

T: Monitorowanie pracy urządzeń sieciowych.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat monitorowania.

Monitorowanie (ang. monitoring) polega na wykonywaniu regularnych pomiarów i obserwowaniu zjawisk zachodzących w sieci komputerowej.

Monitorowanie sieci i urządzeń sieciowych polega na sprawdzeniu:

- dostępności węzłów sieciowych,
- dostępności usług sieciowych,
- obciążenia łączy internetowych,
- obciążenia serwerów sieciowych,
- zdarzeń występujących na urządzeniach sieciowych i serwerach.

Główne cele monitorowania sieci komputerowych:

- nadzór nad konfiguracją urządzeń sieciowych,
- wykrywanie nieuprawnionego dostępu do zasobów sieciowych,
- wczesne wykrywanie problemów,
- zbieranie informacji do planowania rozwoju infrastruktury sieciowej.

Zadanie2:

Odszukaj w serwisie internetowym <http://www.dobreprogramy.pl> informacje na temat oprogramowania służącego do monitoringu sieci komputerowej.

Zadanie3:

Zapoznaj się z informacjami uzyskanymi za pomocą oprogramowania ISA Server podczas monitoringu ruchu sieciowego w szkolnej pracowni komputerowej.

Zadanie4:

Zapoznaj się z programami wymienionymi poniżej i przeanalizuj informacje uzyskane za ich pomocą:

```
ipconfig / ifconfig
```

```
arp -a
```

```
getmac
```

```
netsh (np. netsh interface ipv4 show address)
```

```
ping -l 1480 -f greszata.pl
```

```
pathping
```

```
tracert / traceroute
```

```
route print
```

```
netstat -anop tcp
```

```
nslookup
```

```
nmap -sn 192.168.27.21-35
```

```
wireshark
```

```
apt-get install gnome-nettool #źródło universe
```

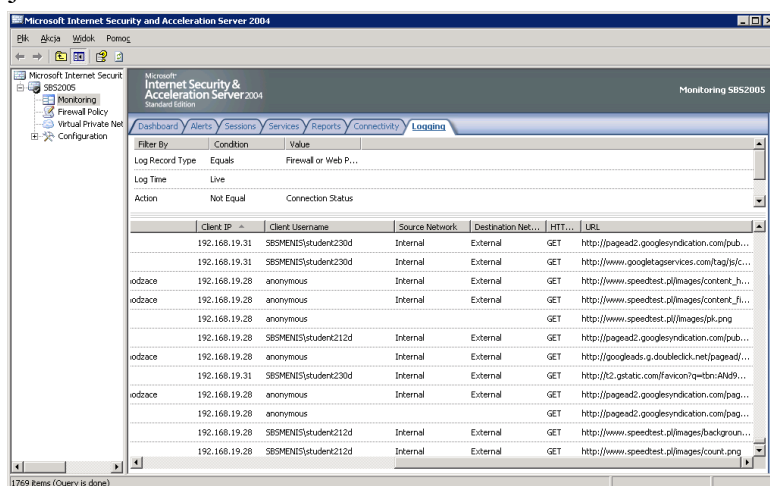
```
tcpdump
```

```
net view
```

```
nbtstat -a s27st01
```

```
Monitor systemu
```

```
Pomoc i obsługa techniczna => Narzędzia => Diagnostyka sieci
```



Zrzuty ekranowe obrazujące wykorzystanie narzędzi do monitorowania sieci w systemie Windows:

```

C:\WINDOWS\system32\cmd.exe
C:\>ping wp.pl

Badanie wp.pl [212.77.100.101] z użyciem 32 bajtów danych:

Odpowiedź z 212.77.100.101: bajtów=32 czas=24ms TTL=250
Odpowiedź z 212.77.100.101: bajtów=32 czas=22ms TTL=250
Odpowiedź z 212.77.100.101: bajtów=32 czas=23ms TTL=250
Odpowiedź z 212.77.100.101: bajtów=32 czas=22ms TTL=250

Statystyka badania ping dla 212.77.100.101:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 22 ms, Maksimum = 24 ms, Czas średni = 22 ms

C:\>

C:\WINDOWS\system32\cmd.exe
C:\>tracert wp.pl

Trasa śledzenia do wp.pl [212.77.100.101]
przewyższa maksymalną liczbę przeskoków 30

    1    4 ms    2 ms    1 ms  192.168.10.17
    2   12 ms   10 ms    8 ms  10.1.0.1
    3    9 ms    9 ms   10 ms  83.145.140.25
    4   21 ms   21 ms   21 ms  wp.pl.ix.pl [195.182.218.204]
    5   21 ms   21 ms   21 ms  rtr2.rtr-int-1.adm.wp-sa.pl [212.77.96.65]
    6   21 ms   21 ms   22 ms  www.wp.pl [212.77.100.101]

Śledzenie zakończone.

C:\>_

```

```

C:\WINDOWS>route print

Lista interfejsów
0x1 ..... MS TCP Loopback interface
0x2 ...00 01 6c b5 f6 98 ..... Realtek RTL8139/810x Family Fast Ethernet NIC -
VirtualBox Bridged Networking Driver Miniport

=====
Aktywne trasy:
Miejsce docelowe w sieci      Maska sieci      Brama            Interfejs      Metryka
-----
0.0.0.0                      0.0.0.0          192.168.19.1     192.168.19.37  20
127.0.0.0                    255.0.0.0        127.0.0.1        127.0.0.1      1
192.168.19.0                  255.255.255.0    192.168.19.37   192.168.19.37  20
192.168.19.37                 255.255.255.255  127.0.0.1        127.0.0.1      20
192.168.19.255                255.255.255.255  192.168.19.37   192.168.19.37  20
224.0.0.0                     240.0.0.0        192.168.19.37   192.168.19.37  20
255.255.255.255              255.255.255.255  192.168.19.37   192.168.19.37  1

Domyślna brama: 192.168.19.1.

Trasy trwałe:
Brak

C:\WINDOWS>route add 192.168.11.0 mask 255.255.255.0 192.168.19.1

C:\WINDOWS>nslookup
Serwer domyślny: sbs2005.sbsmenis.edu.pl
Address: 192.168.19.1

> wp.pl
Serwer: sbs2005.sbsmenis.edu.pl
Address: 192.168.19.1

Nieautorytatywna odpowiedź:
Nazwa: pl.edu.pl
Address: 62.129.200.250
Aliases: wp.pl.edu.pl

> wp.pl.
Serwer: sbs2005.sbsmenis.edu.pl
Address: 192.168.19.1

Nieautorytatywna odpowiedź:
Nazwa: wp.pl
Address: 212.77.100.101

> exit

```

```

C:\WINDOWS>netstat -naop tcp

Aktywne połączenia

Protokół  Adres lokalny      Obcy adres      Stan      PID
-----
TCP      0.0.0.0:23         0.0.0.0:0       NASŁUCHIWANIE  1428
TCP      0.0.0.0:80         0.0.0.0:0       NASŁUCHIWANIE  124
TCP      0.0.0.0:135        0.0.0.0:0       NASŁUCHIWANIE  1180
TCP      0.0.0.0:443        0.0.0.0:0       NASŁUCHIWANIE  124
TCP      0.0.0.0:445        0.0.0.0:0       NASŁUCHIWANIE  4
TCP      0.0.0.0:1064       0.0.0.0:0       NASŁUCHIWANIE  124
TCP      0.0.0.0:1110       0.0.0.0:0       NASŁUCHIWANIE  1728
TCP      0.0.0.0:3389       0.0.0.0:0       NASŁUCHIWANIE  1076
TCP      0.0.0.0:5473       0.0.0.0:0       NASŁUCHIWANIE  972
TCP      0.0.0.0:5475       0.0.0.0:0       NASŁUCHIWANIE  972
TCP      127.0.0.1:1044     127.0.0.1:19492  USTANOWIONO    732
TCP      127.0.0.1:1047     127.0.0.1:6560  USTANOWIONO    1656
TCP      127.0.0.1:1048     127.0.0.1:29186  USTANOWIONO    1656
TCP      127.0.0.1:1049     127.0.0.1:29165  USTANOWIONO    1656
TCP      127.0.0.1:1050     127.0.0.1:9175  USTANOWIONO    1656
TCP      127.0.0.1:1098     0.0.0.0:0       NASŁUCHIWANIE  3504
TCP      127.0.0.1:1110     127.0.0.1:1744  USTANOWIONO    1728
TCP      127.0.0.1:1110     127.0.0.1:1977  USTANOWIONO    1728
TCP      127.0.0.1:1227     127.0.0.1:1110  OCZEKIWANIE_ZAMKN  1804

Stan: lan
Ogólne | Obsługa
-----
Połączenie
Stan: Połączono
Czas trwania: 01:26:40
Szybkość: 100,0 Mb/s

Aktywność
Wysłano | Odebrano
-----
Pakiety: 111 009 | 202 559

Właściwości | Wyłącz | Zamknij

```

```

Menedżer zadań Windows
Dłk Opcje Widok Pomoc
Aplikacje | Procesy | Wydajność | Sieć
lan
100%
50%
0%
Nazwa karty | Wykorzystanie... | Szybko... | Stan
lan | 0,02% | 100 Mb/s | Działa

Procesy: 48 | Użycie procesora: 8% | Pam. zadziałar.: 953M / 2936M

C:\WINDOWS>arp -a

Interfejs: 192.168.19.37 --- 0x2
Adres internetowy      Adres fizyczny      Typ
-----
192.168.19.1           00-13-d4-fa-4e-df   dynamiczne
192.168.19.21          00-01-6c-e5-40-4b   dynamiczne
192.168.19.22          00-01-6c-e5-41-9f   dynamiczne
192.168.19.23          00-01-6c-e5-47-d9   dynamiczne
192.168.19.24          00-01-6c-e5-42-2f   dynamiczne
192.168.19.25          00-01-6c-e5-44-83   dynamiczne
192.168.19.26          00-01-6c-e5-43-5d   dynamiczne
192.168.19.27          00-01-6c-e5-47-1f   dynamiczne
192.168.19.28          00-01-6c-e5-43-f4   dynamiczne
192.168.19.29          00-01-6c-e5-43-d6   dynamiczne
192.168.19.30          00-01-6c-e5-40-85   dynamiczne
192.168.19.31          00-01-6c-e5-3f-7b   dynamiczne
192.168.19.32          00-01-6c-e5-40-9b   dynamiczne
192.168.19.33          00-01-6c-e5-40-bc   dynamiczne
192.168.19.34          00-01-6c-e5-49-25   dynamiczne

C:\WINDOWS>for /L %i in (21,1,34) do ping -c 1 192.168.19.%i

```

Zadanie5:

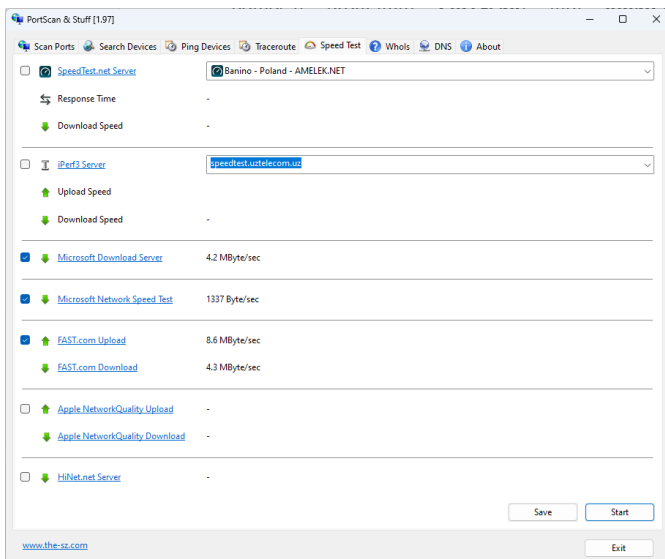
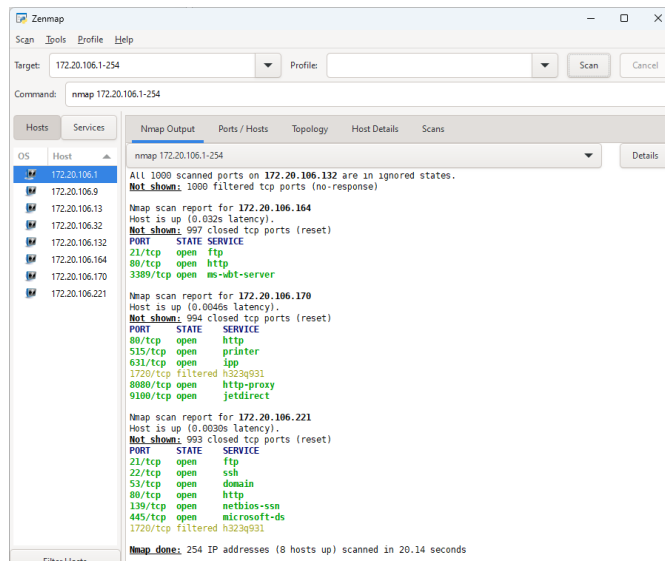
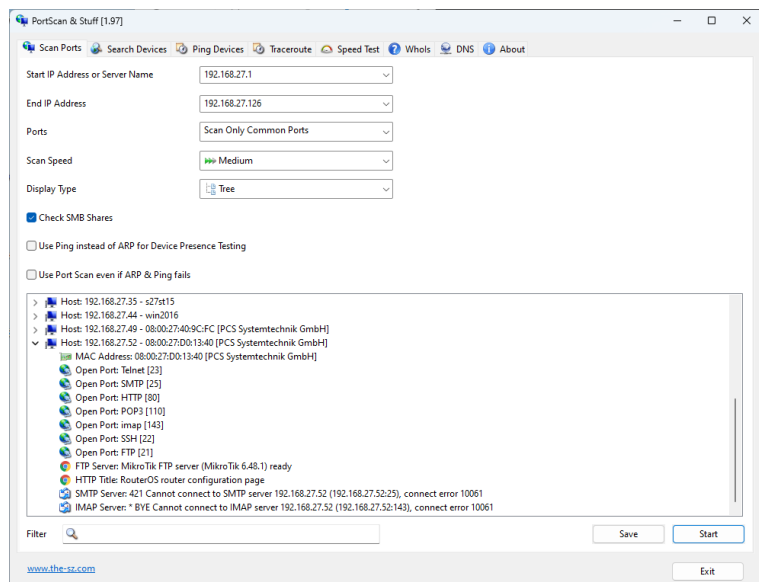
Przeprowadź testowanie prędkości wysyłania i odbierania danych poprzez połączenia sieciowe za pomocą SpeedTestów OnLine. Sprawdź również informacje o dostawcy łącza internetowego. Pomocne linki:

- <http://www.speedtest.net/pl/>
- <http://speedtest.tkk.net.pl/>,
- <https://speedtest.orange.pl/>

- <https://www.ripe.net/>,
- <https://check-host.net/>,
- i inne.

Zadanie6:

0Przeprowadź skanowanie sieci szkolnej za pomocą programu **PortScan** lub **nmap**. Przeanalizuj uzyskane wyniki. Jakie informacje o sieci można otrzymać za pomocą tych programów?



Zadanie7:

Odszukaj w zasobach Internetu informacje na temat programu Nagios <http://www.nagios.org/>.

Funkcje realizowane za pomocą oprogramowania Nagios:

- monitorowanie dostępności węzłów sieciowych,
- monitorowanie usług sieciowych działających na serwerach,
- monitorowanie użycia zasobów systemowych na serwerach,
- projektowanie wtyczek do monitorowania własnych usług,
- powiadamianie o problemach występujących w monitorowanej sieci poprzez pocztę elektroniczną lub SMS.

Zadanie8:

Odszukaj w zasobach Internetu informacje na temat programu NetTools Professional <http://axencesoftware.com/pl>.

Kod aktywacyjny: **MJ1JE-CJBB-KD9K-6HM46** (11.2016 r. - **QK3JH-4MCC-JDCJ-6K034**)
(23.05.2017 r. - **QH4KG-4KDA-K9GL-AHR55**) (12.09.2019 r. - **0KV0D-2J9D-L6BM-1EL11**)
(2022 r. - **QK3JH-4MCC-JDCJ-6K034**)

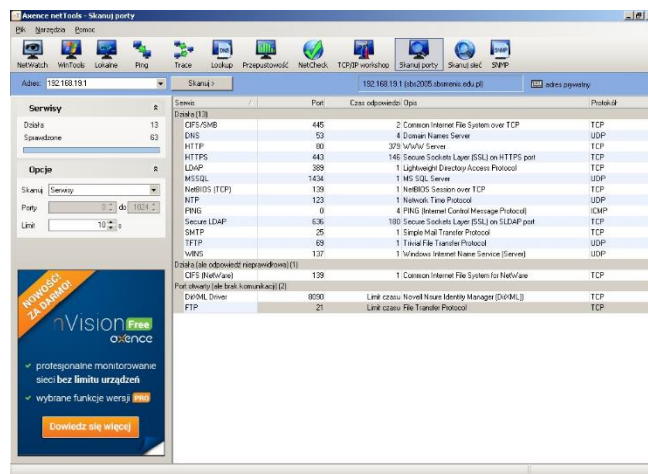
Funkcje realizowane za pomocą oprogramowania NetTools:

- monitorowanie dostępności urządzeń sieciowych wraz z powiadomieniami,
- weryfikowanie usług działających na określonych serwerach,
- skanowanie sieci w celu wykrycia uruchomionych urządzeń,
- przeglądanie bazy SNMP (Simple Network Management Protocol).

Składniki oprogramowania NetTools:

- NetWatch (monit dostępności urządzeń sieciowych, ustawianie alarmów),

- WinTools (monit zdalny dostępnych usług, informacje o dyskach, dzienniki systemowe),
- Lokate (tabela adresów IP, tabela ARP, tabela routingu, otwarte porty, dane o kartach sieciowych, statystyki TCP, UDP i ICMP),
- Ping (zmiany w dostępie do urządzenia),
- Trace (routery na trasie do adresu docelowego),
- Lookup (badanie rekordów DNS),
- Przepustowość (prędkość łącza),
- NetCheck (jakość łącza, dostępność i parametry),
- TCP/IP workshop (bezpośrednie połączenie z portem),
- Skanuj porty (dostępne usługi na urządzeniu),
- Skanuj sieć (skanowanie urządzeń działających w sieci).



Zadanie9:

Przy użyciu oprogramowania Wireshark dokonaj podsłuchu procesu logowania do usługi ftp. Czy można odczytać login i hasło przesyłane protokołem ftp?

Zadanie10:

Wykorzystując dostępne w pracowni narzędzia programowe przeprowadź diagnozę szkolnej sieci komputerowej. Na podstawie otrzymanych wyników sporządź dokumentację dotyczącą sieci. Pracę zachowaj w pliku pod nazwą **\$nazwisko_\$klasa_\$gr_monitoring_sieci** i prześlij plik pocztą elektroniczną do nauczyciela w postaci załącznika na adres greszata@zs9elektronik.pl. Dokumentacja powinna zawierać następujące elementy:

- wprowadzenie (teoria),
- konfigurację urządzenia sieciowego w stacji roboczej (urządzenia sieciowe),
- konfigurację adresów IP w pracowni komputerowej (ipconfig),
- informacje o dostawcy łącza internetowego dla szkoły (ip.wp.pl, ripe.net),
- przepustowość dostępnego połączenia sieciowego lokalnie w pracowni oraz globalnie w internecie (lanspeedtest, speedtest.pl),
- adresy IP urządzeń sieciowych w pracowni komputerowej oraz w całej szkole (portscan, tracert, nmap),
- diagnozę najważniejszych usług sieciowych działających w pracowni (minimum cztery, np. 21, 22, 23, 53, 80, 139, 3389),
- diagnozę najważniejszych usług sieciowych działających w szkole (minimum trzy, np. 21, 22, 23, 53, 80, 139, 3389),
- podsumowanie na temat funkcjonowania szkolnej sieci komputerowej (wnioski).

Zadanie11:

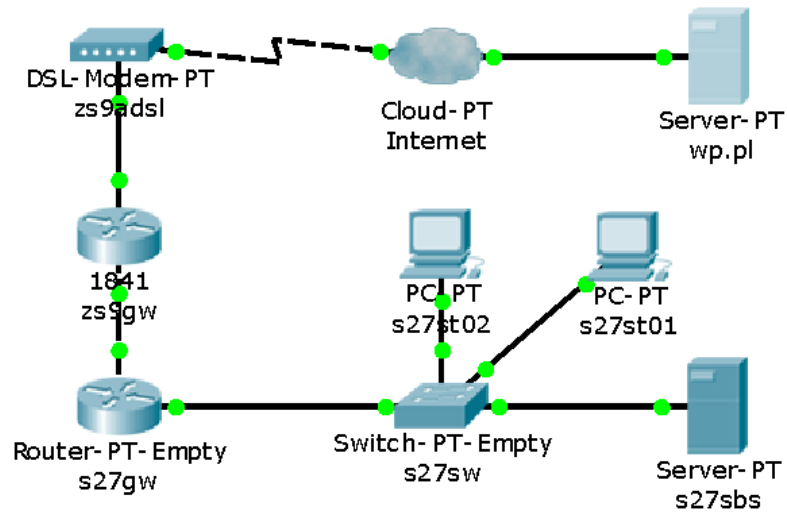
Przeprowadź skanowanie pasma radiowego w szkolnej pracowni i określ używane w sieciach bezprzewodowych urządzenia.

Zadanie12:

Wykorzystując dostępne w pracowni komputerowej wyposażenie oraz oprogramowanie przeprowadź pełną diagnozę szkolnej sieci komputerowej. Sporządź ze swoich działań sprawozdanie, w którym umieścisz wyniki testów i pomiarów sieci. Pracę zachowaj w pliku pod nazwą **\$nazwisko_\$klasa_\$gr_monitoring2** oraz prześlij pocztą elektroniczną do nauczyciela w postaci załącznika na adres greszata@zs9elektronik.pl. Sprawozdanie powinno zawierać następujące pomiary:

- warstwy fizycznej,
- konfiguracji urządzenia sieciowego w systemie,
- warstwy łącza danych,
- warstwy sieciowej,
- warstwy transportowej,
- warstwy sesji,

- warstwy prezentacji,
- warstwy aplikacji.



Zadanie13:

Uruchom w maszynie wirtualnej VirtualBox system Kali Linux i przeprowadź skanowanie dostępnych w szkole sieci bezprzewodowych.