

Warsztaty z Sieci komputerowych

Lista 5

Konfiguracja początkowa

- ▶ Utwórz maszynę *Virbian0* z domyślną konfiguracją sieciową (jedna wirtualna karta sieciowa podłączona przez NAT z kartą fizyczną komputera). Po uruchomieniu maszyny poleceniem `ip` zmień nazwę interfejsu sieciowego na `enp0`.
- ▶ Utwórz cztery maszyny *Virbian1*–*Virbian4*, każdą z jedną kartą sieciową połączoną z wirtualną siecią `local0`. Nie uruchamiaj jeszcze tych maszyn.

Tutorial #1

W tej części przyjrzymy się bliżej protokołowi DHCP.

- ▶ Uruchom Wiresharka i włącz w nim obserwację interfejsu sieciowego `enp0`. Pobierz konfigurację sieciową poleceniem

```
#> dhclient enp0
```

Jakie komunikaty zostają wymienione pomiędzy Twoim komputerem a serwerem DHCP? Zauważ, że DHCP posługuje się protokołami UDP i IP. Jaki jest źródłowy adres IP wysyłanego pakietu, skoro w momencie jego wysyłania *Virbian0* nie ma jeszcze IP?

- ▶ Usuń konfigurację interfejsu `enp0` poleceniem

```
#> dhclient -r enp0
```

Informuje to serwer DHCP, że nie będziemy już używać otrzymanego uprzednio adresu IP (sprawdź to w Wiresharku) i zatrzymuje program `dhclient`.

- ▶ Dezaktywuj kartę `enp0` poleceniem `ip link` i wyłącz maszynę *Virbian0*.

Tutorial #2

W tej części przyjrzymy się dokładniej warstwie łącza danych i współpracy pomiędzy tą warstwą a warstwą sieciową.

- ▶ Uruchom maszyny *Virbian1* i *Virbian2* (połączone siecią `local0`). W obu maszynach zmień nazwę karty sieciowej na `enp0`.

- Aktywuj interfejsy `enp0` obu maszyn i przypisz im adresy IP równe odpowiednio `192.168.0.1/24` i `192.168.0.2/24`. Na każdej maszynie uruchom Wiresharka.

Uwaga: W Wiresharku włącz obserwację *wyłącznie* interfejsu `enp0`; w przeciwnym przypadku podgląd warstwy łącza danych będzie utrudniony.

- Poleceniem `ip link` wyświetl adresy MAC kart sieciowych na obu maszynach. Z maszyny *Virbian1* pingnij maszynę *Virbian2* i obejrzyj przesyłane ramki w Wiresharku. Jakie są pola nadawcy i odbiorcy ramki ethernetowej? A jakie są pola nadawcy i odbiorcy zawartego w niej pakietu IP?
- Z maszyny *Virbian1* pingnij adres rozgłoszeniowy `192.168.0.255`. Jakie są tym razem pola nadawcy i odbiorcy ramki ethernetowej? A jakie są pola nadawcy i odbiorcy zawartego w niej pakietu IP?
- W maszynie *Virbian1* obejrzyj tablicę ARP poleceniem

```
V1$> ip neigh
```

i usuń z niej wszystkie wpisy poleceniem

```
V1#> ip neigh flush all
```

Wykonaj to samo polecenie w maszynie *Virbian2*.

- Z maszyny *Virbian1* pingnij maszynę *Virbian2*. W Wiresharku zaobserwuj, że maszyna najpierw wysyła zapytanie ARP, otrzymuje na nie odpowiedź, a następnie wysyła komunikaty *ICMP echo* i otrzymuje na nie odpowiedzi. Jak zmienił się stan tablicy ARP obu maszyn?
- Przyjrzyj się dokładniej przesyłanemu w poprzednim punkcie zapytaniu i odpowiedzi ARP. Odpowiedz na następujące pytania:
 - ▷ Co jest danymi ramki w przypadku zapytań ARP?
 - ▷ Czy zapytania ARP są wysyłane do konkretnego komputera czy na adres rozgłoszeniowy?
 - ▷ Czy odpowiedzi ARP są wysyłane do konkretnego komputera czy na adres rozgłoszeniowy?

Tutorial #3

Poniższe zadanie ilustruje bezstanowość protokołów i przekazywanie danych pomiędzy warstwami protokołów. Wykorzystamy dwie skonfigurowane w poprzednim zadaniu maszyny *Virbian1* i *Virbian2* połączone interfejsami `enp0` z adresami IP z poprzedniego tutorialu.

- Na maszynie *Virbian1* uruchom polecenie

```
V1$> ping 192.168.0.2
```

i pozostaw je działające. W Wiresharku zaobserwuj komunikaty *ICMP echo request* wysłane przez maszynę *Virbian1* i odpowiedzi *ICMP echo reply* generowane przez maszynę *Virbian2*.

- Na maszynie *Virbian2* zmień adres IP na 192.168.0.123 poleceniem

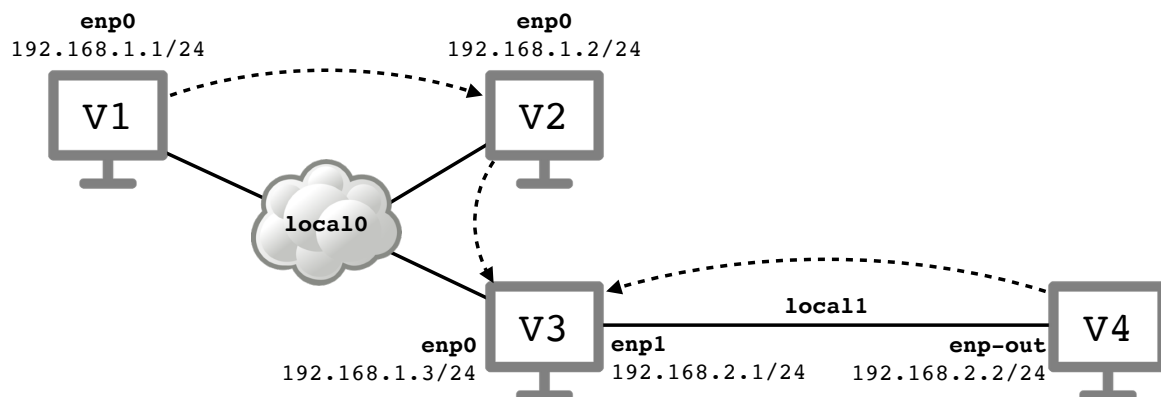
```
V2#> ip addr del 192.168.0.2/24 dev enp0 && sleep 0.1 && ip addr add 192.168.0.123/24 dev enp0
```

Uwaga: wykonaj powyższe polecenie tak, jak jest napisane, tj. nie powinno być za dużego odstępu czasowego pomiędzy powyższymi dwoma wywołaniami polecenia `ip addr`.

- Po paru sekundach wyłącz działanie polecenia `ping` na maszynie *Virbian1*. Zaobserwuj przesłane pakiety w Wiresharku. Postaraj się samodzielnie zrozumieć, co się wydarzyło, a następnie przeczytaj wyjaśnienie poniżej.
 - ▷ Po zmianie adresu interfejsu `enp0` maszyny *Virbian2*, *Virbian1* wysłał kolejny pakiet *ICMP echo request* do już nieistniejącego adresu IP 192.168.0.2. Na podstawie swojej lokalnej tablicy ARP w adresie docelowym ramki wpisał adres MAC karty sieciowej maszyny *Virbian2*.
 - ▷ Włożony w ramkę pakiet *ICMP echo request* dotarł do maszyny *Virbian2*. Maszyna *Virbian2* stwierdziła, że ramka jest zaadresowana do jej adresu MAC i zatem przekazała jej zawartość (komunikat ICMP) do dalszego przetworzenia do warstwy sieciowej.
 - ▷ Na poziomie warstwy sieciowej okazało się, że komunikat ICMP nie jest skierowany do maszyny *Virbian2*, bo docelowy adres IP pakietu to 192.168.0.2, zaś obecnym adresem maszyny *Virbian2* jest już 192.168.0.123.
 - ▷ Taka sytuacja dla routera nie jest niczym niecodziennym i maszyna *Virbian2* postanowiła przekazać pakiet dalej (do adresu IP 192.168.0.2). Na podstawie tablicy routingu maszyna ustaliła, że powinien on zostać przesłany przez interfejs `enp0`.
 - ▷ Żeby utworzyć odpowiednią ramkę maszyna *Virbian2* potrzebuje mapowania adresu 192.168.0.2 na odpowiedni adres MAC. Wszystkie mapowania zostały usunięte z tablicy ARP maszyny *Virbian2* w momencie zmiany adresu IP, więc musi ona w tym celu wysłać odpowiednie zapytanie ARP o treści „Kto ma adres 192.168.0.2? Niech odpowie maszynie 192.168.0.123”. Oczywiście nikt na takie zapytanie nie odpowiada.
 - ▷ Jednocześnie maszyna *Virbian2* zauważyła nieprawidłowość: musiała właśnie przekazać pakiet do tej samej sieci, z której przyszedł. Maszyna *Virbian2* założyła, że w tablicy routingu *Virbian1* znajduje się nieoptymalny wpis „pakiety skierowane do 192.168.0.2 wysyłaj przez 192.168.0.123”. Dlatego też postanowiła powiadomić maszynę *Virbian1* (komunikatem *ICMP redirect*) o konieczności poprawy tablicy routingu.
- Usunąć adresy IP przypisane do maszyn *Virbian1* i *Virbian2*.

Wyzwanie #1

Twoim celem jest konfiguracja adresów i routingu dla topologii sieci przedstawionej na rysunku poniżej.



- Skonfiguruj 4 maszyny wirtualne *Virbian1* – *Virbian4*, tak aby korzystały z sieci *local0* i *local1*, tak jak zaznaczono na rysunku powyżej. Nazwij ich interfejsy tak jak na rysunku (*enp0*, *enp1* i *enp-out*).
- Przypisz trzem interfejsom podłączonym do wirtualnej sieci *local0* adresy z sieci 192.168.1.0/24 takie jak na rysunku. Przypisz dwóm interfejsom podłączonym do wirtualnej sieci *local1* adresy z sieci 192.168.2.0/24 takie jak na rysunku.
- Poleceniem `ping` sprawdź wzajemną osiągalność maszyn podłączonych do tej samej sieci *local0* i maszyn podłączonych do tej samej sieci *local1*.
- Na maszynach *Virbian1*, *Virbian2* i *Virbian4* dodaj trasy domyślne, które na rysunku powyżej zaznaczone są przerywanymi strzałkami. Przykładowo trasa domyślna z maszyny *Virbian2* powinna prowadzić przez adres 192.168.1.3.
- Włącz Wiresharka na wszystkich maszynach. Następnie z maszyny *Virbian1* pingnij maszynę *Virbian4*. Zaobserwuj, że maszyna jest osiągalna, ale oprócz komunikatów *ICMP reply* maszyna *Virbian1* otrzymuje również komunikaty *ICMP redirect*. Są one wysyłane przez maszynę *Virbian2* i informują o tym, że routing na maszynie *Virbian1* jest prawdopodobnie źle skonfigurowany. Odpowiedz na następujące pytania:
 - ▷ Jaka jest sugerowana przez maszynę *Virbian2* modyfikacja tablicy routingu na maszynie *Virbian1*?
 - ▷ Dlaczego taka zmiana ma sens?
 - ▷ W jaki sposób maszyna *Virbian2* mogła wykryć powyższy problem?

Materiały do kursu znajdują się w systemie SKOS: <https://skos.ii.uni.wroc.pl/>.

Marcin Bieńkowski