

Sieci komputerowe

Wykład 5: Niższe warstwy

Marcin Bieńkowski

Instytut Informatyki
Uniwersytet Wrocławski

Warstwa łączy danych

- Umożliwia komunikację między dwoma bezpośrednio połączonymi urządzeniami.
- Zapewnia zawodną usługę wysyłania *ramek*.
- Łączy może być współdzielone między wieloma urządzeniami!
- Musi radzić sobie z błędami transmisji.

Warstwa fizyczna

- Określa szczegóły przesyłania pojedynczych bitów.
- Kodowanie za pomocą sygnałów elektrycznych, fal radiowych, ...

Najczęstsze standardy

- Ethernet (IEEE 802.3): sieć przewodowa.
 - Sieć przewodowa (kable lub światłowody).
- Sieci bezprzewodowe (IEEE 802.11).
 - Różne częstotliwości.
- Standardy często opisują obie warstwy (łącza danych i fizyczną).
- Implementowane na kartach sieciowych (w firmware).

Podział ze względu na skalę

- LAN (*Local Area Network*) — sieć lokalna
 - Ethernet, 802.11, ...
- WAN (*Wide Area Network*) — sieć rozległa
 - Frame Relay, MPLS, PPP, ...
 - Sieci w obrębie miast: MAN (*Metropolitan Area Network*).

Czy możemy nadawać jednocześnie?

- komunikacja simpleksowa
- komunikacja półdupleksowa
- komunikacja pełnodupleksowa

- Dwupunktowe (2 połączone urządzenia).
- Wielopunktowe (wiele urządzeń podpiętych do tego samego kanału komunikacyjnego).
 - Wpiętych do jednej szyny danych / koncentratora (*hub*).
 - Korzystających z tej samej sieci bezprzewodowej.
 - Jak zapewniać, że tylko jedna stacja nadaje?

- Dwupunktowe (2 połączone urządzenia).
- Wielopunktowe (wiele urządzeń podpiętych do tego samego kanału komunikacyjnego).
 - Wpiętych do jednej szyny danych / koncentratora (*hub*).
 - Korzystających z tej samej sieci bezprzewodowej.
 - Jak zapewnić, że tylko jedna stacja nadaje?

Współdzielony kanał

Co jest problemem?

- Jeśli jeden komputer nadaje, to wszyscy go słyszą.
- Jeśli dwa komputery nadają jednocześnie, to pojawiają się kolizje (sieci przewodowe) lub interferencje (sieci bezprzewodowe).
 - Zazwyczaj nie można wtedy odczytać komunikatu.
 - Czasem kolizje są nierozróżnialne od braku wiadomości.

Założenia

- Wiele stacji, jeden współdzielony kanał.
- Wykrywanie nośnej (*carrier sense*): wszyscy wiedzą kiedy ktoś inny nadaje.
- Wykrywanie kolizji: wiemy, że nastąpiła.
- Nie ma dodatkowego kanału na komunikaty kontrolne.

Przykład z życia: rozmowa w grupie

Rozwiązania

Rozwiązania deterministyczne:

- Przekazywanie żetonu.
- Zazwyczaj skomplikowane i podatne na błędy implementacyjne.
 - Gubienie żetonu, duplikacja żetonu, ...

Rozwiązania losowe:

- Protoplasta: sieć ALOHA.
- CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
— Ethernet (≤ 1 Gbit).
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)
— Sieci bezprzewodowe 802.11.
- Proste w implementacji i odporne na awarie.

Podejście losowe (1)

Podejście losowe (Rundowy ALOHA)

- Czas podzielony na rundy, runda wystarcza do nadania jednej ramki danych.
- Jeśli stacja ma ramkę danych do wysłania, wysyła ją z prawdopodobieństwem p .
- Dla $p = 1/n$ (n = liczba stacji, które chcą nadać komunikat) udaje się to średnio co $e \approx 2,71$ tury (\rightarrow ćwiczenie)
- Problem: wykorzystanie łącza dość niskie ($\sim 1/e$).
- Problem: musimy znać n , żeby wybrać optymalne p .
- Problem: potrzebujemy globalnego zegara, żeby ustalać rundy.

Podejście losowe (1)

Podejście losowe (Rundowy ALOHA)

- Czas podzielony na rundy, runda wystarcza do nadania jednej ramki danych.
- Jeśli stacja ma ramkę danych do wysłania, wysyła ją z prawdopodobieństwem p .
- Dla $p = 1/n$ (n = liczba stacji, które chcą nadać komunikat) udaje się to średnio co $e \approx 2,71$ tury (\rightarrow ćwiczenie)
- Problem: wykorzystanie łącza dość niskie ($\sim 1/e$).
- Problem: musimy znać n , żeby wybrać optymalne p .
- **Problem: potrzebujemy globalnego zegara, żeby ustalać rundy.**

Podejście losowe (2)

Podejście losowe (Bezrundowy ALOHA)

- Jak poprzednio, ale bez synchronizacji i podziału na rundy.
- Wykorzystanie łącza dwukrotnie niższe dla $p = 1/n$ wykorzystanie łącza dwukrotnie niższe niż poprzednio (\rightarrow ćwiczenie).
- Faktycznie wykorzystywany na przełomie lat 60 i 70.

Podejście losowe (3)

Protokół CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- Sprawdzaj czy ktoś nadaje na początku.
- Jeśli tylko zauważysz kolizję, przestań nadawać.
- Dopasowuj dynamicznie wartość p :
 - Zaczynamy z $p = 1$
 - Jeśli występuje kolizja, to zmniejszamy prawdopodobieństwo dwukrotnie.
 - Algorytm *odczekiwania wykładniczego*.
- Stosowany w Ethernetie; w praktyce znacznie lepsze wykorzystanie łącza niż w ALOHA.

CSMA/CD

Algorytm CSMA/CD, wysyłanie pojedynczą ramkę

- ❶ $m \leftarrow 1$
 - ❷ Poczekaj aż kanał będzie pusty i zacznij nadawać.
 - ❸ Podczas nadawania, nasłuchuj. Jeśli usłyszysz kolizję:
 - skończ nadawać
 - wyślij krótki sygnał kolizji
 - wybierz K losowo ze zbioru $\{0, 1, \dots, 2^m - 1\}$
 - $m \leftarrow m + 1$
 - odczekaj $K \cdot 512$ jednostek bitowych
 - wróć do kroku 2
-
- Po 16 próbach algorytm poddaje się.
 - 512 bitów wystarcza, żeby początek ramki dotarł do miejsca przeznaczenia.

CSMA/CA (Collision Avoidance)

Unikanie kolizji

- Wariant stosowany w sieciach bezprzewodowych.
- Bezpośrednie wykrywanie kolizji:
 - Brak możliwości (możemy nie usłyszeć interferencji)
 - Zamiast tego potwierdzanie ramek.
 - Ramki są zawsze nadawane do końca.
- CA: odczekujemy pewien czas nawet jeśli kanał właśnie się zwolnił.

Budowa ramki ethernetowej

Budowa ramki ethernetowej

8	6	6	2	0–1500	0–46	4
Preambuła	Adres docelowy	Adres źródłowy	Długość / typ	Dane	Wypełnienie	Suma kontrolna

- *Dane* = pakiet otrzymany z warstwy sieciowej.
- *Preambuła*: ciąg 101010...101011, pozwala zsynchronizować zegar nadajnika z zegarem odbiornika.

Adresy ethernetowe

Adres MAC

- 6-bajtowy unikatowy ciąg, przykładowo: 00:14:2A:1F:F3:BA.
- Przypisany (teoretycznie) na stałe do karty sieciowej.
 - W praktyce można go łatwo zmienić.
- Pierwsze trzy bajty przyznaje IEEE producentowi kart sieciowych, ostatnie trzy nadaje nadaje producent.

Rozgłaszanie

- Często ramki docierają i tak do wszystkich komputerów w sieci lokalnej
 - W oryginalnym (nieprzełączanym) Ethernetie.
 - W sieciach bezprzewodowych.
- Nasz adres = adres docelowy ramki?
 - Tak → ramka interpretowana, jej dane → warstwa sieciowa.
 - Nie → ramka wyrzucana.
- Tryb nasłuchu (*promiscuous mode*).
- Jeśli adres odbiorcy jest równy FF:FF:FF:FF:FF:FF (adres rozgłoszeniowy), to ramkę otrzymują i interpretują wszyscy.

MAC vs. IP

Jak warstwa sieciowa wysyła pakiety?

- W adresie źródłowym w. łącza danych wpisujemy adres MAC swojej karty sieciowej.
- W adresie docelowym w. łącza danych wpisujemy:
 - adres MAC następnego routera na trasie (jeśli jest)
 - adres MAC docelowego komputera (w przeciwnym przypadku)
- Skąd wziąć adres MAC urządzenia jeśli znamy jego IP?

Address Resolution Protocol

- Rozgłasza ramki z zapytaniem „kto ma dany adres IP” na adres rozgłoszeniowy (FF:FF:FF:FF:FF:FF).
- Jeden komputer odpowiada.
- Wszyscy słyszą i zapisują odpowiedź w lokalnej tablicy ARP (na pewien czas).
- Co się stanie, jeśli więcej niż jeden komputer odpowie?

Rozgłaszanie w warstwie sieciowej

Pakiet skierowany do adresu rozgłoszeniowego IP

- Umieszczany w ramce adresowanej do FF:FF:FF:FF:FF:FF.
- Co się stanie, jeśli mamy dwie różne sieci IP działające w tej samej sieci warstwy drugiej?

Odwrotność ARP?

Problem: A jeśli potrzebujemy przekształcenia MAC \rightarrow IP?

- Po co? Warstwa 2 powinna być niezależna od warstwy 3!
- Automatyczne przypisywanie adresów IP
- Niezbędne dla komputerów bezdyskowych (znają tylko adres MAC swojej karty sieciowej).

Protokoły:

- RARP (Reverse ARP)
- DHCP (pobieranie całej konfiguracji sieci)
- Konfiguracja automatyczna (APIPA = Automatic Private IP Addressing (169.254.0.0/16))

Odwrotność ARP?

Problem: A jeśli potrzebujemy przekształcenia MAC \rightarrow IP?

- Po co? Warstwa 2 powinna być niezależna od warstwy 3!
- Automatyczne przypisywanie adresów IP
- Niezbędne dla komputerów bezdyskowych (znają tylko adres MAC swojej karty sieciowej).

Protokoły:

- RARP (Reverse ARP)
- DHCP (pobieranie całej konfiguracji sieci)
- Konfiguracja automatyczna (APIPA = Automatic Private IP Addressing (169.254.0.0/16))

Długość ramki

Maks. długość danych = 1500 bajtów \rightarrow max długość ramki = 1518 (+ preambuła).

- Względy historyczne: droga pamięć RAM.
- Małe ramki są mniej podatne na uszkodzenia.

Min. długość danych = 46 bajtów
(za mało danych \Rightarrow wypełnienie).

- Łatwiej odróżnić poprawną ramkę od śmieci.
- Wysyłanie powinno trwać minimalnie czas $2 \cdot \tau$
(τ = czas propagacji sygnału przez cały kabel).
 \rightarrow Gwarancja, że nadawca dowie się o niepowodzeniu wysyłania.

CSMA/CD \rightarrow ograniczenie na odległość w sieci do 100m.

Długość ramki

Maks. długość danych = 1500 bajtów \rightarrow max długość ramki = 1518 (+ preambuła).

- Względy historyczne: droga pamięć RAM.
- Małe ramki są mniej podatne na uszkodzenia.

Min. długość danych = 46 bajtów
(za mało danych \Rightarrow wypełnienie).

- Łatwiej odróżnić poprawną ramkę od śmieci.
- Wysyłanie powinno trwać minimalnie czas $2 \cdot \tau$
(τ = czas propagacji sygnału przez cały kabel).
 \rightarrow Gwarancja, że nadawca dowie się o niepowodzeniu wysyłania.

CSMA/CD \rightarrow ograniczenie na odległość w sieci do 100m.

Długość ramki

Maks. długość danych = 1500 bajtów \rightarrow max długość ramki = 1518 (+ preambuła).

- Względy historyczne: droga pamięć RAM.
- Małe ramki są mniej podatne na uszkodzenia.

Min. długość danych = 46 bajtów
(za mało danych \Rightarrow wypełnienie).

- Łatwiej odróżnić poprawną ramkę od śmieci.
- Wysyłanie powinno trwać minimalnie czas $2 \cdot \tau$
(τ = czas propagacji sygnału przez cały kabel).
 \rightarrow Gwarancja, że nadawca dowie się o niepowodzeniu wysyłania.

CSMA/CD \rightarrow ograniczenie na odległość w sieci do 100m.

Przełączanie w warstwie łącza danych

Mosty

- Most łączy dwie części sieci.
- „Rozumie” protokoły warstwy drugiej.
- Uczy się w trakcie działania, które adresy MAC leżą w której sieci lokalnej.
- Kolejne transmisje przechodzą przez most tylko w razie konieczności:
 - izolacja kolizji wewnątrz sieci lokalnych, ale komunikacja między sieciami możliwa
 - większa prywatność.

Przełączniki sieciowe

Przełącznik (*switch*)

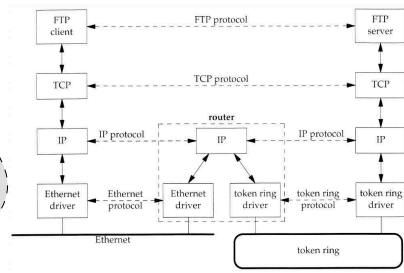
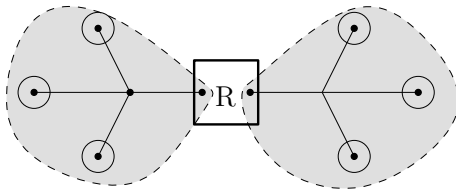
- Jak koncentrator, ale działa w warstwie drugiej.
- Uogólnienie mostu: wiele złączy.
- Do złączy można podpiąć całe sieci lub pojedyncze komputery.

Topologia

- Przełączniki używają STP (*Spanning Tree Protocol*).
- Spośród połączeń wybierają drzewo, inne porty wykorzystywane tylko w wypadku awarii.

Łączenie sieci różnych technologii

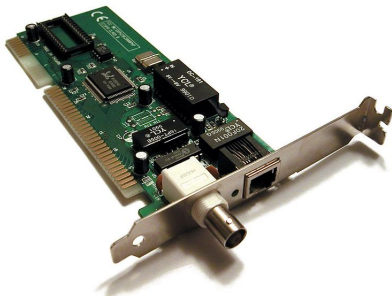
- Mogą być łączone przez routery (poprzednie wykłady).
- Mogą być łączone przez mosty.
 - Szybsze niż routery
 - Ale nie rozumieją IP → nie mogą robić fragmentacji → nie radzą sobie z za dużymi pakietami w stosunku do MTU



Warstwa fizyczna Ethernetu

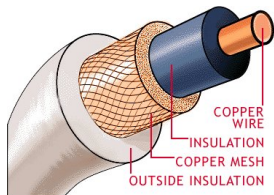
Karta sieciowa

- Interfejs sieciowy = logiczny widok karty w systemie operacyjnym.
- Karta pracuje z określoną częstotliwością nadawania.
 - → przepustowość (w kbit/s, Mbit/s lub Gbit/s)
- Bity kodowane jako zmiany sygnału (amplitudy lub/i przesunięcia)
- Sygnał propaguje się po nośniku (kablu) i jest odbierany (mierzony) po drugiej stronie



Obrazek ze strony http://en.wikipedia.org/wiki/Network_card

Kable: kabel koncentryczny



- Kabel długości do 200m.
- Transmisja półdupleksowa.
- Wiele komputerów spiętych tym samym kablem.

Obrazek ze strony <http://www.phy.davidson.edu/StuHome/phstewart/IL/speed/Cableinfo.html>

Kable: światłowody

Światłowody

- Wszystkie przepustowości (choć stosowany raczej przy wyższych przepustowościach).
- Niewrażliwe na przepięcia, zakłócenia elektromagnetyczne.
- Mogą być bardzo długie.
- Trudno się podpiąć w środku → bezpieczeństwo.
- Transmisja zazwyczaj simpleksowa (po jednej stronie dioda laserowa do nadawania, po drugiej fotodioda do odbierania).
- Połączenie dwupunktowe.

Kable: skrętka (UTP) (1)

Skrętka nieekranowana (ang. *unshielded twisted pair (UTP)*)

- Najtańsze i najpopularniejsze rozwiązanie
- Różne kategorie przewodów z różnymi możliwościami (kat. 3, 5, 5e, 6, ...)
 - Główna różnica to maksymalna częstotliwość z jaką może zmieniać się sygnał.
- Działa na odległość ok. 100m, powyżej tego limitu → wzmacniaki (*repeater*)
- Połączenie dwupunktowe.
- W środku 8 przewodów; możliwa transmisja pełnodupleksowa.



Warstwa fizyczna

3 najczęstsze warianty Ethernetu

- Ethernet (10 Mbit/sek, koncentryk lub skrętka min. kat. 3.)
- Fast Ethernet (100 Mbit/sek, skrętka min. kat. 5 lub światłowód.)
- Gigabit Ethernet (1 Gbit/sek, skrętka min. kat. 5e lub światłowód.)

Sieci bezprzewodowe 802.11

Standardy WLAN

Pasma częstotliwości

- 5Ghz:
 - wyższa częstotliwość → można przesłać więcej bitów
 - mniej zatłoczone pasmo,
 - mały zasięg: ok. 20 m.
 - fale bardziej pochłaniane przez ściany
- 2.4Ghz
 - w tym paśmie działa również: Bluetooth, kuchenki mikrofalowe, bezprzewodowe telefony, niektóre piloty do garażów, ...
 - zasięg: ok. 50 m, lepsze przenikanie ścian
- Oba pasma częstotliwości są dostępne do nadawania bez licencji.

Standardy WLAN, cd.

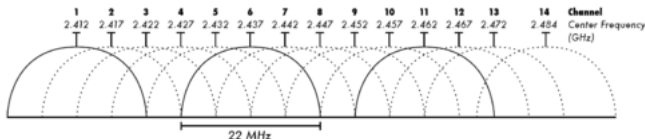
Standardy

- 802.11a: 5 Ghz, do 54 Mbit, stary, obecnie dość rzadko spotykany.
- 802.11b: 2,4 Ghz, do 11 Mbit.
- 802.11g: 2,4 Ghz, do 54 Mbit, wstecznie kompatybilny z 802.11b (obecnie najpopularniejszy)
- 802.11n: 2,4 Ghz + 5 Ghz, do 600 Mbit (do 4 + 4 anten nadających + odbierających)
- 802.11ac: 5 Ghz, do 1 Gbit (do 8 + 8 anten).

2,4 GHz

Kanały

- Całe pasmo podzielone na 14 kanałów, komunikujące się urządzenia muszą korzystać z tego samego kanału.



- Urządzenia nadające w konkretnym kanale zakłócają transmisje w sąsiednich.
- Niektóre państwa nie pozwalają na korzystanie ze wszystkich kanałów:
 - Laptop wyprodukowany w USA będzie korzystał tylko z pierwszych 11 kanałów.
 - Kanał 14 dostępny jest tylko w Japonii.

Obrazek ze strony <http://en.wikipedia.org/wiki/802.11>

Problemy z warstwą fizyczną

Malejąca siła sygnału = sygnał rozchodzi się wielokierunkowo (słabnie z kwadratem odległości lub szybciej)

- Dodatkowo: sygnał rozpraszany, słabnie przy przechodzeniu przez ściany

Interferencje = wzajemne zakłócenia urządzeń pracujących z takimi samymi częstotliwościami (inne karty sieciowe, bezprzewodowe telefony, Bluetooth, ...)

Propagacja wielościeżkowa → ten sam sygnał wędruje do celu ścieżkami różnej długości.

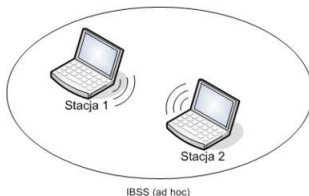
Półduplex ← nie można jednocześnie nadawać i słuchać (tak jak w Ethernetie)

- Nie wiemy, czy wystąpiła kolizja → CSMA/CA zamiast CSMA/CD.

Typy sieci WLAN (1)

Sieci bez punktu dostępowego = sieci ad-hoc

- Brak routingu = zakładamy, że każde urządzenie jest w zakresie nadawania każdego innego.

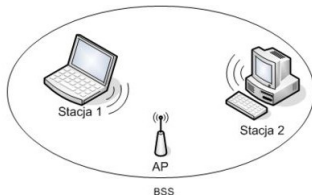


Obrazek ze strony http://pl.wikipedia.org/wiki/Punkt_dostępu

Typy sieci WLAN (2)

Sieci z punktem dostępowym (*access point*)

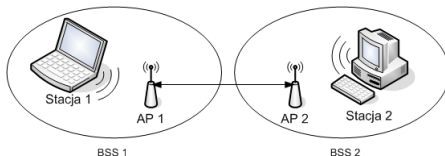
- BSS (*Basic Service Set*)
- Każdy komunikuje się tylko z punktem dostępowym
- Każdy musi być w zasięgu punktu dostępowego
- Punkt dostępowy jest połączony zazwyczaj kablem z routerem, tj. pełni funkcję mostu między sieciami 802.11 i Ethernet.
- Punkt dostępowy rozsyła ramki identyfikacyjne (*beacon frames*)
 - → Stąd nasz komputer „wie” jakie sieci są dostępne
 - Przed transmisją trzeba się związać z wybranym punktem dostępowym → opcjonalne uwierzytelnianie.



Typy sieci WLAN (3)

Większe sieci

- BSS ograniczony przez zasięg anteny punktu dostępowego
- EBSS (*Extended Basic Service Set*) = wiele połączonych (zazwyczaj siecią kablową) punktów dostępowych.



- Wspólny identyfikator sieci ESSID (wysyłany w każdej ramce).
- Obsługa przechodzenia klientów pomiędzy punktami dostępowymi.
- W ramach umieszcza się dodatkowo adresy MAC punktów dostępowych nadawcy i odbiorcy.
- Mogą wykorzystywać różne kanały.

Obrazek ze strony http://pl.wikipedia.org/wiki/Punkt_dostępu

Problemy warstwy drugiej

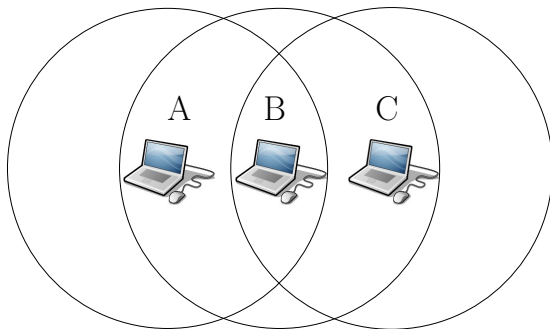
Nie wynikają tylko z zawodności warstwy 1!

- Problem ukrytej stacji
- Problem odkrytej stacji

Strategia „nadawaj jeśli nikt nie nadaje” nie działa

Problem ukrytej stacji (B może być stacją bazową)

- C nadaje do B
- A chce nadać do B, sprawdza stan kanału i nic nie słyszy

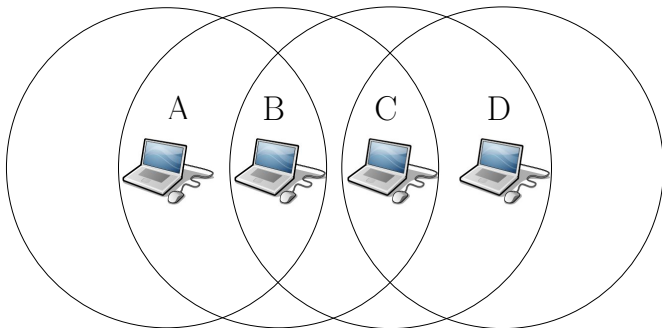


Cliparty ze strony <http://jimmac.musichall.cz/i.php?i=computer-clipart>

Strategia „nadawaj jeśli nikt nie nadaje” nie działa

Problem odkrytej stacji (nie występuje w przypadku pojedynczej stacji bazowej):

- C nadaje do D
- B chce nadać do A, sprawdza stan kanału i wnioskuje, że nie może nadawać

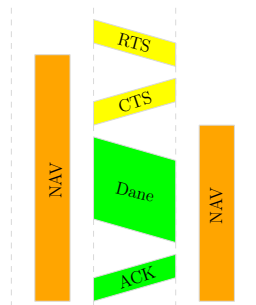
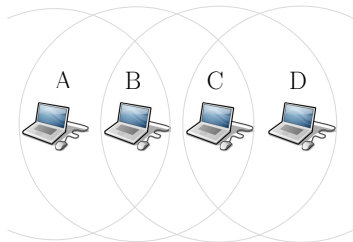


Cliparty ze strony <http://jimmac.musichall.cz/i.php?i=computer-clipart>

Ukryta stacja, cd.

Częściowe rozwiązanie wbudowane w CSMA/CA: RTS+CTS

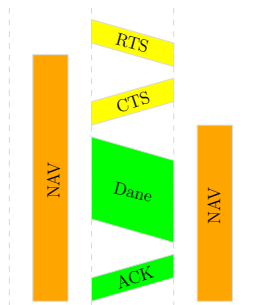
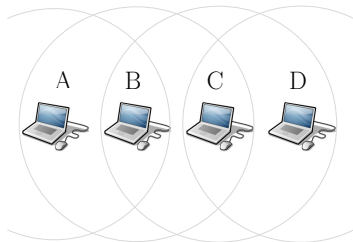
- B chce wysłać do C,
- B wysyła RTS (*Request To Send*), słyszy to też A,
- C wysyła CTS (*Clear To Send*), słyszy to też D,
- A i D będą milczeć (NAV = *Network Allocation Vector*),
- B wysyła dane, C potwierdza.



Ukryta stacja, cd.

Częściowe rozwiązanie wbudowane w CSMA/CA: RTS+CTS

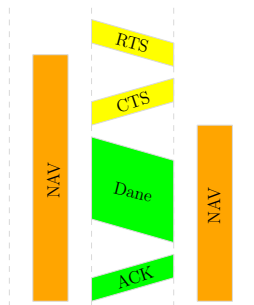
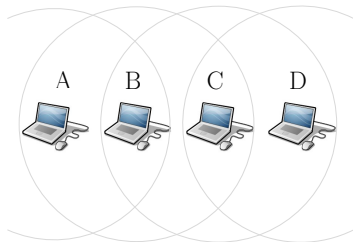
- B chce wysłać do C,
- B wysyła RTS (*Request To Send*), słyszy to też A,
- C wysyła CTS (*Clear To Send*), słyszy to też D,
- A i D będą milczeć (NAV = *Network Allocation Vector*),
- B wysyła dane, C potwierdza.



Ukryta stacja, cd.

Częściowe rozwiązanie wbudowane w CSMA/CA: RTS+CTS

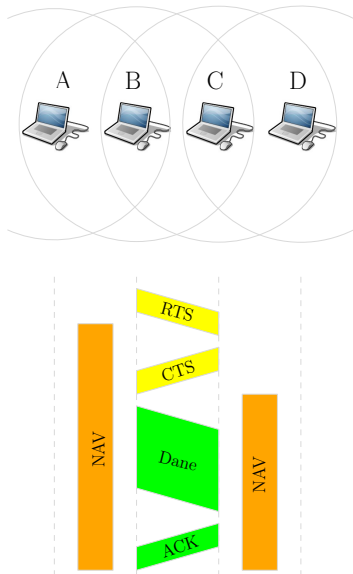
- B chce wysłać do C,
- B wysyła RTS (*Request To Send*), słyszy to też A,
- C wysyła CTS (*Clear To Send*), słyszy to też D,
- A i D będą milczeć (NAV = *Network Allocation Vector*),
- B wysyła dane, C potwierdza.



Ukryta stacja, cd.

Częściowe rozwiązanie wbudowane w CSMA/CA: RTS+CTS

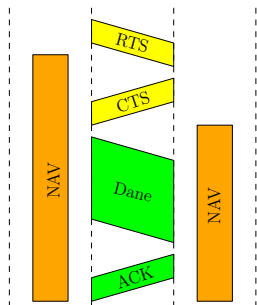
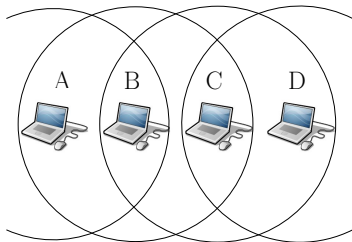
- B chce wysłać do C,
- B wysyła RTS (*Request To Send*), słyszy to też A,
- C wysyła CTS (*Clear To Send*), słyszy to też D,
- A i D będą milczeć (NAV = *Network Allocation Vector*),
- B wysyła dane, C potwierdza.



Ukryta stacja, cd.

Częściowe rozwiązanie wbudowane w CSMA/CA: RTS+CTS

- B chce wysłać do C,
- B wysyła RTS (*Request To Send*), słyszy to też A,
- C wysyła CTS (*Clear To Send*), słyszy to też D,
- A i D będą milczeć (NAV = *Network Allocation Vector*),
- B wysyła dane, C potwierdza.



Szyfrowanie

- WEP (*Wired Equivalent Privacy*)
- WPA (*Wi-fi Protected Access*)
- WPA2 = 802.11i
 - Personal, PSK (*Pre-Shared Key*) = jeden klucz
 - Enterprise = osobny serwer uwierzytelniający (RADIUS)

Lektura dodatkowa

- Kurose, Ross: rozdział 5 i 6
- Tanenbaum: rozdział 4