

Sieci komputerowe

Zarządzanie i monitoring sieci

Rafał Wojciechowski

Zarządzanie sieciami komputerowymi

- ▶ Rozwój i rozrost sieci staje się coraz istotniejszym i bardziej nieodzownym zasobem organizacji
- ▶ Wzrost ilości zasobów dla użytkowników powodowany jest wzrostem złożoności sieci, a zarządzanie nią staje się coraz bardziej skomplikowane
- ▶ Utrata zasobów sieciowych oraz niska wydajność sieci mogą powodować drastyczne straty materialne
- ▶ Sieć jest tworem dynamicznym podlegającym ciągłym zmianom (niekoniecznie planowanym)

Zarządzanie sieciami komputerowymi

- Konieczność aktywnego zarządzania siecią, sprawnej diagnozy problemów oraz ich zapobieganiu celem zapewnienia jak najlepszej wydajności sieci → badania miejscowe sieci

Zadania zarządzania siecią

- ▶ Monitorowanie dostępności sieci
- ▶ Udoskonalanie automatyzacji
- ▶ Monitorowanie czasu odpowiedzi
- ▶ Zapewnienie funkcji zabezpieczeń
- ▶ Przekierowywanie ruchu
- ▶ Przywracanie funkcjonalności
- ▶ Rejestrowanie użytkowników
- ▶ ...

Modele zarządzania sieciami

- ▶ Model organizacyjny
- ▶ Model informacyjny
- ▶ Model komunikacyjny
- ▶ Model funkcjonalny

Modele zarządzania sieciami

- ▶ Model organizacyjny
 - ▶ opis komponentów sieci i ich powiązań
 - ▶ zależna od standardu reprezentacja różnych typów architektur
- ▶ Model informacyjny
 - ▶ reprezentacja struktury przechowywania informacji
 - ▶ powiązanie obiektów i informacji z elementami zarządzania
 - ▶ standaryzacja przez ISO struktury informacji zarządzania (SMI) w celu uporządkowania semantyki i zapisu informacji w bazach MIB

Modele zarządzania sieciami

- ▶ Model komunikacyjny
 - ▶ opis standardów wymiany danych pomiędzy procesami agentów i managerów
 - ▶ 3 aspekty – zagadnienia transportu, aplikacji, standaryzacji poleceń oraz odpowiedzi
- ▶ Model funkcjonalny
 - ▶ opisuje aplikacje zarządzające rezydujące w systemie zarządzania
 - ▶ model zarządzania OSI wprowadza pięć kategorii funkcji – wady (*Fault*), konfiguracja (*Configuration*), monitoring (*Accounting*), wydajność (*Performance*), bezpieczeństwo (*Security*) → model FCAPS

Standardy zarządzania sieciami

CMIP

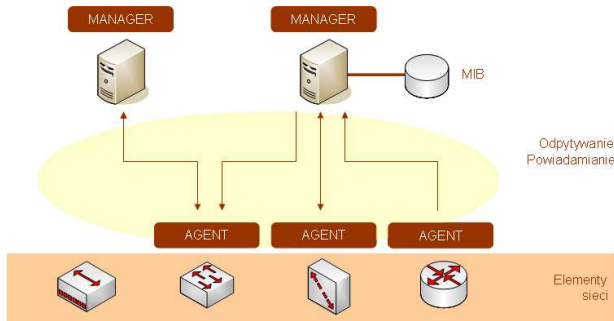
CMIP (*Common Management Information Protocol*) - złożony zestaw standardów ISO obejmujący serwisy zarządzania, protokół, specyfikację struktury bazy danych i zbioru obiektów

Standardy zarządzania sieciami

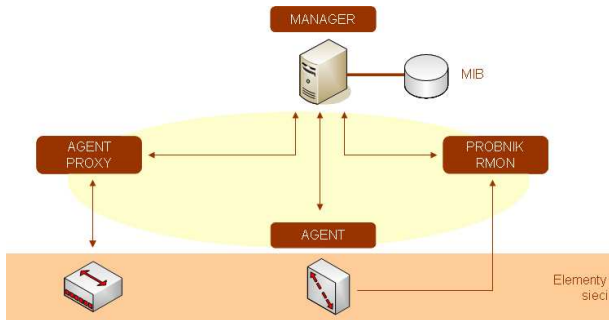
SNMP

SNMP (*Simple Network Management Protocol*) - standard zaakceptowany przez IETF obejmujący protokół, specyfikację struktury bazy danych i zbioru obiektów danych. Od 1989, SNMP wchodzi w skład standardu TCP / IP. Występuje w wersjach 1, 2c, 3

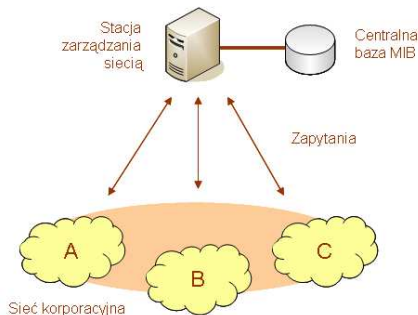
Komponenty modelu organizacyjnego



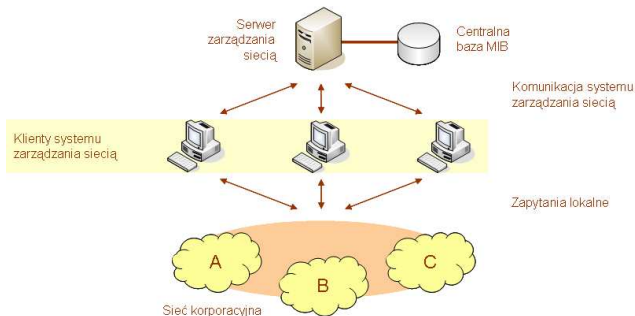
Komponenty modelu organizacyjnego



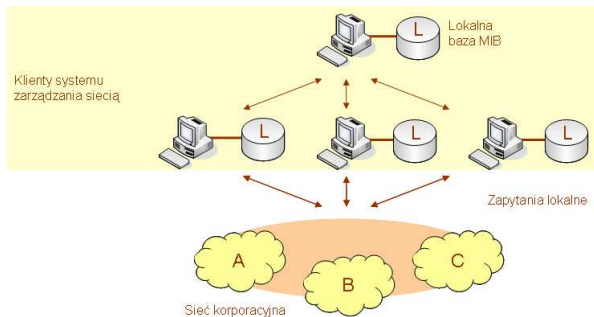
Architektura scentralizowana zarządzania siecią



Architektura hierarchiczna zarządzania siecią



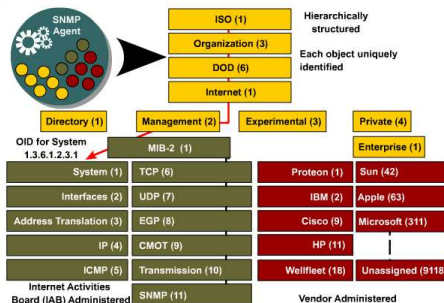
Architektura rozproszona zarządzania siecią



Management Information Base

- ▶ Strukturalne repozytorium informacji o urządzeniach w sieci i ich atrybutach
- ▶ Sama struktura zdefiniowana jako standard SMI (*Structure of Management Information*)
- ▶ Każdy zarządzalny obiekt jest opisywany liczbowym ciągiem identyfikacyjnym → OID w strukturze SMI
- ▶ MIB I – 114 standardowych obiektów możliwych do konfiguracji oraz monitorowania
- ▶ MIB II – 185 obiektów, rozszerzenie MIB I
- ▶ Vendor MIBs – rozszerzenia MIBów konkretnych producentów

Struktura MIBów



MIBy i OIDy

```
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org"                "1.3"
"dod"                "1.3.6"
"internet"           "1.3.6.1"
"directory"          "1.3.6.1.1"
"mgmt"               "1.3.6.1.2"
"experimental"       "1.3.6.1.3"
"private"             "1.3.6.1.4"
"enterprises"        "1.3.6.1.4.1"
"cisco"              "1.3.6.1.4.1.9"
"ciscoMgmt"          "1.3.6.1.4.1.9.9"
"ciscoWirelessIfMIB" "1.3.6.1.4.1.9.9.136"
"curRadioMibObjects" "1.3.6.1.4.1.9.9.136.1"
"curRadioNotification" "1.3.6.1.4.1.9.9.136.2"
"curRadioIfConformance" "1.3.6.1.4.1.9.9.136.3"
"curRadioInternal"   "1.3.6.1.4.1.9.9.136.1.1"
"curRadioCommon"     "1.3.6.1.4.1.9.9.136.1.2"
"curRadioBaseGroup"  "1.3.6.1.4.1.9.9.136.1.3"
"curRadioPhyQualityGroup" "1.3.6.1.4.1.9.9.136.1.4"
"curRadioFreqResGroup" "1.3.6.1.4.1.9.9.136.1.5"
"curRadioMetricsGroup" "1.3.6.1.4.1.9.9.136.1.6"
"curRadioHistoryGroup" "1.3.6.1.4.1.9.9.136.1.7"
"curRadioTimelineGroup" "1.3.6.1.4.1.9.9.136.1.8"
"curRadioSnapshotGroup" "1.3.6.1.4.1.9.9.136.1.9"
```

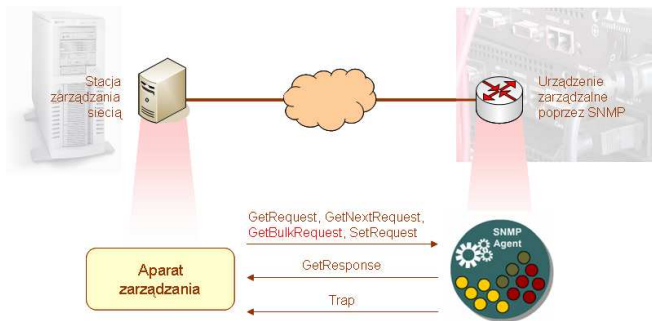
Protokół SNMP

- ▶ Protokół SNMP określa interakcję pomiędzy agentem a managerem
- ▶ Głównym celem projektantów było uproszczenie schematu zarządzania sieciami
- ▶ Podstawowe operacje zdefiniowane w protokole wynikają z założonej prostoty → pobranie oraz ustawienie zmiennej
- ▶ Wykorzystanie UDP – porty 160 oraz 161

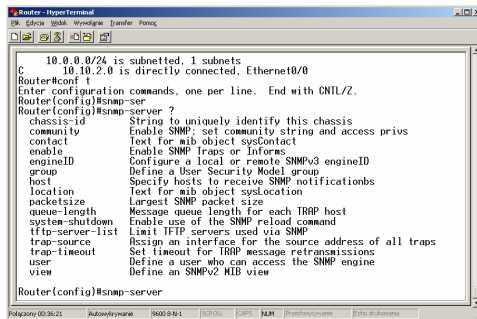
Protokół SNMP

- ▶ Optymalizacja polityki zarządzania – zbyt agresywny monitoring generuje nadmiarowy ruch w sieci, zbyt rzadki – niedoinformowanie administratora
- ▶ Bezpieczeństwo protokołu – dopiero wersja 3 SNMP wprowadza pełne uwierzytelnianie użytkowników oraz możliwość enkrypcji

Działanie SNMP



Konfiguracja SNMP



```
Router - HyperTerminal
File Edit View Window Transfer Port
[Icons]

10.0.0.0/24 is subnetted, 1 subnets
C      10.10.2.0 is directly connected, Ethernet0/0
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#snmp-ser
Router(config)#snmp-server ?
  chassis-id      String to uniquely identify this chassis
  community       Enable SNMP; set community string and access privs
  contact         Text for mib object sysContact
  enable          Enable SNMP traps or Inform
  engineID        Configure a local or remote SNMPv3 engineID
  group           Define a User Security Model group
  host            Specify hosts to receive SNMP notifications
  location        Text for mib object sysLocation
  packetsize      Largest SNMP packet size
  queue-length    Message queue length for each TRAP host
  system-shutdown Enable use of the SNMP reload command
  tftp-server-list Limit TFTP servers used via SNMP
  trap-source     Assign an interface for the source address of all traps
  trap-timeout    Set timeout for TRAP message retransmissions
  user           Define a user who can access the SNMP engine
  view           Define an SNMPv2 MIB view

Router(config)#snmp-server
```

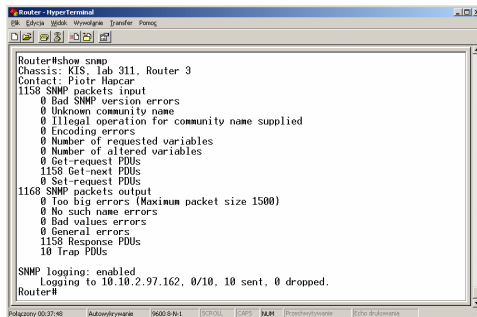


Konfiguracja SNMP, przykład

```
Router(config)# snmp-server community public ro
Router(config)# snmp-server community private rw
Router(config)# snmp chassis-id KIS, lab 311, router 3
Router(config)# snmp location Lodz, Stefanowskiego 18 / 22
Router(config)# snmp contact Jan Kowalski
Router(config)# snmp enable information
```



Weryfikacja działania i statystyki SNMP



```
Router#show snmp
Chassis: KIS, lab 311, Router 3
Contact: Piotr Hapcar
1158 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  1158 Get-next PDUs
  0 Set-request PDUs
1168 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  1158 Response PDUs
  10 Trap PDUs

SNMP logging: enabled
Logging to 10.10.2.97:162, 0/10, 10 sent, 0 dropped.
Router#
```



Konfiguracja serwera SNMP - pakiet *net-snmp*

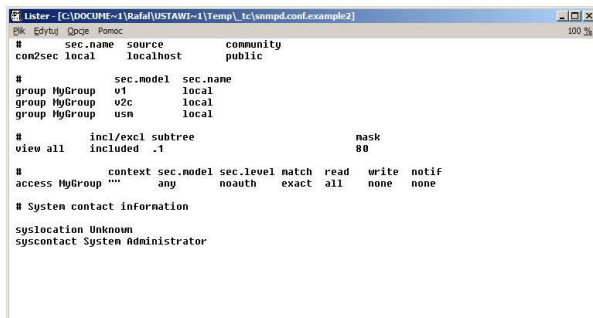
```
10.10.2.97 - PuTTY
eth0      Link encap:Ethernet  HWaddr 00:08:C7:A9:15:E1
          inet addr:10.10.2.97  Bcast:10.10.2.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5777 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4456 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2383350 (2.2 Mb)  TX bytes:379294 (370.4 Kb)
          Interrupt:10 Base address:0x6000

root@lab-xxx:~# snmp
snmpbulkget      snmpdelta      snmpnetstat     snmptranslate  snmpwalk
snmpbulkwalk     snmpdf         snmpset         snmptrap
snmpcheck        snmpget        snmpstatus      snmptrapd
snmpconf         snmpgetnext    snmptable       snmpusm
snmpd            snmpinform     snmptest        snmpvacm
root@lab-xxx:~# snmp
```



Konfiguracja serwera SNMP

- Ustawienia konfiguracyjne - */etc/snmp/snmpd.conf*



```
#      sec.name  source      community
con2sec local    localhost   public

#      sec.model sec.name
group MyGroup v1 local
group MyGroup v2c local
group MyGroup usm local

#      incl/excl subtree      mask
view all included .1        80

#      context sec.model sec.level match read write notif
access MyGroup "" any noauth exact all none none

# System contact information

syslocation Unknown
syscontact System Administrator
```

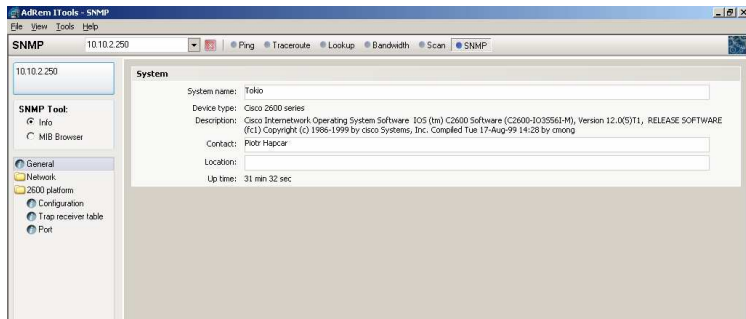


Pakiet *NetCrunch*

- ▶ Narzędzie pozwalające monitorować sieci IP, stacje Windows NT/2000 oraz urządzenia sieciowe i udostępniane usługi w różnych węzłach sieci z graficznym wizualizowaniem mapy w postaci diagramu, analizować wykorzystanie łącza prezentowane w postaci wykresów, informować oraz reagować na zdarzenia zaistniałe w węzłach
- ▶ Pakiet NetCrunch wyposażony jest w zestaw dodatkowych narzędzi → iToolsów umożliwiających monitoring sieci, skanowanie adresów IP, portów, zarządzanie poszczególnymi węzłami poprzez protokół SNMP

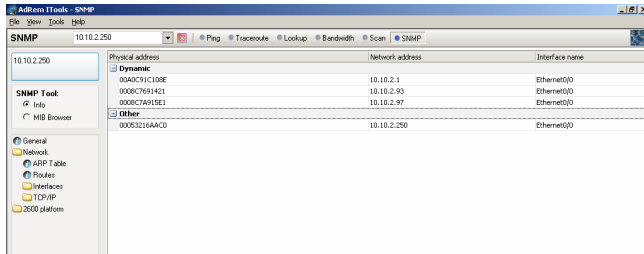
Pakiet *NetCrunch*

► SNMP Info



Pakiet *NetCrunch*

► ARP Table

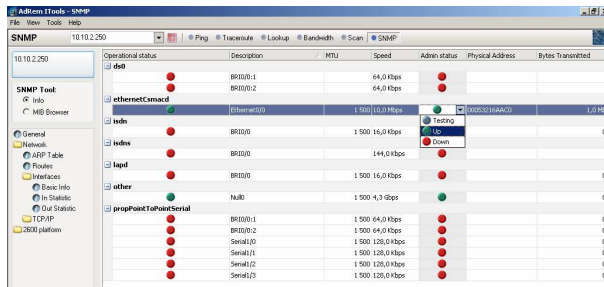


The screenshot shows the AdRem ITTools - SNMP application window. The main pane displays the ARP Table for the selected IP address 10.10.2.250. The table has three columns: Physical address, Network address, and Interface name. It is divided into 'Dynamic' and 'Other' sections. The left sidebar shows a tree view with 'General' selected, and 'Network' expanded to show 'ARP Table'.

Physical address	Network address	Interface name
Dynamic		
00A0C91C108E	10.10.2.1	Ethernet0/0
0006C7691421	10.10.2.93	Ethernet0/0
0006C7A915E1	10.10.2.97	Ethernet0/0
Other		
00053216AAC0	10.10.2.250	Ethernet0/0

Pakiet NetCrunch

► Konfiguracja interfejsów

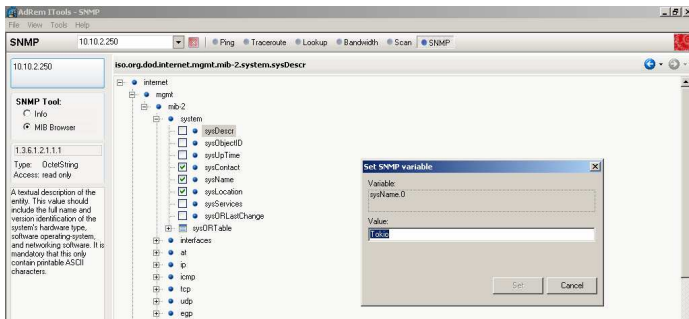


The screenshot shows the 'Aditem Tools - SNMP' window with the 'SNMP' tab selected. The left sidebar shows the 'SNMP Tool' section with 'Info' selected. The main area displays a table of network interfaces for the device '10.10.2.250'.

	Operational status	Description	MTU	Speed	Admin status	Physical Address	Bytes Transmitted
ds0		BR10/0:1		64,0 Kbps			
		BR10/0:2		64,0 Kbps			
ethernetCsmacd		Ethernet0/0	1 500	10,0 Mbps		00063216AA00	1,0 MB
isdn		BR10/0	1 500	16,0 Kbps			0
isdns		BR10/0		144,0 kbps			
lapd		BR10/0	1 500	16,0 Kbps			0
other		Null0	1 500	4,3 Gbps			0
propPointToPointSerial		BR10/0:1	1 500	64,0 Kbps			0
		BR10/0:2	1 500	64,0 Kbps			0
		Serial1/0	1 500	128,0 Kbps			0
		Serial1/1	1 500	128,0 Kbps			0
		Serial1/2	1 500	128,0 Kbps			0
		Serial1/3	1 500	128,0 Kbps			0

Pakiet *NetCrunch*

► MIB Browser



Pakiet *net-snmp*

- ▶ Komplet narzędzi do zarządzania zarówno serwerem SNMP, jak również stacją zarządzającą
- ▶ Intuicyjne korzystanie z aplikacji – pełna funkcjonalność gwarantowana przez trzy programy:
 - ▶ *snmpwalk* – umożliwiający przeglądanie całego drzewa MIBów dla określonej stacji,
 - ▶ *snmpget* – umożliwiający pobranie wartości zmiennej,
 - ▶ *snmpset* – pozwalający na ustawienie zmiennej



Pakiet *net-snmp*

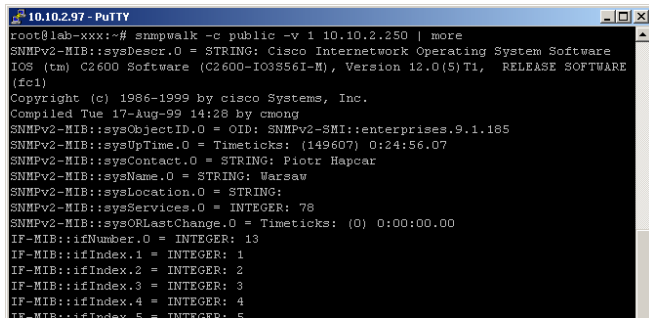
- ▶ Określenie numeru wersji SNMP
`snmpwalk -v [Numer wersji] ...`
- ▶ Wymuszenie określonego community stringu
`snmpwalk -c [Community string] ...`
- ▶ Określenie stacji docelowej
`snmpwalk ... [Adres IP]`



Pakiet *net-snmp*

► Pobranie drzewa obiektów

`snmpwalk -c [Community string] -v [Numer wersji] [Adres IP]`



```
10.10.2.97 - PuTTY
root@lab-xxx:~# snmpwalk -c public -v 1 10.10.2.250 | more
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3S56I-M), Version 12.0(5)T1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 14:28 by cmong
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.185
SNMPv2-MIB::sysUpTime.0 = Timeticks: (149607) 0:24:56.07
SNMPv2-MIB::sysContact.0 = STRING: Piotr Hapcar
SNMPv2-MIB::sysName.0 = STRING: Warsaw
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 13
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
```



Pakiet *net-snmp*

► Pobranie drzewa obiektów

`snmpwalk -c [Community string] -v [Numer wersji] [Adres IP]`

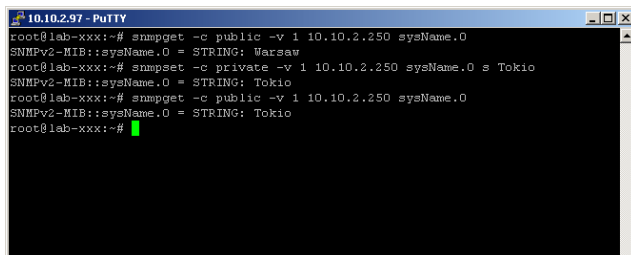
```
10.10.2.97 - PuTTY
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.14 = INTEGER: 14
IF-MIB::ifIndex.15 = INTEGER: 15
IF-MIB::ifIndex.16 = INTEGER: 16
IF-MIB::ifIndex.17 = INTEGER: 17
IF-MIB::ifDescr.1 = STRING: Ethernet0/0
IF-MIB::ifDescr.2 = STRING: BRIO/0
IF-MIB::ifDescr.3 = STRING: BRIO/0:1
IF-MIB::ifDescr.4 = STRING: BRIO/0:2
IF-MIB::ifDescr.5 = STRING: Serial1/0
IF-MIB::ifDescr.6 = STRING: Serial1/1
IF-MIB::ifDescr.7 = STRING: Serial1/2
IF-MIB::ifDescr.8 = STRING: Serial1/3
IF-MIB::ifDescr.9 = STRING: Null0
IF-MIB::ifDescr.14 = STRING: BRIO/0
IF-MIB::ifDescr.15 = STRING: BRIO/0
IF-MIB::ifDescr.16 = STRING: BRIO/0:1
IF-MIB::ifDescr.17 = STRING: BRIO/0:2
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
```



Pakiet *net-snmp*

► Pobranie i ustawienie zmiennej

```
snmpget -c [Community string] -v [Numer wersji] \  
      [Adres IP] [Zmienna]  
snmpset -c [Community string] -v [Numer wersji] \  
      [Adres IP] [Zmienna] [Typ] [Wartość]
```



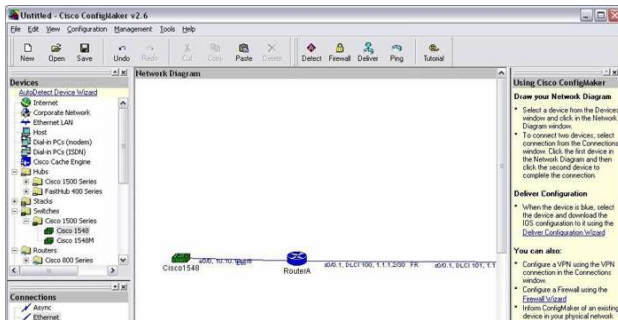
```
10.10.2.97 - PuTTY  
root@lab-xxx:~# snmpget -c public -v 1 10.10.2.250 sysName.0  
SNMPv2-MIB::sysName.0 = STRING: Warsaw  
root@lab-xxx:~# snmpset -c private -v 1 10.10.2.250 sysName.0 s Tokio  
SNMPv2-MIB::sysName.0 = STRING: Tokio  
root@lab-xxx:~# snmpget -c public -v 1 10.10.2.250 sysName.0  
SNMPv2-MIB::sysName.0 = STRING: Tokio  
root@lab-xxx:~#
```



Pakiet *Cisco ConfigMaker*

- ▶ Oprogramowanie umożliwiające zarządzanie oprogramowaniem oraz konfigurację urządzeń Cisco
- ▶ Graficzna prezentacja mapy sieci, konfiguracja interfejsów, tablic routingu, haseł, . . . , pozwala na łatwe zestawienie określonej konfiguracji sieci oraz eksport ustawień do plików tekstowych zgodnych z plikami konfiguracji urządzeń Cisco
- ▶ Możliwe jest również pobranie bieżącej konfiguracji z routera oraz zapis aktualnej do urządzenia

Pakiet *Cisco ConfigMaker*



Sieć komputerowa

Sieć komputerowa

Sieć komputerowa - zbiór mechanizmów umożliwiających komunikowanie się komputerów bądź urządzeń komputerowych znajdujących się w różnych miejscach. Integralnym elementem owej komunikacji jest wzajemne udostępnianie sobie zasobów

[M. Sportack]

Topologia

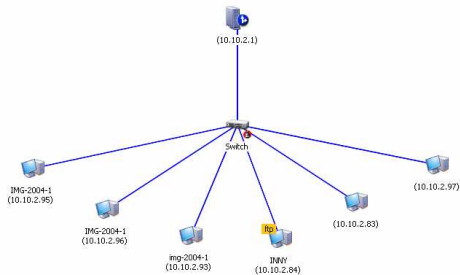
Topologia

Topologia (gr. *topos* - położenie, *logos* - nauka) - nauka zajmująca się badaniem położenia, rozmieszczenia elementów oraz ich wpływu na powiązania między sobą. Wyszczególnia się topologię fizyczną odwzorowującą fizyczne połączenia pomiędzy wszystkimi elementami sieci oraz logiczną obrazującą logiczny przepływ informacji w sieci

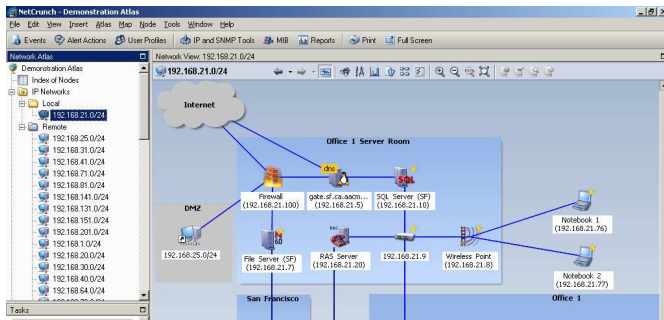
Mapy sieci

- ▶ Tworzenie map sieci jest w rzeczywistości mechanizmem wizualizacji umożliwiającym administratorowi sprawne zarządzanie siecią
- ▶ Niewątpliwą zaletą tej metody jest graficzna reprezentacja mapy będąca odzwierciedleniem zrealizowanej topologii, co ułatwia zarządzanie siecią
- ▶ W rzeczywistości mapy mogą stanowić zarówno obraz fizycznej topologii sieci, jak również logicznej
- ▶ Podstawą mapy są urządzenia (węzły sieci – routery, switchy, huby, hosty, ...) oraz odpowiednie połączenia między poszczególnymi elementami

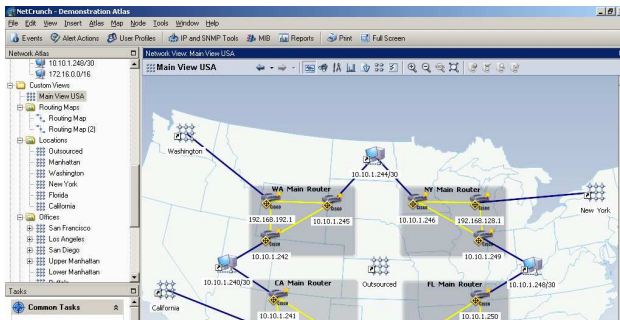
Pakiet *NetCrunch*



Pakiet NetCrunch



Pakiet NetCrunch



Pakiet NetCrunch

NetCrunch - Demonstration Atlas

File Edit View Insert Atlas Map Node Tools Window Help

Events Alert Actions User Profiles IP and SNMP Tools MIB Reports Print Full Screen

Network Atlas

192.168.21.0/24

Na...	Address	Loc...	T...	S...	Interfaces	Services	Avg...	Max...	%	Last Res...	Al...	Last...	% U...	Down...	M...
adam.s...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	< 10	< 10	100		5 200...	63	2 mi...	Wab...
admin...	192.1...	Office 1	Wind...	Wind...	1 1	ping	ang	5	16	2006-02...			100		Enabled
alexa...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	< 10	< 10	100		5 200...	73	2 mi...	Wab...
amand...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	< 10	< 10	100		5 200...	73	2 mi...	Wab...
anna.s...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	5	10	100		5 200...	73	2 mi...	Wab...
barber...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	2	10	100		5 200...	73	2 mi...	Wab...
basil.sf...	192.1...	Office 1	Wind...	Wind...	1 1	ping	ang	< 10	< 10	100		4 200...	63	2 mi...	Wab...
brando...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	< 10	< 10	100		5 200...	73	2 mi...	Wab...
chad.s...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	8	10	100		5 200...	73	2 mi...	Wab...
charles...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	< 10	< 10	100		5 200...	73	2 mi...	Wab...
charles...	192.1...	Office 1	Wind...	Wind...	1 1	snmp	ang	2	10	100		5 200...	73	2 mi...	Wab...
dial1.sf...	192.1...					ping		< 10	< 10	100		2 200...	58	2 mi...	Wab...
dial3.sf...	192.1...					ping		< 10	< 10	100		2 200...	53	2 mi...	Wab...
dial6.sf...	192.1...					ping		< 10	< 10	100		2 200...	75	2 mi...	Wab...
door.sf...	192.1...	San Fra...	Sun S...	Sun S...	1 1 1	snmp	ang	7	14	2006-02...			100		Enabled
fire.wf...	192.1...	Firewall				snmp		< 10	< 10	2006-02...			100		Enabled

Monitorowanie dostępności hostów

- ▶ Podstawowym problemem administratorów jest monitorowanie dostępności węzłów mające na celu nie tylko sprawdzenie komunikacji i osiągalności konkretnych hostów, ale również detekcję stacji niepożądanych podłączonych bez wiedzy administratora a korzystających z usług zarządzanej sieci i współdzielących pasmo
- ▶ Skanowanie sieci możliwe jest do wykonania za pomocą narzędzi: *ping* (systemy unixowe umożliwiają pingowanie adresów broadcastowych), *nmap*, *NetCruncha* i innych

Narzędzie *ping*

```
10.10.2.97 - PuTTY
root@lab-xxx:~# ping -b 10.10.2.255
WARNING: pingng broadcast address
PING 10.10.2.255 (10.10.2.255) 56(84) bytes of data.
64 bytes from 10.10.2.97: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 10.10.2.83: icmp_seq=1 ttl=64 time=0.132 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=2 ttl=64 time=0.010 ms
64 bytes from 10.10.2.83: icmp_seq=2 ttl=64 time=0.097 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=3 ttl=64 time=0.011 ms
64 bytes from 10.10.2.83: icmp_seq=3 ttl=64 time=0.105 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=4 ttl=64 time=0.011 ms
64 bytes from 10.10.2.83: icmp_seq=4 ttl=64 time=0.104 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=5 ttl=64 time=0.011 ms
64 bytes from 10.10.2.83: icmp_seq=5 ttl=64 time=0.104 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=6 ttl=64 time=0.012 ms
64 bytes from 10.10.2.83: icmp_seq=6 ttl=64 time=0.098 ms (DUP!)
64 bytes from 10.10.2.97: icmp_seq=7 ttl=64 time=0.010 ms
64 bytes from 10.10.2.83: icmp_seq=7 ttl=64 time=0.096 ms (DUP!)

--- 10.10.2.255 ping statistics ---
7 packets transmitted, 7 received, +7 duplicates, 0% packet loss, time 599
rtt min/avg/max/mdev = 0.010/0.060/0.132/0.046 ms
```



Narzędzie *nmap*

```
mc - ~
root@lab-xxx:~# nmap -sP 10.10.2.0/24

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 1904-06-30 23:08 WNT
Host 10.10.2.0 seems to be a subnet broadcast address (returned 1 extra pings).
Host 10.10.2.1 appears to be up.
Host 10.10.2.83 appears to be up.
Host 10.10.2.84 appears to be up.
Host 10.10.2.93 appears to be up.
Host 10.10.2.95 appears to be up.
Host 10.10.2.96 appears to be up.
Host 10.10.2.97 appears to be up.
Host 10.10.2.255 seems to be a subnet broadcast address (returned 1 extra pings)
.
Nmap run completed -- 256 IP addresses (7 hosts up) scanned in 8.629 seconds
root@lab-xxx:~#
```



Narzędzie NetCrunch

AdRem IT Tools - Scan

File View Tools Help

Scan 212.191.89.0 [Ping] [Traceroute] [Lookup] [Bandwidth] [Scan] [SNMP]

Name	Address	System	Location	Response Time ...
gate.kis.p.lodz.pl	212.191.89.1			< 10
zty.kis.p.lodz.pl	212.191.89.2			< 10
moon.kis.p.lodz.pl	212.191.89.3			< 10
eridu.kis.p.lodz.pl	212.191.89.5			< 10
switch2.kis.p.lodz.pl	212.191.89.7			10
switch3.kis.p.lodz.pl	212.191.89.8			10
nat114.kis.p.lodz.pl	212.191.89.9			< 10
nat4.kis.p.lodz.pl	212.191.89.10			< 10
nat6.kis.p.lodz.pl	212.191.89.11			< 10
nat9.kis.p.lodz.pl	212.191.89.12			< 10
nat10.kis.p.lodz.pl	212.191.89.13			< 10
sunmiva.kis.p.lodz.pl	212.191.89.14			< 10
ks019.kis.p.lodz.pl	212.191.89.19			< 10
diesel.kis.p.lodz.pl	212.191.89.20			< 10
nowy.kis.p.lodz.pl	212.191.89.21			< 10
ks025.kis.p.lodz.pl	212.191.89.25			< 10
ks027.kis.p.lodz.pl	212.191.89.27			< 10
ks028.kis.p.lodz.pl	212.191.89.28	D-Link 602, 11b+ AP		< 10
ks029.kis.p.lodz.pl	212.191.89.29			< 10

Scan: 212.191.89.0

Services: ☐ Services ☐ Ports ☒ Network

Nodes: Checked 254 Found 42

Options: [v]

Detekcja nielegalnych hostów

- ▶ Do obowiązków administratora należy również detekcja hostów nielegalnie udostępniających połączenie do sieci Internet poprzez zarządzaną sieć
- ▶ Detekcja może opierać się na obserwacji ruchu z komputera bramy (obserwacja otwartych portów, nawiązanych połączeń, ...), analizie czasu życia (TTL) pakietów wychodzących z bramy (przy przejściu przez każdy węzeł liczba TTL jest pomniejszana o 1), próbie odgadnięcia ustawień forwardingu pakietów, etc.
- ▶ Istnieją również dedykowane aplikacje umożliwiające zbadanie systemów pod kątem realizacji NATa (*natdet*, *p02f*)

Narzędzie *natdet*

```
C:\WINDOWS\System32\cmd.exe - natdet -v
NATDet - NAT Detection tool, version 1.0.5
(c) Marcin Ulikowski <elceef@itsec.pl>
win32-port K. Lowczak <projectorsoft@poczta.fm>
[+] device: "\Device\NPF_{GenericNdisWanAdapter}", signatures: 150.
[*] 15-04-2005 12:14:47: NAT at 83.28.223.227 for 2 system(s) [100%]
    Used factors: OSGENRE TTL
[*] 15-04-2005 12:15:23: NAT at 83.28.209.5 for 2 system(s) [100%]
    Used factors: OSGENRE TTL
[*] 15-04-2005 12:24:53: NAT at 217.132.86.120 for 1 system(s) [100%]
    Uptime: ~69 hour(s)
    Used factors: TTL
```

Monitorowanie aktywności hostów

- ▶ Każdy użytkownik wykorzystuje sieć wedle własnych potrzeb i zainteresowań
- ▶ Realizacja w/w celów dokonywana jest za pomocą najrozmaitszego oprogramowania, które niestety, jak pokazuje praktyka, może nie być najwydajniejsze pod kątem wykorzystania pasma

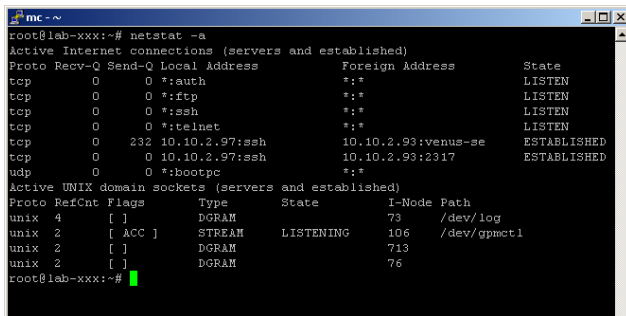
Monitorowanie aktywności hostów

- Grabieżcza polityka użytkowników w wielu sieciach jest jedną z przyczyn osłabienia ogólnej wydajności sieci. Również kwestie bezpieczeństwa systemów oraz wymienianych danych mogą być słabym punktem sieci, dlatego też celowym jest monitorowanie poczynąń użytkowników sieci – badanie aplikacji, z których korzystają, podgląd natężenia ruchu generowanego przez użytkowników, wykluczanie aplikacji zabronionych, ...

Monitorowanie aktywności hostów

- ▶ Najwygodniejszym miejscem analizy ruchu jest węzeł, przez który dany ruch przechodzi, czyli w większości przypadków bramka (router brzegowy) udostępniający połączenie ze światem zewnętrznym, bądź stacja monitorująca należąca do wspólnej domeny kolizyjnej z komputerem forwardującym ruch lub komputerami partycypującymi zasoby sieci
- ▶ Przykładem aplikacji służących do realizacji w/w celu jest *tcpdump*, *nmap*, *netstat*, *Anasil*, *NetCrunch*

Narzędzie *netstat*

A terminal window titled 'mc ~' showing the output of the 'netstat -a' command. The output is divided into two sections: 'Active Internet connections (servers and established)' and 'Active UNIX domain sockets (servers and established)'. The first section lists TCP and UDP connections with columns for protocol, receive/send queue sizes, local/foreign addresses, and state. The second section lists UNIX domain sockets with columns for protocol, reference count, flags, type, state, I-node, and path.

```
root@lab-xxx:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:auth                  *:.*                    LISTEN
tcp        0      0 *:ftp                   *:.*                    LISTEN
tcp        0      0 *:ssh                   *:.*                    LISTEN
tcp        0      0 *:telnet                *:.*                    LISTEN
tcp        0    232  10.10.2.97:ssh          10.10.2.93:venus-se    ESTABLISHED
tcp        0      0 10.10.2.97:ssh          10.10.2.93:2317        ESTABLISHED
udp        0      0 *:bootpc                *:.*                    LISTEN

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix    4      [ ]       DGRAM          73       /dev/log
unix    2      [ ACC ]   STREAM   LISTENING    106      /dev/gpmctl
unix    2      [ ]       DGRAM          713
unix    2      [ ]       DGRAM          76
root@lab-xxx:~#
```

Narzędzie *nmap*

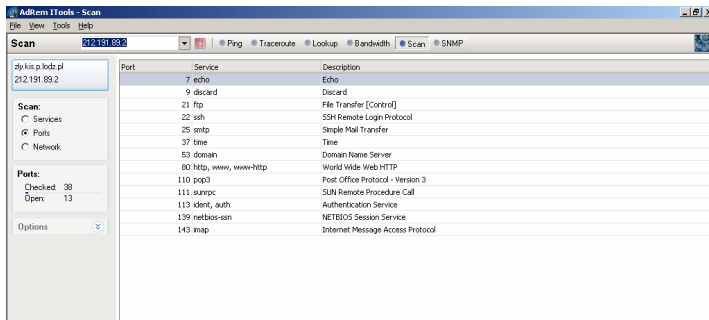
```
mc - ~
root@lab-xxx:~# nmap -O 10.10.2.83

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 1904-06-30 23:17 WMT
Interesting ports on 10.10.2.83:
(The 1655 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
113/tcp   open  auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.025 days (since Thu Jun 30 22:41:26 1904)

Nmap run completed -- 1 IP address (1 host up) scanned in 4.865 seconds
root@lab-xxx:~#
```



Narzędzie *NetCrunch*



Narzędzie *NetCrunch*

AdRem IT Tools - Scan

File View Tools Help

Scan 212.191.89.2 [Ping] [Traceroute] [Lookup] [Bandwidth] [Scan] [SNMP]

zly.kis.p.lodz.pl
212.191.89.2

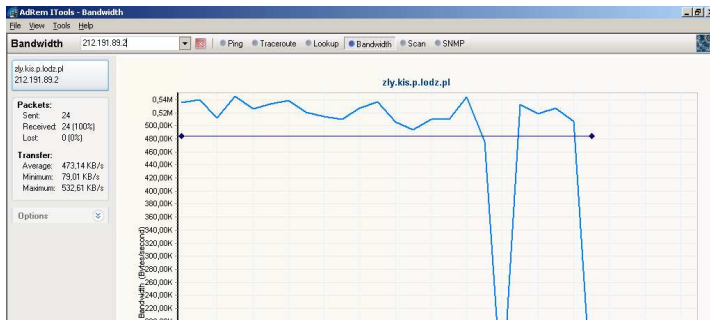
Scan:
☒ Services
☐ Ports
☐ Network

Services:
 Checked: 63
 Running: 12

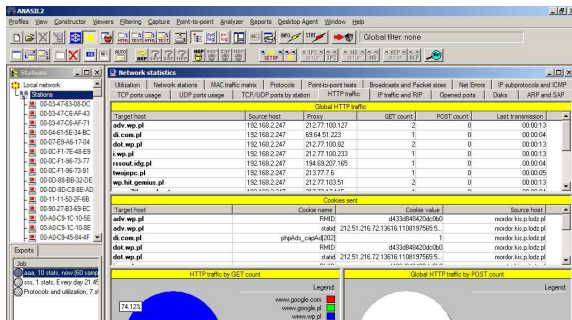
Options: [v]

Service	Response Ti...	Description	Protocol	Port	Status
Running (12)					
CIFS (NetWare)	30	Common Internet File System for NetWare	TCP	139	OK
CIFS/SMB	40	Common Internet File System over TCP	TCP	445	OK
FTP	120	File Transfer Protocol	TCP	21	OK
220- ...					
HTTP	10	WWW Server	TCP	80	OK
HTTP/1.1 200 OK Date:					
HTTPS	80	Secure Sockets Layer (SSL) on HTTPS port	TCP	443	OK
NetBIOS (TCP)	20	NetBIOS Session over TCP	TCP	139	OK
PING	< 10	PING (Internet Control Message Protocol)	ICMP	0	OK
POP3	20	Post Office Protocol - Version 3	TCP	110	OK
+OK					
SMTP	50	Simple Mail Transfer Protocol	TCP	25	OK
220 zly.kis.p.lodz.pl ESMTP []					
SSH	20	Secure Shell	TCP	22	OK
SSH-2.0-Sun_SSH_1.0.1 Protocol major versions differ.					
TIME TCP	10	Time Protocol (via TCP) Returns the number of seconds since 00:...	TCP	37	OK

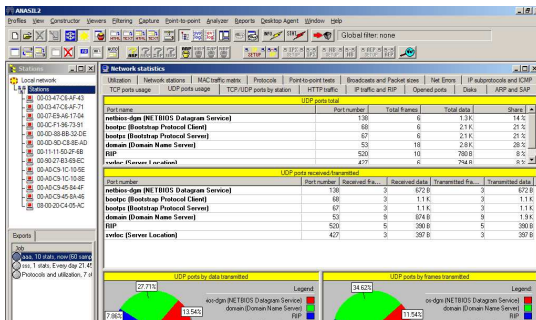
Narzędzie *NetCrunch*



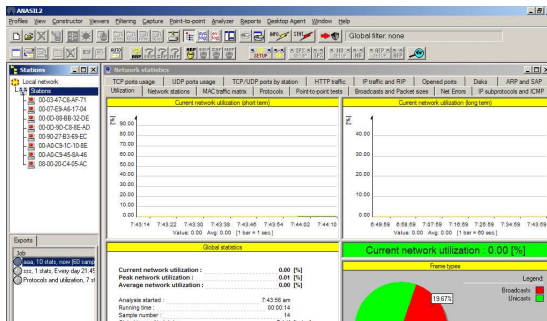
Narzędzie Anasil



Narzędzie Anasil



Narzędzie Anasil



Zarządzanie pasmem i połączeniami

- ▶ Podczas zarządzania siecią wielokrotnie pojawia się problem, co należy zrobić z chwilowo niechcianymi połączeniami. Zaliczyć się do nich mogą połączenia od użytkowników, którzy na skutek niepełności konfiguracji, uzyskują możliwość określonego połączenia ze zdalnymi hostami lub też połączenia od nich przekazywane są na tyle obciążające łącze, że inni użytkownicy nie mają możliwości korzystania z sieci (przy zrównoważonej polityce przydziału pasma)

Zarządzanie pasmem i połączeniami

- ▶ Obojętne jaka była przyczyna, administrator winien skorygować konfigurację dopasowując odpowiednie reguły firewalla, wprowadzając możliwość podziału pasma (→ *shaping łącza*), ...
- ▶ Po zlokalizowaniu określonego portu oraz adresu stacji źródłowej, możliwe jest spowolnienie połączenia (→ *tcprnice*) bądź też zablokowanie go (→ *tcpkill*)

Zawieszanie połączenia

- ▶ Określenie interfejsu, na którym przebiega nasłuchiwanie
`tcpkill -i [Interfejs] ...`
- ▶ Określenie stopnia wykorzystania do zatrzymania połączenia
(skala od 1 do 9, domyślnie 3)
`tcpkill -1 .. -9 ...`
- ▶ Sprecyzowanie filtra zgodnie z notacją *tcpdump*
`tcpkill ... [Wyrażenie filtra]`

Spowolnienie połączenia

- ▶ Określenie interfejsu, na którym przebiega nasłuchiwanie
`tcprun -i [Interfejs] ...`
- ▶ Określenie współczynnika spowolnienia (maksymalnie 20)
`tcprun -n [Współczynnik spowolnienia] ...`
- ▶ Sprecyzowanie filtra zgodnie z notacją *tcpdump*
`tcprun ... [Wyrażenie filtra]`

Zarządzanie pasmem i połączeniami, przykład

- ▶ Administrator wykrył podłączenie do sieci intruza o adresie 192.168.1.29. Wszystkie połączenia z tej stacji chce zablokować.

```
root@Mordor:~ tcpkill -3 -i eth1 src 192.168.1.29
```

Zarządzanie pasmem i połączeniami, przykład

- ▶ Administrator wykrył podłączenie do sieci intruza o adresie 192.168.1.29. Wszystkie połączenia z tej stacji chce zablokować.

```
root@Mordor:~ tcpkill -3 -i eth1 src 192.168.1.29
```

Zarządzanie pasmem i połączeniami, przykład 2

- ▶ Administrator wykrył zapchanie łącza przez transmisję na portach 8888 oraz 6699 (*napster*). Podejmuje próbę maksymalnego spowolnienia blokującego połączenia mając nadzieję na odblokowanie pozostałych transmisji.

```
root@Mordor:~ tcpnice -n 20 -i eth0 port 8888 and port 6699
```

Zarządzanie pasmem i połączeniami, przykład 2

- ▶ Administrator wykrył zapchanie łącza przez transmisję na portach 8888 oraz 6699 (*napster*). Podejmuje próbę maksymalnego spowolnienia blokującego połączenia mając nadzieję na odblokowanie pozostałych transmisji.

```
root@Mordor:~ tcpnice -n 20 -i eth0 port 8888 and port 6699
```

Troubleshooting sieci

- ▶ Proces wdrażania, konfiguracji oraz monitoringu sieci zmusza administratora do wielu czynności testowych mających na celu rozwiązanie problemów i optymalizację sieci
- ▶ Z uwagi na różny charakter możliwych błędów sieci, konieczna jest odpowiednia metodologia rozwiązywania problemów sieci. Najprostszym i jednocześnie najbardziej oczywistym podejściem do troubleshootingu sieci jest podejście warstwowe wynikające bezpośrednio z modelu referencyjnego sieci ISO / OSI

Troubleshooting sieci

- ▶ Analizując i eliminując potencjalne problemy począwszy od warstwy najniższej – warstwy fizycznej, poprzez warstwę łącza danych aż po warstwy wyższe uzyskujemy logiczne określenie powstałego problemu
- ▶ Warstwy modelu OSI / ISO grupujące odpowiednie funkcje skupiają konkretne problemy – połączenie fizyczne, logiczne, trasowanie, reguły filtrujące, ...

Błędy warstwy fizycznej

- ▶ Uszkodzone kable
- ▶ Rozłączone kable
- ▶ Kable podłączone do złych portów
- ▶ Niestabilne połączenia kabli
- ▶ Nieprawidłowe użycie kabli do konsoli, kabli z przeplotem lub kabli prostych
- ▶ Problemy z transceiverem
- ▶ Problemy z kablami w urządzeniach komunikacyjnych DCE
- ▶ Problemy z kablami w urządzeniach DTE
- ▶ Wyłączone urządzenia

Błędy warstwy łącza danych

- ▶ Niepoprawnie skonfigurowane interfejsy szeregowo
- ▶ Niepoprawnie skonfigurowane interfejsy Ethernet
- ▶ Niewłaściwy zestaw enkapsulacji
- ▶ Nieprawidłowe ustawienie zegara w interfejsach szeregowych
- ▶ Problemy z kartami sieciowymi

Błędy warstwy sieciowej

- ▶ Wyłączony protokół routingu
- ▶ Włączony niewłaściwy protokół routingu
- ▶ Niewłaściwy adres IP
- ▶ Nieprawidłowe maski podsieci

Weryfikacja ustawień sieci

► Informacje dotyczące stanu interfejsów

`show interfaces [serial | ethernet | ...] [Nazwa interfejsu]`

```
GAD#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
Hardware is QUICC Serial
Internet address is 10.0.1.1/24
MTU 150 bytes, BW 1544 Kbit, DLY 2000 usec,
relay 255/255, load 131/255
Encapsulation HDLC, loopback not set, keepalive set (10
sec)
Last input 00:00:00 output hang never
Last clearing of "show interface" counters never
Input queue: 8/75/0 (size/max/drops): Total output
```



Weryfikacja ustawień sieci

► Informacje CDP

show cdp neighbors

```
Switch#show cdp neighbors detail
-----
Device ID: Router
Entry address(es):
  IP address: 192.168.16.2
Platform: cisco 2621XM, Capabilities: Router
Interface: FastEthernet0/15, Port ID (outgoing port): FastEthernet0/0
Holdtime : 177 sec

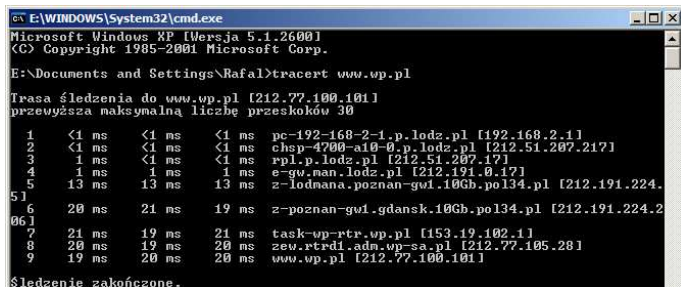
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK8S-M), Version 12.2(12c), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 05-Feb-03 16:36 by kellythw

advertisement version: 2
Duplex: full
```



Weryfikacja ustawień sieci

- ▶ Łączność na poziomie warstwy sieci i wyższych
ping [Adres IP]
tracert [Adres IP]
telnet [Adres IP]



```
E:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Wersja 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Rafal>tracert www.wp.pl

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

  1  <1 ms    <1 ms    <1 ms    pc-192-168-2-1.p.lodz.pl [192.168.2.1]
  2  <1 ms    <1 ms    <1 ms    chsp-4700-a10-0.p.lodz.pl [212.51.207.217]
  3  1 ms     <1 ms    <1 ms    rpl.p.lodz.pl [212.51.207.17]
  4  1 ms     1 ms     1 ms     e-gw.man.lodz.pl [212.191.0.17]
  5  13 ms    13 ms    13 ms    z-lodmana.poznan-gw1.10Gb.pol34.pl [212.191.224.51]
  6  20 ms    21 ms    19 ms    z-poznan-gw1.gdansk.10Gb.pol34.pl [212.191.224.206]
  7  21 ms    19 ms    21 ms    task-wp-rtr.wp.pl [153.19.102.1]
  8  20 ms    19 ms    20 ms    zew.rtrd1.adm.wp-sa.pl [212.77.105.28]
  9  19 ms    20 ms    20 ms    www.wp.pl [212.77.100.101]

Śledzenie zakończone.
```

Weryfikacja ustawień sieci

► Pozyskiwanie informacji o routingu dynamicznym

`show ip route`

`show ip protocols`

```
Gadsden#show ip protocols
Routing Protocol is "igrp 12"
  Sending updates every 90 seconds, next due in 49 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  ----output omitted----
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 15 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
```



Weryfikacja ustawień sieci

- Pozyskiwanie informacji o stanie kontrolerów / kart rozszerzeń oraz przyłączy

`show controllers`

```
GAD#show controllers serial 0/0
```

```
QUICC Serial unit 0  
idb at 0x20A31A3A8, driver data structure at 0x20A4C60  
SCC Registers:  
General [GSMR]= 0x2: 0x00000030, Protocol-specific  
[PSMR]=0x0  
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status  
[SCCS]=0x0006  
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```



Weryfikacja ustawień sieci

- Wyświetlanie danych i zdarzeń dynamicznych
debug ...

```
GAD#debug ip rip events
RIP event debugging is on
GAD#
00:24:16: RIP: sending v1 update to 255.255.255.255 via
Ethernet0/0 (1.0.0.1)
00:24:16:RIP: Update contains 3 routes
00:24:16:RIP: Update queued
00:24:16:RIP: Update sent via Ethernet0/0
00:24:16:RIP: sending v1 update to 255.255.255.255 via
Serial0/0 (2.0.0.1)
00:24:16:RIP: Update contains 1 routes
00:24:16:RIP: Update queued
```



Koniec

Dziękuję za uwagę . . .