

# Projektowanie, wdrażanie i administracja sieci LAN

## Kurs średniozaawansowany

---

### Cele szkolenia

Celem szkolenia jest rozszerzenie wiedzy uczestników na temat projektowania, wdrażania i administracji sieci LAN w środowisku korporacyjnym. Kurs obejmuje techniki konfiguracji przełączników i routerów, implementację mechanizmów redundancji oraz zwiększonego poziomu bezpieczeństwa sieciowego. Uczestnicy zapoznają się z dynamicznym routingiem (OSPF jednoobszarowy), segmentacją sieci (VLAN) mechanizmami redundancji warstwy 2 i 3 (STP, EtherChannel, FHRP), a także metodami zabezpieczania i monitorowania infrastruktury LAN. Szkolenie kładzie nacisk na praktyczne umiejętności związane z konfiguracją i diagnostyką sieci oraz wykorzystaniem nowoczesnych narzędzi wspierających administrację i automatyzację.

### Umiejętności

Po ukończeniu szkolenia uczestnik będzie:

- potrafił projektować i konfigurować średniej wielkości sieci LAN z zapewnieniem wysokiej dostępności,
- konfigurował mechanizmy VLAN,
- implementował mechanizmy redundancji w warstwie 2 (STP) i warstwie 3 (FHRP)
- wdrażał agregację połączeń w celu zwiększenia przepustowości i niezawodności,
- znał i konfigurował protokół routingu dynamicznego (OSPF),
- zabezpieczał przełączniki i routery przed atakami sieciowymi,
- monitorował ruch sieciowy oraz diagnozował problemy, znał i stosował dobre praktyki administracyjne.

### Profil uczestników

Szkolenie jest przeznaczone dla osób, które posiadają podstawową wiedzę z zakresu sieci komputerowych i chcą rozwijać swoje umiejętności w kierunku zaawansowanej konfiguracji i administracji sieciami LAN. Szkolenie jest skierowane do administratorów IT, inżynierów sieciowych, inżynierów bezpieczeństwa sieciowego oraz osób pracujących w obszarze wsparcia technicznego, które chcą pogłębić swoje umiejętności w zakresie zarządzania nowoczesną infrastrukturą sieciową.

### Przygotowanie uczestników

Uczestnicy powinni znać:

- podstawowe zasady działania sieci komputerowych oraz ich warstwową strukturę,
- adresację IPv4 oraz podział na podsieci (subnetting),
- koncepcję segmentacji sieci za pomocą VLAN,

- podstawy routingu statycznego i routingu między VLAN-ami,
- podstawowe narzędzia diagnostyczne (ping, traceroute).

## Szczegółowy program szkolenia

### 1. Zaawansowana konfiguracja sieci LAN

- 1.1. Przegląd architektury sieci LAN – model trójwarstwowy (Access, Distribution, Core).
- 1.2. Konfiguracja i zarządzanie VLAN, Implementacja i konfiguracja trunków 802.1Q.

### 2. Mechanizmy redundancji w sieciach LAN

- 2.1. Przegląd architektury sieci LAN – model trójwarstwowy (Access, Distribution, Core).
- 2.2. Praktyczne aspekty wykorzystania i konfiguracji protokołu Spanning Tree – warianty STP.
- 2.3. Optymalizacja i zabezpieczenia protokołu STP – BPDU Guard, Root Guard, Loop Guard.
- 2.4. Agregacja łączy – konfiguracja EtherChannel (LACP, statyczny).
- 2.5. Redundancja warstwy 3 – protokoły FHRP.

### 3. Dynamiczny routing w sieciach LAN

- 3.1. Porównanie routingu statycznego i dynamicznego.
- 3.2. Konfiguracja i implementacja protokołu OSPF jednobszarowego.
- 3.3. Mechanizmy optymalizacji routingu – sumaryzacja i redystrybucja tras.

### 4. Zabezpieczenia infrastruktury LAN

- 4.1. Bezpieczeństwo portów przełączników – Port Security.
- 4.2. Bezpieczeństwo DHCP – DHCP Snooping,
- 4.3. Ochrona przed atakami ARP Spoofing, Dynamic ARP Inspection (DAI).
- 4.4. Podstawowe mechanizmy kontroli dostępu – Access Control Lists (ACL).

### 5. Podstawy monitorowania i diagnostyki sieci LAN

- 5.1. Wprowadzenie do monitorowania urządzeń sieciowych.
- 5.2. Diagnostyka problemów sieciowych z użyciem Wireshark, ping, traceroute, debug.

### 6. Automatyzacja i zarządzanie konfiguracją sieci

- 6.1. Backup i przywracanie konfiguracji – TFTP, FTP, SCP.
- 6.2. Wprowadzenie do automatyzacji sieci za pomocą Python.

### 7. Wirtualizacja sieci i usług sieciowych (demonstracja)

- 7.1. Wprowadzenie do sieci w Microsoft Azure.
- 7.2. Odzwierciedlenie wielooddziałowej struktury sieciowej w Microsoft Azure.
- 7.3. Podstawy konfiguracji dostępu do sieci wirtualnej, kontrola dostępu.
- 7.4. Wybrane usługi sieciowe w ramach Microsoft Azure.

### 8. Podstawy wykorzystania sztucznej inteligencji w monitorowaniu i administracji siecią

- 8.1. Wybrane metody i narzędzia AI do monitorowania i automatyzacji sieci komputerowych.
- 8.2. Wybrane narzędzia i metody AI do analizy logów i wykrywania incydentów.

## Metoda realizacji szkolenia

Szkolenie jest realizowane metodami takimi jak: prezentacje oraz laboratoria do samodzielnego wykonania przez uczestników z wykorzystaniem symulatora sieciowego.

## Liczba dni, liczba godzin szkoleniowych

4 dni szkoleniowe, łącznie 32 godziny lekcyjne.

## Ścieżka rozwoju po szkoleniu

- Dedykowane szkolenia poświęcone wybranym aspektom sieci komputerowych.