STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**VoIP SIETE V CISCO PACKET TRACER**

**ŠIMON ČÍK**

2025

#### **Úvod**

V tomto projekte sme sa zamerali na návrh a implementáciu siete VoIP (Voice over IP) v prostredí Cisco Packet Tracer, pričom sme využili rozšírenú konfiguráciu zahrňujúcu 10 IP telefónov a 10 PC. Naším cieľom bolo demonštrovať, ako efektívne nakonfigurovať sieť, ktorá umožňuje hlasovú komunikáciu medzi klientmi a zároveň poskytuje prístup k dátovým sieťovým službám.

#### **Popis sieťovej topológie**

**Sieť pozostáva z nasledujúcich zariadení:**

* **Router Cisco 2811:** Základné zariadenie pre smerovanie a rozhranie medzi rôznymi VLAN.
* **Switch Cisco 2960:** Použitý pre pripojenie koncových bodov a konfiguráciu VLAN.
* **IP telefóny a počítače:** 10 IP telefónov a 10 počítačov, kde každý počítač je pripojený k IP telefónu, a IP telefóny sú pripojené k switchu.

**Konfigurácia zahŕňa vytvorenie viacerých VLAN:**

* **VLAN 10 (Data):** Pre dátovú komunikáciu počítačov.
* **VLAN 20 (Voice):** Pre hlasovú komunikáciu cez IP telefóny.
* **VLAN 30 (Management):** Pre správu sieťových zariadení.
* **VLAN 40 (Miscellaneous):** Pre nevyužité porty, zvyšuje bezpečnosť.
* **VLAN 50 (Native):** Nativní VLAN pre trunk spojenia.

#### **Konfiguračné postupy**

* **Nastavenie Switchu:** Porty boli nakonfigurované na trunk a access módy podľa príslušnosti k VLAN. Pre IP telefóny a PC boli nastavené porty s podporou hlasovej a dátovej VLAN.
* **Router Konfigurácia:** Na routeri boli nakonfigurované subinterfejsy pre jednotlivé VLANy s príslušnými IP adresami. Rovnako boli nastavené DHCP pooly pre dynamické priraďovanie IP adries koncovým zariadeniam.
* **DHCP Nastavenia:** Pre obidve siete, dátovú a hlasovú, boli vytvorené samostatné DHCP pooly, ktoré zabezpečujú priraďovanie IP adries zariadeniam na základe ich VLAN príslušnosti.
* **Telefónne Služby:** Konfigurácia IP telefónov zahrnovala nastavenie TFTP servera pre stiahnutie konfiguračných súborov a nastavenie ephone-dn pre jednotlivé telefónne čísla priradené k IP telefónom.

#### **Bezpečnostné riziká**

1. **Neautorizovaný prístup:** Nezabezpečené porty môžu umožniť neautorizovaný prístup k sieťovým zdrojom.
2. **Spoofing a MITM útoky:** Nechránené VLAN môžu byť zraniteľné voči spoofing útokom a útokom typu "man-in-the-middle".
3. **Útoky na služby:** Nechránené IP telefóny a PC môžu byť cieľom DDoS útokov(kybernetické útoky, ktoré zahŕňajú zahltenie cieľového systému) alebo útokov zameraných na vyčerpanie zdrojov DHCP servera.
4. **Zneužitie protokolov:** Nesprávna konfigurácia protokolov ako DHCP alebo TFTP môže viesť k zneužitiu týchto služieb.

#### **Záver**

Dokumentovaná sieťová topológia a konfigurácia demonštrujú efektívne využitie Cisco Packet Tracer na návrh a simuláciu rozsiahlej VoIP siete. Pri ďalšom rozvoji siete je dôležité zvážiť potenciálne bezpečnostné riziká a implementovať príslušné bezpečnostné opatrenia na ich minimalizáciu.