

Zadanie 1 Moduł III

Wprowadzenie do GNS3

Używany przez wielu inżynierów sieci na całym świecie do emulowania, konfigurowania i testowania sieci złożonych z wirtualnego sprzętu jak Cisco czy Juniper. Może również służyć do symulowania ataków sieciowych.

Za pomocą interfejsu graficznego użytkownicy mogą bezproblemowo łączyć wszystkie typy wirtualnych interfejsów w celu tworzenia rzeczywistej reprezentacji sieci. GNS3 działa na tradycyjnym sprzęcie komputerowym i może być używany w wielu systemach operacyjnych w tym Windows, Linux, MacOS.



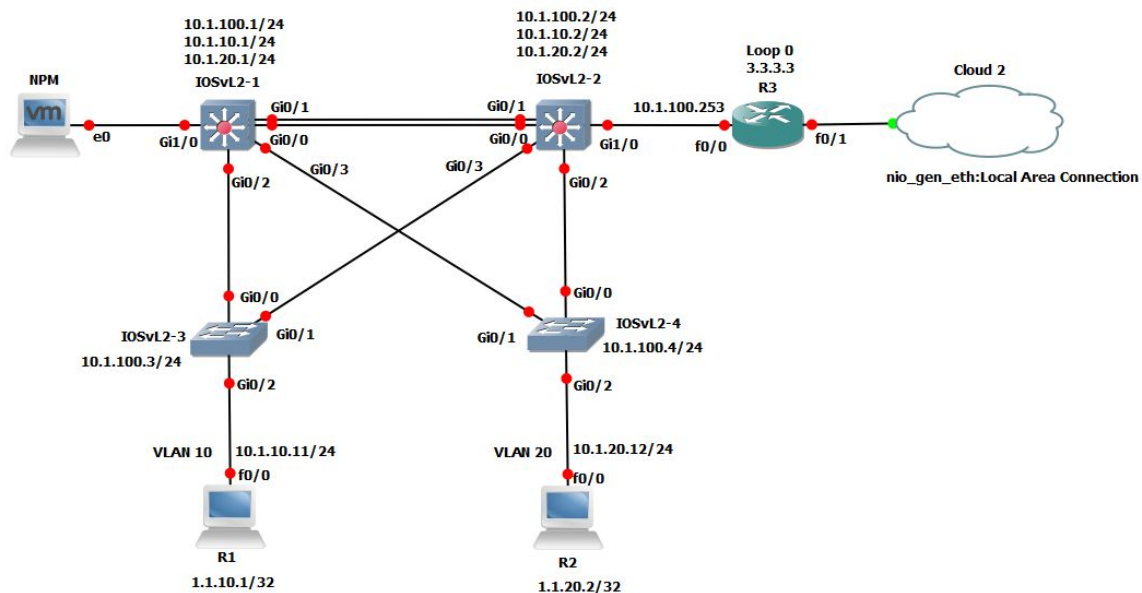
GNS3 oferuje kilka sposobów na uruchamianie wirtualnych urządzeń takich jak routery czy przełączniki.

Składa się z dwóch oprogramowań:

- The GNS3-all-in-one software (GUI)
- The GNS3 virtual machine (VM)



Graficzny interfejs topologii GNS3



Opcje serwera

Kiedy tworzysz topologie w GNS3 używając klienta GUI all-in-one, stworzone urządzenia muszą być hostowane i uruchomione za pomocą serwera.

Masz kilka opcji serwera:

- Local GNS3 server
- Local GNS3 VM
- Remote GNS3 VM



Lokalny serwer GNS3 uruchamia serwer na tym samym komputerze na którym zainstalowałeś GNS3 all-in-one.

Przykładowo jeżeli używasz Windowsa, HNS3 GUI oraz serwer GNS3 będą działać na Windowsie. Jeżeli natomiast uruchomiłeś GNS3 VM (co jest rekomendowane), możesz uruchomić HNS3 VM lokalnie na swoim Pcie używając oprogramowania takiego jak Vmware Workstation, Virtualbox lub Hyper-V; możesz również uruchomić GNS3 VM zdalnie na serwerze używając Vmware ESXi lub na chmurze.




GNS3 pozwala na korzystanie zarówno z urządzeń symulowanych, jak i emulowanych.

W przypadku urządzeń emulowanych, GNS3 udaje bądź emuluje sprzęt takiego urządzenia, a użytkownik korzysta ze skopiowanego z aktualnego urządzenia oprogramowania, np. Cisco IOS skopiowane z serwera Cisco. Takie oprogramowanie jest później uruchamiane jako emulowane urządzenie w programie.

W sytuacji symulacji, GNS3 symuluje cechy i funkcje pożądanego urządzenia za pomocą wbudowanych switchów stworzonych przez GNS3.

Przykładem technologii która emuluje sprzęt, w tym przypadku Cisco, jest Dynamips, a przykładem obrazów systemowych, które są zalecane do użytku z GNS3 są te z Cisco VIRL, które są aktywnie wspierane przez Cisco



Wyświetlanie adresów sprzętowych adapterów sieciowych komputera

```
Windows PowerShell
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Racper> ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Połączenie lokalne* 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Połączenie lokalne* 14:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::f184:be5d:3ec1:f4db%11
    IPv4 Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

PS C:\Users\Racper> |
```

ipconfig - polecenie to służy do wyświetlania adresów sprzętowych adapterów sieciowych komputera.

Wyświetlanie tablicy trasowania

```
Windows PowerShell
PS C:\Users\Wacper> route print

=====
Interface List
  9...c0 e4 34 6c 3b dd .....Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
  3...c2 e4 34 6c 3b dd .....Microsoft Wi-Fi Direct Virtual Adapter #5
  20...e2 e4 34 6c 3b dd .....Microsoft Wi-Fi Direct Virtual Adapter #6
  11...04 d4 c4 7a 48 28 .....Realtek PCIe GbE Family Controller
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.1.1       192.168.1.103    55
127.0.0.0                  255.0.0.0        On-link           127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link           127.0.0.1        331
127.255.255.255            255.255.255.255  On-link           127.0.0.1        331
192.168.1.0                255.255.255.0    On-link           192.168.1.103    311
192.168.1.103              255.255.255.255  On-link           192.168.1.103    311
192.168.1.255              255.255.255.255  On-link           192.168.1.103    311
224.0.0.0                  240.0.0.0        On-link           127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link           192.168.1.103    311
255.255.255.255            255.255.255.255  On-link           127.0.0.1        331
255.255.255.255            255.255.255.255  On-link           192.168.1.103    311
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
-----
1 331 ::1/128 ::1/128 On-link
11 311 fe80::/64 fe80::/64 On-link
11 311 fe80::f184:be5d:3ec1:f4db/128 fe80::f184:be5d:3ec1:f4db/128 On-link
1 331 ff00::/8 ff00::/8 On-link
11 311 ff00::/8 ff00::/8 On-link
=====
Persistent Routes:
None
PS C:\Users\Wacper>
```

route print - polecenie to służy do wyświetlania tablicy trasowania (routingu).

Polecenie pathping

```
Windows PowerShell
Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\Kacper> pathping ms.polsl.pl

Tracing route to ms.polsl.pl [157.158.16.204]
over a maximum of 30 hops:
 0  LAPTOP-D3VQGJQ1 [192.168.1.103]
 1  192.168.1.1
 2  192.168.20.1
 3  10.10.10.1
 4  host-93.179.211.33.static.3s.pl [93.179.211.33]
 5  host892522062.techn.3s.pl [89.25.220.62]
 6  * * *
Computing statistics for 125 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0                                     LAPTOP-D3VQGJQ1 [192.168.1.103]
 1    0ms     0/ 100 = 0%     0/ 100 = 0%     192.168.1.1
 2    2ms     0/ 100 = 0%     0/ 100 = 0%     192.168.20.1
 3    2ms     0/ 100 = 0%     0/ 100 = 0%     10.10.10.1
 4    4ms     0/ 100 = 0%     0/ 100 = 0%     host-93.179.211.33.static.3s.pl [93.179.211.33]
 5    ---    100/ 100 =100%  0/ 100 = 0%     host892522062.techn.3s.pl [89.25.220.62]
Trace complete.
PS C:\Users\Kacper>
```

pathping ms.polsl.pl - jest to połączenie poleceń **ping** oraz **tracert**. Jest to śledzenie trasy z punktu a (mój komputer) do punktu b (witryna wydziału MS). Pingowany jest każdy węzeł. Na końcu wyświetlane są statystyki.

Polecenie ping

```
Windows PowerShell
PS C:\Users\Kacper> ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.
  -f           Set Don't Fragment flag in packet (IPv4-only).
  -i TTL       Time To Live.
  -v TOS       Type Of Service (IPv4-only. This setting has been deprecated
               and has no effect on the type of service field in the IP
               Header).
  -r count     Record route for count hops (IPv4-only).
  -s count     Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout   Timeout in milliseconds to wait for each reply.
  -R           Use routing header to test reverse route also (IPv6-only).
               Per RFC 5095 the use of this routing header has been
               deprecated. Some systems may drop echo requests if
               this header is used.
  -S srcaddr   Source address to use.
  -c compartment Routing compartment identifier.
  -p           Ping a Hyper-V Network Virtualization provider address.
  -4           Force using IPv4.
  -6           Force using IPv6.

PS C:\Users\Kacper>
```

ping -n count - ilość wykonywanych zapytań;

ping -a - zamienianie adresów na nazwy hostów;

ping -t - pinguj hosta aż do zatrzymania polecenia;

ping -6 - użycie IPv6;

Polecenie netstat

```
Windows PowerShell
PS C:\Users\Kacper> netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a           Displays all connections and listening ports.
-b           Displays the executable involved in creating each connection or
             listening port. In some cases well-known executables host
             multiple independent components, and in these cases the
             sequence of components involved in creating the connection
             or listening port is displayed. In this case the executable
             name is in [] at the bottom, on top is the component it called,
             and so forth until TCP/IP was reached. Note that this option
             can be time-consuming and will fail unless you have sufficient
             permissions.
-e           Displays Ethernet statistics. This may be combined with the -s
             option.
-f           Displays Fully Qualified Domain Names (FQDN) for foreign
             addresses.
-n           Displays addresses and port numbers in numerical form.
-o           Displays the owning process ID associated with each connection.
-p proto     Shows connections for the protocol specified by proto; proto
             may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
             option to display per-protocol statistics, proto may be any of:
             IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q           Displays all connections, listening ports, and bound
             nonlistening TCP ports. Bound nonlistening ports may or may not
             be associated with an active connection.
-r           Displays the routing table.
-s           Displays per-protocol statistics. By default, statistics are
             shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
             the -p option may be used to specify a subset of the default.
-t           Displays the current connection offload state.
-x           Displays NetworkDirect connections, listeners, and shared
             endpoints.
-y           Displays the TCP connection template for all connections.
             Cannot be combined with the other options.
interval     Redisplays selected statistics, pausing interval seconds
             between each display. Press CTRL+C to stop redisplaying
             statistics. If omitted, netstat will print the current
             configuration information once.

PS C:\Users\Kacper> |
```

netstat -e - statystyki dotyczące sieci;

netstat -a - wyświetlanie wszystkich portów;

netstat -f - wyświetlanie nazwy naszego urządzenia tak jak widzą go inni;

Polecenie nslookup

nslookup - wysłanie zapytania DNS do serwera. Jeśli serwer DNS nie zostanie sprecyzowany, polecenie automatycznie użyje tego, który jest skonfigurowany z Twoim interfejsem sieciowym, Istnieje jednak możliwość wymuszenia użycia innego serwera.



Polecenie netsh

Aby przypisać statyczny adres IP (192.168.1.1) o masce podsieci (255.255.255.0) i domyślnej bramie (192.168.1.0) dla interfejsu LAN należy w terminalu wpisać kolejno:

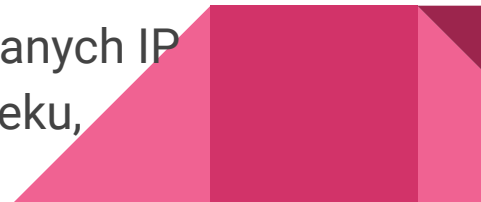
- netsh
- set address [name=]"LAN" [source=]{static [addr=]192.168.1.1 [mask=]255.255.255.0 [gateway=]192.168.1.0}



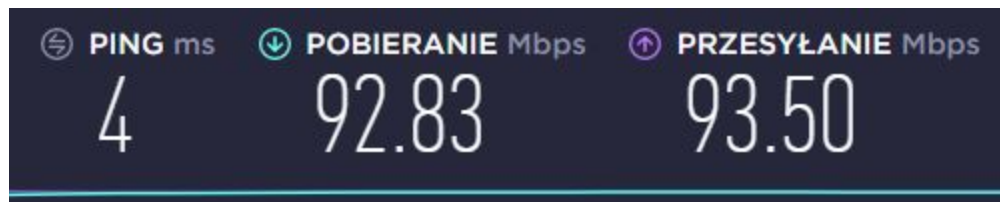
Zasadne użycie polecenia *tracert/traceroute*

Polecenie *tracert* (lub *traceroute* dla systemów Linux i UNIX) pozwala na zmapowanie ścieżki przesyłanej paczki, oraz - pośrednio- czas przejścia takiej ścieżki.

Za zasadne użycie powyższego polecenia uznałby sytuację gdzie:

- A. Ważny jest czas pomiędzy czynnościami - polecenie pozwala określić opóźnienie w przesyłaniu danych
 - B. Jest podejrzenie utraty danych - polecenie pozwala znaleźć punkt w którym ścieżka jest przerywana
 - C. Jest podejrzenie wycieku danych - polecenie, przy znanych IP z przed wycieku, umożliwia namierzenie punktu wycieku, jeśli taki jest w sieci
- 

Stanowisko pracy



Do czego może doprowadzić uruchomienie w laboratorium akademickim narzędzia do skanowania szerokiego zakresu adresów IP?

Uruchomienie takowego narzędzia, poprzez zmapowanie sieci w takim laboratorium umożliwi dostęp do informacji takich jak np. Adres IP, adres MAC, informacje o modelu i języku karty sieciowej wszystkich komputerów podpiętych do sieci.

W zależności od narzędzia i uprawnień, umożliwi to również zdalną kontrolę nad urządzeniem.



Dziękujemy za uwagę!

Piotr Domański, Kacper Grabiec, Maciej Krężel, Łukasz Myśliwiec

