

T: Testy sieci komputerowych.

Podział pomiarów i testów sieci komputerowych:

- testy parametrów fizycznych (okablowanie strukturalne),
- testy i pomiary pasywne (obserwacja funkcjonowania sieci),
- testy i pomiary aktywne (wykorzystanie dodatkowych danych testowych).

Do najczęściej stosowanych procedur lokalizujących uszkodzenia i diagnozujących sieci komputerowe należą:

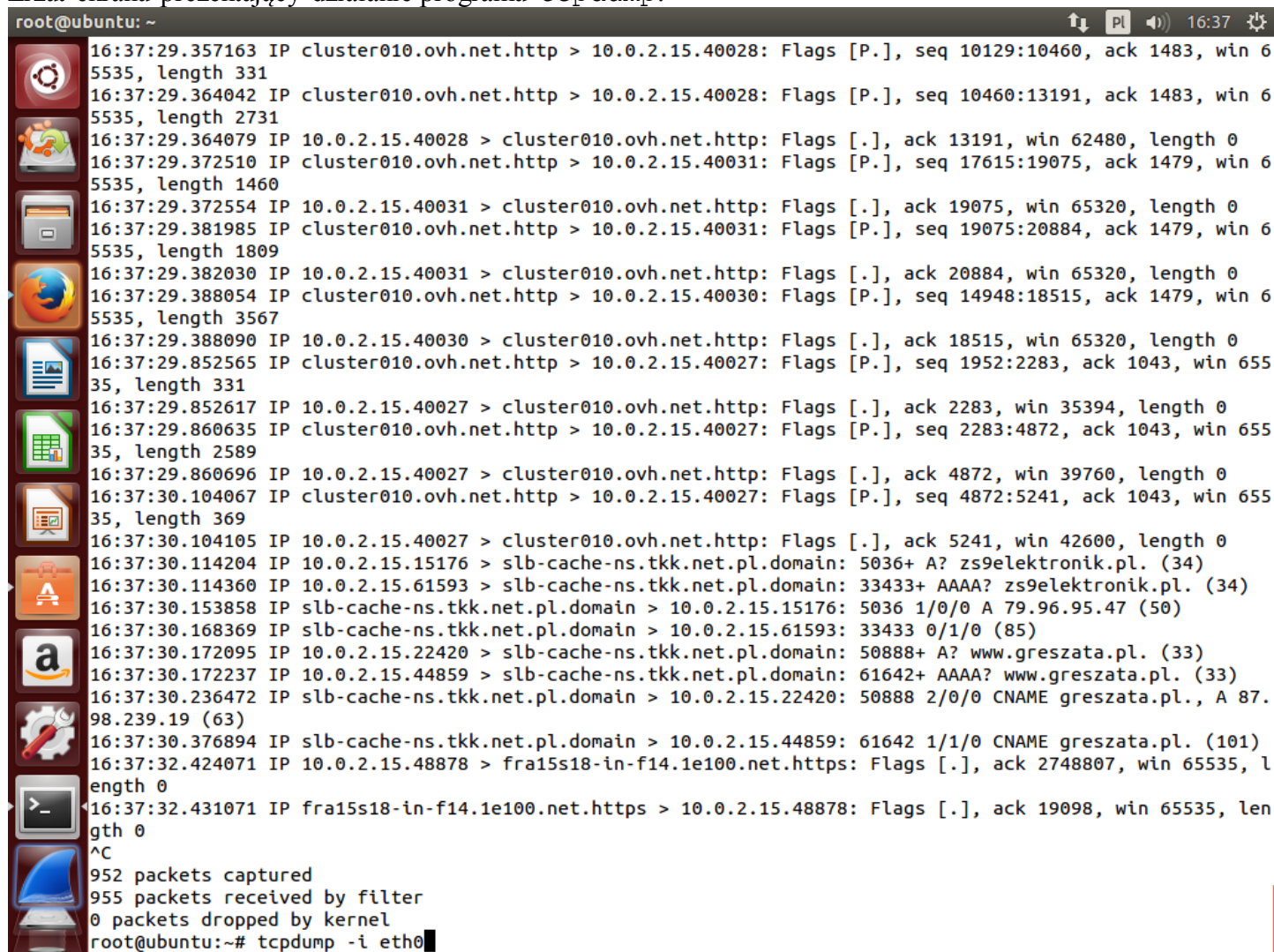
- testowanie okablowania,
- analiza pakietów i protokołów,
- testowanie połączeń między węzłami sieci,
- statystyczna analiza trafiku sieciowego,
- analiza konfiguracji sieci,
- analiza stanu sieci,
- testowanie funkcji i realizacja procedur samotestowania.

W testach pasywnych do analizy funkcjonowania sieci komputerowych można wykorzystać oprogramowanie typu sniffer. Sniffer to program komputerowy służący do przechwytywania i analizowania pakietów sieciowych.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat programów typu sniffery.

Zrzut ekranu prezentujący działanie programu tcpdump:



```
root@ubuntu: ~
16:37:29.357163 IP cluster010.ovh.net.http > 10.0.2.15.40028: Flags [P.], seq 10129:10460, ack 1483, win 6
5535, length 331
16:37:29.364042 IP cluster010.ovh.net.http > 10.0.2.15.40028: Flags [P.], seq 10460:13191, ack 1483, win 6
5535, length 2731
16:37:29.364079 IP 10.0.2.15.40028 > cluster010.ovh.net.http: Flags [.], ack 13191, win 62480, length 0
16:37:29.372510 IP cluster010.ovh.net.http > 10.0.2.15.40031: Flags [P.], seq 17615:19075, ack 1479, win 6
5535, length 1460
16:37:29.372554 IP 10.0.2.15.40031 > cluster010.ovh.net.http: Flags [.], ack 19075, win 65320, length 0
16:37:29.381985 IP cluster010.ovh.net.http > 10.0.2.15.40031: Flags [P.], seq 19075:20884, ack 1479, win 6
5535, length 1809
16:37:29.382030 IP 10.0.2.15.40031 > cluster010.ovh.net.http: Flags [.], ack 20884, win 65320, length 0
16:37:29.388054 IP cluster010.ovh.net.http > 10.0.2.15.40030: Flags [P.], seq 14948:18515, ack 1479, win 6
5535, length 3567
16:37:29.388090 IP 10.0.2.15.40030 > cluster010.ovh.net.http: Flags [.], ack 18515, win 65320, length 0
16:37:29.852565 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 1952:2283, ack 1043, win 655
35, length 331
16:37:29.852617 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 2283, win 35394, length 0
16:37:29.860635 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 2283:4872, ack 1043, win 655
35, length 2589
16:37:29.860696 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 4872, win 39760, length 0
16:37:30.104067 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 4872:5241, ack 1043, win 655
35, length 369
16:37:30.104105 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 5241, win 42600, length 0
16:37:30.114204 IP 10.0.2.15.15176 > slb-cache-ns.tkk.net.pl.domain: 5036+ A? zs9elektronik.pl. (34)
16:37:30.114360 IP 10.0.2.15.61593 > slb-cache-ns.tkk.net.pl.domain: 33433+ AAAA? zs9elektronik.pl. (34)
16:37:30.153858 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.15176: 5036 1/0/0 A 79.96.95.47 (50)
16:37:30.168369 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.61593: 33433 0/1/0 (85)
16:37:30.172095 IP 10.0.2.15.22420 > slb-cache-ns.tkk.net.pl.domain: 50888+ A? www.greszata.pl. (33)
16:37:30.172237 IP 10.0.2.15.44859 > slb-cache-ns.tkk.net.pl.domain: 61642+ AAAA? www.greszata.pl. (33)
16:37:30.236472 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.22420: 50888 2/0/0 CNAME greszata.pl., A 87.
98.239.19 (63)
16:37:30.376894 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.44859: 61642 1/1/0 CNAME greszata.pl. (101)
16:37:32.424071 IP 10.0.2.15.48878 > fra15s18-in-f14.1e100.net.https: Flags [.], ack 2748807, win 65535, l
ength 0
16:37:32.431071 IP fra15s18-in-f14.1e100.net.https > 10.0.2.15.48878: Flags [.], ack 19098, win 65535, len
gth 0
^C
952 packets captured
955 packets received by filter
0 packets dropped by kernel
root@ubuntu:~# tcpdump -i eth0
```

Wireshark jest jednym z popularniejszych programów wykorzystywanych do analizy ruchu sieciowego. W celu uniknięcia problemów z uprawnieniami do zarządzania kartami sieciowymi, program należy uruchomić z poziomu administratora systemu:

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Zapisz

No.	Time	Source	Destination	Protocol	Length	Info
30	4.259196000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [SYN, ACK] Seq=0 Ack=1
31	4.263547000	10.0.2.15	91.121.70.102	TCP	54	52542 > http [ACK] Seq=1 Ack=1 Win=2
32	4.268839000	10.0.2.15	91.121.70.102	HTTP	373	GET /sig/135.jpg HTTP/1.1
33	4.271871000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [ACK] Seq=1 Ack=320 Win
34	5.431637000	10.0.2.15	91.121.70.102	TCP	54	52542 > http [FIN, ACK] Seq=320 Ack=
35	5.431904000	10.0.2.15	87.98.239.19	HTTP	489	GET /psk/2 konfiguracja i obsluga lo
36	5.434168000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [ACK] Seq=1 Ack=321 Win
37	5.434213000	87.98.239.19	10.0.2.15	TCP	60	http > 40034 [ACK] Seq=2083 Ack=1215
38	5.555374000	87.98.239.19	10.0.2.15	TCP	317	[TCP segment of a reassembled PDU]
39	5.555417000	10.0.2.15	87.98.239.19	TCP	54	40034 > http [ACK] Seq=1215 Ack=2346

▶Frame 35: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0

▶Ethernet II, Src: CadmusCo_if:b4:e6 (08:00:27:1f:b4:e6), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

▶Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 87.98.239.19 (87.98.239.19)

▶Transmission Control Protocol, Src Port: 40034 (40034), Dst Port: http (80), Seq: 780, Ack: 2083, Len: 435

▼Hypertext Transfer Protocol

▶GET /psk/2 konfiguracja i obsluga lokalnych sieci komputerowych/ HTTP/1.1\r\n

Host: greszata.pl\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: pl,en-US;q=0.7,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://greszata.pl/psk/\r\n

Cookie: 60gpBAK=R1224225179; 60gp=R477089669\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://greszata.pl/psk/2 konfiguracja i obsluga lokalnych sieci komputerowych/]

0030 87 70 54 52 00 00 47 45 54 20 2f 70 73 6b 2f 32 .pTR..GE T /psk/2

0040 5f 6b 6f 6e 66 69 67 75 72 61 63 6a 61 5f 69 5f konfigu racja i

0050 6f 62 73 6c 75 67 61 5f 6c 6f 6b 61 6c 6e 79 63 obsluga lokalnyc

0060 68 5f 73 69 65 63 69 5f 6b 6f 6d 70 75 74 65 72 h sieci komputer

Text item (text), 75 bytes Packets: 48 · Displayed: 48 (100,0%) Profile: Default

Zadanie2:

Odszukaj w serwisie internetowym dobreprogramy.pl informacje na temat programu Wireshark.

W celu wykorzystania programu Wireshark do analizy sieci wykonaj następujące czynności:

- uruchom program,
- wybierz polecenie Interfaces z menu Capture i wskaż kartę sieciową, z której będą przechwytywane dane,
- uruchom nasłuchiwanie ruchu sieciowego klikając przycisk Start,
- można wymusić ruch sieciowy poprzez połączenie z komputerem skanującym z innej stacji sieciowej dowolnym klientem sieciowym,
- po zarejestrowaniu danych sieciowych wyłączyć skanowanie klikając przycisk Stop z menu Capture.

Po zarejestrowaniu danych należy dokonać analizy przechwyconych pakietów. Do tego celu pomocne może być polecenie Follow TCP Stream dostępne w menu Analize. Wcześniej należy zaznaczyć pakiet, dla którego chcemy przeprowadzić analizę.

Testy aktywne pozwalają określić jakość usług sieciowych (Quality of Service, QoS).

Podczas testów aktywnych dokonuje się pomiarów następujących parametrów:

- dostępność usługi,
- opóźnienie w jednym kierunku (One Way Delay Minimum, OWD),
- zmienność opóźnienia przekazu pakietów (IP Packet Delay Variation, IPDV),
- opóźnienie pakietów w pętli (Round Trip Delay, RTD),
- straty pakietów (One Way Loss, OWL),

- poziom strat pakietów (IP Packet Loss Ratio, IPLR).

Do pomiarów aktywnych wykorzystuje się następujące programy: ping, traceroute.

Zadanie3:

Odszukaj w systemowej pomocy informacje na temat poleceń ping i traceroute.

```
Terminal
root@ubuntu: ~
ubuntu@ubuntu:~$ sudo su -
root@ubuntu:~# ping -4 wp.pl
ping: invalid option -- '4'
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
root@ubuntu:~# mtr wp.pl

My traceroute [v0.85]
ubuntu (0.0.0.0) Wed Nov 9 16:31:45 2016
Keys: Help Display mode Restart statistics Order of fields quit
          Packets
Host      Loss%  Snt   Last   Avg    Best  Wrst  StDev
1. 10.0.2.2
2. ???
3. ???
4. ???
5. ???
6. www.wp.pl      3.9%   78    26.0  27.3  24.5  37.6  2.3

root@ubuntu:~# clear
root@ubuntu:~# tracepath wp.pl
1?: [LOCALHOST] pmtu 1500
1: 10.0.2.2      0.246ms
1: 10.0.2.2      0.530ms
2: no reply
3: no reply
4: no reply
5: no reply
^C
root@ubuntu:~#
```