Pracovní list Topologie počítačové sítě vzor

Josef Novák

Třída V2

**Zadání:**

Zapojte, nakonfigurujte, zkontrolujte, monitorujte a předveďte síťovou komunikaci na síti dle zadání a realizujte pomocí aktivity v PT:

K úloze vypracujte protokol (jako docx soubor) v následujícím tvaru:

* Titulní list
* Zadání
* Kopie obrazovky z aplikace Packet Tracer (vložit jako obrázek)
* IP adresace
* Použité nástroje pro identifikaci síťové komunikace
* Závěr (hodnocení)

Zkontrolujte, zachytávejte data, segmenty, pakety a zjistěte možné chyby počítačové sítě dle zadání a realizujte pomocí aktivity v PT:

Máte přepínanou síť dle přiloženého schématu viz Obrázek 1. Do sítě je připojen PC s OS Windows a aplikací Wireshark. Na serveru jsou spuštěné základní služby pro klienty - PC.

Adresace: MNGMT – 192.168.1.0/24; GUEST – 192.168.100.0/25. Propoje mezi přepínači jsou řešeny optickými propoji, ostatní metalickým propojem. Hraniční směrovač R1 a směrovač ISP je nastaven. Veřejná přidělená IP adresa směrovači R1 je 100.200.100.2/30. Přístup ke všem aktivním prvkům je řešen pomocí protokolu SSH. Použijte aplikaci Wireshark nebo virtualizační nástroj (PT) pro zachytávání paketů a diagnostické nástroje OS Windows. Zjistěte chyby a navrhněte úpravy k dosažení optimálního provozu a předveďte použité síťové protokoly u jednotlivých služeb na serveru.



Obrázek 1

Vytvořenou aktivitu v aplikaci Packet Tracer si zálohujte do PC pro další použití.

**IP adresace sítě:**

**ISP:**Veřejná IP adresa: 100.200.100.2
Maska sítě: 255.255.255.252

**R1:**Veřejná IP adresa: 100.200.100.1Maska sítě: 255.255.255.252

**MNGMT:**Adresní prostor: 192.168.1.0/24Maska sítě: 255.255.255.0Výchozí brána: 192.168.1.1

**GUEST:**Adresní prostor: 192.168.100.0/25Maska sítě: 255.255.255.128Výchozí brána: 192.168.100.1

**SERVER:**IP adresa: 192.168.1.10/24Maska sítě: 255.255.255.0Výchozí brána: 192.168.1.1

**PC:**IP adresa: 192.168.100.10/25Maska sítě: 255.255.255.128Výchozí brána: 192.168.100.1

Použité služby: DHCP, DNS, WWW, FTP, TELNET

Zjištěné a ověřené protokoly: DHCP, DNS, HTTP, HTTPS, FTP, TELNET, POP3, SMTP

Použité nástroje, příkazy a aplikace pro detekci chyb a monitorování a identifikaci síťové komunikace (cmd, ipconfig, ping, arp, net, route, netstat, virtualizační nástroj, aplikace Wireshark atd.)

Pro ověření jsme použili jak simulaci v aplikaci Packet Tracer tak a v aplikaci Wireshark.

Pomocí simulace předvedeme použití TCP/IP modelu při komunikaci PC se serverem.

1. PC (webový prohlížeč) – server (služba WWW) – důkaz TCP na portu 80 a IP adresa zdroje a cíle.
2. PC (FTP klient) – server (služba FTP) – důkaz TCP, UDP na portech 20 a 21 a IP adresa zdroje a cíle.
3. PC (klient DHCP) – server (služba DHCP) – důkaz TCP, UDP na portech 67 a 68 a IP adresa zdroje a cíle.
4. PC (klient DNS) – server (služba DNS) – důkaz TCP, UDP na portu 53 a IP adresa zdroje a cíle.
5. PC (poštovní klient) – server (poštovní služba) – důkaz TCP na portech 110 a 25 a IP adresa zdroje a cíle.

**Obrázky a licence:**

* Použitá aktivita je vytvořena autorem materiálu v aplikaci pro virtualizaci počítačových sítí (Packet Tracer od firmy Cisco, který je zdarma).
* Obrázek je kopií obrazovky z aplikace Packet Tracer

**Závěr (hodnocení):**

Zde žáci doplní vlastní hodnocení (např. s čím měli problémy, co funguje jinak, než si mysleli atd.