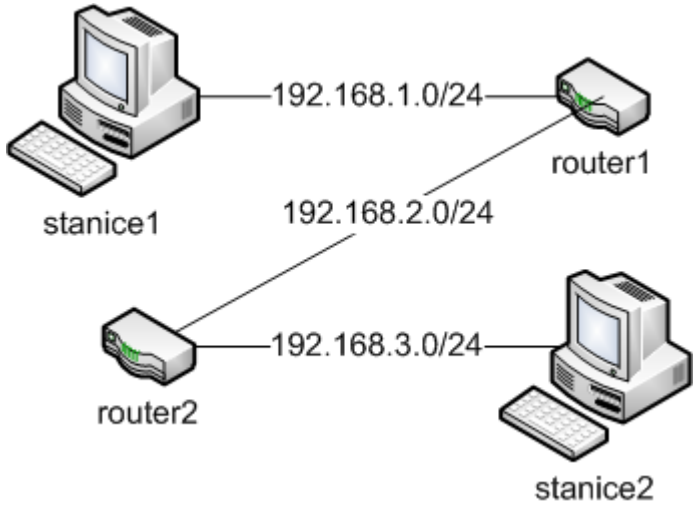
XMW3 / IW3 – Sítě 2

Štefan Pataky, Martin Poisel

TCP/IP – statické směrování

- **Úkol**
  - zprovozněte dva routery a dvě stanice podle obrázku
  - staticky přidělte adresy routerům i stanicím
  - nastavte směrování
  - zkontrolujte funkčnost pingem z jedné stanice na druhou



TCP/IP – NAT

- **NAT – network address translation (source nat)**
  - technologie k překladu privátních adres na adresy veřejné
  - umožní nám pomoci jedné veřejné IP adresy připojit celou síť do internetu
  - dále přináší jistou „anonymitu“ na internetu
  - u IPv6 se s NATem nepočítá, pro anonymitu je možné použít dočasné adresy – hostitel si pravidelně (jednou za pár hodin) generuje novou veřejnou IP adresu, kterou používá na „běžné serfování po internetu“ (více google IPv6 IATA)
- **Mapování portů (destination nat)**
  - technologie k „protunelování“ spojení z routeru na počítač na vnitřní sítí, který nemá veřejnou adresu
- **1:N NAT**
  - RFC 1918, lokální použití (privátni na verejné)

TCP/IP – Firewall

- **Firewall**
  - program/hw na filtrování síťového provozu na základě našich pravidel
- **Stavový firewall**
  - udržuje si tabulku spojení a automaticky povoluje odpovědi na vytvořená spojení
- **Paketové filtry**
  - Adresa a port (3 a 4 vrstva OSI)
  - ACL
- **Proxy brány**
  - 7 vrstava OSI
- **Stavové paketové filtry**
  - Urdžuje stav spojení, pozná protokoly (FTP 21 pro spojení 20 pro posílaní dat)
- **Stavové paketové filtry s kontrolou protokolů a IDS**

TCP/IP – VPN

- **VPN (virtual private network)**
  - technologie na bezpečný přístup do lokální sítě přes internet (nebo jinou nebezpečnou síť)
  - mnoho technologií (otevřené standardy i zavřené technologie) postavených na síťové, transportní i aplikační vrstvě
    - IP tunnel, IPSec, EoIP, teredo, 6o4, ISATAP
    - L2TP, PPTP
    - SSTP, OpenVPN
    - Direct Access (IPv6 tunelování)

TCP/IP – DNS

- **DNS**
  - slouží k překladu jména na IP adresu a naopak
  - hierarchický systém domén
  - TCP 53, UDP 53
  - RFC 1035
  - Typy záznamů
    - A
    - AAAA
    - CNAME
    - MX
    - NS
    - PTR
    - SOA

Prerekvizity pro další postup

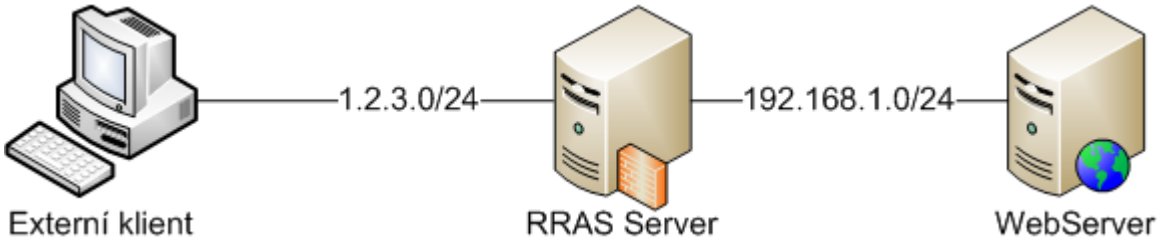
- **TCP/IP verze 4 a 6**
  - adresace
  - statické směrování
  - konfigurace DHCP a DNS v MS Windows Serveru
  - princip firewallu a NATu
- **VPN**
  - teoretický princip fungování PPTP, L2TP a SSTP

Microsoft Network Policy and Access Services

- softwarový router, vpn, a radius serverstatické směrování
- podporuje:
  - statické a dynamické
  - základní nat
  - PPTP, L2TP, SSTP a připojení modemem

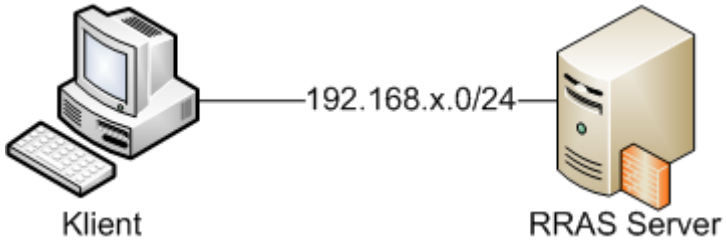
TCP/IP – MS NPAAS – NAT a Routing – řízený lab

1. Pomoci **Server Manageru** nainstalujte **DirectAccess and VPN (RAS)**
   - zvolte role services **Remote Access**
2. spusťte administrační konzoli **Routing and Remote Access**
   - klikněte **Configure and Enable RRAS**
   - na druhé záložce vyberte **Custom Configuration**
   - zatrhněte **NAT** a **LAN Routing**
   - seznamte se s konfigurací směrování a NATu
3. Podle obrázku do sítě připojte další server a klient
   - připojte do sítě další virtuální server (klidně DC) a nainstalujte na něm **webserver**
   - nastavte NAT na **RRAS** serveru a namapujte port 80 na **webserver**
   - z klienta otestujte dostupnost webových stránek
   - stejně tak, pokud na klientovi vypnete firewall, můžete otestovat **source nat** z **webserveru**



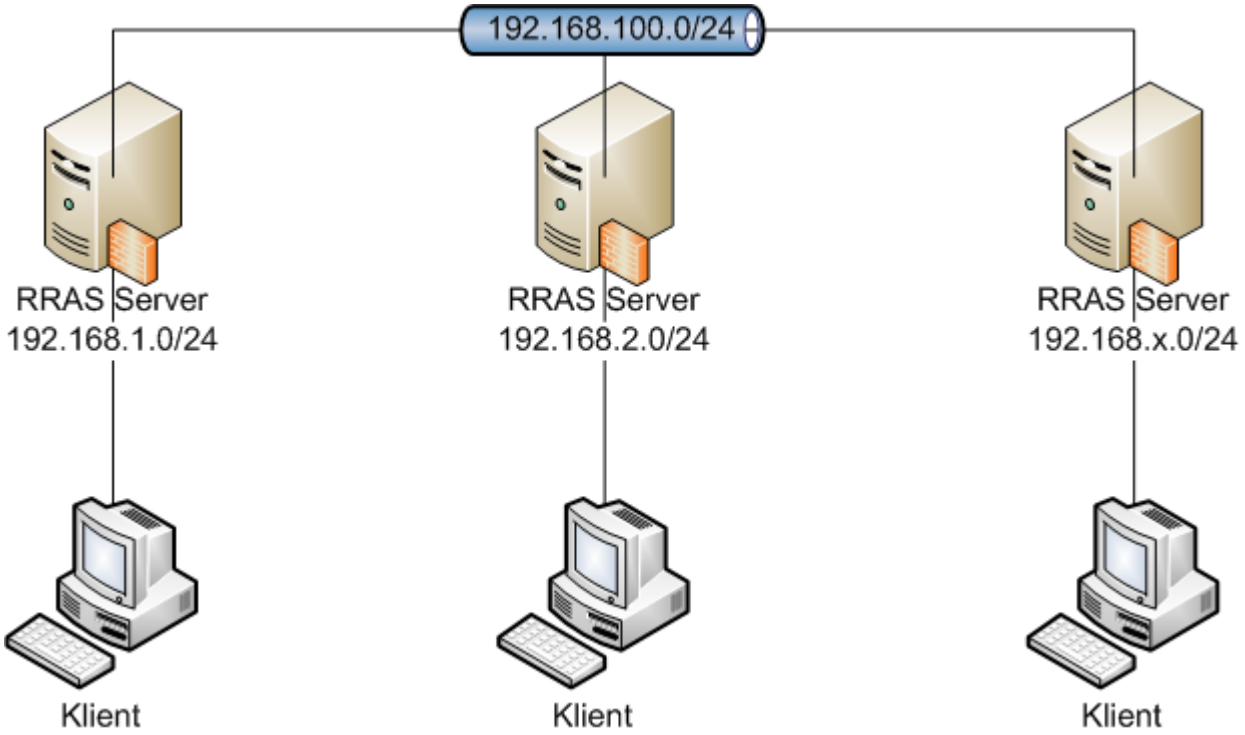
TCP/IP – MS NPAAS – Routing – samostatný lab

1. využijte **RRAS** server z předchozího labu nebo nainstalujte nový
   - pro správnou funkčnost akorát zrušte NAT
   - budete potřebovat 3. síťové rozhraní
2. do lokální sítě připojte klienta s vyplým firewall (nebo povoleným ping)
   - dle obrázku proveďte zapojení
   - IP subnet lokální sítě je podle čísla PC na kterém sedíte (PC3 má subnet **192.168.3.0/24**)



3. Podle obrázku do se propojte se zbylími kolegy
   - nastavte správně statické trasy aby se všichni dostali všude
   - nastavte NAT na **RRAS** serveru abyste se z klienta dostali na internet (lektor poradí s nastavením Hyper-V)
   - otestujte dostupnost ostatním klientů a www.google.com příkazy ping a tracert

TCP/IP – MS NPAAS – Routing – samostatný lab



4. pokud vše funguje, zaimplementujte do své konfigurace DNS a DHCP
   - nakonfigurujte DHCP server aby na vnitřním rozhraní přiděloval klientům IP adresy
   - nakonfigurjte DNS server pro zónu domenaX.local a nastavte forward dotazů pro ostatní domény na dns servery kolegů

Opakování & Dotazy

- Opakování
- Dotazy