

## Pytania z wykładów 8-14 do zaliczenia

Jan Ściga

### **1. Podaj cechy charakterystyczne Ethernetu przemysłowego.**

Charakterystycznymi cechami Ethernetu przemysłowego są:

- Niskie opóźnienia (*low latency*).
- Wykorzystywanie pełnego duplexu aby kolizje nie wpływały w niedopuszczalny sposób na czas trwania transmisji.
- Wysoka dostępność.
- Konieczność kompatybilności z obecnymi jak i starszymi systemami.
- Wydajność i łatwość konserwacji.
- Zabezpieczenie przed włamaniami z zewnątrz zakładu przemysłowego jak i przed nieumyślnym i nieuprawnionym dostępem z wewnątrz zakładu.
- Bardziej wytrzymałe (np. na wibracje) i wodoszczelne złącza takie jak M12 lub M8, a nie podatne na uszkodzenia złącza 8P8C.
- Brak mechanizmów zatraskowych w złączach (konieczne cięższe mechanizmy blokujące).
- Kable przemysłowe mają większy przekrój aby wytrzymać większe temperatury, ekranowaną konstrukcję zapobiegającą hałasom, materiały osłonowe.
- Wsparcie komunikacji w czasie rzeczywistym.
- Można łączyć wiele mediów transmisyjnych (światłowód, radio).
- Szeroki zakres adresowy.
- Determinizm Ethernetu przemysłowego (opóźnienia mogą skończyć się poważną wadą produkcyjną).

### **2. Jaki rodzaj ataku na sieć WiFi jest najbardziej niebezpieczny? Odpowiedź krótko uzasadnij.**

Najbardziej niebezpiecznym atakiem na sieć WiFi jest według mnie atak Man in the Middle polegający na przechwyceniu ruchu pomiędzy użytkownikiem sieci a Access Pointem (AP). Atak tego typu może być trudno wykrywalny w sieciach bezprzewodowych, zwłaszcza dla starszych lub tanich urządzeń nie posiadających mechanizmów obrony przed tego typu zagrożeniem (np. systemu WISS). Może spowodować modyfikację wysyłanych pakietów pomiędzy użytkownikiem a AP, wykradać poufne informacje podczas gdy użytkownik myśli, że łączy się z prawdziwym Access Pointem. Dodatkowym zagrożeniem jest istnienie wielu rodzajów tego ataku co może dodatkowo utrudniać zadanie urządzeniom lub administratorom systemu. Innym niebezpieczeństwem jest istnienie coraz większej liczby publicznych sieci WiFi (restauracje, galerie), które mogą być doskonałym miejscem dla takiego ataku, podczas gdy użytkownicy często bezkrytycznie podchodzą do tego rodzaju sieci, korzystając tam z usług banku czy logując się do mediów społecznościowych.

### 3. Wymień zalety i wady sieci PLC (Power Line Communications).

#### ZALETY:

- Rozwiązanie atrakcyjne finansowo w budowie (wykorzystuje istniejącą infrastrukturę sieci zasilających, brak wydatków na utrzymanie i konserwację sprzętu sieciowego)
- Możliwość dostępu do internetu w budynkach, w których nie ma specjalnej instalacji dedykowanej dla sieci komputerowej
- Brak konieczności użycia dodatkowego okablowania, a jedynie użycie specjalnych adapterów
- Dużą zaletą dla operatorów energetycznych jest to, że mają nad medium transmisyjnym pełną kontrolę
- Możliwość wykorzystania tej technologii przy sygnalizacji lub zdalnym monitoringu (np. liczniki mediów w gospodarstwie domowym)

#### WADY:

- Ograniczone możliwości transmisji wyższych częstotliwości (system dystrybucji został przeznaczony do dystrybucji prądu przy 50/60 Hz).
- Stosunkowo łatwa możliwość podsłuchiwania transmisji z wewnątrz budynku.
- Na wielu częstotliwościach mogą występować duże zakłócenia i interferencje (urządzenia pracujące w sieci elektrycznej, szумы indukowane przez zewnętrzne pola elektromagnetyczne).
- W przypadku systemów wąskopasmowych występuje niewielka przepustowość
- Szerokopasmowe systemy mają ograniczony zasięg
- W Polsce pojawiają się skoki napięcia znacznie utrudniające funkcjonowanie sieci PLC, niezadawalający stan niektórych linii energetycznych