

SPRAWOZDANIE Z LABORATORIUM

Sieci komputerowych

Karol Kozłowski Karol Nikšcin Mirosław Rogotowicz Łukasz Sujka	Grupa lab.: 4	Termin: WTOREK/N 13¹⁵	Data: 24-10-2006
Ćwiczenie nr 4 Instalacja Routera (D-Link DI-604)			Ocena

1. **Celem ćwiczenia** jest zapoznanie się z podstawowymi problemami związanymi z budową niewielkiej sieci LAN podłączonej do sieci WAN. W ramach ćwiczenia student zapoznaje się: z budową kabla sieciowego UTP, gniazdek RJ45, konfiguracją stacji i routera umożliwiającą korzystanie z sieci Internet, podstawowymi metodami zabezpieczenia sieci LAN podłączonej do sieci WAN.

2. Przebieg ćwiczenia:

- 2.1. Odczytaliśmy adresy sieciowe przydzielone przez serwer DHCP aby ustawić je później na routerze:

- IP: 156.17.43.33
- Mask: 255.255.255.224
- Bramka: 156.17.43.62
- DNS: 156.17.30.100, 156.15.5.2

- 2.2. Zarobiliśmy kabel typu „skrętka” (UTP) 1:1 aby móc podłączyć wszystkie urządzenia ze sobą.

- 2.3. Podłączyliśmy router i ustawiliśmy na nim statyczne adresy uprzednio odczytane z komputera. Następnie skonfigurowaliśmy serwer DHCP w sieci LAN tak, aby przydzielał adresy z puli: 192.168.0.10 – 192.168.0.20.

- 2.4. Po odświeżeniu ustawień komputerów zostały im przydzielone adresy:

- 192.168.0.15 (lab03-k01)

- 192.168.0.20 (lab03-k02)

2.5. Po uzyskaniu adresów można było korzystać z dostępu do sieci internet (np.: serwisów internetowych takich jak wp.pl czy onet.pl)

2.6. Filtrowanie pakietów:

a) **IP Filter.** Włączyliśmy filtrowanie pakietów dla następujących adresów:

192.168.0.18 - 192.168.0.22; TCP 0-2000. Po czym komputer lab03-k02 nie mógł korzystać z większości popularnych usług internetowych ze względu na blokowanie portów <1024.

b) **MAC Filters.** Skonfigurowaliśmy blokowanie adresów MAC tak, aby dostęp miały komputery z tzw. „białej listy”. Dodaliśmy MAC-adres komputera lab03-k02 i tylko ten host miał dostęp do sieci zewnętrznej. Następnie dodaliśmy adres drugiego komputera w wyniku czego ten komputer również uzyskał dostęp do internetu.

c) **URL Blocking.** Do listy blokowanych wyrażeń dodaliśmy „bla” oraz „wp” p czym dostęp do stron, których URL'e zawierały podane wyrażenia został zablokowany.

d) **Domain Blocking.** Zablokowaliśmy dostęp do domeny onet.pl. Po tej operacji dostęp do tej strony (oraz innych usług na onet.pl) został zablokowany.

2.7. Firewall

a) Dodaliśmy regułę odrzucającą pakiety ICMP z sieci LAN wysyłane do hosta 212.77.100.101 (wp.pl) po tej operacji „pingowanie” tego serwera stało się niemożliwe. Potem zablokowaliśmy tylko TCP:80 do 212.77.100.101 (wp.pl) - od tego momentu pomimo, że „pingowaliśmy” wp.pl serwer http nie odpowiadał na żądania przeglądarki.

3. Wnioski:

3.1. Badane przez nas urządzenie jest bardzo powszechnie stosowane do udostępniania internetu w sieciach lokalnych/domowych. Pozwala udostępnić takie łącze dla wielu użytkowników dysponując tylko jednym łączem fizycznym.

- 3.2.Opcjom takim jak IP Filter czy Firewall można nadać restrykcje czasowe, czyli zabronić klientom pewnych usług w zależności od, godziny, dnia tygodnia itp...
- 3.3.Metoda blokowania adresów opisane w punkcie 2.5.c oraz 2.5.d są niedoskonałe, ponieważ łatwo je obejść znając adres IP odpowiadający blokowanej domenie.
- 3.4.Niestety nie udało nam się skonfigurować urządzenia tak, aby blokowało przychodzące żądania echa (ICMP, ping) z sieci zewnętrznej (WAN). Może to być spowodowane błędami w oprogramowaniu urządzenia. Ponieważ odpowiednie opcje istnieją ale router na nie nie reaguje.