Sieci Komputerowe

Grzegorz Gutowski

Uniwersytet Jagielloński

2023/24

Ethernet

- Historia

Ethernet

- Historia
- IEEE 802

Ethernet

- Historia
- IEEE 802.3

Ethernet

- Historia
- IEEE 802.3
- Wersje

Ethernet

- Historia
- IEEE 802.3
- Wersje 100BASE-T
  - Duplex
  - Jeden kanał w każdą stronę
  - 125 MHz
  - 3 sygnały
  - 4b5b + NRZI + MLT-3

Ethernet

- Historia
- IEEE 802.3
- Wersje 1000BASE-T
  - Duplex
  - Cztery kanały w każdą stronę
  - 125 MHz
  - 5 sygnałów

Nadawanie większych komunikatów

- Ethernet:
  - Nagłówek (7 x 10101010 + 10101011)
  - Adres odbiorcy (6)
  - Adres nadawcy (6)
  - Typ protokołu / długość komunikatu (2)
  - Dane (46-1500)
  - Suma kontrolna (4)

Wykrywanie i korekcja błędów

- Parity bit.

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.
- CRC.

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.
- CRC.
- Kody korygujące.

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.
- CRC.
- Kody korygujące.

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.
- CRC.
- Kody korygujące.
- Ethernet: CRC32

Wykrywanie i korekcja błędów

- Parity bit.
- Haszowanie.
- CRC.
- Kody korygujące.
- Ethernet: CRC32

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Dzielenie kanału komunikacji

- ALOHA

Dzielenie kanału komunikacji

- ALOHA
  - Wysyłaj!
  - Jeśli nie dostałeś potwierdzenia, to poczekaj i wysyłaj!

Dzielenie kanału komunikacji

- ALOHA
- „slotted” ALOHA

Dzielenie kanału komunikacji

- ALOHA
- „slotted” ALOHA
- CSMA/CD

Dzielenie kanału komunikacji

- ALOHA
- „slotted” ALOHA
- CSMA/CD
- Exponential Backoff

Dzielenie kanału komunikacji

- ALOHA
- „slotted” ALOHA
- CSMA/CD
- Exponential Backoff
- Tokeny

Dzielenie kanału komunikacji

- ALOHA
- „slotted” ALOHA
- CSMA/CD
- Exponential Backoff
- Tokeny
- Ethernet: już nie

Ethernet dokładniej

- Adres MAC

Ethernet dokładniej

- Adres MAC
- *Xerox internets and Ethernet local computer networks use 48-bit absolute host numbers. This is a radical departure from practices currently in use in internetwork systems and local networks.* (Czerwiec 1981)

Ethernet dokładniej

- Adres MAC
- Broadcast

Ethernet dokładniej

- Adres MAC
- Broadcast
- Protokół ARP

Ethernet dokładniej

- Adres MAC
- Broadcast
- Protokół ARP
- Switche

Ethernet dokładniej

- Adres MAC
- Broadcast
- Protokół ARP
- Switche
- Cykle

Ethernet dokładniej

- Adres MAC
- Broadcast
- Protokół ARP
- Switche
- Cykle
- VLANy

Gdzie to wszystko jest zaimplementowane?

Sieci mobilne

- WiFi.

Sieci mobilne

- WiFi.
- Sieci komórkowe.

Zagadnienia

- Specyfika kanału komunikacji.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy” podział zasobów.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy” podział zasobów.
- Punkty dostępowe.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy” podział zasobów.
- Punkty dostępowe.
- Połączenie z większymi sieciami.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy” podział zasobów.
- Punkty dostępowe.
- Połączenie z większymi sieciami.
- Mobilność urządzeń.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy" podział zasobów.
- Punkty dostępowe.
- Połączenie z większymi sieciami.
- Mobilność urządzeń.
- Energia.

Zagadnienia

- Specyfika kanału komunikacji.
- Błędy.
- Współdzielenie kanału komunikacji.
- „Sprawiedliwy” podział zasobów.
- Punkty dostępowe.
- Połączenie z większymi sieciami.
- Mobilność urządzeń.
- Energia.
- Bezpieczeństwo.

THEORETICAL COMPUTER SCIENCE Jagiellonian University

Specyfika kanału komunikacji

- Słabnący sygnał.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.
- Problemy z obserwacją innych uczestników.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.
- Problemy z obserwacją innych uczestników.
- Problem ukrytej stacji.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.
- Problemy z obserwacją innych uczestników.
- Problem ukrytej stacji.
- Problem eksponowanej stacji.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.
- Problemy z obserwacją innych uczestników.
- Problem ukrytej stacji.
- Problem eksponowanej stacji.
- Kształtowanie wiązki.

Specyfika kanału komunikacji

- Słabnący sygnał.
- Zakłócenia.
- Autozakłócenia.
- Problemy z obserwacją innych uczestników.
- Problem ukrytej stacji.
- Problem eksponowanej stacji.
- Kształtowanie wiązki.
- QAM w WiFi.

THEORETICAL COMPUTER SCIENCE Jagiellonian University

Role punktów dostępowych

- AP w WiFi.
- BTS w GSM.

Role punktów dostępowych

- AP w WiFi.
- BTS w GSM.
- Nawiązywanie połączenia.

Role punktów dostępowych

- AP w WiFi.
- BTS w GSM.
- Nawiązywanie połączenia.
- Sterowanie komunikacją.

Role punktów dostępowych

- AP w WiFi.
- BTS w GSM.
- Nawiązywanie połączenia.
- Sterowanie komunikacją.
- Przekazywanie połączeń.

Role punktów dostępowych

- AP w WiFi.
- BTS w GSM.
- Nawiązywanie połączenia.
- Sterowanie komunikacją.
- Przekazywanie połączeń.
- Bezpieczeństwo.

Błędy komunikacji

- CRC, kody korygujące (LDPC).

Błędy komunikacji

- CRC, kody korygujące (LDPC).
- ACK, ARQ w WiFi.

Współdzielenie kanału komunikacji

- Ukryte konflikty.

Współdzielenie kanału komunikacji

- Ukryte konflikty.
- RTS, CTS w WiFi.

Bezpieczeństwo WiFi

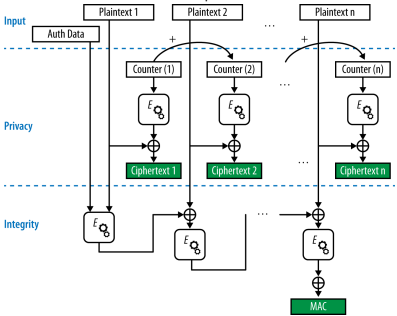
- szyfrowanie kluczem symetrycznym AES

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP = CTR + CBC-MAC



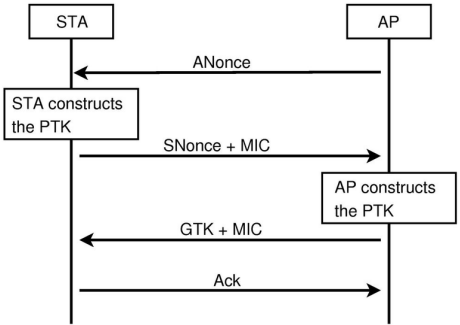
źródło: Gast, *802.11ac: A Survival Guide*

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP = CTR + CBC-MAC
- WPA-PSK

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP = CTR + CBC-MAC
- WPA-PSK, 4-way handshake



$$PTK = Hash(Key, ANonce, SNonce, APMAC, STAMAC)$$

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP = CTR + CBC-MAC
- WPA-PSK, 4-way handshake

$$PTK = Hash(Key, ANonce, SNonce, APMAC, STAMAC)$$

- WPA-Enterprise

THEORETICAL COMPUTER SCIENCE Jagiellonian University

Bezpieczeństwo WiFi

- szyfrowanie kluczem symetrycznym AES
- CCMP = CTR + CBC-MAC
- WPA-PSK, 4-way handshake

$$PTK = Hash(Key, ANonce, SNonce, APMAC, STAMAC)$$

- WPA-Enterprise
- SAE (Diffie-Hellman) w WPA3

Połączenie z większymi sieciami

- WiFi + Ethernet

WiFi

- Zmiana AP w WiFi.

WiFi

- Zmiana AP w WiFi.
- Negocjacja prędkości.

WiFi

- Zmiana AP w WiFi.
- Negocjacja prędkości.
- point-to-point WiFi.

WiFi

- Zmiana AP w WiFi.
- Negocjacja prędkości.
- point-to-point WiFi.
- Ramka WiFi.

WiFi

- Zmiana AP w WiFi.
- Negocjacja prędkości.
- point-to-point WiFi.
- Ramka WiFi.
- Oszczędzanie energii.

Inne sieci bezprzewodowe

- LTE.

Inne sieci bezprzewodowe

- LTE.
- Ad-hoc.

Inne sieci bezprzewodowe

- LTE.
- Ad-hoc.
- Sensor networks.

Inne sieci bezprzewodowe

- LTE.
- Ad-hoc.
- Sensor networks.
- Bluetooth.

Inne sieci bezprzewodowe

- LTE.
- Ad-hoc.
- Sensor networks.
- Bluetooth.
- Zigbee.

Gdzie to wszystko jest zaimplementowane?