Testowanie połączenia sieciowego (2026)

Ten materiał rozszerza i szczegółowo wyjaśnia wszystkie zagadnienia wymagane do wykonania ćwiczeń CW5 w systemach Ubuntu/Debian. Zawiera teorię krok po kroku, przykłady poleceń, przykładowe wydruki, dokładną interpretację wyników oraz wskazówki diagnostyczne i dobre praktyki.

1. Podstawy sieci (TCP/IP, OSI, adresacja, podsieci)

Warstwy i ich rola w ćwiczeniach:

- Warstwa łącza danych (Ethernet): przenosi ramki; identyfikacja przez adres MAC; interfejsy sieciowe (np. enp0s3).
- Warstwa sieci (IP): adresacja IPv4/IPv6, TTL (Time To Live), fragmentacja, MTU; routowanie między podsieciami.
- Warstwa transportowa (TCP/UDP): TCP – połączeniowy, niezawodny; UDP – bezpołączeniowy, szybki, bez gwarancji dostarczenia.
- Warstwa aplikacji: protokoły i usługi (DNS, HTTP); narzędzia: host, dig, whois, nmap.

Adresacja IPv4 i CIDR: 10.0.0.30/24 oznacza maskę 255.255.255.0; zakres hostów 10.0.0.1–10.0.0.254; broadcast 10.0.0.255; brama domyślna (default gateway) kieruje ruch poza podsieć.

2. ICMP i ping – teoria, opcje i interpretacja

ICMP (Internet Control Message Protocol) przenosi komunikaty kontrolne: echo request/echo reply, time exceeded, destination unreachable. Polecenie ping wysyła echo request i mierzy czas round-trip (RTT).

- Najważniejsze opcje pingu: -c <liczba> (liczba pakietów), -i <sek> (interwał), -s <bajty> (rozmiar danych), -M do (flaga „don’t fragment”), -t <TTL> (maksymalna liczba przeskoków), -W <ms> (timeout), -I <interfejs/IP> (źródło), -4/-6 (wymuszenie IPv4/IPv6), -f (flood).
- RTT min/avg/max/mdev: min – najkrótszy czas, avg – średni, max – najdłuższy; mdev – miara zmienności (stabilności) połączenia.
- TTL: startowa wartość ustawiana przez host źródłowy (np. 64, 128, 255); maleje o 1 na każdym routerze; zbyt niski TTL powoduje komunikat „Time Exceeded”.
- MTU i fragmentacja: typowe MTU Ethernet = 1500 B; dane pingu 1472 B + nagłówki IP/ICMP 28 B = 1500 B. Z -M do (DF) router nie może fragmentować i zgłosi potrzebę mniejszego pakietu.
- PMTUD (Path MTU Discovery): mechanizm wykrywania MTU na trasie – host zmniejsza rozmiar na podstawie komunikatów ICMP „Fragmentation needed”.

2.1 Przykłady poleceń ping i jak czytać wyniki

1. Podstawowy test do adresu publicznego

Polecenie: ping -c 5 8.8.8.8

- Oczekuj odpowiedzi z czasami ~10–50 ms (zależnie od łącza).
- Statystyki na końcu: ile wysłano/odebrano, procent strat, rtt min/avg/max/mdev.

2. Test nazwy hosta zależny od DNS

Polecenie: ping -c 5 cke.gov.pl

- Możliwy brak odpowiedzi – serwery instytucji często blokują ICMP (usługa WWW może działać).

3. Loopback (sprawdzenie stosu TCP/IP)

Polecenie: ping -c 5 localhost

- Adres 127.0.0.1; brak strat i czasy ~0.0–0.5 ms; potwierdza lokalną poprawność stosu sieciowego.

4. Broadcast w sieci /24

Polecenie: ping -c 5 10.0.0.255

- Zapytanie trafia do wszystkich hostów; wiele systemów ignoruje broadcast – brak odpowiedzi nie oznacza awarii.

5. Diagnostyka zasięgu (TTL)

Polecenie: ping -c 5 -t 1 8.8.8.8

- Pakiety zostaną zatrzymane na pierwszym routerze; zobaczysz „Time Exceeded”.

6. Test MTU bez fragmentacji

Polecenie: ping -c 5 -s 1472 -M do 8.8.8.8

- Przejdzie, jeśli ścieżka obsługuje MTU 1500; komunikat o konieczności fragmentacji oznacza MTU < 1500 (np. PPPoE 1492).

Przykładowy wpis pingu i interpretacja:

64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=25.3 ms

- icmp_seq=1 – kolejny numer pakietu (ułatwia wykrywanie braków).

- ttl=116 – pozostałe przeskoki; duża wartość sugeruje, że cel jest daleko, ale „116” to wynik wysokiej wartości początkowej u Google.
- time=25.3 ms – opóźnienie w obie strony (round-trip).

3. Traceroute – analiza trasy pakietów

Traceroute domyślnie w Linux wysyła sondy UDP do wysokich portów; można wymusić ICMP (-I) lub TCP SYN (-T). Mierzy czasy przejścia przez kolejne hop-y i identyfikuje punkty opóźnień lub filtracji.

- Opcje kluczowe: -n (bez DNS – szybciej i czytelniej), -I (ICMP), -T (TCP), -m <TTLmax>, -q <próby/ hop>, -w <timeout>.
- „*” – brak odpowiedzi od routera (filtrowanie ICMP/UDP/TCP lub zbyt krótki timeout).
- Duża zmienność czasów między próbami na tym samym hop-ie wskazuje na przeciążenie lub niestabilność.

3.1 Przykłady i interpretacja traceroute

7. Standardowy pomiar

Polecenie: traceroute www.google.pl

- Kolejne routery na trasie; trzy czasy na każdy hop; analiza największych opóźnień.

8. Bez DNS

Polecenie: traceroute -n 8.8.8.8

- Wyświetla surowe IP – szybciej, brak opóźnień DNS, łatwiejsze porównania.

9. ICMP echo do hosta z filtrowaniem UDP

Polecenie: traceroute -I cke.gov.pl

- Użyteczne, gdy UDP jest blokowane; brak odpowiedzi nadal możliwy z powodu polityk bezpieczeństwa.

10. TCP SYN na port 443

Polecenie: traceroute -T -p 443 www.ubuntu.com

- Diagnoza ścieżki dla ruchu przypominającego HTTPS – przydatne za zaporami.

4. MTR – ciągły monitoring trasy i jakości

MTR łączy ping i traceroute: interaktywnie pokazuje straty (Loss%), liczbę prób (Snt) oraz statystyki czasów (Last/Avg/Best/Wrst/StDev) dla każdego hop-a.

- Opcje: -r (raport nieinteraktywny), -c <liczba> (próby na hop), -i <sek> (interwał), -n (bez DNS), --udp/--tcp (rodzaj sondy), -w (szerszy raport).
- Interpretacja: wysokie Loss% na konkretnym hop-ie zwykle oznacza filtrację sond ICMP; jeżeli Loss% rośnie dopiero po danym hop-ie i utrzymuje się dalej, wskazuje na realny problem na ścieżce.

5. DNS – host i dig

DNS tłumaczy nazwy na IP. W praktyce używamy host/dig do inspekcji rekordów i diagnostyki.

- Rekordy: A (IPv4), AAAA (IPv6), CNAME (alias), NS (autorytatywne serwery), PTR (odwrotne mapowanie IP>nazwa).
- Resolver lokalny: /etc/resolv.conf; nazwy lokalne: /etc/hosts (ma pierwszeństwo nad DNS).
- Wiele IP (Google, CDN-y) = load balancing/anycast; oczekuj rotacji adresów w czasie.

6. WHOIS – dane rejestrowe

WHOIS dla domen i adresów IP podaje rejestratora, daty (created/updated), właściciela zakresu (inetnum/netrange), kraj, adres, kontakt abuse-mailbox. Dla domen publicznych część danych może być ukryta.

7. ARP i ip neighbour

ARP mapuje IP na MAC w LAN. Polecenie ip neighbour wyświetla tablicę sąsiadów (ARP/ND).

- Typowe stany wpisów: REACHABLE (aktywny), STALE (wymaga odświeżenia), DELAY/PROBE (sondowanie).
- Brak poprawnego wpisu ARP = brak komunikacji z hostem w tej samej podsieci.

8. Routing – ip route show

Tabela routingu decyduje którędy idzie ruch. Znajdziesz w niej trasę dla podsieci lokalnej, trasę domyślną (default via <gateway>) i metrykę, która określa preferencję trasy.

9. netstat i ss – gniazda i porty

Gniazda (sockets) to punkty komunikacji procesów. ss jest nowocześniejszy i szybszy niż netstat, pokazuje PID-y i stany TCP.

- Stany TCP: LISTEN (nasłuch), ESTABLISHED (połączenie aktywne), SYN-SENT/RECV (nawiązywanie), TIME-WAIT/CLOSE-WAIT/FIN-WAIT (zamykanie).
- Tryb -n (bez DNS) – przyspiesza i pokazuje surowe IP/porty.

10. nmap – skanowanie

nmap aktywnie sprawdza hosty i porty, wykrywa usługi, próbuje rozpoznać system operacyjny.

- Tryby: -sT (TCP connect), -sS (SYN – szybszy), -sU (UDP), -sn (ping sweep – wykrywanie hostów), -O (rozpoznawanie OS), -sV (wersje usług).
- Stany portów: open (otwarty), closed (zamknięty), filtered (filtr/ firewall), open|filtered (brak jednoznacznej odpowiedzi – typowe dla UDP).
- Aspekty prawne/etyczne: skanuj tylko własne zasoby lub za zgodą; intensywne skanowanie może być traktowane jako nadużycie.

11. tcpdump – podsłuch i filtry BPF

tcpdump przechwytuje pakiety i pokazuje nagłówki; -w zapisuje do PCAP, -r odczytuje z pliku. Filtry BPF pozwalają skupić się na konkretnym ruchu.

- Przykładowe filtry: icmp (tylko ping), port 53 (DNS), host 10.0.0.30 (konkretny host), net 10.0.0.0/24 (cała podsieć).
- Interpretacja linii: timestamp, źródło>cel, protokół, parametry (id/seq/ttl/length).

12. Praca na wielu TTY i uprawnienia (sudo)

Używaj dwóch TTY: jeden do generowania ruchu (ping), drugi do tcpdump. Przełączanie: Ctrl+Alt+F1…F6. Zatrzymywanie: Ctrl+C. Sudo tylko gdy potrzebne – minimalizuj pracę jako root.

13. Checklist – co zapisać po każdym teście

- Ping: wysłane/odebrane, straty (%), min/avg/max/mdev; IP źródło>cel.
- host/dig: typy rekordów, liczba adresów dla domeny; TTL rekordów.
- traceroute/mtr: liczba hopów, gdzie są „*”, Loss% i największe opóźnienia.
- whois: registrar, created/updated, zakres inetnum/netrange, org-name, abuse-mailbox.
- netstat/ss: porty nasłuchujące, stany TCP, PID-y.
- nmap: lista otwartych portów/usług, rozpoznany OS (jeśli), parametry skanu.
- ip neighbour/ip route: wpisy ARP, domyślna brama i trasy.
- tcpdump: protokół, IP źródło>cel, id/seq/ttl/length.

14. Dobre praktyki i bezpieczeństwo

- Używaj -n (bez DNS) dla szybkich wyników i czytelnych IP/portów.
- Flood ping (-f) wyłącznie w środowisku testowym; może przeciążyć hosty i sieć.
- Brak odpowiedzi na ping nie oznacza awarii – usługa może działać mimo filtrowania ICMP.
- Porównuj wyniki z różnych narzędzi (ping, traceroute, mtr, tcpdump, ss/nmap), aby uzyskać pełny obraz.

15. FAQ – typowe problemy i szybkie rozwiązania

Problem: Brak odpowiedzi na ping do hosta publicznego
Wyjaśnienie / rozwiązanie: Najczęściej filtrowanie ICMP; sprawdź dostępność przez HTTP (curl) lub traceroute -T.

Problem: Gwiazdki w traceroute
Wyjaśnienie / rozwiązanie: Router nie odpowiada na sondy albo odpowiedź dotarła po czasie; zwiększ -w, użyj -I/-T.

Problem: Duże opóźnienia/straty
Wyjaśnienie / rozwiązanie: Zator na łączu lub hop-ie; sprawdź MTU (ping -s 1472 -M do), priorytety ruchu, okablowanie.

Problem: Brak/STALE wpisów ARP
Wyjaśnienie / rozwiązanie: Host nieodpowiedni VLAN lub błąd adresacji; odśwież tablicę ARP przez ruch w podsieci.

Problem: Nie widać ruchu w tcpdump
Wyjaśnienie / rozwiązanie: Podsłuchujesz zły interfejs lub ruch idzie inną trasą; sprawdź ip route i ss -tulnp.

Problem: nmap bardzo wolny na UDP
Wyjaśnienie / rozwiązanie: To normalne – użyj -T4, zwiększ timeout, rozważ skupienie na TCP.