nameservers:
    # addresses: [10.0.0.30]
```

```
root@dlp:~# netplan apply
```

```
root@bolek-VirtualBox:~# ip a |grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    inet 10.0.0.69/24 brd 10.0.0.255 scope global dynamic enp0s3
root@bolek-VirtualBox:~# _
```

**Przejdź do Windows:**

7. Ustaw automatyczne ip

Właściwości: Protokół internetowy w wersji 4 (TCP/IPv4)

Ogólne Konfiguracja alternatywna

Przy odpowiedniej konfiguracji sieci możesz automatycznie uzyskać niezbędne ustawienia protokołu IP. W przeciwnym wypadku musisz uzyskać ustawienia protokołu IP od administratora sieci.

Uzyskaj adres IP automatycznie

Użyj następującego adresu IP:

Adres IP: . . .

Maska podsieci: . . .

Brama domyślna: . . .

Uzyskaj adres serwera DNS automatycznie

Użyj następujących adresów serwerów DNS:

Preferowany serwer DNS: . . .

Alternatywny serwer DNS: . . .

Sufiks DNS konkretnego... **srv.world**

Opis Karta Intel(R) PR

Adres fizyczny 08-00-27-CD-5E-

DHCP włączone Tak

Adres IPv4 **10.0.0.124**

Maska podsieci IPv4 **255.255.255.0**

Dzierżawa uzyskana 10 października :

Dzierżawa wygasa 10 października :

Brama domyślna IPv4 **10.0.2.15**

Serwer DHCP IPv4 **10.0.0.30**

Serwer DNS IPv4 **10.0.2.15**

## Zgłoszenie 1

Przywróć migawkę pierwszą i skonfiguruj ponownie interfejsy sieciowe (patrz str2)

### 1.2 Konfiguracja serwer DHCP (Dynamic Host Configuration Protocol).

Serwer DHCP używa 67 / UDP.

Instalacja serwera DHCP dla Ubuntu serwer

8. Wykonaj `root@d1p:~# apt -y install isc-dhcp-server`

Jeżeli nie jest możliwe zainstalowanie należy wykonać aktualizację

`apt-get update` - aktualizowanie listy pakietów

jeśli nie jest możliwe należy wykonać

`apt-get upgrade` - aktualizacja systemu

9. Wykonaj kopie pliku konfiguracyjnego.

`root@d1p:~# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf backup`

10. Otwieramy plik isc-dhcp-server

`nano /etc/default/isc-dhcp-server`

11. Określamy na którym interfejsie serwer będzie nasłuchiwał żądań od klientów

```
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s8"
```

## 12. Konfiguracja serwera DHCP dla Ubuntu serwer

Otwieramy plik dhcpd.conf

```
nano /etc/dhcp/dhcpd.conf
```

wiersz 10: podaj nazwę domeny

```
option domain-name "srv.world";
```

wiersz 11: podaj nazwę hosta lub adres IP serwera nazw

```
option domain-name-servers dlp.srv.world;
```

```
# option definitions common to all supported networks...
option domain-name "srv.world";
option domain-name-servers dlp.srv.world;
```

wiersz 24: odkomentowanie

```
authoritative;
```

```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
```

dodaj na końcu pliku

podaj adres sieci i maskę podsieci

```
subnet 10.0.0.0 netmask 255.255.255.0 {
```

określ domyślną bramkę

```
option routers 10.0.2.15;
```

określ maskę podsieci

```
option subnet-mask 255.255.255.0;
```

określ zakres dzierżawionego adresu IP



```
range dynamic-bootp 10.0.0.160 10.0.0.254;
```

```
}
```

```
subnet 10.0.0.0 netmask 255.255.255.0 {  
option routers 10.0.2.15;  
option subnet-mask 255.255.255.0;  
range dynamic-bootp 10.0.0.160 10.0.0.254;  
}
```

13. Zapisz w zeszycie przykładowe instrukcje w plik `dhcpd.conf`

**subnet** – określa adres danej sieci

**netmask** – określa maskę podsieci danej sieci

**range** – określa zakres adresów IP, jakie będą przydzielane

**option domain-name-servers** – adresy serwerów DNS

**option domain-name** – nazwa domeny

**option routers** – określa adres routera sieciowego

**option broadcast-address** – określa adres broadcastu w naszej sieci

**default-lease-time** – domyślny czas dzierżawy adresów IP (wyrażony w sekundach)

**max-lease-time** – maksymalny czas dzierżawy adresów IP (wyrażony w sekundach)

14. Kolejno zatrzymaj i uruchom usługę dhcp

```
root@dlp:~# /etc/init.d/isc-dhcp-server stop  
[ ok ] Stopping isc-dhcp-server (via systemctl): isc-dhcp-server.service.  
root@dlp:~# /etc/init.d/isc-dhcp-server start  
[ ok ] Starting isc-dhcp-server (via systemctl): isc-dhcp-server.service.
```

15. Zrestartuj usługę dhcp

```
root@dlp:~# systemctl restart isc-dhcp-server
```

16. Zrestartuj usługę dhcp a następnie sprawdź jej stan za pomocą systemctl

```

root@dlp:~# systemctl status isc-dhcp-server
• isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2018-10-10 00:46:37 CEST; 20s ago
    Docs: man:dhcpd(8)
  Main PID: 13420 (dhcpd)
    Tasks: 1 (limit: 1112)
  CGroup: /system.slice/isc-dhcp-server.service
          └─13420 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp

Oct 10 00:46:37 dlp sh[13420]: Sending on Socket/fallback/fallback-net
Oct 10 00:46:37 dlp dhcpd[13420]:
Oct 10 00:46:37 dlp dhcpd[13420]: No subnet declaration for enp0s3 (10.0.2.15).
Oct 10 00:46:37 dlp dhcpd[13420]: ** Ignoring requests on enp0s3. If this is not what
Oct 10 00:46:37 dlp dhcpd[13420]: you want, please write a subnet declaration
Oct 10 00:46:37 dlp dhcpd[13420]: in your dhcpd.conf file for the network segment
Oct 10 00:46:37 dlp dhcpd[13420]: to which interface enp0s3 is attached. **
Oct 10 00:46:37 dlp dhcpd[13420]:
Oct 10 00:46:37 dlp dhcpd[13420]: Sending on Socket/fallback/fallback-net
Oct 10 00:46:37 dlp dhcpd[13420]: Server starting service.

```

17. Sprawdzić, czy demon serwera DHCP jest uruchomiony

```

root@dlp:~# ps ax | grep dhcpd
13420 ?        Ss      0:00 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /
etc/dhcp/dhcpd.conf
13440 tty1    S+      0:00 grep --color=auto dhcpd

```

18. Sprawdź, czy serwer nasłuchuje na porcie 67 poprzez lsof

```

root@debian:~# lsof -i :67
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
dhcpd   2937 root   7u  IPv4  21901      0t0  UDP *:bootps

```

19. Sprawdź poleceniem NETSTAT aktywne połączenia protokołu UDP, czy jest otwarty port 67 odpowiadający za dhcpd (serwer dhcp)

```

root@dlp:~# lsof -i :67
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
dnsmasq 1953 dnsmasq 4u  IPv4  25365      0t0  UDP *:bootps
dhcpd   13420 dhcpd   7u  IPv4  39155      0t0  UDP *:bootps

```

```

root@dlp:~# netstat -anp | grep dhcpd | grep 67
udp      0          0 0.0.0.0:*          0.0.0.0:*          13420/dhcpd

```

Jeśli nie jest to zainstaluj program nmap `root@dlp:~# apt -y install nmap`

20. Sprawdź czy usługa dhcp jest uruchomiona.

```

root@dlp:~# nmap -sU -p 67 10.0.0.30

Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-10 00:51 CEST
Nmap scan report for dlp.srv.world (10.0.0.30)
Host is up.

PORT      STATE      SERVICE
67/udp    open|filtered  dhcpd

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds

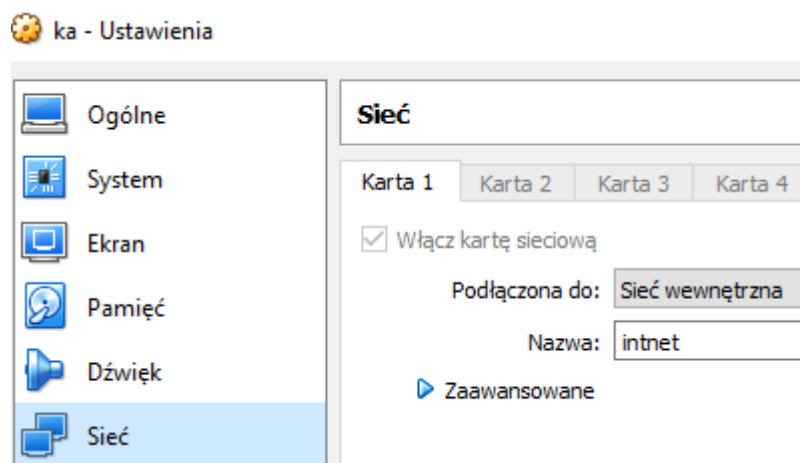
```

Zinterpretuj uzyskane efekty, zapisz interpretację w zeszycie.

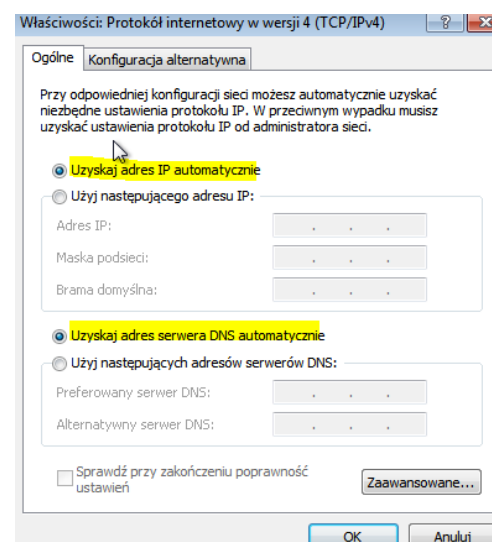
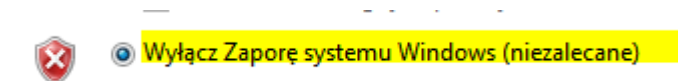
## Zgłoszenie 2

### Część 2 – Konfigurowanie klienta DHCP - Windows.

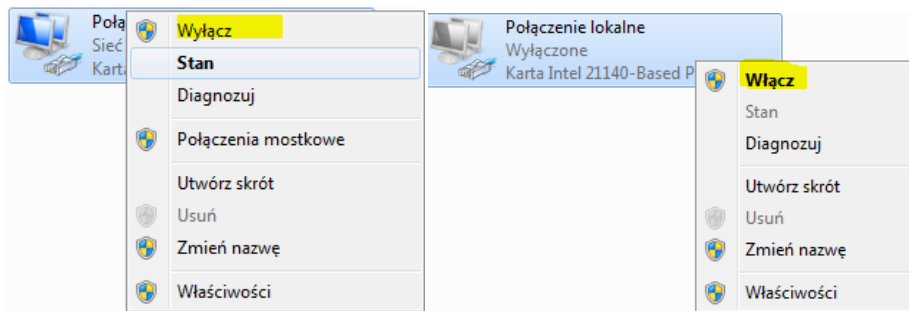
1. Dodajemy maszynę wirtualną dla 7-ki lub 10-ki. Ustawiamy parametry sieci.



2. Ustawiamy klienta do automatycznego pobierania adresu.



3. Wybieramy kolejno dla Połączenie lokalne > Wyłącz > Włącz



#### 4. Sprawdzamy stan ustawień dla Połączenie lokalne a szczególnie adres MAC

Szczegóły połączenia sieciowego

Szczegóły połączenia sieciowego:

Właściwość	Wartość
Sufiks DNS konkretnego...	srv.world
Opis	Karta Intel(R) PRO/
Adres fizyczny	08-00-27-28-35-50
DHCP włączone	Tak
Adres IPv4	10.0.0.130
Maska podsieci IPv4	255.255.255.0
Dzierżawa uzyskana	10 października 201
Dzierżawa wygasa	10 października 201
Brama domyślna IPv4	10.0.2.15
Serwer DHCP IPv4	10.0.0.30
Serwer DNS IPv4	10.0.2.15
Serwer WINS IPv4	

Zinterpretuj uzyskane efekty, zapisz interpretację w zeszycie.

### Zgłoszenie 3

#### Część 3 – Rekonfiguracja serwera DHCP.

1. Modyfikujemy plik dhcpd.conf

Wprowadzamy instrukcje globalne do pliku dhcpd.conf

```
nano /etc/dhcp/dhcpd.conf
```

2. Ustawiamy parametry interfejsu dla adresu przydzielanego statycznie.

Podajemy odczytany wyżej adres MAC i adres ipv4 10.0.0.161

```
# Always allocate the host with Ethernet address 11:22:33:44:55:66
# The IP address 192.168.0.60
dhcp-host=08:00:27:28:35:50,10.0.0.161
```

lub

```
host komp {  
  
hardware ethernet 00:1F:6A:21:71:3F;  
  
fixed-address 10.0.0.161;  
  
}
```

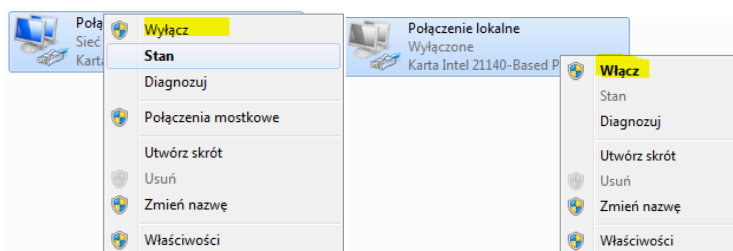
Składnia:

```
host komp { hardware ethernet <mac address>; fixed-address <ip address>; }
```

3. Restartujemy serwer dhcp (należy to zrobić po każdej modyfikacji pliku dhcpd.conf)

```
/etc/init.d/isc-dhcp-server restart lub systemctl restart isc-dhcp-server
```

4. Dla Windows wybieramy kolejno dla Połączenie lokalne > Wyłącz > Włącz



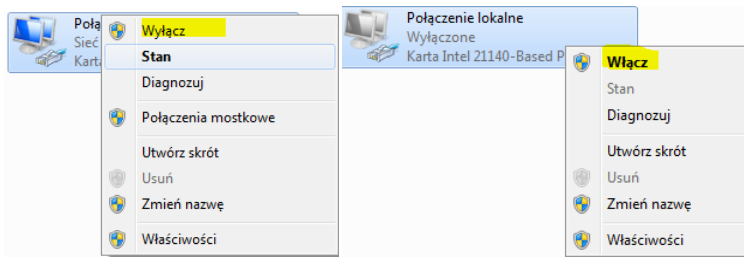
5. Sprawdzamy w wierszu polecenia stan interfejsu `ipconfig /all`

6. Sprawdzamy stan dla Połączenie lokalne.

7. Wyłącz serwer dhcp

```
root@debian:~# systemctl stop isc-dhcp-server  
root@debian:~# _
```

8. Dla Windows wybieramy kolejno dla Połączenie lokalne > Wyłącz > Włącz



9. Otrzymasz parametry interfejsu sieciowego
10. Zapisz w zeszycie odpowiedzi na poniższe pytania.
  - a) Jaki otrzymałeś adres ip z jakiej klasy?
  - b) Co możesz napisać dodatkowo o tym adresie?

Opisz procedurę instalacji, konfiguracji i testowania serwera dhcp oraz klienta dhcp.

## Zgłoszenie 4

### Część 4 – Dodatkowa modyfikacja pliku dhcpd.conf

1. Wprowadzamy instrukcje globalne do pliku dhcpd.conf `default-lease-time 600;`

```
range 192.167.0.10 192.167.0.200;  
default-lease-time 600;  
max-lease-time 86400;
```

Sprawdź w części 1 punkcie 7 za co odpowiada powyższa instrukcja i zapisz to w zeszycie.

2. Restartujemy serwer dhcp (należy to zrobić po każdej modyfikacji pliku dhcpd.conf)

```
/etc/init.d/isc-dhcp-server restart
```

3. Wyłączamy dynamicznego DNS:

```
authoritative;
```

Dyrektywa wskazuje, że serwer DHCP powinien wysyłać wiadomości DHCPNack skonfigurowanym klientom. Jeśli tego nie zrobi, klienci nie będą mogli uzyskać właściwy adres IP po zmianie podsieci aż ich stare dzierżawy wygasną, co może trwać dość długo.

4. Ustawiamy zapobieganie otrzymywania informacji od klientów DNS do serwera DHCP

```
ddns-update-style none;
```

```
ping-check = 1;
authoritative;
ddns-update-style none;
option domain-name-servers 217.172.224.160;
```

5. Ustaw Odmów **deny declines** do uniknięcia ataku DoS against serwera DHCP.

Urządzenie klienta może wysłać wiadomości DHCPDECLINE wiele razy, że może wyczerpać pole adresów IP serwera DHCP, powodując serwer DHCP zapomni przydziały adresów:

**deny declines;**

```
ddns-update-style none;
deny declines;
option domain-name-servers 217.172.224.160;
```

6. Wyłącz obsługę starszych klientów BOOTP:

**deny bootp;**

```
deny declines;
deny bootp;
option domain-name-servers 217.172.224.160;
```

7. Restartujemy serwer dhcp (należy to zrobić po każdej modyfikacji pliku dhcpd.conf)

```
/etc/init.d/isc-dhcp-server restart
```

Zinterpretuj uzyskane efekty, zapisz interpretację w zeszycie.

## **Zgłoszenie 5**

### **Część 5 – Kontrola serwera DHCP.**

1. Aby sprawdzić składnię pliku dhcpd.conf czy zawiera błędy, uruchom:

```
root@d1p:~# dhcpd -t
```

2. Wykonaj sprawdzenie statusu serwera dhcp.

```
root@d1p:~# /etc/init.d/isc-dhcp-server status
```

```
root@d1p:~# systemctl status isc-dhcp-server
```

Zinterpretuj uzyskane efekty, porównaj, zapisz interpretację w zeszycie.

3. Domyślnie dhcpd będzie rejestrować wszystkie dane wyjściowe za pomocą funkcji syslog z dziennika, czyli plik /var/log/syslog:

a) tail -f /var/log/syslog `root@dlp:~# tail -f /var/log/syslog`

b) grep dhcpd /var/log/syslog `root@dlp:~# grep dhcpd /var/log/syslog`

4. Aby zobaczyć więcej informacji o dzierżawie ip, przez serwer DHCP klientów:

```
root@dlp:~# cat /var/lib/dhcp/dhcpd.leases
```

Zinterpretuj uzyskane efekty, zapisz interpretację w zeszycie.

### Zgłoszenie 6

**Zgłoś zakończenie ćwiczenia w celu sprawdzenia.**