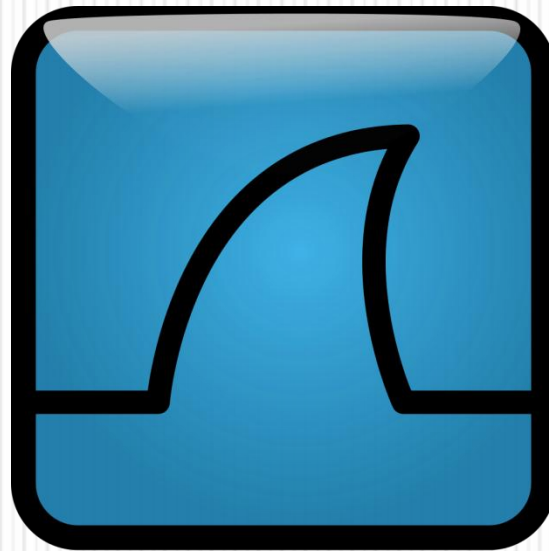


Programy narzędziowe TCP/IP



IPCONFIG

Pozwala sprawdzić adresy przypisane poszczególnych interfejsów. Narzędzie to pomaga przy wykrywaniu błędów w konfiguracji protokołu IP.

Najczęściej polecenie *ipconfig* jest wykorzystywane w następujący sposób:

- *ipconfig* — pokazuje skróconą informację o połączeniu.
- *ipconfig /all* — pokazuje szczegółowe dane o konfiguracji wszystkich interfejsów.
- *ipconfig /renew* — odnawia wszystkie karty.
- *ipconfig /release* — zwalnia wszystkie połączenia.
- *ipconfig / ?* — wyświetla komunikat pomocy.

Odpowiednikiem polecenia *ipconfig* w systemie Linux jest *ifconfig*

PING

Pozwala ono na sprawdzenie, czy istnieje połączenie między dwoma urządzeniami i umożliwia sprawdzanie jego jakości poprzez mierzenie liczby zgubionych pakietów oraz czasu ich dotarcia do celu i z powrotem.

ping www.onet.pl

Polecenie *ping* jest dostępne zarówno w systemie Windows, jak i Linux.

ping -t www.onet.pl

TRACERT

Służy do badania trasy pakietów IP w systemie Windows. Sprawdza ona czasy dostępu do kolejnych routerów znajdujących się na drodze do adresu docelowego.

tracert onet.pl

Odpowiednikiem dla systemów Linux jest komenda

traceroute

NETSTAT

Umożliwia wyświetlanie aktywnych połączeń sieciowych TCP, a także portów, na których komputer nasłuchuje, tabeli routingu, statystyk itp.

Polecenie *netstat* użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP. Inne najważniejsze parametry polecenia to:

- *-a* — służy do wyświetlania wszystkich aktywnych połączeń oraz portów nasłuchu protokołów TCP i UDP,
- *-b* — służy do wyświetlania aktywnych połączeń protokołu TCP i nazw programów które są przypisane do obsługi danego portu.
- *-e* — wyświetla statystykę sieci Ethernet.
- *-n* — wyświetla aktywne połączenia TCP (adresy i numery portów są wyraża numerycznie).
- *-o* — wyświetla aktywne połączenia TCP i identyfikatory procesów (PID) poszczególnych połączeń.
- *-p* protokół — ukazuje połączenia wybranego protokołu (udp, tcpv6, tcp lub udpv6).
- *-s* — służy do wyświetlania oddzielnych statystyk dla poszczególnych protokołów.
- *-r* — służy do wyświetlania zawartości tabeli trasowania protokołu IP.

WIRESHARK

Capturing from eth0 - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1603	81.287288	IntelCor 5b:fb:12	Broadcast	ARP	Who has 10.0.0.21? Tell 10.0.
1604	81.207356	CadmusCo ad:25:1e	IntelCor 5b:fb:12	ARP	10.0.0.21 is at 00:00:27:ad:25
1605	81.288040	10.0.0.25	10.0.0.21	ICMP	Echo (ping) request
1606	81.288097	10.0.0.21	10.0.0.25	ICMP	Echo (ping) reply
1607	81.434106	10.0.0.21	173.194.65.138	HTTP	GET /safebrowsing/rd/ChNnb29nL
1608	81.528648	173.194.65.138	10.0.0.21	TCP	[TCP segment of a reassembled
1609	81.528725	10.0.0.21	173.194.65.138	TCP	42450 > http [ACK] Seq=5997 Ac
1610	81.534160	173.194.65.138	10.0.0.21	TCP	[TCP segment of a reassembled

Frame 1607 (720 bytes on wire, 720 bytes captured)

- Ethernet II, Src: CadmusCo_ad:25:1e (08:00:27:ad:25:1e), Dst: D-Link 94:69:9b (00:11:95:94:69:9b)
- Internet Protocol, Src: 10.0.0.21 (10.0.0.21), Dst: 173.194.65.138 (173.194.65.138)
- Transmission Control Protocol, Src Port: 42450 (42450), Dst Port: http (80), Seq: 5343, Ack: 9283
- Hypertext Transfer Protocol

0000 00 11 95 94 69 9b 00 00 27 ad 25 1e 00 00 45 00 ...i... '%...E.
0010 02 c2 9f 75 40 00 40 06 9f 5f 0a 00 00 15 ad c2 ...u@.
0020 41 8a a5 d2 00 50 ee 27 a2 63 6b ee a0 23 80 18 A...P.' ck.#..
0030 08 e3 fc 15 00 00 01 01 08 0a 00 05 53 30 42 c550B.

Frame (frame), 720 bytes Packets: 2751 Displayed: 2751 Marked: 0 Profile: Default

Możliwość **filtrowania** danych

Przechwycone dane,
zaznaczenie wiersza wyświetla
w dolnych oknach strukturę
i surową zawartość ramki

Struktura zaznaczonej **ramki**,
widoczne „opakowane” danych
przez protokoły poszczególnych
warstw ISO/OSI

Surowa zawartość zaznaczonej
ramki