

Warsztaty nr 5 z Sieci komputerowych

Konfiguracja początkowa

Utwórz i uruchom maszyny *Virbian1* i *Virbian2*. Każda z nich powinna mieć jedną kartę sieciową połączoną z siecią `local0`. W obu maszynach zmień nazwę interfejsu sieciowego na `en0` i aktywuj te interfejsy.

Tutorial 1

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

- ▶ Na maszynach *Virbian1* i *Virbian2* przypisz interfejsom `en0` 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 `en0`; w przeciwnym przypadku podgląd warstwy łącza danych nie będzie możliwy.

- ▶ Poleceniem `ip link` wyświetl adresy MAC interfejsów 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?
- ▶ Odpowiedz na pytania z poprzedniego punktu, ale tym razem pingając z maszyny *Virbian1* adres rozgłoszeniowy `192.168.0.255`.
- ▶ Na 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 na 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 Request* i otrzymuje na nie odpowiedzi. Jak zmienił się stan tablicy ARP obu maszyn?
- ▶ Przyjrzyj się dokładniej zapytaniu i odpowiedzi ARP, które zostały przesłane w poprzednim punkcie. 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?
- ▶ Zauważ, że po zakończeniu pingania (albo też podczas niego) maszyna *Virbian1* wysyła również zapytania ARP. Czy te dodatkowe zapytania są wysyłane do konkretnego komputera czy na adres rozgłoszeniowy? A odpowiedzi na nie?

Tutorial 2

Poniższe zadanie ilustruje bezstanowość protokołów i przekazywanie danych pomiędzy warstwami protokołów.

- ▶ 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 en0 && sleep 0.1 && \  
ip addr add 192.168.0.123/24 dev en0
```

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 `en0` 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 interfejsu sieciowego 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 `en0`.
 - ▶ Żeby utworzyć odpowiednią ramkę maszyna *Virbian2* potrzebuje przekształcić 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.

Tutorial 3

W tej części przyjrzymy się podstawom protokołu IPv6. Wykorzystamy maszyny *Virbian1* i *Virbian2* połączone siecią *local0* z poprzednich tutoriali. Usuń adresy IPv4 z interfejsów *en0* i dezaktywuj je poleceniami

```
V#> ip addr flush dev en0
V#> ip link set down dev en0
```

Upewnij się, że działające na tych maszynach Wiresharki obserwują wyłącznie interfejs *en0*. Najlepiej nie wyłączaj ich — zapisane w nich pakiety IPv4 przydadzą się nam do porównania.

- ▶ Aktywuj interfejsy *en0* na obu maszynach.
- ▶ Poleceniem `ip addr`, sprawdź, że do interfejsu *en0* został automatycznie przypisany adres IPv6 z sieci `fe80::/64` (tzw. adres *link-local*).¹
 - ▶ Jaki jest ten adres?
 - ▶ Porównaj go z adresem MAC interfejsu sieciowego. W jaki sposób adres link-local jest z niego wprowadzony?

- ▶ Poleceniem

```
V$> ip -6 route
```

sprawdź, że do tablicy routingu został dodany wpis mówiący, że sieć `fe80::/64` jest osiągalna przez interfejs *en0*.

- ▶ Z maszyny *Virbian1* pingnij adres link-local maszyny *Virbian2*. Dla takich adresów docelowych konieczne będzie podanie interfejsu:

```
V1$> ping adres_V2%en0
```

W Wiresharku zaobserwuj komunikaty *Echo Request* i *Echo Reply* protokołu ICMPv6.

- ▶ Jakie są warstwy tych komunikatów? Czy ICMPv6 jest enkapsulowany w pakietach IPv6, IPv4 czy też bezpośrednio w ramach?
- ▶ Zwróć uwagę na wszystkie pola ramki ethernetowej. Czy różnią się czymś od ramek wykorzystywanych w przypadku pingowania adresów IPv4?
- ▶ Obejrzyj dokładnie nagłówek IPv6 i porównaj go z nagłówkiem IPv4 z poprzednich tutoriali. Jakie są adresy IP nadawcy i odbiorcy pakietu? Czym zostało zastąpione pole TTL w IPv6? W których wersjach protokołu IP jest pole sumy kontrolnej?
- ▶ Zwróć uwagę, że przed komunikatami *Echo Request* i *Echo Reply* pojawiły się komunikaty *Neighbor Solicitation* i *Neighbor Advertisement* protokołu ICMPv6 będące odpowiednikami komunikatów ARP. Odpowiedz na następujące pytania:
 - ▶ Na jaki adres docelowy warstwy sieciowej wysyłany jest komunikat *Neighbor Solicitation*? Czy jest to adres unicastowy czy multicastowy? (Pamiętaj, że w przypadku IPv6 nie ma adresów rozgłoszeniowych). Porównaj ten komunikat z zapytaniami ARP z pierwszego tutoriala.
 - ▶ Na jaki adres docelowy warstwy łącza danych wysyłany jest ten komunikat?

¹Adresy link-local są odpowiednikiem adresów `169.254.0.0/16` przypisywanych automatycznie przez protokół DHCP w przypadku braku łączności z serwerem DHCP.

- ▶ Na jaki adres (warstwy sieciowej i łącza danych) wysyłana jest odpowiedź *Neighbor Advertisement*?
 - ▶ Wyświetl tablicę sąsiadów (odpowiednik tablicy ARP) poleceniem


```
V$> ip -6 neigh
```
 - ▶ Pingnij adres multicastowy `ff02::1` (odpowiednik adresu rozgłoszeniowego dla całej sieci lokalnej) poleceniem


```
V$> ping ff02::1%en0
```
- Kto odpowiada na takie zapytanie? Ponownie obejrzyj te pakiety w Wiresharku zwracając uwagę na adresy warstwy sieciowej i łącza danych.
- ▶ Dezaktywuj interfejsy `en0` i wyłącz maszyny *Virbian1* i *Virbian2*.

Tutorial 4

W tej części przyjrzymy się bliżej protokołowi DHCP i części protokołu ICMPv6 wykorzystywanemu do bezstanowej konfiguracji adresów IPv6. W przypadku maszyny wirtualnej taka konfiguracja sieci dostarczana jest przez Virtualboksa.

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 `en0`. Uruchom Wiresharka i włącz w nim obserwację wszystkich interfejsów sieciowych.
- ▶ Aktywuj interfejs `en0` poleceniem `ip link` i sprawdź, że został do niego przypisany adres link-local protokołu IPv6 (z sieci `fe80::/64`) oraz drugi adres IPv6 z zakresu `fd00::/8` (z tzw. puli adresów *unique local*). Zignoruj chwilowo ten drugi adres i komunikaty ICMPv6 wyświetlane w Wiresharku; zajmiemy się nimi za chwilę.
- ▶ Pobierz konfigurację sieciową IPv4 poleceniem

```
V0#> dhcpcd --noipv6rs en0
```

Opcja `--noipv6rs` powoduje, że wykorzystany będzie tylko protokół DHCP, a konfiguracja IPv6 zostanie pozostawiona jądru.

- ▶ Ponownie wyświetl adresy IP przypisane do interfejsu `en0`. Powinien mieć on teraz dodatkowo prywatny adres IPv4.²
- ▶ W Wiresharku przyjrzyj się komunikatom wymienione pomiędzy maszyną *Virbian0* a serwerem DHCP.
 - ▶ Jakie informacje są w nich zawarte? Zlokalizuj adres IPv4 oferowany przez serwer DHCP. Jakie dodatkowe informacje umożliwiające konfigurację sieci są w tym komunikacie?
 - ▶ Jaki protokół warstwy transportowej wykorzystuje DHCP? Jakie są porty źródłowe i docelowe tych komunikatów?

²W przypadku Virtualboksa adres IPv4 będzie prawdopodobnie z sieci `10.0.2.0/24`, zaś adres IPv6 *unique-local* będzie z sieci `fd17:625c:f037:2::/64`.

- ▶ Jaki jest źródłowy adres IP wysyłanego pakietu, skoro w momencie jego wysyłania *Virbian0* nie ma jeszcze IP? Jaki jest docelowy adres IP?
- ▶ Następnie obejrzyj w Wiresharku pakiety protokołu IPv6. Widoczny powinien być komunikat *Router Solicitation* oraz odpowiedź na niego *Router Advertisement* protokołu ICMPv6. Są to odpowiedniki zapytania i odpowiedzi DHCP. Odpowiedz na następujące pytania:
 - ▶ Jakie są warstwy protokołów tych komunikatów?
 - ▶ Z jakiego adresu źródłowego wysyłany jest komunikat *Router Solicitation*? (Zauważ, że w przypadku IPv6 mamy już do dyspozycji adres link-local dodawany zaraz po aktywacji interfejsu).
 - ▶ Do jakiego adresu docelowego wysyłany jest komunikat *Router Solicitation*? Jeśli jest to adres multicastowy, to do jakiej grupy odbiorców jest on kierowany?
 - ▶ Z jakiego adresu źródłowego i do jakiego adresu docelowego wysyłany jest komunikat *Router Advertisement*?
 - ▶ Obejrzyj dokładnie zawartość komunikatu *Router Advertisement*. Zwróć uwagę, że w odróżnieniu od odpowiedzi protokołu DHCP zwracany jest tylko prefiks sieci. Jaki to prefiks?
- ▶ Zwróć uwagę, że w przypadku obu adresów IPv6 prefiks sieci ma 64 bity i jest albo ustalony przez standard (`fe80::/64`) albo przypisany przez komunikat *Router Advertisement*. Z drugiej strony, pozostałe 64 bity adresu są przypisane przez samą maszynę. W przypadku adresów link-local są one zazwyczaj deterministyczną funkcją adresu MAC, ze względu na prywatność w przypadku pozostałych adresów są one współcześnie generowane losowo bądź pseudo-losowo.

- ▶ Wyświetl tablice routingu poleceniami

```
V0#> ip -4 route
V0#> ip -6 route
```

Zwróć uwagę, że w przypadku IPv6 adres bramy domyślnej jest adresem link-local routera (`fe80::2`).

- ▶ Pingnij teraz jakiś publiczny adres IPv6, np. wykonując polecenie

```
V0$> ping 2001:4860:4860::8888
```

Zaobserwuj w terminalu i w Wiresharku, od kogo otrzymujesz odpowiedzi. Czy jest to odpowiedź od routera `fe80::2` czy też bezpośrednio od docelowego adresu IPv6? Co jest prawdopodobną przyczyną niepowodzenia?

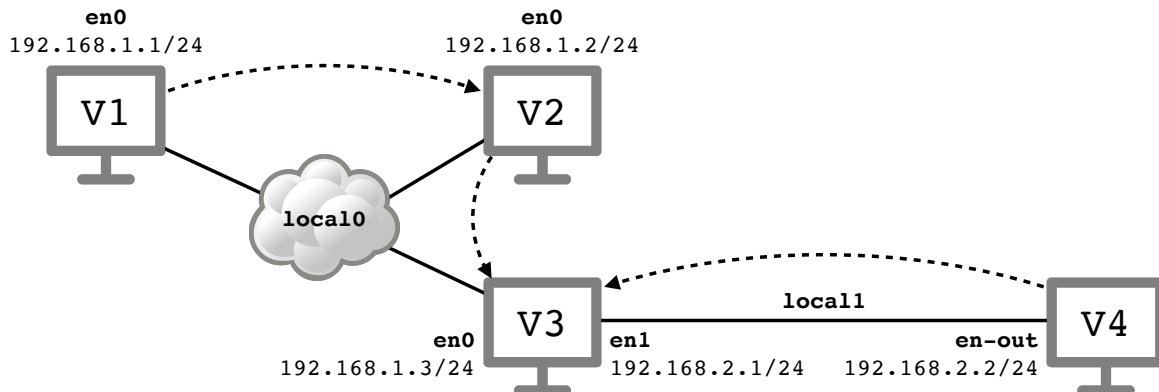
- ▶ Usuń konfigurację interfejsu `en0` poleceniem

```
V0#> dhcpcd -k en0
```

i następnie wyłącz maszynę *Virbian0*.

Wyzwanie

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



- ▶ Skonfiguruj 4 maszyny *Virbian1* – *Virbian4*, tak aby korzystały z sieci *local0* i *local1*, tak jak zaznaczono na rysunku powyżej. Nazwij ich interfejsy tak jak na rysunku (*en0*, *en1* i *en-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 Echo 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