# Konfigurace síťového prostředí

Prezentace představuje základní nástroje a postupy pro nastavení a správu sítě v operačních systémech, včetně IP adresování, DNS, firewallu, VPN a monitorování síťového provozu. Zaměřuje se na význam správné konfigurace pro stabilitu a bezpečnost sítě a obsahuje praktické příklady a diagnostické postupy pro řešení síťových problémů.

# Co je síťové prostředí?

## 1. Definice síťového prostředí

- Síťové prostředí jako prostředek pro propojení zařízení a umožnění jejich komunikace, sdílení dat a přístup ke zdrojům.

## 2. Význam síťového prostředí

- Zajišťuje přístup k serverům, tiskárnám, internetu a dalším síťovým zdrojům.
- Podpora dostupnosti a výkonu.
- Význam pro bezpečnost síťových operací.

# Co je síťové prostředí?

## 1. Základní aspekty síťového prostředí v OS

- IP adresování (statické a dynamické přidělování)
- Správa síťových adaptérů (HW pro připojení k síti)
- Konfigurace DNS (překlad doménových jmen)
- Zabezpečení sítě (Firewall a VPN)
- Monitorování a diagnostika (sledování síťového provozu)

# IP adresování

## 1. Co je IP adresa?

- Unikátní identifikátor zařízení v síti (IPv4 vs. IPv6).

## 2. Statické vs. dynamické adresy

- **Statická adresa:** Ručně přiřazena, nemění se, využívá se pro servery a síťová zařízení.
- **Dynamická adresa:** Automatické přidělení přes DHCP, ideální pro běžné klienty v síti.

## 3. Praktické příkazy pro zjištění IP adresy

- **Windows:** `ipconfig`
- **Linux:** `ifconfig` nebo `ip addr`
- **Popis výstupu příkazů:** Co jednotlivé položky znamenají (IP, subnet mask, default gateway).

## 4. Doporučení pro správné IP adresování

- Rozvržení rozsahů adres dle typu sítě (LAN, WAN).
- Pravidla pro statické a dynamické adresy (např. DHCP rozsah pro klienty, statické adresy mimo tento rozsah).

# Správa síťových adaptérů

## 1. Síťové adaptéry a jejich úloha

- Hardware pro připojení k různým typům sítí (Ethernet, Wi-Fi, mobilní sítě).

## 2. Možnosti správy adaptérů

- **Windows:** Ovládací panely > Síťová připojení, nebo přes PowerShell (`Get-NetAdapter`, `Enable-NetAdapter`).
- **Linux:** NetworkManager pro GUI nebo příkazové nástroje `ifup` a `ifdown`

## 3. Praktické příklady správy adaptérů

- Jak povolit/zakázat síťový adaptér.
- Změna nastavení adaptérů (rychlost, duplex, IP nastavení).

## 4. Řešení problémů se síťovými adaptéry

- Diagnostika problémů (např. deaktivovaný adaptér, nesprávné ovladače).
- Obnovení adaptérů (přes restartování adaptérů nebo aktualizaci ovladačů).

# Konfigurace DNS (Domain Name System)

## 1. Úloha DNS v síti

- Překlad doménových jmen na IP adresy, umožňuje uživatelům přistupovat k webovým stránkám pomocí názvů.

## 2. Typy DNS konfigurace

- **Ruční konfigurace:** Uživatel nastaví DNS server v síťovém adaptéru.
- **Automatické přidělení:** DNS servery přiděleny přes DHCP server.

## 3. Příklady DNS nastavení

- Nastavení primárního a sekundárního DNS serveru.
- Nastavení veřejného DNS (např. Google DNS 8.8.8.8).

## 4. Diagnostické příkazy pro DNS

- **Windows/Linux:** `nslookup` pro testování překladu DNS.
- **Linux:** `dig` (detaily o DNS záznamech, a odpovědi DNS serveru).

# Zabezpečení sítě

## 1. Firewall jako klíčový bezpečnostní prvek

- Filtrace příchozích a odchozích paketů dle pravidel, ochrana před neoprávněným přístupem.

## 2. Možnosti nastavení firewallu

- **Windows:** Windows Defender Firewall, PowerShell příkazy (`New-NetFirewallRule`).
- **Linux:** `iptables` (příkazové nastavení) nebo `firewalld` (pro pokročilejší pravidla).

## 3. VPN (Virtual Private Network)

- Šifrovaný kanál pro bezpečný vzdálený přístup.
- Typické konfigurace (PPTP, L2TP/IPsec, OpenVPN).
- Možnosti nastavení VPN ve Windows a Linuxu (GUI nastavení a příkazové možnosti).

## 4. Doporučení pro bezpečnost sítě

- Vytváření pravidel firewallu dle potřeb.
- Výběr a správa VPN podle bezpečnostních standardů (šifrování, autentizace).

# Monitorování a diagnostika sítě

## 1. Význam monitorování sítě

- Detekce problémů, optimalizace výkonu, předcházení výpadkům.

## 2. Nástroje pro monitorování síťového provozu

- **Windows:** Resource Monitor, Task Manager (přehled síťové aktivity aplikací).
- **Linux:** `iftop` (monitorování síťového provozu na úrovni rozhraní), `netstat` (přehled otevřených spojení).

## 3. Diagnostické příkazy

- `ping`: Kontrola dostupnosti jiného zařízení (možnost nastavit velikost paketů, počet opakování).
- `traceroute/tracert`: Sledování cesty paketů k cílovému zařízení.
- `netstat`: Zobrazení aktivních síťových spojení a poslouchajících portů.

## 4. Praktické příklady a analýza

- Krok za krokem diagnostika síťového problému (např. ztráty paketů).
- Optimalizace sítě na základě monitoringu (např. omezení aplikací zatěžujících síť).

# Příklady praktické konfigurace

## 1. Ukázky nastavení IP adres a DNS

- Nastavení IP adresy a DNS v OS Windows a Linuxu.

## 2. Firewallová pravidla a VPN připojení

- Příklady vytvoření pravidla ve firewallu.
- Konfigurace VPN (výběr protokolu, zadání přístupových údajů).

## 3. Ukázky diagnostických nástrojů v praxi

- Použití příkazů `ping`, `traceroute/tracert` a `nslookup` k řešení síťových problémů.

# Závěr

## 1. Shrnutí klíčových aspektů konfigurace síťového prostředí

- Význam správného IP adresování, konfigurace adaptérů, DNS, firewallu a VPN.

## 2. Role správné konfigurace

- Zajištění stability a bezpečnosti sítě, podpora plynulého provozu.

## 3. Monitorování a jeho význam

- Předcházení problémům a optimalizace síťového výkonu.

# Kontrolní otázky

1. Jaká je hlavní funkce DNS v síti?
2. Který příkaz zobrazí aktuální IP adresu zařízení v operačním systému Windows?
3. Jaká je základní role firewallu v operačním systému?
4. Který typ IP adresy je přidělován automaticky pomocí DHCP?
5. Jaký příkaz se používá pro kontrolu dostupnosti jiného zařízení v síti?

# Literatura


1. **Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer Networks* (5th ed.). Prentice Hall.**

   Tato kniha poskytuje komplexní přehled o principech počítačových sítí, včetně IP adresování, směrování, DNS a síťové bezpečnosti.

2. **Hucaby, D. (2020). *Cisco CCNA Command Guide: Best Commands to Learn Routing and Switching* (3rd ed.). Independently Published.**

   Praktický průvodce příkazovými nástroji a konfigurací sítě, vhodný pro pochopení správy a monitorování síťového prostředí.

3. **Microsoft Documentation - Windows Network Management (**docs.microsoft.com)

   Podrobné návody a dokumentace k síťovým nástrojům a konfiguracím v operačním systému Windows.

4. **The Linux Documentation Project - Network Management (**tldp.org)

   Užitečné zdroje pro konfiguraci a správu sítí v Linuxu, včetně IP nastavení, DNS, firewallu a dalších nástrojů pro správu.

5. **Stallings, W. (2016). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (1st ed.). Pearson Education.**

   Moderní přístup k sítím, zahrnuje správu a konfiguraci síťových prostředí s ohledem na aktuální trendy v oblasti softwarově definovaných sítí a bezpečnosti.

6. **Cisco Packet Tracer - Cisco Networking Academy (**netacad.com)

   Praktický nástroj pro simulaci a trénink síťové konfigurace, ideální pro procvičení IP adresování, DNS a firewallu v síťovém prostředí.

7. **Nmap Network Scanning (**Nmap Project. nmap.org)

   Kniha a dokumentace k nástroji Nmap, který je široce používaný pro monitorování a diagnostiku sítě.

8. **Jang, M., & Bresnahan, A. (2017). *Linux+ and LPIC-1 Guide to Linux Certification* (4th ed.). Cengage Learning.**

   Kniha obsahuje kapitoly o správě síťových nastavení, DNS a firewallu v Linuxu, vhodná i pro pokročilé uživatele.

9. **Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.**

   Výklad o síťových protokolech a správě sítě s příklady týkajícími se DNS, IP adresování a zabezpečení.

10. **Pyles, J. (2015). *Microsoft Windows Networking Essentials*. Sybex.**

    Tato příručka poskytuje přehled o správě sítě v prostředí Windows, včetně konfigurace síťových adaptérů, IP adres a zabezpečení.