České vysoké učení technické v Praze
Fakulta elektrotechnická

Semestrální práce

Správa počítačových sítí

Konfigurace malé sítě

Daniel Milde

Studijní program: Softwarové technologie a management

Obor: Softwarové inženýrství

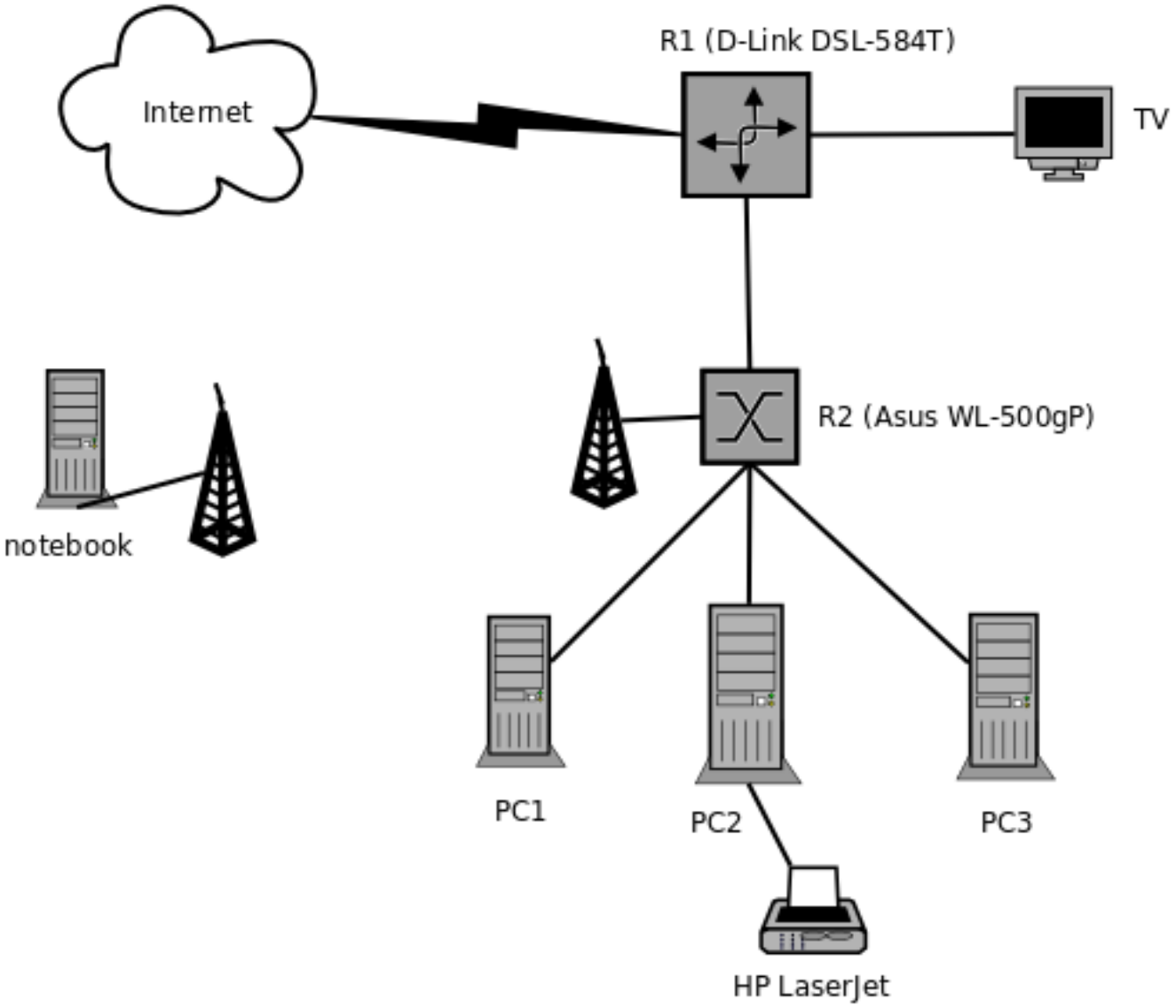
květen 2009

Obsah

1 Zadání

Cílem semestrální práce je lépe nakonfigurovat malou síť s důrazem na využití všech možností použitého hardwaru. V současné době je síť nastavena jen velmi jednoduše: chybí jakákoliv bezpečnostní politika, není využito všech možností routeru Asus WL-500gP, tiskárna je sdílena přes SMB, NAT má pouze základní nastavení, firewall je vypnut. Kromě vytvoření bezpečnostní politiky, návrhu nové topologie a nastavení základních služeb (DHCP, NAT, firewall, DNS, SMB, SSH, FTP) se pokusím zprovoznit také wake-on-lan a VPN.

2 Původní stav sítě



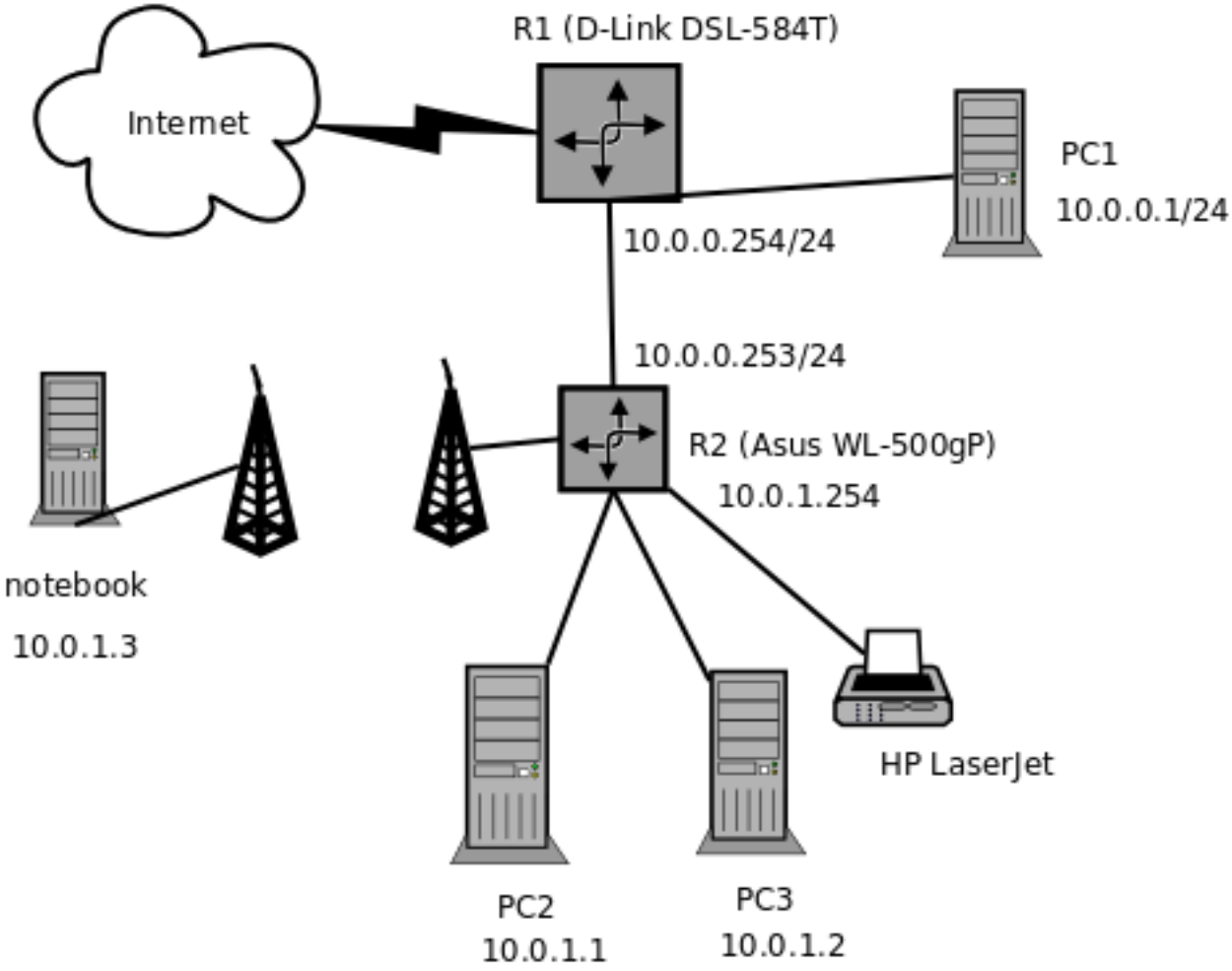
Celá síť je nakonfigurována jen velmi povrchně. Jediné, co je nastaveno obstojně je WiFi.

- firewall není nastaven vůbec
- DNS a FTP není provozněno
- pro tisk je nutné mít zapnutý PC2 (sdílení přes SMB)

3 Návrh

3.1 Topologie

Rozhodl jsem se pro vytvoření DMZ, kam bude umístěn PC1 (linux). Změna topologie bude tedy spočívat v rozdělení sítě na dvě (přepnutí R2 ze switch módu do router módu) a přepojení PC1 přímo do R1. DMZ bude mít IP adresu 10.0.0.0/24, vnitřní síť pak 10.0.1.0/24. Klientské stanice budou číslovány od spodu adesního rozsahu, směrovače od shora. Všechny IP adresy budou přidělovány pomocí dvou DHCP serverů podle MAC adres stanic.



3.2 Bezpečnostní politika

Pro komunikaci WAN-LAN bude zvolena politika: co není explicitně povoleno, je zakázáno. V opačném směru bude přístup přesně opačný. Na routeru R1 budou pro komunikaci WAN-LAN otevřeny pouze porty pro SSH, FTP a VPN. Směrovač R2 nebude mít pro komunikaci WAN-LAN otevřen port žádný, povoleno bude pouze navazování komunikace ven.

3.3 Služby

Na PC1 bude spuštěn DNS server a SSH démon. Pro PC1 se pokusím zprovoznit také wake-on-lan. FTP server a VPN server se pokusím zprovoznit přímo na R2.

4 Realizace

4.1 Konfigurace hostingu

Vytvořen A záznam home.milde.cz směřující na veřejnou IP adresu.

4.2 Konfigurace R1

- Nastaveno DHCP (DNS1: 10.0.0.5, DNS2: 10.0.0.254).
- PC1 umístěn do DMZ. Kvůli nastavení bylo nutné změnit IP adresu na 10.0.0.5 (ověřena vzdálená funkčnost HTTP a SSH).
- Spuštěn firewall.
- Zapnuto hlídání SYN flood, ICMP rediraction. Zapnuta Port Scan Protection.

4.3 Konfigurace R2

- Do routeru R2 nainstalován nejnovější firmaware upravený od Olega[1].
- Mód routeru R2 změněn na HomeGateway. V tomto módu je automaticky spuštěn NAT.
- Nastaven DHCP server (přidělování podle MAC adres) i klient (příjem IP adresy a DNS serverů od R1).
- U R2 nastaven firewall (DoS protection, ICMP filtering). Ze zkušností doporučuji nekombinovat nastavování přes webové rozhraní a iptables.
- Zprovozněna podpora SSH (podle návodu Olega).
- Na firewallu otevřeny pouze porty pro SSH a HTTP.
- K R2 připojena tiskárna HP LaserJet, tisk na jednotlivých stanicích nastaven podle návodu Olega.
- WiFi zabezpečena pomocí WPA-TKIP. Přístup omezen pomocí seznamu povolených MAC adres.
- K R2 připojen 1GB flash disk a namountován jako FTP úložiště. Spuštěna služba FTP bez anonymního účtu.
- VPN se zprovoznit nepodařilo, bude proto zprovozněno na PC1.

4.4 Konfigurace PC1 - Ubuntu linux

- V BIOSu povoleno power/wake-on-lan.
- Nainstalováno SSH, OpenVPN.
- Nakonfigurováno OpenVPN[2] [3].

[1] *http://oleg.wl500g.info/*
[2] *http://openvpn.net/index.php/documentation/howto.html#quick*
[3] *http://www.thebakershome.net/openvpn_tutorial*

- Nainstalováno a nakonfigurováno DNS.
- Wake-on-lan bohužel nesplňuje, co jsem očekával - vzdálené spuštění počítače. Je možné budit pouze počítače lokální při znalosti jejich MAC adresy.

4.5 Konfigurace PC4 (notebook) - Ubuntu linux

- Nainstalováno network-manager-openvpn.

5 Závěr

Přestože se nepodařilo zprovoznit veškerou plánovanou funkcionalitu, považuji provedené změny za velký pokrok. Síť je nyní mnohem lépe zabezpečena a důležité služby jsou dostupné i vzdáleně.