PODSTAWY SIECI KOMPUTEROWYCH

SPRAWOZDANIE

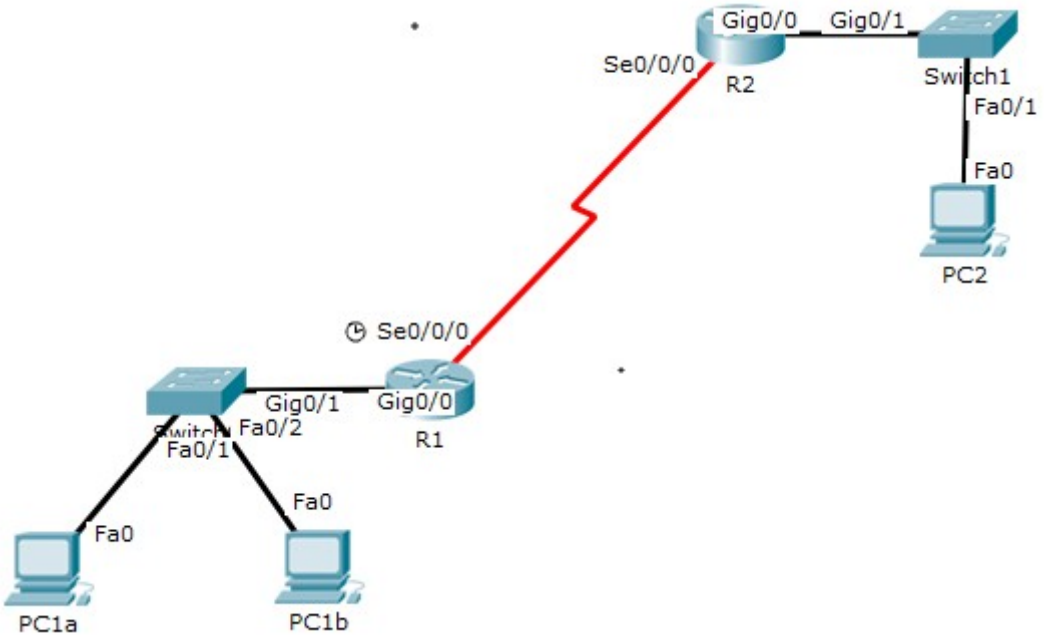
z realizacji zadania

Translacja adresów – NAT

Autor: posk_NAT_Michał_Gebel.odt

Wartości występujące w zadaniu: <I1>=37, <I2>=25, <I3>=79

Topologia



Schemat adresacji

Nazwa urządzenia	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	192.168.37.1	255.255.255.0	–
	S0/0/0 (DCE)	100.25.0.1	255.255.255.252	–
R2	G0/0	200.79.0.1	255.255.255.0	–
	S0/0/0	100.25.0.2	255.255.255.252	–
PC1a	ens33	192.168.37.2	24	R1
PC1b	ens33	192.168.37.4	24	R1
PC2	ens33	200.79.0.3	24	R2

1. Wykonaj podstawową konfigurację ruterów zgodnie z podaną wyżej topologią i schematem adresacji:

- Nadaj ruterom odpowiednie nazwy (hostname)
- Skonfiguruj interfejsy sieciowe, nadając im odpowiednie adresy IP (ip address) (w przypadku interfejsu szeregowego DCE ustaw szybkość taktowania np. na 57600 (clock rate)).
- Na ruterze R1 skonfiguruj trasę prowadzącą do podsieci 200.79.0.0 przez ruter R2. Dlaczego nie można zgodnie z zasadami skonfigurować analogicznie na ruterze R2 trasy do podsieci 192.168.37.0?

2. Zweryfikuj konfigurację wykonaną na obu ruterach poprzez:

- **Wyświetlenie konfiguracji i stanu interfejsów** (show ip interface brief).
- **Wyświetlenie tablic rutingu** (show ip route).
- **Przetestowanie łączności** pomiędzy ruterami w łączu szeregowym (ping).

```
R1#sh ip int b
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         192.168.37.1    YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
Serial0/0/0                100.25.0.1      YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
SM1/0                      unassigned      YES unset  administratively down down
SM1/1                      unassigned      YES unset  up                    up
Vlan1                      unassigned      YES unset  up                    up
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        100.25.0.0/30 is directly connected, Serial0/0/0
L        100.25.0.1/32 is directly connected, Serial0/0/0
      192.168.37.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.37.0/24 is directly connected, GigabitEthernet0/0
L        192.168.37.1/32 is directly connected, GigabitEthernet0/0
S     200.79.0.0/24 [1/0] via 100.25.0.2
R1#ping 100.25.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.25.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms

R2#sh ip int b
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         200.79.0.1      YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
Serial0/0/0                100.25.0.2      YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override

Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        100.25.0.0/30 is directly connected, Serial0/0/0
L        100.25.0.2/32 is directly connected, Serial0/0/0
      200.79.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.79.0.0/24 is directly connected, GigabitEthernet0/0
L        200.79.0.1/32 is directly connected, GigabitEthernet0/0
R2#ping 100.25.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.25.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
```

3. Wszystkim stacjom roboczym nadaj nazwy zgodne z tabelą (hostnamectl). Skonfiguruj statycznie adresy interfejsów enp0s33 stacji roboczych, przyjmując dowolne poprawne wartości x, y, z. **Przedstaw wyniki działania poleceń ip address show** oraz **ip route show**. **Przetestuj łączność między hostami a ruterami w segmentach Ethernet (ping).**

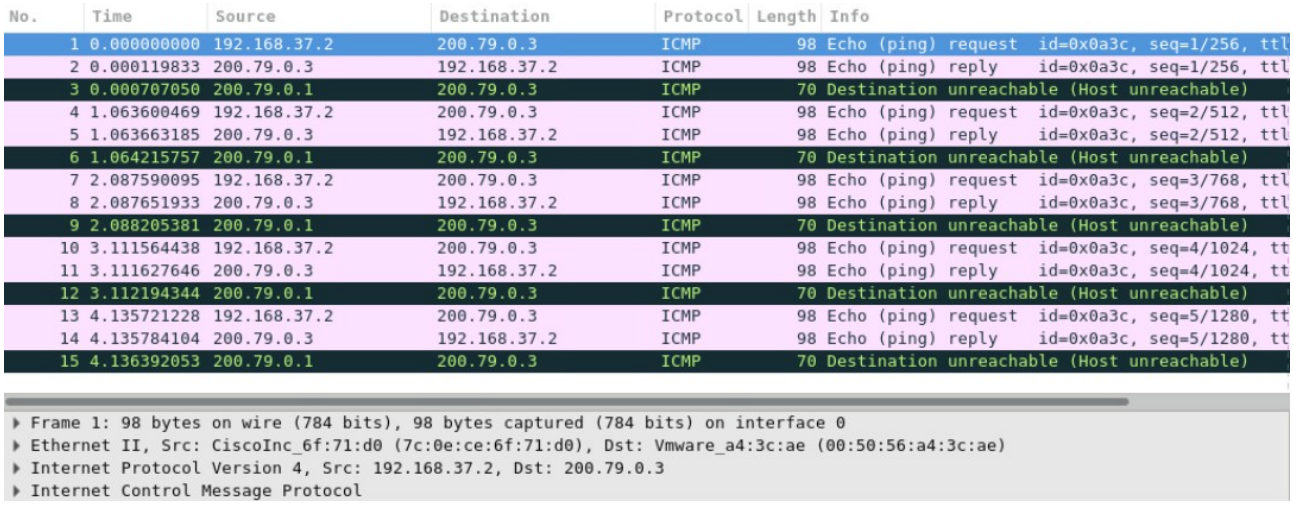
```
[root@PC1a lsk]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:a4:c1:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.2/24 brd 192.168.37.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::1e0b:b633:3e1f:cacf/64 scope link
       valid_lft forever preferred_lft forever
[root@PC1a lsk]# ip route show
default via 192.168.37.1 dev ens33  proto static  metric 100
192.168.37.0/24 dev ens33  proto kernel  scope link  src 192.168.37.2  metric 100
[root@PC1a lsk]# ping 192.168.37.1
PING 192.168.37.1 (192.168.37.1) 56(84) bytes of data.
64 bytes from 192.168.37.1: icmp_seq=1 ttl=255 time=1.22 ms
64 bytes from 192.168.37.1: icmp_seq=2 ttl=255 time=0.650 ms
64 bytes from 192.168.37.1: icmp_seq=3 ttl=255 time=0.569 ms
64 bytes from 192.168.37.1: icmp_seq=4 ttl=255 time=0.639 ms
64 bytes from 192.168.37.1: icmp_seq=5 ttl=255 time=0.647 ms
^C
--- 192.168.37.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4069ms
rtt min/avg/max/mdev = 0.569/0.746/1.229/0.245 ms
```

```
[root@PC1b lsk]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:a4:f5:bd brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.4/24 brd 192.168.37.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::a485:a899:244d:16e3/64 scope link
       valid_lft forever preferred_lft forever
[root@PC1b lsk]# ip route show
default via 192.168.37.1 dev ens33  proto static  metric 100
192.168.37.0/24 dev ens33  proto kernel  scope link  src 192.168.37.4  metric 100
[root@PC1b lsk]# ping 192.168.37.1
PING 192.168.37.1 (192.168.37.1) 56(84) bytes of data.
64 bytes from 192.168.37.1: icmp_seq=1 ttl=255 time=1.39 ms
64 bytes from 192.168.37.1: icmp_seq=2 ttl=255 time=0.594 ms
64 bytes from 192.168.37.1: icmp_seq=3 ttl=255 time=0.697 ms
^C
--- 192.168.37.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.594/0.896/1.398/0.358 ms
```

4. Na stacjach PC1a i PC2 włącz monitorowanie ruchu na interfejsach ens33 ograniczając wyświetlanie do komunikatów ICMP. **Dokonaj próby dostępności hosta PC2 z poziomu hosta PC1a**, z**aprezentuj historię komunikatów na obu hostach.** Dlaczego próba nie powiodła się?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=1/256, ttl=64 (no response
2	1.063617060	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=2/512, ttl=64 (no response
3	2.087592457	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=3/768, ttl=64 (no response
4	3.111649811	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=4/1024, ttl=64 (no respons
5	4.135743048	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=5/1280, ttl=64 (no respons

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_a4:c1:f0 (00:50:56:a4:c1:f0), Dst: CiscoInc_6f:79:00 (7c:0e:ce:6f:79:00)
▸ Internet Protocol Version 4, Src: 192.168.37.2, Dst: 200.79.0.3
▸ Internet Control Message Protocol
```

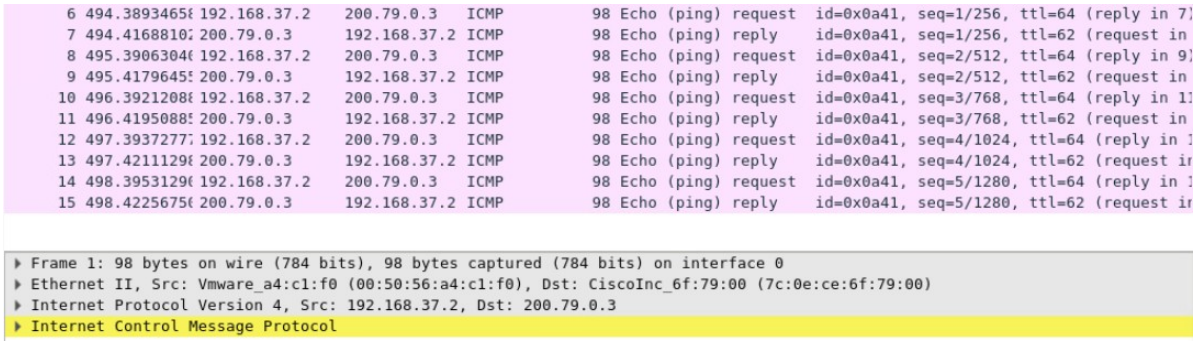


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=1/256, ttl
2	0.000119833	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a3c, seq=1/256, ttl
3	0.000707050	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
4	1.063600469	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=2/512, ttl
5	1.063663185	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a3c, seq=2/512, ttl
6	1.064215757	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
7	2.087590095	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=3/768, ttl
8	2.087651933	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a3c, seq=3/768, ttl
9	2.088205381	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
10	3.111564438	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=4/1024, tt
11	3.111627646	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a3c, seq=4/1024, tt
12	3.112194344	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
13	4.135721228	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a3c, seq=5/1280, tt
14	4.135784104	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a3c, seq=5/1280, tt
15	4.136392053	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)

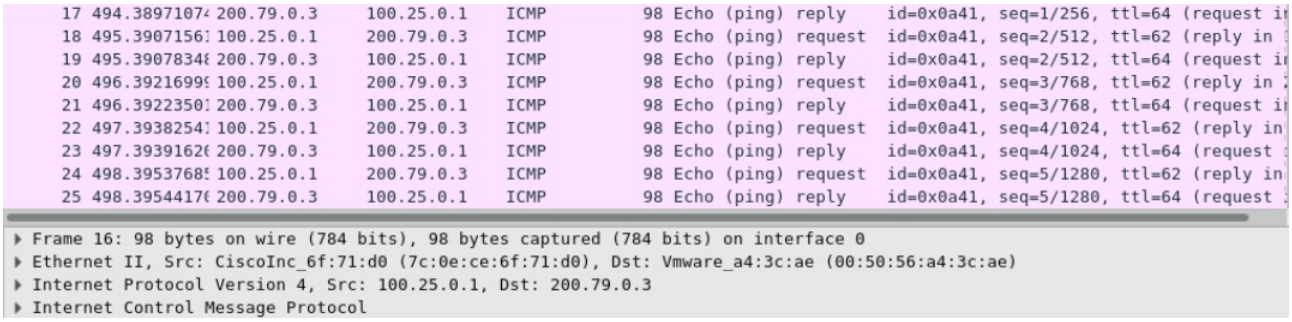
Próba nie powiodła się ponieważ trasa routingu jest skonfigurowana tylko w jedną stronę. Dlatego Odpowiedź nie może dotrzeć, ponieważ nie ma trasy.

5. Na ruterze R1 **skonfiguruj statyczną translację adresu źródłowego z adresu hosta PC1a na adres interfejsu szeregowego rutera R1 (tryb config, ip nat inside source static)**. Następnie **zadeklaruj interfejs ethernet rutera jako wewnętrzny, zaś interfejs szeregowy jako zewnętrzny w translacji (tryb interfejsu, ip nat inside/outside)**. Ponownie **dokonaj próby dostępności hosta PC2 z poziomu hosta PC1a**, z**aprezentuj historię komunikatów na obu hostach.**

```
R1(config)#ip nat inside source static 192.168.37.2 100.25.0.1
R1(config)#interface g0/0
R1(config-if)#ip nat inside
R1(config)#interface s0/0/0
R1(config-if)#ip nat outside
```



6	494.3893465	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=1/256, ttl=64 (reply in 7
7	494.4168810	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a41, seq=1/256, ttl=62 (request in
8	495.3906304	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=2/512, ttl=64 (reply in 9
9	495.4179645	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a41, seq=2/512, ttl=62 (request in
10	496.3921208	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=3/768, ttl=64 (reply in 1
11	496.4195088	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a41, seq=3/768, ttl=62 (request in
12	497.3937277	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=4/1024, ttl=64 (reply in 1
13	497.4211129	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a41, seq=4/1024, ttl=62 (request in
14	498.3953129	192.168.37.2	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=5/1280, ttl=64 (reply in 1
15	498.4225675	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) reply id=0x0a41, seq=5/1280, ttl=62 (request in



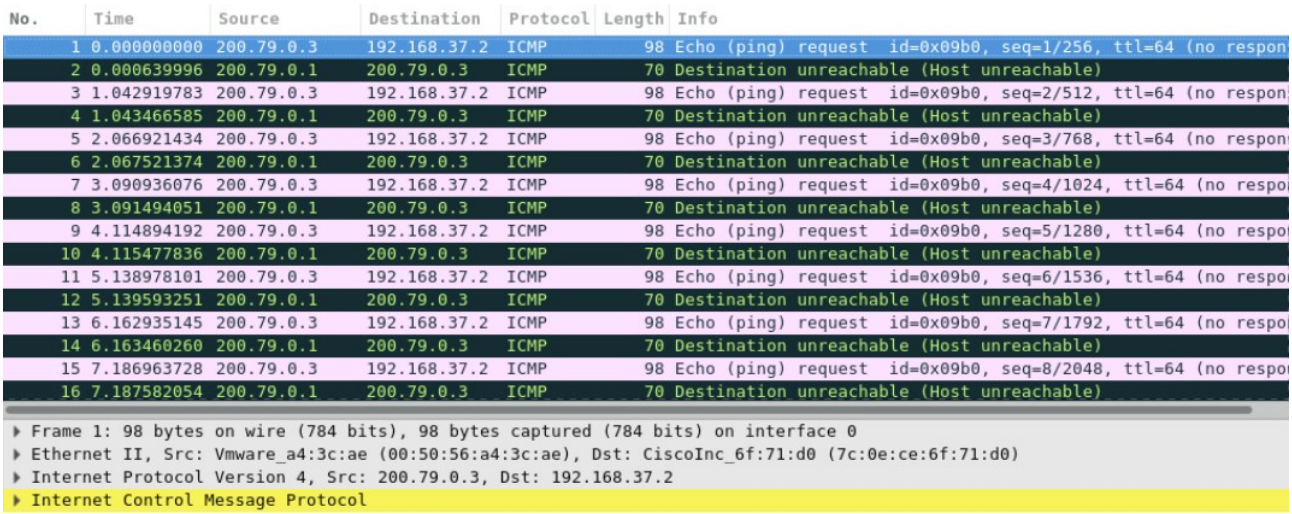
17	494.3897107	200.79.0.3	100.25.0.1	ICMP	98	Echo (ping) reply id=0x0a41, seq=1/256, ttl=64 (request i
18	495.3907156	100.25.0.1	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=2/512, ttl=62 (reply in
19	495.3907834	200.79.0.3	100.25.0.1	ICMP	98	Echo (ping) reply id=0x0a41, seq=2/512, ttl=64 (request i
20	496.3921699	100.25.0.1	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=3/768, ttl=62 (reply in
21	496.3922350	200.79.0.3	100.25.0.1	ICMP	98	Echo (ping) reply id=0x0a41, seq=3/768, ttl=64 (request i
22	497.3938254	100.25.0.1	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=4/1024, ttl=62 (reply in
23	497.3939162	200.79.0.3	100.25.0.1	ICMP	98	Echo (ping) reply id=0x0a41, seq=4/1024, ttl=64 (request
24	498.3953768	100.25.0.1	200.79.0.3	ICMP	98	Echo (ping) request id=0x0a41, seq=5/1280, ttl=62 (reply in
25	498.3954417	200.79.0.3	100.25.0.1	ICMP	98	Echo (ping) reply id=0x0a41, seq=5/1280, ttl=64 (request

6. W analogiczny do poprzednich punktów sposób **(próba dostępności hosta, historia komunikatów)** sprawdź, czy wprowadzone mapowanie statyczne działa niezależnie od tego, która strona (zewnętrzna czy wewnętrzna) jest inicjatorem konwersacji. **Następnie z poziomu hosta PC2 odwołaj się za pomocą przeglądarki do adresu interfejsu szeregowego rutera R1**. W wyświetlonej stronie zidentyfikuj wartość zdradzającą prywatny adres serwera. Po zakończeniu eksperymentu **usuń mapowanie statyczne wprowadzone w poprzednim punkcie (no ip nat…)** pozostawiając konfigurację interfejsów jako zewnętrzny i wewnętrzny.

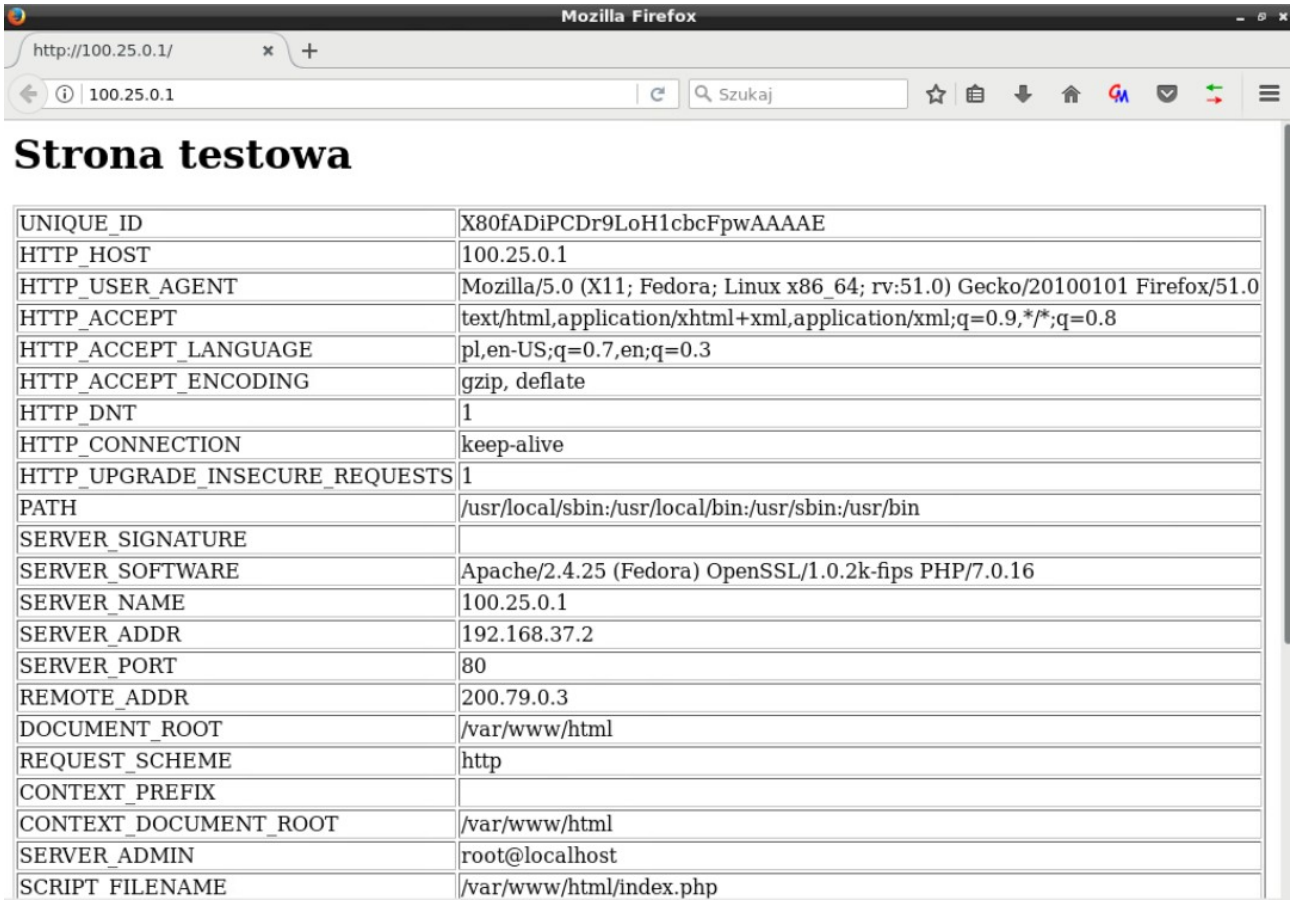
PC1a

No.	Time	Source	Destination	Protocol	Length	Info

PC2



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=1/256, ttl=64 (no respon
2	0.000639996	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
3	1.042919783	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=2/512, ttl=64 (no respon
4	1.043466585	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
5	2.066921434	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=3/768, ttl=64 (no respon
6	2.067521374	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
7	3.090936076	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=4/1024, ttl=64 (no respo
8	3.091494051	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
9	4.114894192	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=5/1280, ttl=64 (no respo
10	4.115477836	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
11	5.138978101	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=6/1536, ttl=64 (no respo
12	5.139593251	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
13	6.162935145	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=7/1792, ttl=64 (no respo
14	6.163460260	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)
15	7.186963728	200.79.0.3	192.168.37.2	ICMP	98	Echo (ping) request id=0x09b0, seq=8/2048, ttl=64 (no respo
16	7.187582054	200.79.0.1	200.79.0.3	ICMP	70	Destination unreachable (Host unreachable)




```
R1(config)#no ip nat inside source static 192.168.37.2 100.25.0.1
```

7. Na ruterze R1 **zdefiniuj pulę adresów** które będą uprawnione do korzystania z dynamicznej translacji adresu źródłowego (tryb config, access-list <numer> permit ip <podsieć> <maska_hosta> any; znaczenie parametrów: <numer> - arbitralny numer listy, <podsieć> - podsieć adresów, które będą poddawane translacji, <maska_hosta> odpowiednik maski podsieci jednak wskazujący część adresu IP należącą do hosta). Następnie **skonfiguruj translację dynamiczną** (ip nat inside source list <numer> interface <interfejs>). Wartości <podsieć>, <maska_hosta> i <interfejs> dobierz mając na uwadze jakie adresy źródłowe mają być poddawane translacji i którym interfejsem poddane translacji pakiety będą opuszczać ruter R1. Z poziomu hostów PC1a oraz PC1b dokonaj próby dostępności hosta PC2 (ping). **Na ruterze R1 wyświetl tablicę aktualnych translacji** (show ip nat translations). Poprzez próbę **odwołania się za pomocą przeglądarki z poziomu hosta PC2 do adresu interfejsu szeregowego rutera R1** sprawdź, czy mapowanie dynamiczne również działa niezależnie od tego, która strona (zewnętrzna czy wewnętrzna) jest inicjatorem konwersacji.

```
R1(config)#access-list 1 permit 192.168.37.0 0.0.0.255
R1(config)#do show access-lists
Standard IP access list 1
    10 permit 192.168.37.0, wildcard bits 0.0.0.255
R1(config)#ip nat inside source list 1 interface s0/0/0
R1(config)#do sh ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
icmp 100.25.0.1:2665   192.168.37.2:2665  200.79.0.3:2665    200.79.0.3:2665
icmp 100.25.0.1:2299   192.168.37.4:2299  200.79.0.3:2299    200.79.0.3:2299
```

```
[root@PC1a lsk]# ping -c 20 200.79.0.3
PING 200.79.0.3 (200.79.0.3) 56(84) bytes of data.
64 bytes from 200.79.0.3: icmp_seq=1 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=2 ttl=62 time=27.4 ms
64 bytes from 200.79.0.3: icmp_seq=3 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=4 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=5 ttl=62 time=27.4 ms
64 bytes from 200.79.0.3: icmp_seq=6 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=7 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=8 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=9 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=10 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=11 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=12 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=13 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=14 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=15 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=16 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=17 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=18 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=19 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=20 ttl=62 time=27.2 ms

--- 200.79.0.3 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19026ms
rtt min/avg/max/mdev = 27.104/27.254/27.490/0.237 ms
```

```
[root@PC1b lsk]# ping -c 20 200.79.0.3
PING 200.79.0.3 (200.79.0.3) 56(84) bytes of data.
64 bytes from 200.79.0.3: icmp_seq=1 ttl=62 time=27.5 ms
64 bytes from 200.79.0.3: icmp_seq=2 ttl=62 time=27.4 ms
64 bytes from 200.79.0.3: icmp_seq=3 ttl=62 time=27.5 ms
64 bytes from 200.79.0.3: icmp_seq=4 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=5 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=6 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=7 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=8 ttl=62 time=27.4 ms
64 bytes from 200.79.0.3: icmp_seq=9 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=10 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=11 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=12 ttl=62 time=27.2 ms
64 bytes from 200.79.0.3: icmp_seq=13 ttl=62 time=27.0 ms
64 bytes from 200.79.0.3: icmp_seq=14 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=15 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=16 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=17 ttl=62 time=27.3 ms
64 bytes from 200.79.0.3: icmp_seq=18 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=19 ttl=62 time=27.1 ms
64 bytes from 200.79.0.3: icmp_seq=20 ttl=62 time=27.1 ms

--- 200.79.0.3 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19027ms
rtt min/avg/max/mdev = 27.056/27.342/27.587/0.192 ms
```

8. Na hoście PC2 włącz monitorowanie ruchu na interfejsie ens33 ograniczając wyświetlanie do segmentów TCP. **Za pomocą programu ncat nawiąż (i pozostaw) połączenia z hostów PC1a oraz PC1b z serwerem HTTP działającym na hoście PC2**, w obu przypadkach jawnie określając ten sam port źródłowy. **Przedstaw historię komunikacji** i przeanalizuj porty źródłowe połączeń z perspektywy hosta PC2. **Na ruterze R1 wyświetl tablicę aktualnych translacji** (show ip nat translations). Jak uzasadnisz powstałą zmianę portu?

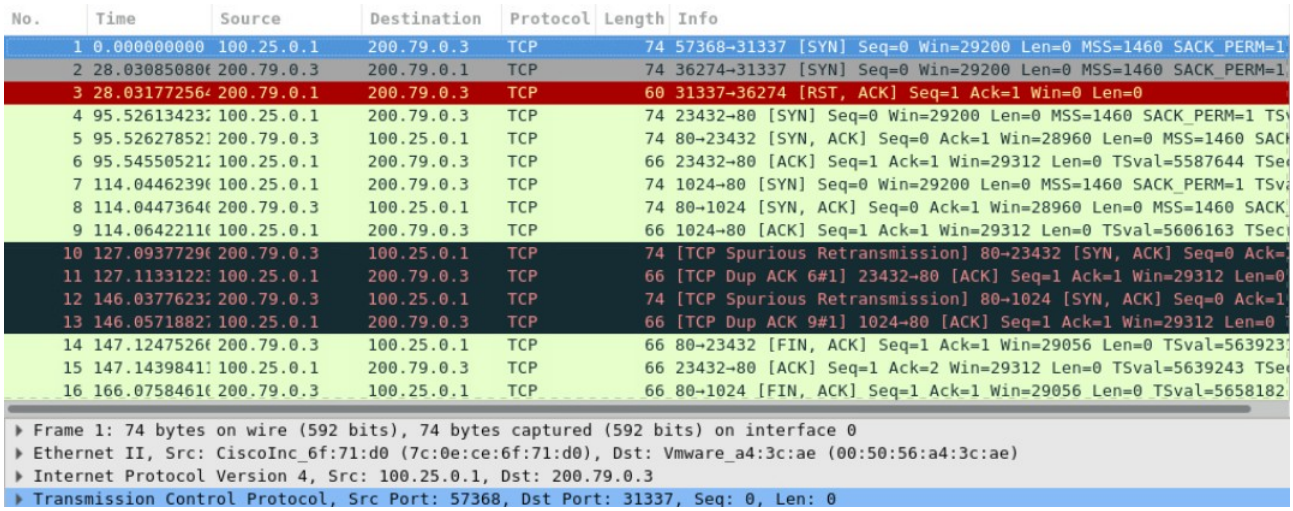
PC1a

```
[root@PC1a lsk]# ncat 200.79.0.3 80 -p23432
```

PC1b

```
[root@PC1b lsk]# ncat 200.79.0.3 80 -p23432
```

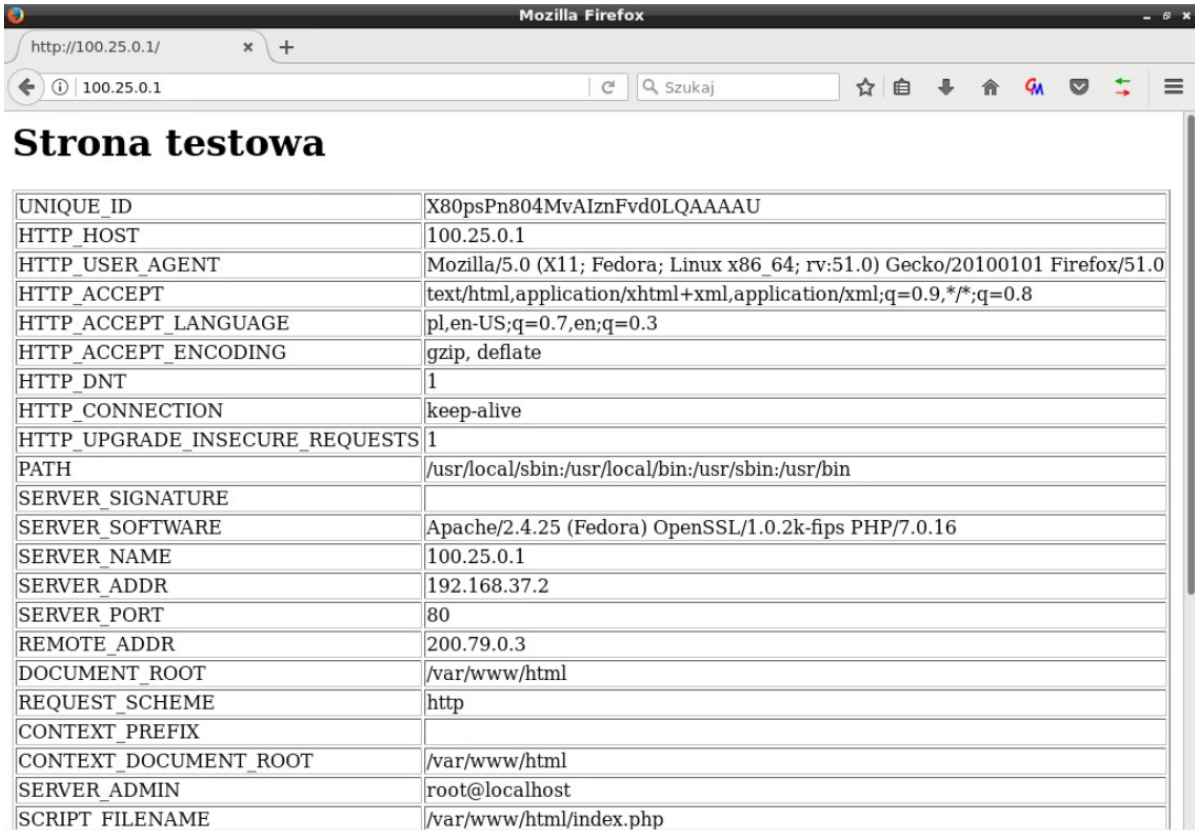
PC2




```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.25.0.1:23432   192.168.37.2:23432 200.79.0.3:80      200.79.0.3:80
tcp 100.25.0.1:1024    192.168.37.4:23432 200.79.0.3:80      200.79.0.3:80
```

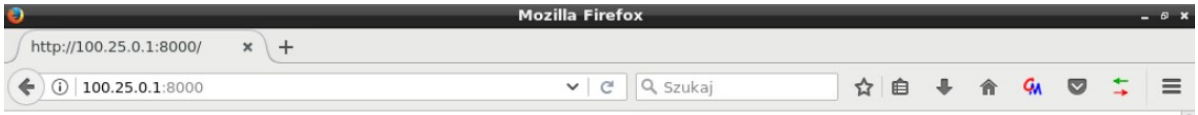
9. Na ruterze R1 **skonfiguruj statyczną translację dla protokołu TCP, z adresu hosta PC1a i portu 80 na adres interfejsu szeregowego rutera R1 i port 80 oraz z adresu hosta PC1b i portu 80 na adres interfejsu szeregowego rutera R1 i port 8000** (tzw. port forwarding)(tryb config, ip nat inside source static tcp). **Wyświetl wprowadzone translacje** (show ip nat translations). **Następnie z poziomu hosta PC2 odwołaj się za pomocą przeglądarki do adresu interfejsu szeregowego rutera R1 i portu domyślnego 80, a także portu 8000**. W wyświetlanych stronach zidentyfikuj wartości zdradzające prywatne adresy serwerów.

```
R1(config)#ip nat inside source static tcp 192.168.37.2 80 100.25.0.1 80
R1(config)#ip nat inside source static tcp 192.168.37.4 80 100.25.0.1 8000
R1(config)#do sh ip nat tr
Pro Inside global      Inside local       Outside local      Outside global
tcp 100.25.0.1:80      192.168.37.2:80    ---                ---
tcp 100.25.0.1:23432   192.168.37.2:23432 200.79.0.3:80      200.79.0.3:80
tcp 100.25.0.1:8000    192.168.37.4:80    ---                ---
tcp 100.25.0.1:1024    192.168.37.4:23432 200.79.0.3:80      200.79.0.3:80
```



Strona testowa

UNIQUE_ID	X80psPn804MvAIznFvd0LQAAAAU
HTTP_HOST	100.25.0.1
HTTP_USER_AGENT	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	pl,en-US;q=0.7,en;q=0.3
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_DNT	1
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
SERVER_SIGNATURE	
SERVER_SOFTWARE	Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips PHP/7.0.16
SERVER_NAME	100.25.0.1
SERVER_ADDR	192.168.37.2
SERVER_PORT	80
REMOTE_ADDR	200.79.0.3
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	
CONTEXT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	root@localhost
SCRIPT_FILENAME	/var/www/html/index.php



Strona testowa

UNIQUE_ID	X80pyC0COqOALoU@Wz00jwAAAAA
HTTP_HOST	100.25.0.1:8000
HTTP_USER_AGENT	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:51.0) Gecko/20100101 Firefox/51.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	pl,en-US;q=0.7,en;q=0.3
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_DNT	1
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
SERVER_SIGNATURE	
SERVER_SOFTWARE	Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips PHP/7.0.16
SERVER_NAME	100.25.0.1
SERVER_ADDR	192.168.37.4
SERVER_PORT	8000
REMOTE_ADDR	200.79.0.3
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	
CONTEXT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	root@localhost
SCRIPT_FILENAME	/var/www/html/index.php