Jak działa Internet
Model OSI, warstwa fizyczna, adresy MAC i IP

Jest to pierwszy z serii artykułów, w których chciałbym wprowadzić czytelnika w podstawy działania „Internetu". Zaczniemy od omówienia modelu OSI, opisując pobieżnie warstwę fizyczną połączeń w sieciach, adresów MAC oraz IP (w obecnym artykule), dojdziemy kolejno do bardziej szczegółowego opisu protokołu TCP, systemu DNS, a skończymy na witrynach internetowych oraz API korzystających z HTTP. Przy okazji poznamy program Wireshark do analizy ruchu sieciowego. Zaczynajmy!

Od razu wyjaśnijmy jedną rzecz: w artykule nie będziemy się skupiali na Internecie jako takim. Internet jest zbiorem połączonych ze sobą sieci, które komunikują się ze sobą. Żeby zrozumieć tę komunikację, będziemy upraszczać sieci do kilku urządzeń lub kilku małych sieci. Nie sposób jednak poruszyć tematu komunikacji bez omówienia modelu OSI.

MODEL OSI

Model OSI (Open Systems Interconnection) to bardzo ogólny model komunikacji. Dzieli on technologiczny stos komunikacyjny na warstwy o pojedynczych odpowiedzialnościach. W rzeczywistości implementacja stosów komunikacyjnych nie jest w pełni zgodna z tym modelem (poszczególne warstwy mogą nie być rozdzielone od siebie w taki sam sposób). Mimo to model jest bardzo popularny i szeroko stosowany w żargonie sieciowym. Często np. będziemy mówili o tym, którą warstwę sieci wspierają urządzenia.

Rysunek 1. Model OSI

Jak widzimy, model OSI składa się z siedmiu warstw, zgodnie z intuicją wyższe warstwy odpowiadają wyższym poziomom abstrakcji.

W tym artykule zajmiemy się głównie warstwami 1-3. Warstwę Fizyczną omówimy bardzo pobieżnie, ponieważ jest ona najmniej ciekawa z „Programisty" punktu widzenia. Z warstwą łącza danych będziemy mieć do czynienia od czasu do czasu, a z warstwą sieciową często.

Warstwa Fizyczna

Tak jak sama nazwa wskazuje, Warstwa Fizyczna opisuje komunikację na najniższym – fizycznym poziomie. Mam tutaj na myśli opis tego, jak wyglądają symbole, jak np. zera i jedynki przy połączeniu przewodem elektrycznym, czy jak synchronizować długość trwania przesyłanego bitu. Podobnie, to właśnie ta warstwa opisuje częstotliwości używane przez połączenia Wi-Fi.

Przykładami implementacji warstw fizycznych są:

- Przewody UTP, FTP, STP – przewody ethernetowe kolejno bez ekranowania, z ekranowaniem całej skrętki i z ekranowaniem poszczególnych par. Różne ekranowania odpowiadają odporności na zakłócenia elektromagnetyczne.
- Opisy fal elektromagnetycznych i ich częstotliwości używanych chociażby w połączeniach bezprzewodowych.
- Urządzenia takie jak huby ethernetowe. (Obecnie raczej nie zobaczymy hubów w praktyce. Są to stare urządzenia. Warto jednak o nich pamiętać przy omawianiu różnych warstw sieci, chociażby po to, żeby porównać ich sposób działania do popularnych switchy, o czym później).

Warstwa Łącza Danych

Jest to warstwa protokołu, która pozwala na komunikację między urządzeniami *znajdującymi się w jednej sieci lokalnej*. Co to znaczy jedna sieć lokalna? Na nasze potrzeby chodzi o komunikację tych urządzeń między sobą, które znajdują się w jednym mieszkaniu i używają tego samego routera do dostępu do Internetu (mimo że nie omawialiśmy routerów, to zakładam, że intuicyjnie wszyscy wiemy, o które dokładnie urządzenie w mieszkaniu chodzi).

Jest to dość ciekawa warstwa, ponieważ często rozdziela się ją na 2 pomniejsze warstwy:

- LLC (ang. *Logical Link Control*), która jest warstwą wyższą oraz
- MAC (ang. *Media Access Control*), będąca warstwą niższą

Do Warstwy Łącza Danych należą przede wszystkim karty sieciowe (ang. NIC – Network Interface Card). To właśnie karty sieciowe

implementują logikę związaną z pakowaniem i rozpakowywaniem danych z tzw. ramek danych (warstwa LLC), adresowaniem danych (również warstwa LLC), a także bezpośrednio obsługują warstwę fizyczną (warstwa MAC).

Ramka danych to określenie, które jest przypisane bezpośrednio do warstwy drugiej modelu OSI. Dane kolejnych warstw będą nazywane kolejno:

- pakietami – warstwa 3,
- segmentami, datagramami – warstwa 4,
- żądaniami i odpowiedziami HTTP – warstwa 7 (w kolejnych częściach tej serii będziemy omawiać właśnie protokół HTTP, natomiast inne protokoły mogą mieć model komunikacji inny niż żądania i odpowiedzi).

Wrócimy jeszcze do tego w dalszej części artykułu.

Z warstwą MAC możemy kojarzyć odpowiadające jej adresy – MAC. Adres MAC to jedno z pól struktury danych znajdujących się w ramce, która odpowiada za identyfikowanie urządzenia w sieci. Jest to tzw. *adres fizyczny*, ponieważ nadawany jest urządzeniom już podczas ich produkcji (można je jednak zmieniać również poprzez oprogramowanie). Konkretniej, adres MAC jest przypisany do karty sieciowej (ang. NIC - Network Interface Card). Komputery, czy inne urządzenia, mogą mieć wiele kart sieciowych, w tym wirtualnych kart sieciowych (vNIC). Adresy te zajmują 48 bitów informacji (6 bajtów). Pierwsze 3 z nich identyfikują firmę, która wyprodukowała urządzenie, a kolejne wskazują na konkretne urządzenie, co przedstawiono na Rysunku 2.

W zapisie często stosuje się zapis szesnastkowy. Przykładowy adres MAC wygląda wtedy następująco: `28:97:C1:38:51:E2`.

W ramach sieci lokalnej urządzenia wysyłają do siebie wiadomości, używając właśnie adresów MAC, możemy również sprawdzić adresy MAC naszego urządzenia. W przypadku systemu operacyjnego Windows możemy wywołać komendę `ipconfig /all`, a w środowiskach typu UNIX odpowiednią komendą może być `ip a` (na macOS znajdziemy komendę `ifconfig`). Przykładowe wyjście komendy możemy zobaczyć poniżej:

```
1: lo: <LOOPBACK,UP,LOWER_UP> …
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP>...
    link/ether 74:e5:f9:86:f9:0c brd ff:ff:ff:ff:ff:ff
    inet 10.11.0.75/24 brd 10.11.0.255
       scope global dynamic noprefixroute wlp2s0
       valid_lft 82888sec preferred_lft 82888sec
    inet6 fe80::a494:5de9:603c:9f77/64
       scope link noprefixroute valid_lft forever
       preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP>…
    link/ether 02:42:36:87:00:08 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255
      scope global docker0 valid_lft forever
      preferred_lft forever
```

Powyższa komenda pokazuje nam, że nasza maszyna ma 3 interfejsy sieciowe:

- `lo` (tzw. loopback),
- `wlp2s0` (interfejs Wi-Fi),
- `docker0` (wirtualny interfejs stworzony na potrzeby narzędzia docker).

Adres MAC jest przypisany do każdego z interfejsów osobno i są to kolejno:

- 00:00:00:00:00:00
- 74:e5:f9:86:f9:0c
- 02:42:36:87:00:08

Jak już wspomnieliśmy, adres MAC jest częścią ramki, której obsługą zajmuje się warstwa druga modelu OSI. Uproszczony schemat takiej ramki zamieszczono na Rysunku 3.

Kolejno adres MAC odbiorcy i nadawcy służą do tego, żeby ramka danych dotarła do określonego urządzenia, a także by odbiorca wiedział, do kogo wiadomość odesłać.

Typ danych informuje o formacie danych w polu Dane, co pozwala na ich prawidłową interpretację. W naszym przypadku zazwyczaj będziemy mówić o danych pakietu IP, o którym będzie mowa w dalszej części artykułu.

Ramkę kończy FCS – Frame Check Sequence – matematycznie wyliczony skrót danych, pozwalający określić, czy dane zostały odebrane prawidłowo. Czasami w wyniku zakłóceń elektromagnetycznych lub innych problemów w warstwie fizycznej może dojść do błędów transferu danych. Taki błąd może się objawić chociażby odebraniem złego bitu danych. Wysyłający wylicza wartość FCS, przesyła go do odbiorcy, który jeszcze raz liczy FCS i sprawdza jego poprawność. Jeśli wartości są sobie równe, to z dużym prawdopodobieństwem można stwierdzić, że dane zostały odebrane bez problemu.

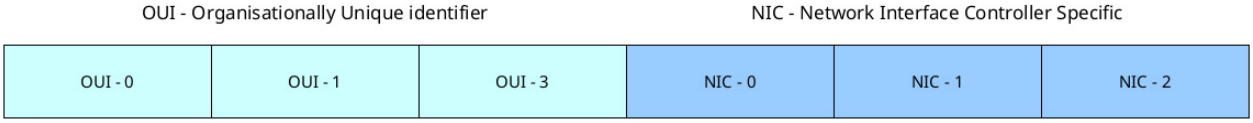
Chociaż istnieje teoretyczna możliwość błędu w przesyle danych, że zarówno dane, jak i FCS ulegną modyfikacji i wartość FCS nadal będzie poprawnie wyliczona dla niepoprawnie przesłanych danych, prawdopodobieństwo takiego zdarzenia jest niezwykle małe (w praktyce nie trzeba się tym przejmować, a protokoły wyższych warstw również implementują algorytmy sprawdzające spójność danych).

Urządzenia warstwy 1 i 2.

Zanim przejdziemy do omawiania kolejnych warstw i ich implementacji, spójrzmy na 2 urządzenia – huby oraz switche. Są to odpowiednio urządzenia warstwy pierwszej i drugiej.

Zarówno do hubów, jak i switchy możemy podłączyć wiele urządzeń, co umożliwi im komunikację ze sobą. Jednak w obu przypadkach ta komunikacja będzie wyglądać nieco inaczej.

Huby to urządzenia warstwy pierwszej. Jako takie nie rozumieją one ramek danych warstwy drugiej (Rysunek 3). Oznacza to, że wszystkie urządzenia podłączone do huba, komunikując się, rozsyłają



Rysunek 2. Opis adresu MAC

ANGULAR I KOMPONENTY WEBOWE – INTEGRACJA ZA POMOCĄ CONTROL VALUE ACCESSOR

INDEX: 285358

www.programistamag.pl

Magazyn programistów i liderów zespołów IT

programista

4/2024 (114)

Cena 28,90 zł (w tym VAT 8%)

JAK DZIAŁA INTERNET

MODEL OSI, WARSTWA FIZYCZNA, ADRESOWANIE

NOWY NR

JUŻ W EMPIKACH

ISSN 2084-9400

9 772084 940404 04

Podatności LLMów na ataki – Prompt Injection

Zarządzanie stanem i danymi z RTK Query

Zbuduj własnego Linuxa z Buildrootem i Raspberry Pi

Architektura oprogramowania w obrazkach

Konteneryzacja, orkiestracja i automatyzacja wdrażania aplikacji