Warsztaty z Sieci komputerowych
Lista 5

Przed zajęciami

- 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*. 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: 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 do końca tego zadania. 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 && 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`.

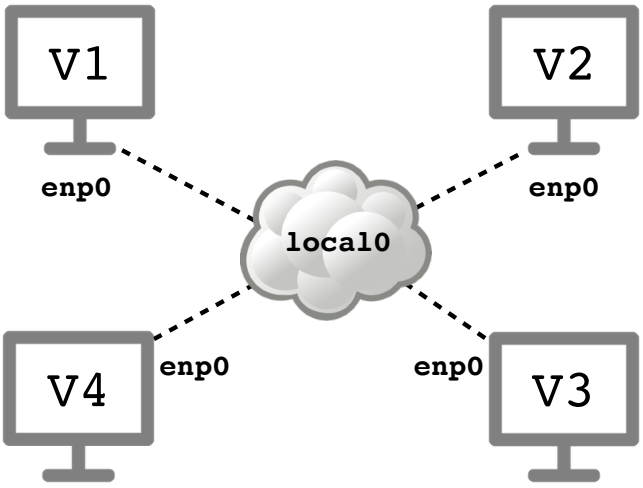
- Po paru sekundach wyłącz działanie polecenia `ping` na maszynie *Virbian1*. Zaobserwuj przesłane pakiety w Wiresharku. Postaraj się samodzielnie zrozumieć, co się wydarzyło, a następnie przeczytaj wyjaśnienie poniżej.

  - 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, wiec 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.

- Usuń adresy IP przypisane do maszyn *Virbian1* i *Virbian2*.

Wyzwanie #1

Uruchom dwie dodatkowe maszyny wirtualne *Virbian3* i *Virbian4*. Zmień nazwę ich kart sieciowych na `enp0` otrzymując konfigurację z poniższego rysunku.



W tej części sprawdzimy, do czego prowadzi mieszanie wielu sieci IP w jednej sieci Ethernet. Włącz na maszynach Wiresharka, jeśli jeszcze nie jest włączony.

- Przypisz interfejsom `enp0` maszyn wirtualnych następujące adresy:
  - *Virbian1*: `192.168.1.1/24`
  - *Virbian2*: `192.168.1.2/25`
  - *Virbian3*: `192.168.1.129/24`
  - *Virbian4*: `192.168.1.130/25`
- Zauważ, że maszyny leżą w jednej sieci warstwy drugiej, ale w trzech różnych podsieciach IP (różnych sieciach warstwy trzeciej). Jakie są zakresy adresów tych sieci?
- Z maszyny *Virbian1* pingnij jej adres rozgłoszeniowy, a następnie odpowiedz na następujące pytania:
  - Które maszyny otrzymały komunikat *ICMP echo request*? Które nie otrzymały i dlaczego?
  - Które maszyny wysłały w odpowiedzi komunikat *ICMP echo reply*? Które nie wysłały i dlaczego?
  - Które odpowiedzi dotarły do maszyny *Virbian1*? Które nie dotarły i dlaczego?
- Wykonaj powyższy punkt, ale z maszyny *Virbian2*, z maszyny *Virbian3*, a na końcu z maszyny *Virbian4*.
- Zdekonfiguruj interfejsy `enp0` i wyłącz wszystkie maszyny.

Materiały do kursu znajdują się w systemie Canvas: https://canvas.ii.uni.wroc.pl/.

Marcin Bieńkowski