Laboratorní cvičení č.2: Směrování

# Topologie

Zapojte síť dle uvedeného obrázku. Rozhraní **Ether 1** použijte pro připojení lokální sítě. Rozhraní **Ether 2** a **Ether 3** slouží pro připojení k okolním směrovačům.   
  
Pro adresování sítí použijte adresy vypočtené podle následujícího principu:

* Propojovací síť mezi směrovačem X a směrovačem Y (kde X < Y) bude mít adresu 10.X.Z.0/24
* Lokální síť směrovače X bude mít adresu: 10.X.0.0/24.

# Základní konfigurace

1. Nakonfigurujte IP adresy na všechna **Ether** rozhraní směrovače, viz **Manual\_IP\_Address.pdf**
2. Nakonfigurujte DHCP server na Mikrotiku tak, aby přiděloval dynamicky adresy klientům z lokální sítě (viz **Manual\_IP\_DHCP\_Server.pdf**). Jako DNS server použijte adresu 10.10.10.1.
3. Ověřte nastavení konfigurace pomocí příkazů ip dhcp-server print a ip pool print.
4. Nastavte na počítačích způsob získávání konfigurace pomocí DHCP protokolu.
5. Ověřte konfiguraci počítačů pomocí příkazu ipconfig/ifconfig
6. Ověřte, že směrovač je dostupný z počítače pomocí nástroje ping

# Statické směrování

Konfigurace statického směrování znamená na každém ze směrovačů uvést lokální sítě připojené k ostatním směrovačů a cestu k nim. Pozor, statické směrovací informace musí být konsistentní.

|  |
| --- |
| /ip route add dst-address= *<ip adresa sítě>* gateway= *<ip adresa next-hop zařízení>* |

Nakonfigurujte statické směrování na Vašem routeru pomocí následujícího příkazu. Uveďte všechny ostatní lokální sítě. Dejte si pozor na nastavení správného next-hop zařízení.

* Otestujte komunikaci v takto nakonfigurované síti:
  + Pomocí nástroje ping zkuste konektivitu na počítač v jiné lokální síti.
  + Pomocí nástroje tracert zjistěte cestu k počítači v jiné lokální síti
* Test dostupnosti proveďte ideálně pro všechny ostatní sítě, v případě nedostupnosti zkuste najít příčinu.

# Dynamické směrování

**Před konfigurací dynamické směrovaní odstraňte konfiguraci statického směrování.**

Nakonfigurujte směrování na Vašem routeru a sledujte jak se postupně plní směrovací tabulka.

* Zapněte šíření informací protokolem RIP o lokálních a statických sítích:

|  |
| --- |
| /routing rip set redistribute-connected=yes  /routing rip set redistribute-static=yes |

* Povolte šíření implicitní cesty, toto umožní použití vašeho přístupu do Internetu ostatním sítím v případě, že jejich implicitní cesta bude nedostupná.

|  |
| --- |
| /routing rip set distribute-default=if-installed |

* Zapněte výměnu směrovacích informací mezi směrovači (a také na rozhraní do lokální sítě pro možnost sledovat RIP komunikaci):

|  |
| --- |
| /routing rip interface all |

* Vložte obě propojovací sítě a na každém routeru jeho lokální sít:

|  |
| --- |
| /routing rip network add network= *<ip adresa propojovací sítě>*  /routing rip network add network= <*ip adresa lokálně připojené sítě>* |

* Otestujte komunikaci v takto vytvořené síti:
  + Pomocí nástroje ping zkuste konektivitu na počítač v jiné lokální síti.
  + Pomocí nástroje tracert zjistěte cestu k počítači v jiné lokální síti

Výše uvedená konfigurace by měla být dostačující. V některých případech spolu sousední směrovače nekomunikují. V tomto případě je možné vynutit zasílání RIP aktualizací na určitou adresu pomocí:

|  |
| --- |
| /routing rip neighbor <ip adresa souseda> |

# Analýza protokolu RIP

Sledujte směrovací tabulku pomocí příkazu **/ip route print** na Vašem routeru. Vyberte několik řádků a ty vyplňte do následující tabulky.

|  |
| --- |
|  |

* Programem wireshark zachyťte RIP komunikaci a vyplňte vybrané údaje o protokolu do následující tabulku:

|  |
| --- |
|  |

Zkuste upravit parametry konfigurace a sledovat jak se změnily RIP zprávy. Změňte časovače, verze zpráv a autentizaci RIP protokolu, tak jak je uvedeno dále.

## Změna časovačů:

Změna časovače pro zasílání aktualizací. Změnou tohoto časovače je možné vynutit posílání aktualizací dříve než je implicitně nastavených 30s. Pomocí následujícího příkazu zkraťte například na 5s.

|  |
| --- |
| /routing rip update-timer <hodnota v sekundách> |

## Verze zasílání zpráv

Implicitně se používá verze 2, která mimo jiné umožňuje posílat informaci o síťovém prefixu pro každou cílovou síť.. Změňte na verzi 1 a sledujte obsah RIP zpráv:

|  |
| --- |
| /routing rip interface send <v1 | v1-2 | v2 > |

Nastavte zpět verzi 2, neboť autentizace zpráv pracuje pouze v této verzi.

## Autentizace zpráv

Zapněte autentizaci RIP zpráv. Podívejte se na obsah RIP zprávy. Autentizaci je možné konfigurovat pro každé rozhraní zvlášť, proč? Zkuste různé režimy (simple nebo md5).

|  |
| --- |
| /routing rip interface <název rozhraní> authentication <none | simple | md5>  /routing rip interface <název rozhraní> authentication-key <autentizační řezězec> |

Ověřte, že směrovače mají správnou informaci ve směrovací tabulce i po zapnutí autentizace.

Pomocí programu *Wireshark* se podívejte, jak se liší autentizovaná RIP zpráva od neautentizované. Popište jaký je rozdíl mezi autentizací simple a md5:

|  |
| --- |
|  |

# Konec

Restartujte router příkazem **/system reset-configuration** aodhlašte se z PC.