

T: Testowanie połączenia sieciowego, kontrola wydarzeń w sieci.

Cel ogólny lekcji: nauczenie uczniów kontrolowania wydarzeń w sieci poprzez przetestowanie połączenia sieciowego za pomocą poleceń, takich jak ping -c 5 oraz odpowiedzi na pytania dotyczące adresów IP, hostów i adresów DNS.

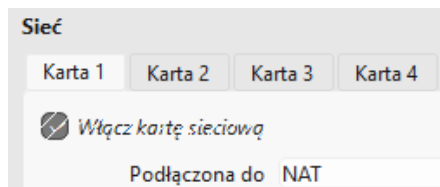
Cele szczegółowe lekcji:

1. Uczniowie będą potrafili
 - a. przetestować połączenie sieciowe za pomocą poleceń ping -c 5.
 - b. odpowiedzieć na pytania dotyczące adresów IP, hostów i adresów DNS.
 - c. ustawić statyczny adres IP dla Ubuntu na Adapterze 2.
 - d. otworzyć plik opisujący interfejsy sieciowe i pozostawić zalecane wpisy.
 - e. zastosować ustawienia sieciowe.
 - f. wysłać rozgłoszeniowy komunikat ping -c 5 do całej sieci.
 - g. interpretować wyniki poleceń ping -c 5.
2. Uczniowie będą w stanie
 - a. zastosować w praktyce podstawowe polecenia służące do testowania połączenia sieciowego, takie jak ping -c 5, w celu określenia szybkości łącza i ilości traconych pakietów.
 - b. zastosować w praktyce wiedzę na temat protokołów warstwy łącza danych oraz IP i zrozumieją, jak działają te protokoły.
 - c. dokonać konfiguracji pierwszej i drugiej karty sieciowej według instrukcji oraz sprawdzić, czy ustawienia maszyny wirtualnej pozwalają na dostęp do Internetu.
 - d. opisać, jakie informacje można uzyskać dzięki poleceniu ping -c 5 oraz jakie zagrożenia mogą wystąpić w sieci przy niewłaściwym jego wykorzystaniu.
 - e. opisać, dlaczego nie otrzymują odpowiedzi od konkretnych adresów IP i co może być przyczyną tego problemu.
 - f. zastosować w praktyce rozgłoszeniowe komunikaty ping -c 5, aby przetestować połączenie sieciowe i okablowanie.

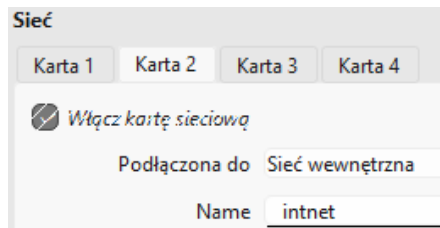
Przygotowanie środowiska:

- Przywróć migawkę „Stan początkowy”.
- Upewnij się, że VM ma dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu. Zalecane ustawienia maszyny z Ubuntu serwer 24.04

Adapter 1



Adapter 2



- Wykonaj ćwiczenie na maszynie wirtualnej z Ubuntu Server 24.04 LTS.

Po uruchomieniu Ubuntu podaj kolejno:

login: ubuntu **password:** ubuntu zalogowanie do ubuntu

sudo -s **password:** ubuntu - logowanie z podniesionymi uprawnieniami

1. Skopiuj przykładową konfigurację statycznego adresu IP Netplan do katalogu /etc/netplan/ poleceniem:

```
sudo cp /usr/share/doc/netplan/examples/static.yaml /etc/netplan/01-netcfg.yaml
```

2. Poprawnie ustaw IPv4:

Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/0 tabulator - nazwa pliku zostanie uzupełniona do postaci *.yaml Plik: /etc/netplan/01-netcfg.yaml pozostaw:

```
network:
```

```
  version: 2
```

```
  renderer: networkd
```

```
  ethernets:
```

```
    enp0s3:
```

```
      dhcp4: true
```

```
    enp0s8:
```

```
      dhcp4: false
```

```
      addresses:
```

```
        - 10.0.0.30/24
```

3. Zastosowanie ustawień:

```
sudo netplan apply
```

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu podaj i wyjaśnij odpowiedzi na pytania zadane w treści zadań.

Zadanie 1

Podstawowe polecenia testujące

A. Polecenie ping -c 5

Testowanie komputerów i sieci na poziomie IP. Program jest podstawowym narzędziem administratora sieci. Możemy za jego pomocą uzyskać wiele informacji. Uwaga, wersje polecenia ping -c 5 są różne w zależności od systemu operacyjnego. Niektóre opcje mogą być inne lub niedostępne.

Warto pamiętać, że polecenie ping -c 5 bada sieć na poziomie protokołów warstwy łącza danych oraz IP. Oznacza to, że TCP i UDP nie mają żadnego wpływu, ponieważ ICMP używane przez ping -c 5 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:

1. `ping -c 5 10.0.0.30`

po pięciu odpowiedziach Ctrl+C

2. `ping -c 5 ubuntu2204`

Zapisz w zeszycie: z jakiego adresu IP otrzymujesz odpowiedzi (odeczytaj z wyników polecenia).

3. Wyświetl plik /etc/hosts: `cat /etc/hosts`,

Zapisz w zeszycie: jaki adres IP jest przypisany do hosta ubuntu2204, jak nazywa się host odpowiadający temu adresowi.

4. `ping -c 5 localhost`

Zapisz w zeszycie: z jakiego adresu IP otrzymujesz odpowiedzi podczas pingowania localhost.

Następnie, korzystając z pliku /etc/hosts (nie trzeba go wpisywać drugi raz): zapisz, jaki adres IP przypisany jest do localhost, zapisz, jaka nazwa hosta odpowiada temu adresowi.

5. `ping -c 5 cke.gov.pl`

Zapisz w zeszycie odpowiedź na pytanie:

Dlaczego nie otrzymujesz odpowiedzi z serwera cke.gov.pl?

Wskazówka: Wiele serwerów instytucji państwowych blokuje odpowiedzi ICMP (ping) w ramach zabezpieczeń. Dlatego serwer działa, ale nie odpowiada na ping.

6. Wysłanie komunikatu rozgłoszeniowego (broadcast) Polecenie (dla sieci 10.0.0.0/24):

`ping -c 5 10.0.0.255`

Zapisz w zeszycie: Co oznacza wysłanie pingu na adres broadcast.

Dlaczego odpowiedzi mogą pochodzić od wielu hostów (jeśli odpowiadają) lub dlaczego mogą nie pojawić się wcale - wiele systemów blokuje ping na broadcast ze względów bezpieczeństwa.

Wyjaśnienie: Adres broadcast (np. 10.0.0.255 w sieci /24) służy do wysłania komunikatu do wszystkich urządzeń w sieci. Niektóre systemy mogą ignorować broadcast, aby nie generować ruchu ICMP storm i nie ujawniać obecności hostów.

7. Test przeciążeniowy (flood ping) Wyjaśnienie polecenia flood: `ping -c 5 -f 127.0.0.1`

Zapisz w zeszycie interpretację wyników: Ile pakietów zostało wysłanych i odebranych.

Dlaczego na adresie 127.0.0.1 (loopback) nie pojawiają się straty pakietów.

Co oznacza bardzo wysoka szybkość wysyłania pakietów - test odbywa się wewnątrz systemu, bez udziału karty sieciowej i bez opóźnień sieciowych.

Dodatkowy opis do zeszytu: Wysłanie określonej liczby komunikatów przy użyciu -c oraz obserwacja statystyk ICMP pozwala ocenić poprawność działania interfejsu loopback i stosu TCP/IP systemu.

8. `ping -c 30 10.0.0.30`

Zapisz w zeszycie interpretację wyników polecenia. Uczeń powinien zanotować:

Wynik pingu - czy pakiety dotarły i czy wróciła odpowiedź.

Uczeń powinien zanotować: Wyniki pingu, ile pakietów wysłano, ile odebrano, czy wystąpiły straty, jaka była minimalna, maksymalna i średnia wartość czasu odpowiedzi (latency).

Znaczenie większej liczby pakietów (-c 30): im więcej pakietów, tym dokładniej można ocenić stabilność połączenia, 30 pakietów pozwala zauważyć ewentualne chwilowe zaniki lub przeciążenia, można ocenić, czy sieć działa równomiernie (stałe czasy odpowiedzi) czy zmiennie (skoki ms).

Wniosek:

jeśli wszystkie 30 pakietów dotarły, połączenie z hostem 10.0.0.30 jest stabilne,

jeśli występują straty, może to wskazywać na: słabą jakość połączenia, przeciążenie sieci, problemy z kartą sieciową lub okablowaniem, problemy po stronie hosta 10.0.0.30.

9. `ping -c 5 -t 1 10.0.0.30`

Zapisz w zeszycie interpretację wyników polecenia.

TTL=1 oznacza, że pakiet może pokonać maksymalnie 1 przeskok (router).

Jeśli host jest dalej niż 1 hop, pakiet zostanie odrzucony i router zwróci błąd „Time Exceeded”.

Polecenie pozwala sprawdzić, na którym etapie trasy pakiet jest zatrzymywany.

Jest to podobne do działania traceroute (badanie kolejnych wartości TTL).

10. `ping -c 5 -s 1000 10.0.0.30`

Zapisz w zeszycie interpretację wyników polecenia.

11. `ping -c 5 -s 1472 10.0.0.30`

Zapisz w zeszycie interpretację wyników polecenia:

Uczeń powinien zanotować:

a. Co sprawdza to polecenie?

Testuje maksymalny rozmiar pakietu, jaki może zostać przesłany bez fragmentacji.

MTU (Maximum Transmission Unit) określa największy pakiet, jaki można przesłać jednym kawałkiem przez interfejs sieciowy.

b. Dlaczego używamy wartości -s 1472?

Standardowy pakiet ping ma:

- 20 bajtów nagłówka IP
- 8 bajtów nagłówka ICMP

Maksimum bez fragmentacji w Ethernet to:

1500 bajtów MTU – 28 bajtów nagłówków = 1472 bajty danych

Dlatego 1472 to „maksymalny payload” mieszczący się w MTU 1500.

c. Znaczenie opcji -M do

-M do = don't fragment

Ping wysyła pakiety z ustawioną flagą „nie fragmentować”.

Jeśli pakiet musi zostać podzielony na mniejsze — router go odrzuci i zwróci błąd:

Frag needed and DF set

d. Jak interpretować wyniki?

Uczeń zapisuje:

Jeśli odpowiedzi wracają > ścieżka obsługuje MTU 1500.

Jeśli pojawia się komunikat:

ping: local error: Message too long

albo router zwraca informację o potrzebie fragmentacji >

MTU na ścieżce jest mniejsze niż 1500 (np. 1492, 1450...).

e. Wniosek

Test MTU pozwala wykryć problemy takie jak:

- błędnie ustawiona wartość MTU na routerach, przełącznikach lub VPN-ach,
- tunelowanie (PPPoE, GRE, IPsec),
- błędne auto-negocjacje lub problemy z konfiguracją.

12. Test fragmentacji pakietów IP

Polecenie 1 - z próbą wymuszenia fragmentacji:

```
ping -c 5 -s 2000 10.0.0.30
```

Polecenie 2 - test z flagą „nie fragmentować”:

```
ping -c 5 -s 2000 -M do 10.0.0.30
```

Zapisz w zeszycie interpretację wyników polecenia

Uczeń powinien zanotować:

- a. Co robi pierwsze polecenie (-s 2000 bez -M do)
 - Wysyła pakiet **2000 bajtów**,
 - Routery **mogą fragmentować pakiet**, jeśli MTU jest mniejsze,
 - Jeśli sieć obsługuje fragmentację: > **ping może się udać**, mimo dużego rozmiaru pakietu.

Wynik, jaki uczeń powinien opisać:

- Czy pakiety dotarły?
- Czy routery dokonały fragmentacji? (widoczne w czasie odpowiedzi)
- b. Co robi drugie polecenie (-s 2000 -M do)
 - -M do = don't fragment > **NIE WOLNO** dzielić pakietu,
 - Jeśli MTU < 2000 bajtów (a w Ethernet jest zawsze 1500):

Router zwróci błąd:

ping: local error: Message too long, mtu=1500

lub

Frag needed and DF set

Wniosek:

- Ten test **ujawnia różnicę między rzeczywistym MTU a rozmiarem wysyłanego pakietu**,
- Praktycznie *zawsze* pokaże błąd dla 2000 B, bo Ethernet ma MTU 1500.

Uczeń powinien zapisać:

„Pakiet nie może zostać przesłany bez fragmentacji, bo jest większy niż MTU 1500. Sieć zwróciła komunikat o konieczności fragmentacji.”

- c. Co test fragmentacji pozwala wykryć?

Uczeń zapisuje:

- problemy z MTU (zbyt niskie wartości, np. na VPN),
- fragmentację pakietów na trasie (co obniża wydajność),
- błędy konfiguracji tuneli (PPPoE, GRE, IPsec),
- różnice MTU między segmentami sieci,
- ustawienia DF i PMTUD (Path MTU Discovery).

(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. Zainstaluj pakiet net-tools: **sudo apt install net-tools**

Po zainstalowaniu możesz sprawdzić wersję netstat za pomocą:

netstat -V

b) Wykonaj kolejno polecenia netstat

1. Podgląd połączeń maskowanych przez system (jeśli jest używany moduł maskarady).

Chodzi o połączenia, które przechodzą przez nasz komputer jako router dostępu do internetu.

netstat -M

Zapisz w zeszycie interpretacje wyników polecenia.

2. Gadatliwe wyjście programu, pokazuje nam więcej szczegółów.

netstat -v

Zapisz w zeszycie interpretacje wyników polecenia.

3. Nie rozwiązuje nazw domenowych tylko pokazuje IP. Bardzo przydatne, gdyż lookupy nazw DNS są bardzo wolne.

netstat -n

Zapisz w zeszycie interpretacje wyników polecenia.

4. Powtarza wykonanie co sekundę. Jeśli chcemy w sposób w miarę ciągły podglądać status lub oczekujemy na jakieś połączenia testując nasze aplikacje lub sieć.

netstat -c

po pięciu sekundach Ctrl+C

Zapisz w zeszycie interpretacje wyników polecenia.

5. Pokazuje nasłuchujące porty.

netstat -l (l jak lokaj)

Zapisz w zeszycie interpretacje wyników polecenia.

6. Pokazuje wszystkie połączenia nie tylko w stanie połączonym.

netstat -a

Zapisz w zeszycie interpretacje wyników polecenia.

7. Pokazuje tylko połączenia z danej rodziny protokołów (w przykładzie IP)

netstat -A inet

Zapisz w zeszycie interpretacje wyników polecenia.

8. Przydatna forma polecenia:

netstat -an

Zapisz w zeszycie interpretacje wyników polecenia.

9. Pokazuje tablicę routingu:

netstat -r

Zapisz w zeszycie interpretacje wyników polecenia.

10. Nawiązane połączenia i otwarte porty protokołu TCP/IP możemy kontrolować za pomocą:

netstat -tua

Zapisz w zeszycie interpretację wyników polecenia.

11. Pokaż procesy używające portów

netstat -p

Zapisz w zeszycie interpretację wyników polecenia.

12. Pokaż statystyki protokołów

netstat -s

Zapisz w zeszycie interpretację wyników polecenia.

13. Pokaż kto nasłuchuje (wersja kompletna)

netstat -tupln

Zapisz w zeszycie interpretację wyników polecenia.

14. Pokaż ciągły monitoring wszystkich połączeń

netstat -c -an

Zapisz w zeszycie interpretację wyników polecenia.

(zgłoszenie) 2

C. Polecenie ss (socket statistics) – nowoczesny następca netstat

ss to współczesne narzędzie do analizy połączeń i gniazd sieciowych w systemach Linux. W przeciwieństwie do netstat, polecenie ss:

- jest **szybsze**,
- daje **bardziej szczegółowe dane**,
- działa **bezpośrednio na Netlink**,
- pokazuje więcej informacji o protokołach TCP/UDP,
- jest **domyślnie instalowane** w nowych dystrybucjach (Ubuntu, Debian, Fedora).

Polecenie ss powinno być stosowane **zamiast** netstat.

Wykonaj kolejne polecenia ss:

1. Wyświetlanie wszystkich gniazd TCP

ss -t

Zapisz w zeszycie interpretację wyników:

- aktywne połączenia TCP,
- stan połączeń (ESTAB, SYN-SENT, TIME-WAIT).

2. Wyświetlanie wszystkich gniazd UDP

ss -u

Uczeń zapisuje:

- otwarte gniazda UDP,
- brak stanu (bo UDP jest bezpołączeniowe).

3. Wyświetlanie nasłuchujących portów TCP

ss -lt

(L = LISTEN, T = TCP)

Uczeń zapisuje:

- które usługi nasłuchują,
- na jakich portach i interfejsach.

Przykład:

*:22 > SSH nasłuchuje na wszystkich interfejsach.

4. Wyświetlanie nasłuchujących portów UDP

ss -lu

Uczeń zapisuje:

- usługi działające na UDP (np. DNS – port 53).

5. Wyświetlanie wszystkich połączeń TCP i UDP w trybie liczbowym

ss -tun

Interpretacja:

- -t TCP
- -u UDP
- -n pokazuj IP zamiast nazw DNS

Przydatne, bo:

- rozwiązywanie DNS spowalnia komendy,
- widać surowe adresy i porty (np. 10.0.0.30:22).

6. Wyświetlanie procesów, które używają portów

ss -p

Co zapisuje uczeń:

- PID procesów,
- nazwy programów,
- jakich portów używają.

To jest główna przewaga ss nad netstat.

7. Pełny widok wszystkich połączeń (TCP + UDP + procesy)

ss -tulnp

Uczeń zapisuje:

- pełną tabelę połączeń,

- listę usług i portów,
- procesy powiązane z portami.

To odpowiednik:

netstat -tupln

ale **dokładniejszy**.

8. Ciągłe monitorowanie ruchu

ss -tun -o

-o pokazuje timery TCP (czas do retransmisji, timeouty).

Uczeń notuje:

- zmieniające się czasy i stany połączeń,
- opóźnienia, czas do retransmisji.

Świetne jako uzupełnienie pinga i traceroute.

9. Informacje o backlogach, buforach i kolejce

ss -s

Uczeń zapisuje:

- statystyki TCP/UDP,
- zajętość buforów,
- liczbę otwartych połączeń,
- informacje o RTO, SYN retries.

Bardzo przydatne do diagnozy wydajności.

Podsumowanie – dlaczego ss jest lepsze niż netstat

Uczeń powinien dopisać:

- ss działa szybciej niż netstat
- ss pokazuje więcej szczegółów
- ss jest aktywnie rozwijane
- netstat jest przestarzałe (w pakiecie net-tools)
- nowe dystrybucje Linuksa rekomendują ss

(zgłoszenie) 3

D. 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.

Zainstaluj pakiet `apt -y install nmap`

1. Wykonaj proste aktywne skanowanie TCP jednego adresu IP oraz pokaż wyniki.

```
nmap -sT 10.0.2.15
```

Zapisz w zeszycie interpretacje wyników polecenia.

2. Wykonaj proste aktywne skanowanie UDP oraz pokaż wyniki.

```
nmap -sU 10.0.2.15
```

Zapisz w zeszycie interpretacje wyników polecenia.

3. Wykryj które komputery w sieci odpowiadają na ping -c 5 oraz wyświetl podstawowe informacje.
Pozwala na wykrycie jakie mamy zajęte adresy IP np w sieci z DHCP.

```
nmap -sP 10.0.0.0/24
```

Zapisz w zeszycie interpretacje wyników polecenia.

4. Skanuj zakres portów.

```
nmap -sT 10.0.2.15 -p 0-3000
```

Zapisz w zeszycie interpretacje wyników polecenia.

5. Rozpoznaj system operacyjny.

```
nmap -O 10.0.2.15
```

Zapisz w zeszycie interpretacje wyników polecenia.

6. Wykonaj skanowanie z pokazaniem dużej ilości informacji.

```
nmap -O -sU -sT -v 10.0.2.15 -p 0-5000
```

Zapisz w zeszycie interpretacje wyników polecenia.

(zgłoszenie) 3

E. Polecenie host

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

`host nazwa_strony_www` lub `tracert nazwa_hosta`

Zastanów się nad wynikami (dlaczego niektóre mają kilka IP inne tylko jedno).

Zapisz w zeszycie interpretację wyników poleceń host:

1. Zapytania dotyczące domen CKE

```
host www.cke.gov.pl
```

```
host cke.gov.pl
```

2. Zapytania dotyczące domen OKE Gdańsk

host www.oke.gda.pl

host oke.gda.pl

3. Zapytania dotyczące domen Zespołu Szkół Łączności

host www.zsl.gda.pl

host zsl.gda.pl

4. Zapytania dotyczące domen Google

host www.google.pl

host google.pl

5. Zapytanie dotyczące domeny Ubuntu

host Ubuntu.com

(zgłoszenie) 4

F. 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 *).

Zainstaluj pakiet `apt -y install traceroute`

Zapisz w zeszycie interpretacje wyników poleceń traceroute:

1. Trasa do serwerów CKE

traceroute www.cke.gov.pl

traceroute cke.gov.pl

2. Trasa do serwerów OKE Gdańsk

traceroute www.oke.gda.pl

traceroute oke.gda.pl

3. Trasa do serwerów Zespołu Szkół Łączności

traceroute www.zsl.gda.pl

traceroute zsl.gda.pl

4. Trasa do serwerów Google

traceroute www.google.pl

traceroute google.pl

5. Trasa do serwerów Ubuntu

traceroute Ubuntu.com

(zgłoszenie) 5

G. Polecenie whois

Zainstaluj pakiet `apt -y install whois`

Zapisz w zeszycie interpretacje wyników poleceń.

a) Sprawdź za pomocą komendy `whois`

1. Kto zarejestrował domenę `cke.gov.pl` i kiedy.

```
whois cke.gov.pl | grep -Ei "registrant|created|registrar"
```

2. Kiedy dokonano ostatniej zmiany wpisów.

```
whois cke.gov.pl | grep -Ei "last modified|updated"
```

3. Do jakiej sieci (o jakim zakresie adresów) należy adres IP: `213.192.73.194`.

```
whois 213.192.73.194 | less
```

```
whois 213.192.73.194 | grep -Ei "inetnum|netrange"
```

4. Kto jest właścicielem ww. adresu IP, w jakim kraju, pod jakim adresem pocztowym.

```
whois 213.192.73.194 | grep -Ei "org-name|descr|address|country"
```

5. Z jakim adresem mailowym należy się kontaktować w przypadku nadużycia pochodzącego z ww. adresu IP.

```
whois 213.192.73.194 | grep -Ei "abuse-mailbox|abuse"
```

(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 routing.

```
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 `apt -y install tcpdump`

Przejdź do Ctrl+Alt+F3 podaj **login:** `ubuntu` **Password:** `ubuntu`

Wpisz `sudo -s` **Password:** `ubuntu`

2 Wykonaj `ping -c 5 enp0s3`

3 Przejdź do Ctrl+Alt+F3 (lub F2, F4, F5, F6 - byle nie ten, gdzie będzie tcpdump).

4 Wykonaj podsłuch pakietów: `tcpdump -i enp0s3`

Po wyświetleniu ok. 5 odpowiedzi ICMP > przerwij:

`Ctrl+C`

Zapisz w zeszycie interpretacje wyników polecenia.

Uczeń powinien zapisać:

a. `tcpdump -i enp0s3` – uruchamia podsłuch interfejsu sieciowego enp0s3.

b. W wynikach widać pakiety ICMP:

- ICMP echo request > pakiety wysyłane przez ping
- ICMP echo reply > odpowiedzi z tego samego adresu

c. W każdym wpisie widoczne są:

- czas (timestamp) – kiedy pakiet został wychwycony
- źródłowy adres IP > docelowy adres IP
- typ protokołu (ICMP)
- id, seq, ttl, length – parametry pakietu

d. `tcpdump` rejestruje tylko nagłówki pakietów, dzięki czemu można analizować ruch sieciowy.

Przykładowa interpretacja jednego wpisu:

13:32:15.123456 IP 192.168.1.10 > 192.168.1.1: ICMP echo request, id 5, seq 1, length 64

To oznacza:

- komputer 192.168.1.10 wysłał ping do 192.168.1.1
- był to ICMP echo-request
- to pierwszy pakiet (seq=1)

- rozmiar pakietu: 64 bajty

e) Polecenie tcpdump z zapisem do pliku. Zapis przechwyconych pakietów do pliku

Opcja “-w” pozwala zapisać wynik do wskazanego pliku:

```
tcpdump -v -w informacje_o_ruchu_w_sieci
```

Co zapisuje?

> wszystkie surowe pakiety (format PCAP) – można otworzyć w Wireshark.

Przerwanie po 5 odpowiedziach:

Ctrl + C

f) Odczyt przechwyconych pakietów z pliku

Opcja “-r” pozwala odczytać zawartość z wskazanego pliku:

```
tcpdump -r informacje_o_ruchu_w_sieci
```

Interpretacja do zeszytu (sekcja e)

Uczeń wpisuje:

a. Opcja -w zapisuje podsłuchane pakiety do pliku w formacie PCAP.

b. Plik PCAP można potem:

analizować offline

otworzyć w Wireshark

c. Opcja -r odczytuje plik i wyświetla pakiety w takim formacie, jakby były przechwycone na żywo.

d. W odczycie pojawiają się te same pakiety ICMP (echo request / reply) co w ćwiczeniu d, ponieważ były zapisane z pingowania interfejsu.

01. Powtórz ćwiczenie d zapisując wynik podsłuchu sieci do pliku.

02. Odczytaj wynik podsłuchu sieci z pliku.

Zapisz w zeszycie interpretacje wyników polecenia.

(zgłoszenie) 7

Przywróć pierwszą migawkę.

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.