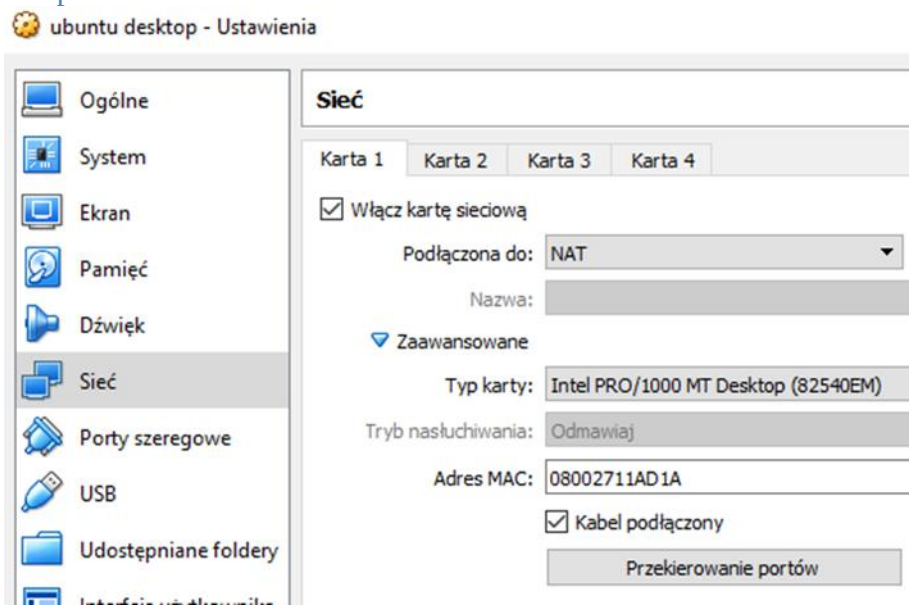
T: Kontrola wydarzeń w sieci.

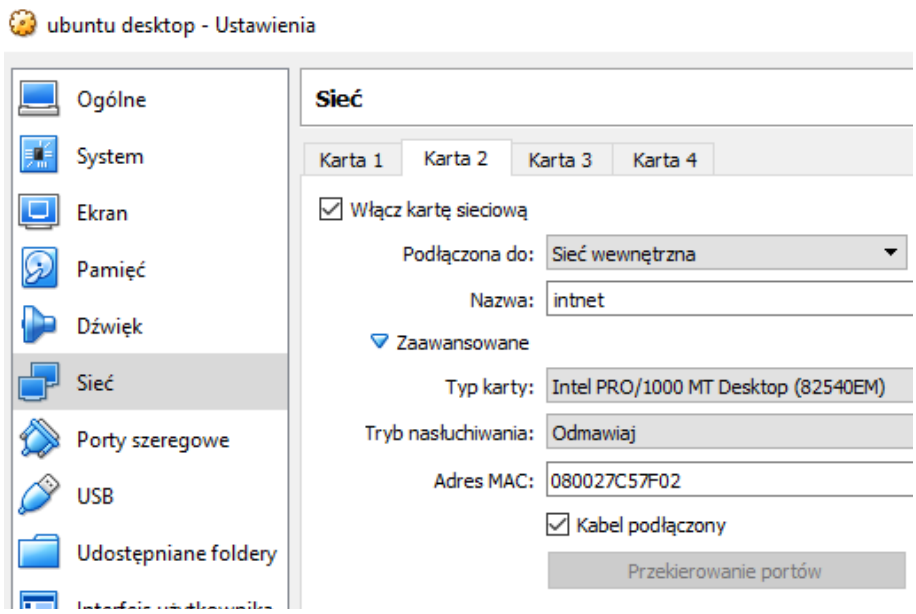
Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu podaj i wyjaśnij
1. polecenia, które użyjesz, aby przetestować połączenie sieciowe.
2. odpowiedzi na pytania zadane w treści zadań.

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.

Adapter 1



Adapter 2



Po uruchomieniu Ubuntu wybierz Ctrl+Alt + F5 podaj **login**: root **Password**: 1234

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Pozostaw adres IP dla Ubuntu na Adapter 2 na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/0 <tab>

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

Pozostaw zalecane wpisy w tym pliku

```
  GNU nano 2.9.3                /etc/netplan/01-network-manager-all.yaml

# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
    enp0s8:
      dhcp4: no
      addresses: [10.0.0.30/24]
```

2. Jeżeli dokonałeś zmian zastosuj ustawienia
root@ubuntusrv:~# netplan apply

```
root@bolek-VirtualBox:~# netplan apply
```

W celu sprawdzenia

```
root@bolek-VirtualBox:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
0
    link/ether 08:00:27:11:ad:1a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic e
       valid_lft 86334sec preferred_lft 86334sec
    inet6 fe80::bd38:d3cd:8b7c:bf9c/64 scope link noprefixr
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
0
    link/ether 08:00:27:c5:7f:02 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.30/24 brd 10.0.0.255 scope global enp0s8
       valid_lft forever preferred_lft forever
root@bolek-VirtualBox:~#
```

Zadanie 1

Podstawowe polecenia testujące

A. Polecenie ping
Testowanie komputerów i sieci na poziomie IP. Program jest podstawowym narzędziem administratora sieci. Możemy za jego pomocą uzyskać wiele informacji. Uwaga, wersje polecenia ping są różne w zależności od systemu operacyjnego. Niektóre opcje mogą być inne lub niedostępne.
Warto pamiętać, że polecenie ping bada sieć na poziomie protokołów warstwy łącza danych oraz IP. Oznacza to że TCP i UDP nie maja żadnego wpływu ponieważ ICMP używane przez ping działa bezpośrednio na IP. Jest to pomocne przy badaniu szybkości łącza i ilości traconych pakietów.
W TCP nic nie ginie, w IP pakiet może się zapodziać. Nie ma też narzutu związanego z nawiązywaniem połączenia.

a) Wykonaj kolejno polecenia ping (żądania echa ICMP) ping ADRES_IP_LUB_DOMENA
1. ping 10.0.0.30
po pięciu odpowiedziach Ctrl+C

2. ping ubuntusrv
po pięciu odpowiedziach Ctrl+C
Zapisz w zeszycie z jakiego adresu otrzymujesz odpowiedz?
Wpisz cat /etc/hosts, zapisz adres, z którego otrzymujesz odpowiedz? Zapisz w zeszycie jak nazywa się przypisany do niego host.

3. ping localhost
po pięciu odpowiedziach Ctrl+C
Z jakiego adresu otrzymujesz odpowiedz?
Wpisz cat /etc/hosts, zapisz adres, z którego otrzymujesz odpowiedz? Zapisz w zeszycie jak nazywa się przypisany do niego host.

4. ping cke.gov.pl
po pięciu odpowiedziach Ctrl+C
Zapisz w zeszycie, dlaczego nie otrzymujesz odpowiedzi.
5. Zapisz w zeszycie: Wysłanie rozgłoszeniowego komunikatu ping do całej sieci poprzez podanie adresu broadcast sieci (dla sieci 10.0.0.0/24 komunikat wyglądałby następująco)
ping 10.0.0.255.
Polecenie ping -f IP wysyła tak dużo komunikatów ping, ile to tylko możliwe, zalewa sieć maksymalną ilością poleceń ping. Można w ten sposób łatwo sprawdzić, czy okablowanie jest poprawne patrząc czy ilość utraconych pakietów jest zbliżona do oczekiwanej. Nie powinno sie tego używać w normalnych sieciach, bo powoduje natychmiastowe przeciążenie.

6. ping -f 127.0.0.1
po pięciu sekundach Ctrl+C
Zapisz w zeszycie interpretacje wyników polecenia.

Wysłanie określonej ilości komunikatów i pokaz statystyk
7. ping -c 30 10.0.0.30
Zapisz w zeszycie interpretacje wyników polecenia.

Wysyłanie komunikatów z określoną wartością TTL. Za pomocą tej opcji możemy określić maksymalna ilość routerów jakie chcemy przejść nim pakiet zostanie porzucony lub zwrócony przez router z kodem przekroczenia max ttl.
8. ping -t 1 10.0.0.30
po pięciu sekundach Ctrl+C
Zapisz w zeszycie interpretacje wyników polecenia.

Wysłanie komunikatów o określonym rozmiarze. Ta opcja pozwoli nam zdiagnozować problemy rzadkie i trudne do wykrycia związane z full duplex lub niepoprawnym MTU.
9. ping -s 1000 10.0.0.30
po pięciu sekundach Ctrl+C
Zapisz w zeszycie interpretacje wyników polecenia.

(zgłoszenie) 1

B. Polecenie netstat
Program pozwala na przeglądanie / monitorowanie lokalnych połączeń i gniazd. Program pozwala na przeglądanie jakie połączenia są obecnie zestawione z naszym komputerem oraz jakie lokalne porty nasłuchują na nadchodzące połączenia. Pozwala to łatwo zlokalizować jakie aplikacje sieciowe działają na naszym komputerze.

b) Wykonaj kolejno polecenia netstat
Podgląd połączeń maskowanych przez system (jeśli jest używany moduł maskarady).
Chodzi o połączenia, które przechodzą przez nasz komputer jako router dostępu do internetu.
1. netstat –M
Zapisz w zeszycie interpretacje wyników polecenia.

Gadatliwe wyjście programu, pokazuje nam więcej szczegółów.
2. netstat -v
Zapisz w zeszycie interpretacje wyników polecenia.
Nie rozwiązuje nazw domenowych tylko pokazuje IP. Bardzo przydatne, gdyż lookupy nazw DNS są bardzo wolne.
3. netstat -n
Zapisz w zeszycie interpretacje wyników polecenia.

Powtarza wykonanie co sekundę. Jeśli chcemy w sposób w miarę ciągły podglądać status lub oczekujemy na jakieś połączenia testując nasze aplikacje lub sieć.
4. netatat –c
po pięciu sekundach Ctrl+C
Zapisz w zeszycie interpretacje wyników polecenia.

Pokazuje nasłuchujące porty.
5. netstat -l
Zapisz w zeszycie interpretacje wyników polecenia.

Pokazuje wszystkie połączenia nie tylko w stanie połączonym.
6. netstat -a
Zapisz w zeszycie interpretacje wyników polecenia.

Pokazuje tylko połączenia z danej rodziny protokołów (w przykładzie IP)
7. netstat -A inet
Zapisz w zeszycie interpretacje wyników polecenia.

Przydatna forma polecenia:
8. netstat -an
Zapisz w zeszycie interpretacje wyników polecenia.

Pokazuje tablicę routingu:
9. netstat -r
Zapisz w zeszycie interpretacje wyników polecenia.

Nawiązane połączenia i otwarte porty protokołu TCP/IP możemy kontrolować za pomocą:
10. netstat -tua
Zapisz w zeszycie interpretacje wyników polecenia. (zgłoszenie) 2

C. Polecenie nmap
Program nmap (w dokumentacji polecenia szczegóły oraz dostępne parametry) pozwala na

- bardzo zaawansowane testowanie zabezpieczeń, ustawień oraz szczegółów konfiguracji hostów.
- skanowanie komputerów w trybie aktywnym oraz pasywnym. Tryb aktywny to wysyłanie spreparowanych pakietów by sprawdzić, czy host jest aktywny lub jaki jest jego system operacyjny itd. Tryb pasywny to sniffing nakierowany na tworzenie mapy sieci lokalnej z listą serwerów oraz usług a nawet wersji oprogramowania.

- wykrywanie jakie usługi sieciowe dostępne są na skanowanym hoscie.

Wykonaj proste aktywne skanowanie TCP jednego adresu IP oraz pokaż wyniki.
1. nmap -sT 10.0.2.15

Zapisz w zeszycie interpretacje wyników polecenia.

Wykonaj proste aktywne skanowanie UDP oraz pokaż wyniki.
2. nmap -sU 10.0.2.15

Zapisz w zeszycie interpretacje wyników polecenia.

Wykryj które komputery w sieci odpowiadają na ping oraz wyświetl podstawowe informacje. Pozwala na wykrycie jakie mamy zajęte adresy IP np w sieci z DHCP.
3. nmap -sP 10.0.0.0/24

Zapisz w zeszycie interpretacje wyników polecenia.
Skanuj zakres portów.
4. nmap -sT 10.0.2.15 -p 0-3000

Zapisz w zeszycie interpretacje wyników polecenia.

Rozpoznaj system operacyjny.
5. nmap -O 10.0.2.15

Zapisz w zeszycie interpretacje wyników polecenia.

Skanowanie z pokazaniem dużej ilości informacji.
6. nmap -O -sU -sT -v 192.168.92.34 -p 0-5000

Zapisz w zeszycie interpretacje wyników polecenia.

(zgłoszenie) 3

D. Polecenie host

a) Użyj w systemie Linux w stosunku do kilku hostów internetowych polecenia host nazwa_strony_www lub traceroute nazwa_hosta

Zastanów się nad wynikami (dlaczego niektóre mają kilka IP inne tylko jedno).
Zapisz w zeszycie interpretacje wyników poleceń.

1. host www.cke.gov.pl
2. host cke.gov.pl
3. host www.oke.gda.pl
4. host oke.gda.pl
5. host www.zsl.gda.pl
6. host zsl.gda.pl
7. host www.google.pl
8. host google.pl
9. host Ubuntu.com

(zgłoszenie) 4

E. Polecenie traceroute

a) Użyj w systemie Linux w stosunku do kilku hostów internetowych polecenia

traceroute nazwa_strony_www lub traceroute nazwa_hosta
Zastanów się nad wynikami (dlaczego czasami w odpowiedzi są *).
Zapisz w zeszycie interpretacje wyników poleceń.

1. traceroute www.cke.gov.pl
2. traceroute cke.gov.pl
3. traceroute www.oke.gda.pl
4. traceroute oke.gda.pl
5. traceroute www.zsl.gda.pl
6. traceroute zsl.gda.pl
7. traceroute www.google.pl
8. traceroute google.pl
9. traceroute Ubuntu.com

(zgłoszenie) 5

F. Polecenie whois

Zapisz w zeszycie interpretacje wyników poleceń.

a) Sprawdź za pomocą komendy whois

1. Kto zarejestrował domenę cke.gov.pl i kiedy.
2. Kiedy dokonano ostatniej zmiany wpisów.
3. Do jakiej sieci (o jakim zakresie adresów) należy adres IP: 213.192.73.194.
4. Kto jest właścicielem ww. adresu IP, w jakim kraju, pod jakim adresem pocztowym.
5. Z jakim adresem mailowym należy się kontaktować w przypadku nadużycia pochodzącego z ww. adresu IP.

(zgłoszenie) 6

Zadanie 2

a) Użyj w systemie Linux polecenia wyświetlającego tablicę ARP.
ip neighbour
arp (przestarzałe)
Zapisz w zeszycie interpretacje wyników polecenia.

b) Użyj w systemie Linux polecenia pokazującego ruting.
ip route show
route (przestarzałe)
Zapisz w zeszycie interpretacje wyników polecenia.

c) Użyj w systemie Linux polecenia do wyszukiwania szczegółowych informacji odnoszących się do serwerów DNS włączając adres IP poszczególnych komputerów, nazwę domeny czy aliasy jakie posiada.

1 Sprawdź serwer lokalny.

dig 127.0.0.1
nslookup 127.0.0.1 (przestarzałe)
Zapisz w zeszycie interpretacje wyników polecenia.

2 Sprawdź serwer zdalny.
dig Ubuntu.com
nslookup Ubuntu.com (przestarzałe)
Zapisz w zeszycie interpretacje wyników polecenia.

d) Polecenie tcpdump.
1 Zainstaluj pakiet tcpdump aptitude install tcpdump

Przejdź do Ctrl+Alt+F3 podaj **login**: root **Password**: 1234

2 Wykonaj ping na adres z karty enp0s8

3 Przejdź do Ctrl+Alt+F5

4 Wykonaj tcpdump -i enp0s8

po pięciu odpowiedziach Ctrl+C

Zapisz w zeszycie interpretacje wyników polecenia.
e) Polecenie tcpdump z zapisem.
Opcja "-w" pozwala zapisać wynik do wskazanego pliku:

tcpdump -v -w informacje_o_ruchu_w_sieci

Opcja "-r" pozwala odczytać zawartość z wskazanego pliku:

tcpdump -r informacje_o_ruchu_w_sieci

1 Powtórz ćwiczenie d zapisując wynik podsłuchu sieci do pliku.

2 Odczytaj wynik podsłuchu sieci z pliku.

Zapisz w zeszycie interpretacje wyników polecenia.

(zgłoszenie) 7