ZAKŁAD SYSTEMÓW KOMPUTEROWYCH

Teletransmisja i sieci komputerowe

LABORATORIUM

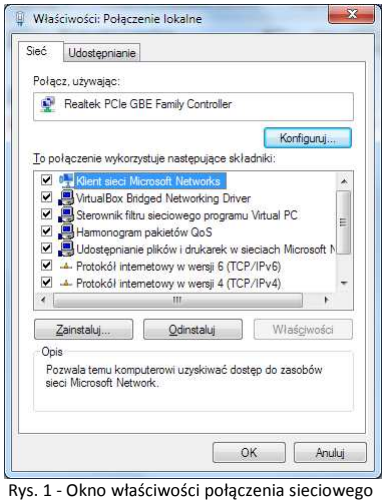
Tomasz Orczyk

Bielsko-Biała 2010-2011

Zajęcia 1

Konfiguracja sieci w systemie Windows® Seven™

W celu wyświetlenia apletu konfiguracji sieci należy z *Menu Start* wybrać *Panel Sterowania -> Centrum Sieci i Udostępniania*, w otwartym oknie z listy po lewej stronie należy wybrać pozycję *Zmień ustawienia karty sieciowej*, a następnie z menu kontekstowego połączenia należy wybrać opcję *Właściwości*.



Rys. 1 - Okno właściwości połączenia sieciowego

W oknie tym mamy możliwość konfiguracji karty kontrolera sieci oraz dodawania, usuwania i konfiguracji składników. Składniki dzielą się na następujące kategorie:

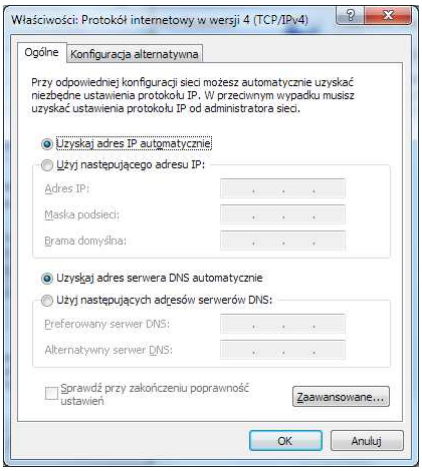
- Klient
- Usługa
- Protokół

Składnikiem niezbędnym do podłączenia stacji roboczej do sieci Internet jest *Protokół internetowy w wersji 4 (TCP/IPv4)*, ponadto składnikami koniecznymi do udostępniania plików i drukarek w sieci lokalnej jest *Klient sieci Microsoft Networks* oraz usługa *Udostępnianie plików i drukarek w sieciach Microsoft Networks*.

Warto tu wspomnieć na temat pewnych problemów i różnic w funkcjonowaniu usługi udostępniania plików i drukarek w różnych wersjach systemu Windows®. Systemy rodziny Windows® 9x posiadały udostępnianie na hasło, Windows® NT™ wprowadził udostępnianie dla użytkownika (nazwa użytkownika i hasło), natomiast w Windows® Vista™ doszła *Grupa Domowa*. Najczęstszym problemem związanym z uwierzytelnianiem na podstawie kont użytkowników jest istnienie na komputerach w sieci kont o tej samej nazwie lecz z różnymi hasłami. W przypadku gdy na komputerach są różne konta możliwe jest udostępnianie dla konta *Gość*, ale w nowszych systemach jest ono domyślnie wyłączone, podobnie jak udostępnianie dla kont, które nie mają założonego hasła. Drugim częstym problemem jest niewłaściwa konfiguracja firewalla na komputerze, który został wybrany *Główną Przeglądarką* (Master Browser). Jeśli taki komputer będzie miał możliwość rozgłaszania do sieci, że jest domyślną przeglądarką, a jednocześnie jego firewall będzie blokował nowe połączenia przychodzące z wewnątrz sieci, *Otoczenie sieciowe* przestanie funkcjonować. Główna Przeglądarka jest usługą gromadzącą i udostępniająca informacje na temat zasobów udostępnionych w sieci lokalnej, jej alternatywą jest serwer WINS. Dodatkowo istnieje możliwość ręcznego skojarzenia nazw NetBIOS z adresami IP stacji roboczych poprzez dodanie odpowiednich wpisów do pliku *LMHOSTS* (podobną

funkcjonalność w odniesieniu do nazw domenowych ma plik *HOSTS*). W celu grupowania komputerów w obrębie jednej sieci LAN można się posłużyć *grupami roboczymi*. Ich konfiguracja sprowadza się do zmiany nazwy grupy do której jest przypisany dany komputer (domyślnie jest to grupa *MSHOME*). Nazwę grupy roboczej określamy w *Panel sterowania -> System i zabezpieczenia -> System -> Nazwa komputera, domena i ustawienia grupy roboczej -> Zmień ustawienia -> Nazwa komputera -> Zmień… -> Grupa robocza: [ ]*. Po zmianie nazwy grupy roboczej konieczny jest restart systemu. Nazwa grupy roboczej nie powinna być dłuższa niż 15 znaków i nie powinna zawierać znaków specjalnych. Warto również pamiętać iż włączając usługę udostępniania plików automatycznie udostępniamy wszystkie partycje naszego dysku w ukrytych udziałach, tzw. administracyjnych, do których pełne prawa ma konto lokalnego administratora. Nazwy ukrytych udziałów kończą się znakiem *$*, co można wykorzystać przy tworzeniu własnych udziałów. W celu uzyskania większej liczby szczegółów i ciekawostek dotyczących usługi SMB polecam stronę **http://banita.pl/konf/smb.html**.

Konfiguracja protokołu TCP/IPv4 sprowadza się do określenia źródła uzyskiwania adresu IP oraz konfiguracji serwerów DNS. Okno konfiguracja *TCP/IPv4* prezentuje się następująco:



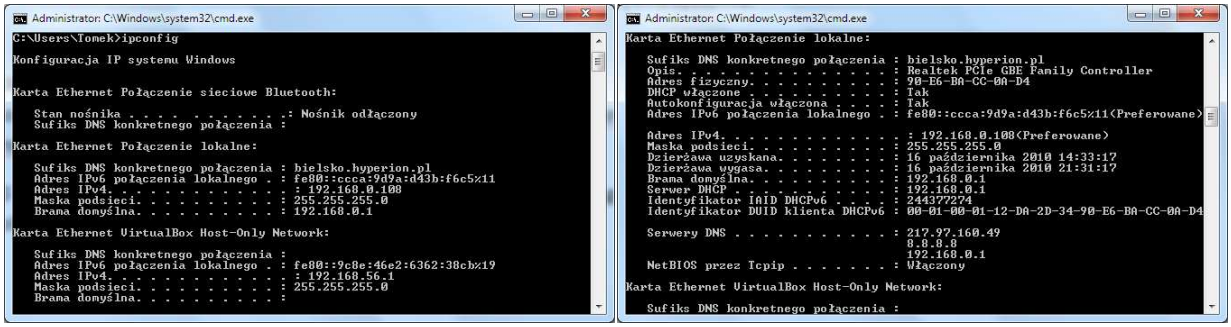
Rys. 2 – Okno właściwości protokołu TCP/IPv4

W przypadku wybrania opcji Uzyskaj adres IP automatycznie system będzie próbował pozyskać konfigurację IP z serwera DHCP (możemy jednak wymusić używanie wprowadzonego ręcznie serwera DNS), w razie niepowodzenia będą obowiązywały ustawienia z zakładki *Konfiguracja alternatywna*, w której możemy wybrać pomiędzy przydzieleniem losowego adresu z puli APIPA (169.254.0.0/24), a statyczną konfiguracją IP. W przypadku ręcznego określenia konfiguracji IP musimy określić przynajmniej Adres IP i maskę, choć do dostępu do Internetu niezbędne będzie podanie bramy domyślnej oraz serwera/ów DNS. Serwery DNS służą do tłumaczenia nazw domenowych na adresy IP. Dodatkowo, jeśli w sieci LAN nie ma lokalnego serwera DNS, w ustawieniach zaawansowanych DNS warto wyłączyć opcję *Zarejestruj adresy tego połączenia w DNS*.

Narzędzia do diagnostyki sieci

Podstawowe narzędzia służące do diagnostyki sieci to: *ipconfig*, *ping*, *tracert*, *pathping*, *netstat*, *arp* i *route*[1] oraz nieco bardziej zaawansowane narzędzie – *netsh*[2].

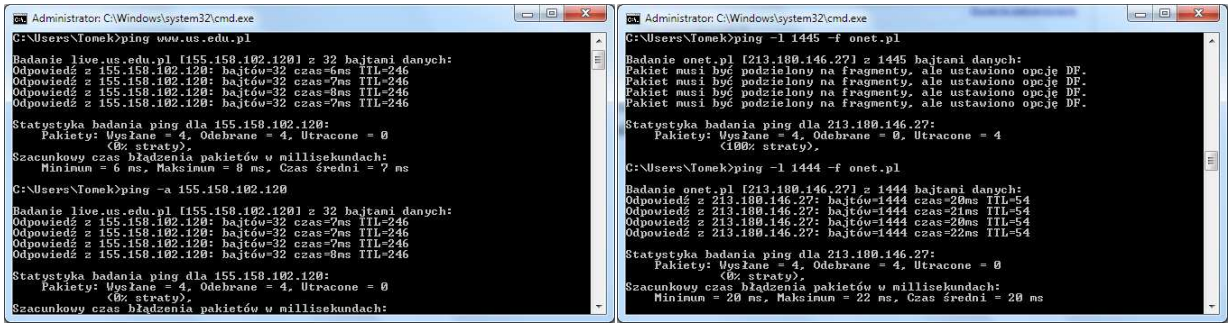
IPCONFIG jest poleceniem umożliwiającym wyświetlenie aktualnej konfiguracji interfejsów sieciowych obecnych w systemie. W celu wyświetlenia bardziej szczegółowych informacji należy użyć przełącznika */ALL*.



Rys. 3 - Wynik polecenia IPCONFIG i IPCONFIG /ALL

W podstawowej wersji wyświetlony zostanie adres IP, maska oraz brama domyślna, wersja rozszerzona podaje dodatkowo m. in. adresy DNS, adres fizyczny oraz nazwę karty sieciowej jak również adres serwera DHCP i czas dzierżawy adresu IP.

PING jest podstawowym narzędziem do diagnostyki sieci. Działa w oparciu o protokół ICMP, a jego głównym zastosowaniem jest sprawdzanie łączności z innym komputerem w sieci.

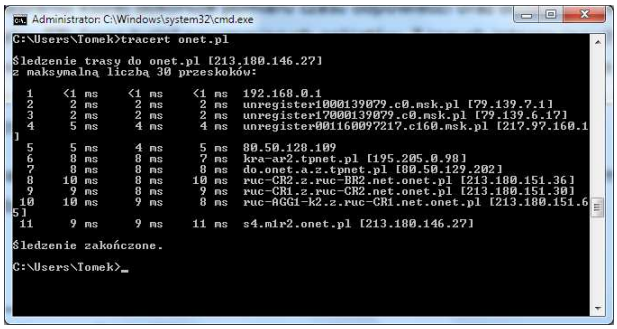


Rys. 4 - Wyniki polecenia PING z różnymi parametrami

W standardowym wywołaniu wysyła cztery pakiety do hosta o wskazanym adresie i oczekuje jego odpowiedzi, po odebraniu której dokonuje pomiaru czasu odpowiedzi oraz dodatkowo wyświetla informację o wartości parametru TTL (czas życia) powracających pakietów. Z innych interesujących zastosowania tego polecenia warto wspomnieć o przełączniku -a umożliwiającym ustalenie nazwy hosta na podstawie jego adresu IP (operacja Reverse DNS), oraz parametrach -l <rozmiar> i -f które użyte razem umożliwiają ustalenie maksymalnego rozmiaru datagramu (MTU) przesyłanego bez fragmentacji.

[1] http://commandwindows.com/tcpiputil.htm
[2] http://commandwindows.com/netsh.htm

TRACERT jest narzędziem służącym do śledzenia trasy pakietów między naszym komputerem, a hostem docelowym. Podobnie jak PING wykorzystuje protokół ICMP.



Rys. 5 - Wynik polecenia TRACERT

PATHPING jest połączeniem obydwu w/w narzędzi – śledzi trasę pakietu i jednocześnie bada dostępność i stabilność czasów odpowiedzi każdego z węzłów pośrednich trasy.

NETSTAT pozwala na uzyskanie informacji na temat aktywnych połączeń sieciowych, portów oczekujących na połączenia (-a) oraz na wyświetlenie statystyk połączenia (-e) i tabeli trasowania (-r).

ARP z przełącznikiem -a umożliwia podgląd tablicy ARP, czyli tablicy kojarzącej adresy IP (logiczne) z adresami MAC (fizycznymi).

ROUTE z przełącznikiem *PRINT* umożliwia wyświetlenie tablicy routingu (trasowania), efekt wydania tego polecenie jest tożsamy z efektem polecenie *netstat -r*.

NETSH jest poleceniem służącym przede wszystkim do konfiguracji składników sieciowych systemu (umożliwia tworzenie skryptów konfiguracyjnych), można go również użyć również do przejrzenia bieżącej konfiguracji. W Windows® XP™ posiadał dodatkowe funkcje diagnostyczne (poziom *DIAG*), których jednak został pozbawiony w nowszych systemach. Przykładowo polecenie *netsh **int**erface ipv4 **sh**ow **conf**iguration* wyświetli bieżącą konfigurację protokołu IPv4 na wszystkich interfejsach – efekt działania będzie podobny do polecenia *ipconfig*. Narzędzie może działać w trybie wsadowym bądź interaktywnym.

Typowa procedura diagnostyczna sieci składa się z następujących kroków:

- PING 127.0.0.1 – w celu sprawdzenia poprawności funkcjonowania sterownika sieci;
- IPCONFIG /ALL – w celu zweryfikowania przyznania prawidłowego adresu IP, bramy domyślnej oraz adresów serwerów DNS;
- PING <adres IP bramy domyślnej> – w celu sprawdzenia dostępności bramy domyślnej i możliwości „wyjścia” poza lokalny interfejs;
- PING <adres IP serwera poza bramą> – w celu sprawdzenia poprawności funkcjonowania łącza dostępowego do Internetu (dobrym pomysłem jest „spingowanie” serwera DNS);
- PING <nazwa domenowa serwera poza siecią> – w celu sprawdzenia poprawności działania serwerów DNS.

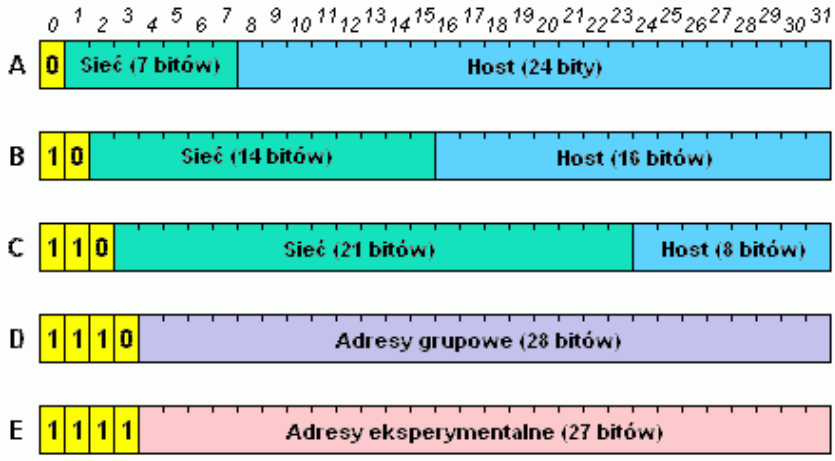
Zajęcia 2

Adresacja IP v4

Wstęp

Adres IP jest 32 bitową liczbą identyfikującą węzeł sieci. Tradycyjnie zapisywany jest w postaci dziesiętnej z rozbiciem na bajty, jednak podczas wszelkich obliczeń i przekształceń należy go traktować jako pojedynczą liczbę.

Historycznie adresy IP dzielą się na klasy A, B, C oraz specjalne D i E. O przynależności adresu do danej klasy decydują najstarsze bity pierwszego oktetu. Klasy A, B i C określają sieci różnej wielkości i odpowiadają im maski /8, /16 i /24.



Rys. 6 - Schemat budowy adresu IP v4

Powyższa tabela przekłada się na następujące zakresy adresów:

Klasa	*Najniższy adres*	*Najwyższy adres*	*Maska*
A	1.0.0.0	127.255.255.255	/8
B	128.0.0.0	191.255.255.255	/16
C	192.0.0.0	223.255.255.255	/32
D	224.0.0.0	239.255.255.255	-
E	240.0.0.0	255.255.255.255	-

Tab. 1 - Klasy adresów IP

W każdej z klas (a właściwie w każdej z sieci) istnieją dwa adresy zarezerwowane:

- adres hosta = 0 -> adres sieci,
- adres hosta = max -> adres rozgłoszeniowy.

Dodatkowo istnieją adresy specjalne – sieć 127.0.0.0/8 to pętla zwrotna, natomiast adres 0.0.0.0 to trasa domyślna.

W sieciach klas A, B i C zarezerwowano również pewną pulę adresów dla sieci LAN, są to tzw. Adresy prywatne bądź nieroutowalne:

Klasa	*Adresy sieci*	*Liczba sieci*	*Adres VLSM*
A	**10.0.0.0**	**1**	**10.0.0.0/8**
B	**172. 16.0.0 – 172.31.0.0**	**16**	**172.16.0.0/12**
C	**192.168.0.0 – 192.168.255.0**	**256**	**192.168.0.0/16**

Tab. 2 - Adresy prywatne

Istnieje również grupa adresów dla automatycznej adresacji IP – APIPA: 169.254.0.0/16.

W późniejszym okresie wprowadzono adresację bezklasową – opiera się ona o tzw. maski sieci, które określają która część adresu jest adresem sieci (1), a która jest adresem hosta (0). Maska może być zapisywana podobnie jak adres IP – dziesiętnie w formie czterech oktetów, bądź „binarnie" jako liczba początkowych bitów, które są ustawione (=1). Zapisowi 255.255.0.0 odpowiada więc zapis /16, maska ta jest zaś przynależna klasie adresowej B.

Wyznaczanie adresu sieci i rozgłoszeniowego

W celu wyznaczenia adresu sieci na podstawie adresu hosta należy wykonać operację iloczynu logicznego (AND) na adresie hosta i masce sieci.

Poniższy przykład przedstawia obliczenia dla adresu 192.168.245.196/26.

SIEĆ																										HOST					
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0
AND (&)																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	1	1	1	1	0	1	0	1	.	1	1	0	0	0	1	0	0
=																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	1	1	1	1	0	1	0	1	.	1	1	0	0	0	0	0	0

Rys. 7 - Obliczanie adresu sieci

Adres sieci – 192.168.245.192.

W celu wyznaczenia adresu rozgłoszeniowego należy wykonać operację sumy logicznej (OR) na adresie hosta i negacji (NOT) maski sieci:

SIEĆ																										HOST					
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0
NOT (~)																															
0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0	.	0	0	1	1	1	1	1	1
OR (|)																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	1	1	1	1	0	1	0	1	.	1	1	0	0	0	1	0	0
=																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	1	1	1	1	0	1	0	1	.	1	1	1	1	1	1	1	1

Rys. 8 - Obliczanie adresu rozgłoszeniowego

Adres rozgłoszeni owy - 192.168.245.255.

Podział na podsieci

Sieci można dzielić na mniejsze sieci – jest to tzw. podział na podsieci. Do podziału na podsieci można wykorzystać od 1 do n-2 bitów adresu hosta, gdzie n to liczba bitów adresu hosta (zer w masce sieci). Podział zawsze dokonuje się na podsieci o równej wielkości, ale możliwy jest dalszy podział podsieci na kolejne podsieci w celu uzyskania podsieci mieszczących różne ilości hostów. Należy zawsze pamiętać aby podziału dokonywać od największych podsieci, do najmniejszych.

Poniższy przykład pokazuje podział sieci 192.168.0.0/24 na 4 podsieci mieszczące 100, 50, 10 i 10 hostów:

- Wyznaczenie ilości bitów potrzebnych do zaadresowania wskazanej liczby hostów / maski:
  - 100 hostów -> 7 bitów (max. liczba adresów: 2^7= 128) ->maska /25
  - 50 hostów -> 6 bitów (max. liczba adresów: 2^6=64) -> maska /26
  - 10 hostów -> 4 bity (max. liczba adresów: 2^4=16) -> maska /28
- Wyznaczenie adresów podsieci pierwszego rzędu:

SIEĆ																								HOST							
Sieć bazowa																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0
Maska sieci bazowej																															
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	0	0	0	0	0	0	0	0
SIEĆ																								P	HOST						
Maska podsieci pierwszego rzędu																															
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	0	0	0	0	0	0	0
Adres pierwszej podsieci pierwszego rzędu																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0
Adres drugiej podsieci pierwszego rzędu																															
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	0	0	0	0	0	0	0

Wybieramy pierwszą podsieć do użytku dla 100 komputerów, a drugą dzielimy na kolejne podsieci.

PODSIEĆ A: **192.168.0.0**/25

- Wyznaczenie adresów podsieci drugiego rzędu:

SIEĆ																										HOST							
Sieć bazowa																																	
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	0	0	0	0	0	0	0
Maska sieci bazowej																																	
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	0	0	0	0	0	0	0
SIEĆ																									P	HOST							
Maska podsieci drugiego rzędu																																	
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0
Adres pierwszej podsieci drugiego rzędu																																	
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	0	0	0	0	0	0	0
Adres drugiej podsieci drugiego rzędu																																	
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	1	0	0	0	0	0	0

Wybieramy pierwszą podsieć do użytku dla 50 komputerów, a drugą dzielimy na kolejne podsieci.

PODSIEĆ B: **192.168.0.128**/26

- Wyznaczenie adresów podsieci trzeciego rzędu:

SIEĆ																								HOST					
Sieć bazowa																													
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	0	0	0	0	0	0
Maska sieci bazowej																													
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0
SIEĆ																								P		HOST			
Maska podsieci trzeciego[3] rzędu																													
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	0	0	0	0
Adres pierwszej podsieci trzeciego rzędu																													
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	1	0	0	0	0	0	0
Adres drugiej podsieci trzeciego rzędu																													
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	1	0	1	0	0	0	0
Adres trzeciej podsieci trzeciego rzędu																													
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	1	1	0	0	0	0	0
Adres czwartej podsieci trzeciego rzędu																													
1	1	0	0	0	0	0	0	.	1	0	1	0	1	0	0	0	.	0	0	0	0	0	0	0	0	.	1	1	1	1	0	0	0	0

Wybieramy dwie pierwsze podsieci do użytku dla 10 komputerów, reszta adresów pozostaje wolna. Pozostałe dwie podsieci możemy dalej dzielić na kolejne podsieci, bądź potraktować je jako sieć **192.168.0.224**/27.

PODSIEĆ C: **192.168.0.192**/28

PODSIEĆ D: **192.168.0.208**/28

Jak widać z powyższego nie jest konieczne rozszerzanie podsieci po jednym bicie, możliwy jest podział od razu na większą liczbę mniejszych podsieci. Można jednak zauważyć inną prawidłowość:

PODSIEĆ A: **192.168.0.0** na 128 adresów,

PODSIEĆ B: 192.168.0.0 + 128 = **192.168.0.128** na 64 adresy,

PODSIEĆ C: 192.168.0.128 + 64 = **192.168.0.192** na 16 adresów,

PODSIEĆ D: 192.168.0.192 + 16 = **192.168.0.208** na 16 adresów.

[3] Formalnie jest to podsieć czwartego rzędu.

Zajęcia 3

Adresacja IP v4 - ćwiczenia

1. Określ adres sieci, adres rozgłoszeniowy, klasę adresową oraz numer podsieci (licząc od 1 i przyjmując, że sieć danej klasy została podzielona na maksymalną liczbę podsieci z daną maską) dla podanych adresów IP:
    a. 192.168.100.230/28
    b. 10.250.130.180/24
    c. 172.20.1.230/26
    d. 192.168.250.163/25
    e. 172.22.36.12/20
    f. 10.0.100.10/20
    g. 192.168.24.199/28
    h. 172.30.111.55/18
    i. 10.10.10.10/14
2. Mając dany adres sieci, podziel ją na minimalnych rozmiarów podsieci posiadające co najmniej tyle ile podano **użytecznych** adresów IP:
    a. 172.18.0.0 {100, 50, 300, 200}
    b. 172.16.0.0 {50, 10, 1000, 600}
    c. 172.17.0.0 {25, 40, 200, 400}
    d. 10.0.0.0 {400, 5000, 50, 1000}
    e. 10.0.0.0 {500, 600, 700, 800}
    f. 10.0.0.0 {1000, 5000, 2000, 40}
    g. 192.168.10.0 {20, 10, 50, 50}
    h. 192.168.100.0 {60, 30, 30, 100}
    i. 192.168.1.0 {10, 10, 30, 60}

Wskazówki

Pamiętaj, że adres sieci jest zawsze parzysty (najmłodszy bit wyzerowany), natomiast adres rozgłoszeniowy jest zawsze nieparzysty (najmłodszy bit ustawiony). Adresy użyteczne zawierają się między adresem sieci, a adresem rozgłoszeniowym, więc pierwszy jest zawsze nieparzysty, a ostatni parzysty.

Pamiętaj, że 16 adresów to jest np. od 192.168.0.0 do 192.168.0.15, a nie 192.168.0.16 i że taka sieć posiada 14 użytecznych adresów, więc w praktyce pomieści 13 komputerów i jeden router.

Aby ułatwić sobie podział na podsieci można się posłużyć następującą tabelą:

Max host.	8190	4094	2046	1022	510	254	126	62	30	14	6	2
Il. adr.	8192	4096	2048	1024	512	256	128	64	32	16	8	4
Maska	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30
Nast. sieć +	.32.0	.16.0	.8.0	.4.0	.2.0	.1.0	.128	.64	.32	.16	.8	.4

Posługując się tą tabelą należy jednak szczególnie pamiętać o obliczaniu podsieci od największych do najmniejszych.

Rozwiązania zadań

Zadanie 1.

Zad.	*Adres sieci*	*Adres rozgłoszeniowy*	*Klasa sieci*	*Numer podsieci*
A	192.168.100.224	192.168.100.239	C	15
B	10.250.130.0	10.250.130.255	A	64131
C	172.20.1.192	172.20.1.255	B	8
D	192.168.250.128	192.168.250.255	C	2
E	172.22.32.0	172.22.47.255	B	3
F	10.0.96.0	10.0.111.255	A	7
G	192.168.24.192	192.168.24.207	C	13
H	172.30.64.0	172.30.127.255	B	2
I	10.8.0.0	10.11.255.255	A	3

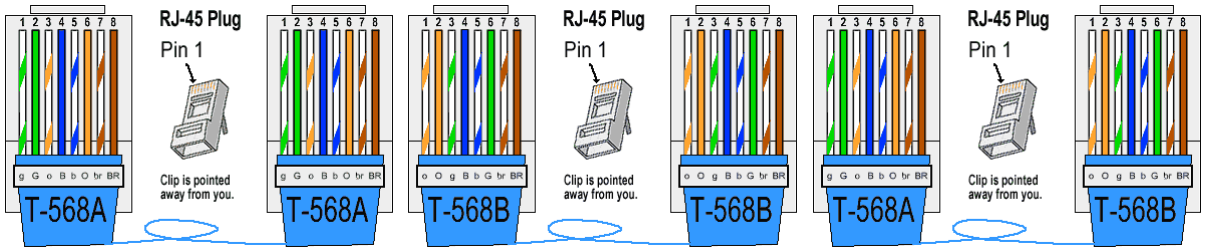
Zadanie 2.

Zad.	*Podsieć 1*	*Podsieć 2*	*Podsieć 3*	*Podsieć 4*
A	172.18.0.0/23	172.18.2.0/24	172.18.3.0/25	172.18.3.128/26
B	172.16.0.0/22	172.16.4.0/22	172.16.8.0/26	172.16.8.64/28
C	172.17.0.0/23	172.17.2.0/24	172.17.3.0/26	172.17.3.64/27
D	10.0.0.0/19	10.0.32.0/22	10.0.36.0/23	10.0.38.0/26
E	10.0.0.0/22	10.04.0/22	10.0.8.0/22	10.0.12.0/23
F	10.0.0.0/19	10.0.32.0/21	10.0.40.0/22	10.0.44.0/26
G	192.168.10.0/26	192.168.10.64/26	192.168.10.128/27	192.168.10.160/28
H	192.168.100.0/25	192.168.100.128/26	192.168.100.192/27	192.168.100.224/27
I	192.168.1.0/26	192.168.1.64/27	192.168.1.96/28	192.168.1.112/28

Zajęcia 4

Warstwa fizyczna modelu OSI – okablowanie

Okablowanie sieci Ethernet opisuje norma *EIA/TIA 568-B*. Najczęściej przywołuję się tą normę w odniesieniu do kolejności przewodów w złączu – norma definiuje dwa rodzaje zakończenia przewodów: T568A oraz T568B. Należy pamiętać, że standardy 10BASE-T i 100BASE-TX wykorzystują jedynie 2 z 4 dostępnych w przewodzie par oraz o tym, że kabel prosty to taki który ma obydwa zakończenia tego samego rodzaju (obojętnie którego), natomiast kabel skrosowany (ang. cross-over cable) z jednej strony posiada zakończenie jednego rodzaju, a z drugiej – drugiego.



Rys. 9 - Rodzaje zakończeń kabla Ethernetowego opisane w normie EIA/TIA 568-B

Obecnie w powszechnym użyciu są kable Ethernetowe kategorii 5e bądź 6. Kabel taki ma 8 żył skręconych ze sobą w 4 parach. Impedancja charakterystyczna takiego kabla dla częstotliwości nominalnej (100MHz) wynosi 100 Ohm. Najpopularniejszym wariantem tego kabla jest skrętka UTP – czyli nieekranowana, występuje również skrętka STP, FTP oraz S/FTP – odpowiednia z ekranowaniem par, z ekranowaniem kabla oraz jednocześnie z ekranowaniem par jak i całego kabla. Ponadto ze względu na budowę żył kabla, można wyróżnić linkę i drut. Linki używa się do wykonywania patchcordów, czyli kabli połączeniowych do komputerów i do łączenia urządzeń sieciowych z patchpanelami (panelami krosowniczymi) – jest to tzw. okablowanie poziome. Drutu używa się do wykonania okablowania strukturalnego w budynku – tzw. okablowanie pionowe.

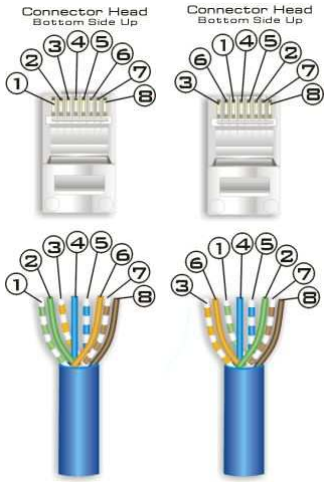
Rys. 10 – Rodzaje kabli sieciowych – UTP, FTP, S/FTP (© 2009 Brand-Rex)

Wykonanie kabla typu patchcord

- Minimalna średnica gięcia kabla nie może przekraczać jego 4-ro krotnego promienia.
- Maksymalna dopuszczalna długość na jakiej można rozkręcić skrętkę to ½".
- Kable sieciowe nie powinny przebiegać w bezpośrednim sąsiedztwie kabli prądowych ani w pobliżu urządzeń generujących silne pola elektromagnetyczne.
- Przewody nieparzyste są w paski, natomiast parzyste jednokolorowe.

Przystępując do zakończenia kabla wtyczką należy usunąć ok. 1,5cm zewnętrznej izolacji kabla, rozpleść i ułożyć przewody w odpowiedniej kolejności (zgodnie z poniższym rysunkiem), a następnie dociąć równo na długość ok. 1,2cm. Z przewodów poszczególnych żył nie usuwa się izolacji. Należy pamiętać o doborze odpowiedniej do użytego kabla wtyczki, tj. ekranowanej lub nie i ze stykami do linki bądź drutu. Żyły przewodów muszą dochodzić do końca wtyczki a zewnętrzna izolacja wchodzić na tyle głęboko do wtyczki by po jej zaciśnięciu zatrzask we wtyczce docisnął ją do przeciwległej powierzchni wtyczki.

#	Kolor
1	Biało-zielony
2	Zielony
3	Biało-pomarańczowy
4	Niebieski
5	Biało-niebieski
6	Pomarańczowy
7	Biało-brązowy
8	Brązowy



Rys. 11 - Sposób przygotowania kabla do zakończenia wtyczką

Konfiguracja routera SOHO

Routery klasy SOHO zazwyczaj są urządzeniami łączącymi funkcjonalność routera z translacją adresów, przełącznika Ethernetowego, serwera DHCP oraz niekiedy punktu dostępowego sieci bezprzewodowej i modemu ADSL. Urządzenie łączące te funkcje można nazwać bramą dostępową do Internetu (Internet Gateway). Router taki ma dwa interfejsy sieciowe na stałe przypisane do funkcji portu LAN i portu WAN. Port WAN jest dostępny bezpośrednio (gniazdo RJ-45 opisane jako WAN lub Internet) lub jest do niego podłączony modem ADSL (takie routera nie da się wykorzystać w roli routera Ethernetowgo, poza nielicznymi wyjątkami modemu nie da się pominąć). Do portu LAN najczęściej jest podłączony switch i to jego porty (zazwyczaj cztery) są dostępne na zewnątrz obudowy i opisane jako LAN. Opcjonalnie do switch może być (wewnętrznie) podłączony punkt dostępowy sieci bezprzewodowej (niektóre routery mają możliwość przełączania modułu WiFi między interfejs LAN a WAN).

Panele konfiguracyjne

Czołowi producenci sprzętu sieciowego umożliwiają dostęp do interfejsów konfiguracyjnych symulowanych urządzeń na swoich stronach internetowych:

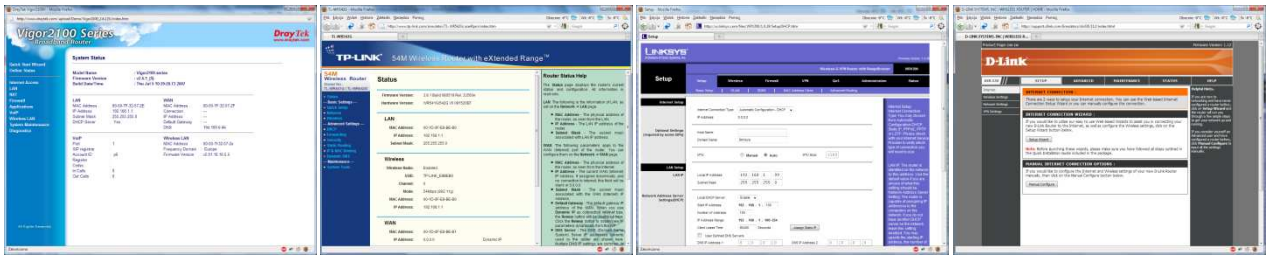
- **D-link**: http://support.dlink.com/emulators/ (należy wybrać kraj – Stany Zjednoczone)

- **Linksys**: http://ui.linksys.com/
- **DrayTek**: http://www.draytek.com/user/SupportLiveDemo.php
- **TP-Link**: http://www.tp-link.com/support/simulator.asp

Jest to dobra metoda na zapoznanie się z możliwościami wybranego urządzenia przed jego zakupem.

Konfiguracja interfejsów

W przypadku routerów Ethernetowych (zwanych też routerami szerokopasmowymi, bądź nieco myląco – routerami DSL) w zasadzanie nie jest konieczna żadna konfiguracja i powinny działać zaraz „po wyjęciu z pudełka" i podłączeniu. Panele konfiguracyjne routerów różnych producentów różnią się niekiedy dość znacznie, ale we wszystkich można odnaleźć pewne wspólne, podstawowe parametry.

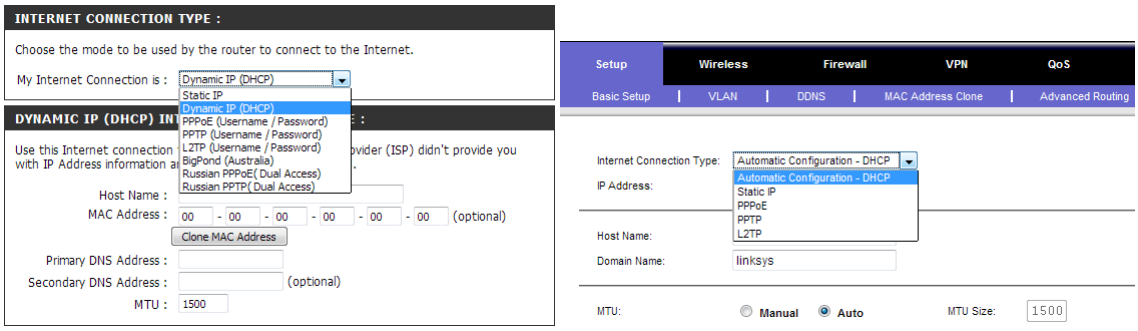


Rys. 12- Panele konfiguracyjne routerów: Vigor 2100, TL-WR541G, WRV200, DIR-330

Routera Ethernetowego używamy w przypadku podłączenia go do sieci osiedlowej, modemu kablowego, bądź modemu DSL. Dostawcy Internetu często wymagają rejestracji adresu fizycznego (MAC) karty podłączonej do ich sieci. Jeśli więc wcześniej komputer był podłączony bezpośrednio do gniazda sieciowego/modemu, warto w pierwszej kolejności podłączyć komputer, który dotychczas był podłączony sieci, do pierwszego portu LAN routera, włączyć router do prądu i po wejściu na jego panel konfiguracyjny wybrać opcję klonowania adresu MAC podłączonego komputera na interfejs WAN/Internet routera (zależnie od routera będzie to pierwszy podłączony komputer lub dostępna będzie lista z możliwością wskazania komputera, którego adres chcemy sklonować). Routery mają domyślnie włączony serwer DHCP, więc system operacyjny powinien być skonfigurowany na automatyczne pobieranie adresu sieciowego. Po sklonowaniu adresu MAC można już podłączyć port WAN/Internet routera do sieci dostawcy Internetu.

Pierwszym krokiem konfiguracji będzie ustalenie adresu pod jakim znajduje się panel konfiguracyjny, jest to adres bramy domyślnej, który możemy odczytać w bieżącej konfiguracji sieci w systemie. Standardowy login i hasło są różne dla różnych urządzeń i należy odszukać je w instrukcji obsługi.

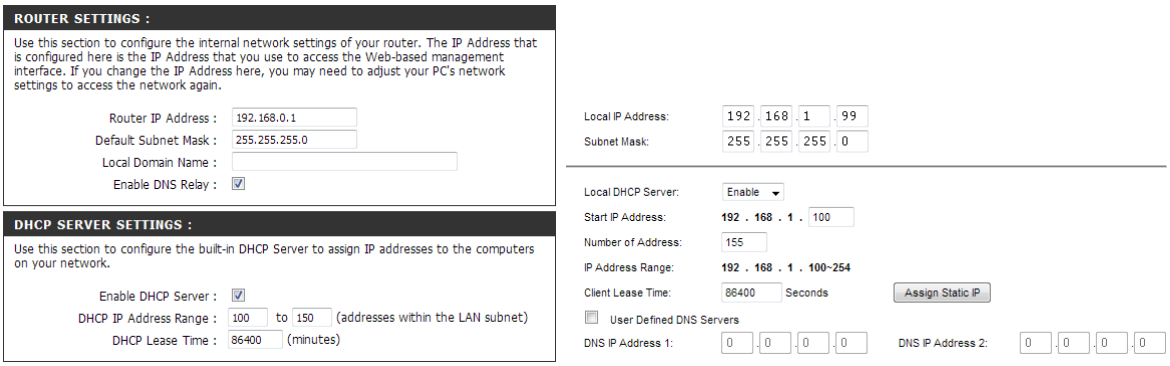
Po wejściu do panelu warto skonfigurować połączenie z Internetem – domyślnie będzie to automatyczne pobieranie konfiguracji z serwera DHCP, jeśli nasz dostawca nie ma serwera DHCP lub wymaga bardziej zaawansowanej autoryzacji należy wybrać stosowną opcję w konfiguracji interfejsu WAN/Internet routera.



Rys. 13 - Konfiguracja interfejsu WAN w routerach DIR-330 oraz WRV200

Zazwyczaj w tym miejscu można również określić wartość parametru MTU – omówionego w rozdziale **Zajęcia 1: Narzędzia do diagnostyki sieci** oraz wymusić używanie własnych serwerów DNS (w przypadku konfiguracji automatycznej).

Kolejnym etapem podstawowej konfiguracji jest określenie adresu konfiguracyjnego routera po stronie LAN i co za tym idzie adresu sieci LAN. Należy pamiętać, że interfejsy WAN i LAN muszą należeć do dwóch różnych sieci.



Rys. 14 - Konfiguracja interfejsu LAN w routerach DIR-330 i WRV200

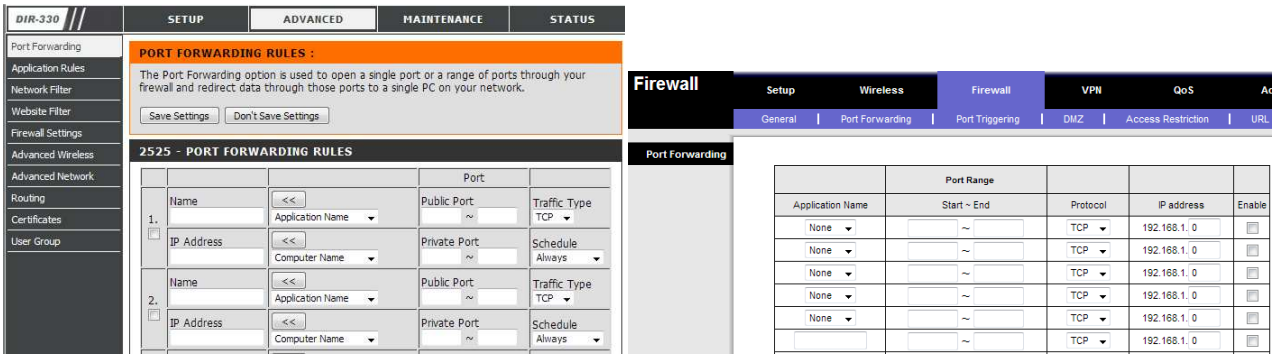
Na tym etapie możliwe jest również skonfigurowanie serwera DHCP – można określić pulę adresów oraz czas dzierżawy adresu. Czas dzierżawy należy dobrać zależnie od potrzeb – w sieciach gdzie krótkotrwale podłącza się wiele różnych klientów (dotyczy to głównie sieci WiFi) powinien być on możliwie krótki – np. 10 minut, w sieciach gdzie zawsze są podłączone te same komputery, może on być dłuższy – doba lub więcej.

Kroki te są wystarczające do udostępniania dostępu do Internetu dla komputerów podłączonych do routera. Z uwagi na translację adresów (NAT, maskarada) działającą na routerze jedynie komputery z sieci LAN mają dostęp do Internetu, jednak inne komputery podłączone do Internetu nie mogą uzyskać dostępu do komputerów w sieci LAN.

Konfiguracja usług – przekierowanie portów

Jeśli zachodzi potrzeba udostępnienia usług poza siecią lokalną istnieje możliwość tzw. Przekierowania portów. Warto pamiętać aby serwer udostępniający usługi miał przypisany stały adres IP – musi więc albo mieć skonfigurowany statyczny adres IP spoza puli serwera DHCP, albo serwer DHCP musi mieć możliwość wiązania adresów IP z adresami fizycznymi, tak by serwery zawsze otrzymywały te same adresy IP. Przekierowanie portów może się kryć pod różnymi nazwami – **Port Forwarding, Port Redirection lub Virtual Servers**. Poza przekierowaniem portów istnieje możliwość zdefiniowania tzw. Strefy Zdemilitaryzowanej

(DMZ) – jest to pojedynczy komputer w sieci do którego będzie kierowany cały ruch przychodzący do routera a nie skojarzony z żadnym istniejącym połączeniem ani nie objęty przekierowaniem.



Rys. 15 - Panel przekierowania portów w routerach DIR-330 i WRV200

Trzeba jednak pamiętać, że translacja adresów obejmuje jedynie adresy w nagłówkach pakietów IP, jeśli protokoły wyższego rzędu wykorzystują do jakiś celów adresy IP, to pozostaną one w tych data gramach niezmienione. Przykładem protokołu który sprawia problemy z tego tytułu jest protokół FTP. Protokół ten operuje na wielu połączeniach i w głównym połączeniu – zwanym połączeniem kontrolnym, bądź połączeniem poleceń przesyła klientowi adres i numer portu z którym ma się połączyć w celu pobrania danych (tryb pasywny). Jeśli serwer nie jest właściwie skonfigurowany, bądź nie posiada możliwości konfiguracji (np. serwery FTP w urządzeniach typu NAS), „poprosi" klienta o połączenie z lokalnym (nieosiągalnym z Internetu) adresem IP (wiele klientów FTP potrafi wykryć taką sytuację i odpowiednio ją obsłużyć – użyć poprawnego, publicznego adresu serwera), drugi problem – to otworzy i poda wysoki (>1024), losowy port do połączenia – nie ma więc możliwości przekserowania jednego czy kilku portów na potrzeby tej usługi, pozostaje umieszczenie serwera FTP w strefie DMZ. Naturalnie istnieją serwery FTP (choćby popularny vsftpd), które pozwalają na określenie puli portów używanych do połączeń jak i wymuszenie podawania innego adresu IP.

```
Łączenie z xxx.xxx.7.49:21...
Status:
Połączenie nawiązanie, oczekiwanie na wiadomość powitalną...
(...)
Status:
Połączono
(...)
Polecenie:
PASV
Odpowiedź
227 Entering Passive Mode (192,168,0,10,82,73)
Status:
Serwer wysłał pasywną odpowiedź z nieroutowalnym adresem. Zamiast tego zostanie użyty adres serwera.
Polecenie:
LIST
Odpowiedź
150 Here comes the directory listing.
Odpowiedź
226 Directory send OK.
Status:
Listowanie katalogów zakończone pomyślnie
```
Rys. 16 - Przykładowa sesja z nieprawidłowo skonfigurowanym serwerem FTP za NATem

Nieco podobną funkcją jest też Port Triggering (wyzwalanie portów), w odróżnieniu od klasycznego przekierowania portów nie definiuje się tu komputera docelowego – wskazany port lub porty są przekierowane na ten komputer, który połączy się usługą działającą na wskazanym porcie (wyzwalaczu).

Zajęcia 5

Routing w sieciach lokalnych

Routing to mechanizm kierujący pakiety do docelowych węzłów sieci. Routing stosuje się nie tylko w sieciach rozległych, z różnych względów może być stosowany również w sieciach lokalnych, np. jeśli zachodzi potrzeba segmentacji sieci, czyli podziału jej na podsieci, bądź w przypadku konieczności połączenia dotychczas niezależnych sieci. Jest to routing wewnętrzny – wykonywany wewnątrz pojedynczego *systemu autonomicznego*. Routing dotyczy trzeciej warstwy modelu *OSI* – warstwy sieciowej, w języku polskim można się spotkać również z pojęciem trasowania bądź marszrutowania. Urządzenia które odpowiadają za ten proces nazywane są routerami, choć ich funkcje może pełnić odpowiednio skonfigurowany i oprogramowanych komputer PC. Podstawą do prowadzenia routingu są *tablice routingu* (tablice trasowania) utrzymujące informacje o adresach zdalnych sieci oraz wskaźniki do tych sieci – adresy najbliższych węzłów (routerów) przez który te sieci są dostępne lub informację o tym, że są bezpośrednio przyłączone. Opcjonalnie może zawierać informacje o interfejsie sieciowym i metryce (koszcie) trasy oraz specjalny wpis – trasę do sieci 0.0.0.0/0 – jest to tzw. *trasa domyślna*, na którą są kierowane wszystkie pakiety, których adres docelowy nie należy do żadnej z istniejących w tablicy routingu sieci.

Tablice routingu mogą być wypełniane ręcznie przez administratora sieci, bądź automatycznie za pomocą protokołów routingu. W pierwszym przypadku mówimy o routingu statycznym, w drugim – o routingu dynamicznym.

Routing statyczny

Routing statyczny w sieci oznacza ręczne wypełnienie tablic routingu na wszystkich routerach w sieci. Nie obciąża on sieci i umożliwia jej działanie niezwłocznie po podłączeniu urządzeń. Jest jednak pracochłonny i nie potrafi się adaptować do zmian w sieci (zmienne obciążenie, awaria segmentu sieci, dodanie lub usunięcie jakiegoś urządzenia z sieci).

Routing dynamiczny

W przypadku routingu dynamicznego tablice routingu wypełniane są automatycznie na podstawie informacji wymienianych między sobą przez urządzenia sieciowe. W wymianie tych informacji pośredniczą protokoły routingu. Można je podzielić na dwie grupy:

- protokoły wektora odległości (distance-vector)
- protokoły stanu łącza (link-state)

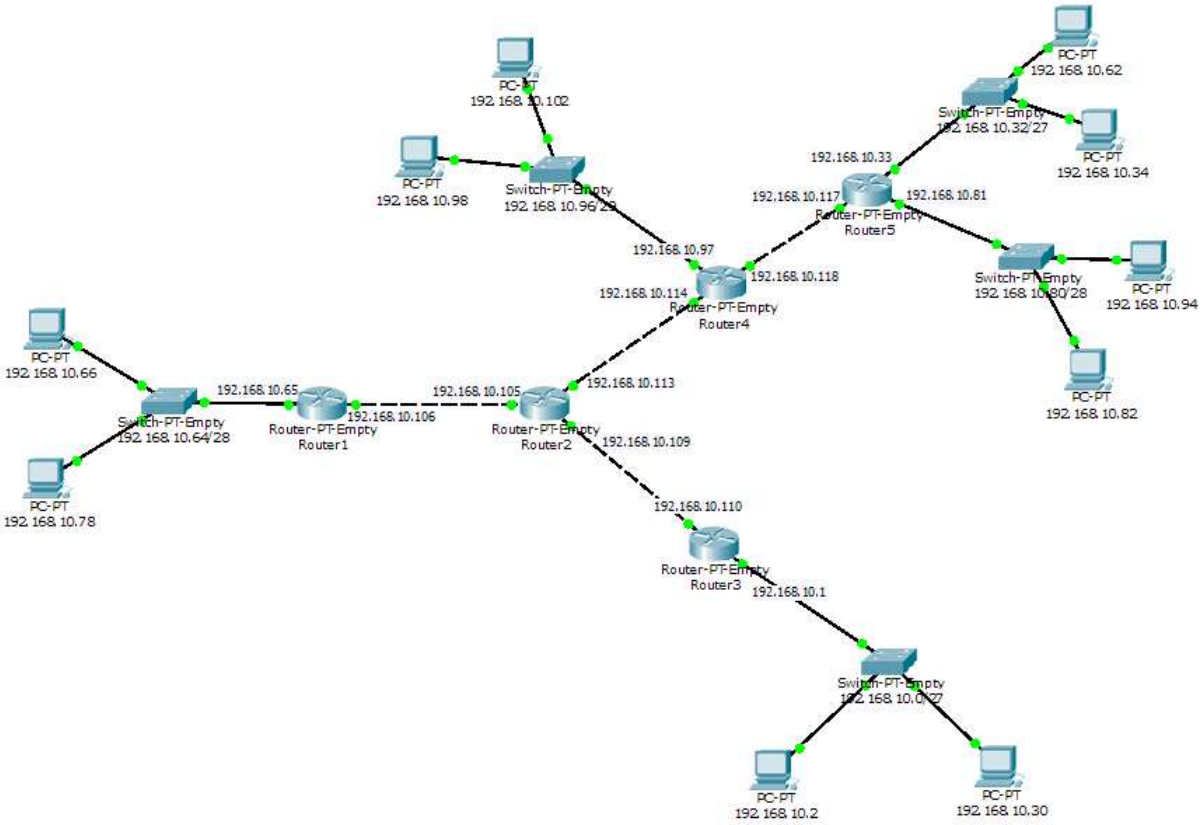
Protokoły wektora odległości bazują na algorytmie Bellmana-Forda. W protokołach tych routery wymieniają między sobą informacje o znanych im trasach (przesyłają sobie wzajemnie własne tablice routingu uzupełniając numer skoku). Decyzja o wyborze optymalnej trasy jest dokonywana na podstawie kosztu trasy. Przykładem takiego protokołu routingu może być RIP w którym o wyborze trasy decyduje ilość przeskoków bądź IGRP dla którego kosztem jest kombinacja takich parametrów łącza jak przepustowość, obciążenie, niezawodność i opóźnienia. Routery wymieniają informacje tylko z bezpośrednio przyłączonymi sąsiadami i nie znają całej topologii sieci, a jedynie adres najbliższego routera na drodze do celu (kierunek) oraz odległość do celu. Routery wymieniają się między sobą swoimi tablicami routingu co zadany okres czasu (zazwyczaj co 30 do 90 sek. Protokoły tej kategorii zużywają mniej zasobów systemowych routerów jednak powoli osiągają zbieżność i nie nadają się do użycia w dużych sieciach.

Protokoły stanu łącza bazują na algorytmie Dijkstry. Routery przesyłają sobie informacje o swoich sąsiadach i każdy z nich tworzy i utrzymuje kompletną mapę topologii sieci (w formie drzewa) oraz wytyczają najkrótsze ścieżki do każdej możliwej sieci docelowej (stąd inna ich nazwa to SPF czyli Shortest Path First) by ostatecznie umieścić ją w swojej tablicy routingu. Protokoły tej kategorii cechuje większe obciążenia procesora i pamięci routera oraz po zainicjowaniu generują znaczny ruch w sieci, szybko jednak osiągają zbieżność, a po jej osiągnięciu przesyłają niewielkie pakiety informujące o zmianach w topologii sieci (niezwłocznie po ich zaistnieniu). Przykładem protokołu stanu łącza jest OSPF.

Innym sposobem podziału protokołów routingu jest podział na protokoły klasowe i bezklasowe. Protokoły klasowe to takie, które bazują na klasach adresów, np. RIP v.1 czy IGRP – nie można ich stosować w sieciach które zostały podzielone na podsieci. Nowsze protokoły routingu jak RIP v.2 czy EIGRP są protokołami bezklasowymi (CIDR), czyli przesyłają nie tylko adres ale i maskę sieci.

Przykład

Mając dany schemat sieci:



Rys. 17- Schemat przykładowej sieci LAN

Oraz schemat adresacji tej sieci:

ilość	maska	hosty			adres sieci	brama	broadcast	
20	/27	192.168.10.1	-	192.168.10.30	192.168.10.0	192.168.10.1	192.168.10.31	
16	/27	192.168.10.33	-	192.168.10.62	192.168.10.32	192.168.10.33	192.168.10.63	
12	/28	192.168.10.65	-	192.168.10.78	192.168.10.64	192.168.10.65	192.168.10.79	
10	/28	192.168.10.81	-	192.168.10.94	192.168.10.80	192.168.10.81	192.168.10.95	
4	/29	192.168.10.97	-	192.168.10.102	192.168.10.96	192.168.10.97	192.168.10.103	komputery
4	/30	192.168.10.105	-	192.168.10.106	192.168.10.104		192.168.10.107	routery
4	/30	192.168.10.109	-	192.168.10.110	192.168.10.108		192.168.10.111	
4	/30	192.168.10.113	-	192.168.10.114	192.168.10.112		192.168.10.115	
4	/30	192.168.10.117	-	192.168.10.118	192.168.10.116		192.168.10.119	

Tab. 3 - Schemat adresacji w przykładowej sieci LAN

Tak przedstawia się zawartość tablic routingu poszczególnych routerów w tej sieci (w tym przypadku wypełnione przez protokół RIP v.2):

Router1: 192.168.10.0/27 [120/2] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.32/27 [120/3] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.64/28 is directly connected, FastEthernet1/0 192.168.10.80/28 [120/3] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.96/29 [120/2] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.104/30 is directly connected, FastEthernet0/0 192.168.10.108/30 [120/1] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.112/30 [120/1] via 192.168.10.105, 00:00:13, FastEthernet0/0 192.168.10.116/30 [120/2] via 192.168.10.105, 00:00:13, FastEthernet0/0	Router2: 192.168.10.0/27 [120/1] via 192.168.10.110, 00:00:04, FastEthernet8/0 192.168.10.32/27 [120/2] via 192.168.10.114, 00:00:12, FastEthernet7/0 192.168.10.64/28 [120/1] via 192.168.10.106, 00:00:02, FastEthernet9/0 192.168.10.80/28 [120/2] via 192.168.10.114, 00:00:12, FastEthernet7/0 192.168.10.96/29 [120/1] via 192.168.10.114, 00:00:12, FastEthernet7/0 192.168.10.104/30 is directly connected, FastEthernet9/0 192.168.10.108/30 is directly connected, FastEthernet8/0 192.168.10.112/30 is directly connected, FastEthernet7/0 192.168.10.116/30 [120/1] via 192.168.10.114, 00:00:12, FastEthernet7/0
Router3: 192.168.10.0/27 is directly connected, FastEthernet1/0 192.168.10.32/27 [120/3] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.64/28 [120/2] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.80/28 [120/3] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.96/29 [120/2] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.104/30 [120/1] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.108/30 is directly connected, FastEthernet0/0 192.168.10.112/30 [120/1] via 192.168.10.109, 00:00:05, FastEthernet0/0 192.168.10.116/30 [120/2] via 192.168.10.109, 00:00:05, FastEthernet0/0	Router4: 192.168.10.0/27 [120/2] via 192.168.10.113, 00:00:24, FastEthernet0/0 192.168.10.32/27 [120/1] via 192.168.10.117, 00:00:21, FastEthernet1/0 192.168.10.64/28 [120/2] via 192.168.10.113, 00:00:24, FastEthernet0/0 192.168.10.80/28 [120/1] via 192.168.10.117, 00:00:21, FastEthernet1/0 192.168.10.96/29 is directly connected, FastEthernet2/0 192.168.10.104/30 [120/1] via 192.168.10.113, 00:00:24, FastEthernet0/0 192.168.10.108/30 [120/1] via 192.168.10.113, 00:00:24, FastEthernet0/0 192.168.10.112/30 is directly connected, FastEthernet0/0 192.168.10.116/30 is directly connected, FastEthernet1/0
Router5: 192.168.10.0/27 [120/3] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.32/27 is directly connected, FastEthernet0/0 192.168.10.64/28 [120/3] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.80/28 is directly connected, FastEthernet2/0 192.168.10.96/29 [120/1] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.104/30 [120/2] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.108/30 [120/2] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.112/30 [120/1] via 192.168.10.118, 00:00:21, FastEthernet1/0 192.168.10.116/30 is directly connected, FastEthernet1/0	

Tab. 4 - Zawartość tablic routingu w przykładowej sieci

Zajęcia 6

Protokoły warstwy aplikacji modelu TCP/IP

Warstwa aplikacji znajduje się na szczycie modelu TCP/IP, protokoły które wchodzą w jej skład zapewniają komunikację między aplikacjami – klientami i serwerami. Łączy ona w sobie warstwy sesji, prezentacji oraz aplikacji z modelu OSI. Część, historycznie najstarszych, protokołów tej warstwy bazuje na poleceniach tekstowych, a odpowiedzi serwera są czytelne dla człowieka. Przykładem takich protokołów mogą być protokoły POP3 oraz FTP. Do nawiązania połączenia z takim serwerem wystarczy aplikacja typu emulator terminala, np. telnet lub PuTTY.

Przykładowa sesja protokołu POP3

```
+OK Dovecot DA ready.
USER demo@tzok.elektroda.eu
+OK
PASS demo
+OK Logged in.
LIST
+OK 2 messages:
1 1773
2 1824
.
RETR 1
+OK 1773 octets
Return-path: <tomasz.orczyk@us.edu.pl>
Envelope-to: demo@tzok.elektroda.eu
Delivery-date: Wed, 13 Jan 2010 18:17:24 +0100
Received: from services.us.edu.pl ([155.158.102.210])
        by serwer.elektroda.eu with esmtps (TLSv1:AES256-SHA:256)
        (Exim 4.69)
        (envelope-from <tomasz.orczyk@us.edu.pl>)
        id 1NV6qS-0001EX-Hx
        for demo@tzok.elektroda.eu; Wed, 13 Jan 2010 18:17:24 +0100
Received: from prac.us.edu.pl (prac.us.edu.pl [155.158.102.50])
        by services.us.edu.pl (Postfix) with ESMTP id DE34F75B
        for <demo@tzok.elektroda.eu>; Wed, 13 Jan 2010 18:18:25 +0100 (CET)
Received: from localhost (services [192.168.10.210])
        by prac.us.edu.pl (Postfix) with ESMTP id C0C9BFCF74
        for <demo@tzok.elektroda.eu>; Wed, 13 Jan 2010 18:18:25 +0100 (CET)
X-Virus-Scanned: amavisd-new at us.edu.pl
Received: from prac.us.edu.pl ([192.168.10.50])
        by localhost (services.us.edu.pl [192.168.10.210]) (amavisd-new, port 10024)
        with ESMTP id hhCy7wNbdk2V for <demo@tzok.elektroda.eu>;
        Wed, 13 Jan 2010 18:18:24 +0100 (CET)
Received: from tzoklap2 (pcb112.tech.us.edu.pl [155.158.112.112])
        (Authenticated sender: tomasz.orczyk@us.edu.pl)
        by prac.us.edu.pl (Postfix) with ESMTPSA id B37FFFCF57
        for <demo@tzok.elektroda.eu>; Wed, 13 Jan 2010 18:18:24 +0100 (CET)
Message-ID: <60693B2C7CD54738882E16051B5FB530@tzoklap2>
From: "Tomasz Orczyk" <tomasz.orczyk@us.edu.pl>
To: <demo@tzok.elektroda.eu>
Subject: Test
Date: Wed, 13 Jan 2010 18:18:25 +0100
MIME-Version: 1.0
Content-Type: text/plain;
        format=flowed;
        charset="iso-8859-2";
        reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5843
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579

Wiadomosc testowa.
.
QUIT
+OK Logging out.
```

Tab. 5 - Zapis przykładowej sesji POP3

Podstawowy zestaw poleceń protokołu POP3 obejmuje 9 poleceń:

- `USER` – wyślij nazwę użytkownika
- `PASS` – wyślij hasło
- `STAT` – wyświetl statystykę wiadomości (ilość i rozmiar)
- `LIST` – wyświetl listę wiadomości
- `RETR` – pobierz wiadomość
- `DELE` – usuń wiadomość

- RSET – Zresetuj sesję (cofnij oznaczenie wiadomości do usunięcia)
- TOP – pobierz nagłówek wiadomości (i n linii treści)
- QUIT – zakończ połączenie

Oraz 2 odpowiedzi:

- +OK
- -ERR

Przykładowa sesja protokołu FTP

Połączenie kontrolne	*Połączenie danych*
220 Microsoft FTP Service USER anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. PASS demo@demo.com 230 Anonymous user logged in. PASV 227 Entering Passive Mode (127,0,0,1,5,157). LIST 125 Data connection already open; Transfer starting. 226 Transfer complete.	01-06-10 12:16PM 13012 cat.jpg 01-07-11 02:25PM 18 demo.txt 01-06-10 12:21PM 10015 Dog1.jpg 01-06-10 12:22PM 8841 Dog2.jpg 01-07-10 12:26PM 679 Program.cs
PASV 227 Entering Passive Mode (127,0,0,1,5,174). RETR demo.txt 125 Data connection already open; Transfer starting. 226 Transfer complete. QUIT 221	Wiadomosc testowa.

Tab. 6 - Zapis przykładowej sesji FTP

Podstawowy zestaw poleceń protokołu FTP obejmuje 21 poleceń:

- ABOR – przerwij transfer pliku
- CWD – zmień katalog roboczy
- DELE – usuń zdalny plik
- LIST – wyświetl listę plików
- MDTM – zwróć czas modyfikacji pliku
- MKD – utwórz katalog
- NLST – wyświetl listę nazw plików z wskazanego katalogu
- PASS – wyślij hasło
- PASV – przejdź do trybu pasywnego
- PORT – otwórz port danych (przejdź do trybu aktywnego)
- PWD – wyświetl katalog roboczy
- QUIT – zakończ połączenie
- RETR – pobierz zdalny plik
- RMD – usuń zdalny katalog
- RNFR – zmień nazwę z
- RNTO – zmień nazwę na
- SITE – wykonaj polecenie na serwerze
- SIZE – zwróć rozmiar pliku
- STOR – zapisz plik na zdalnym hoście
- TYPE – ustal typ transferu (ASCII lub binarny)
- USER – wyślij nazwę użytkownika

Spis treści

Zajęcia 1 1

Konfiguracja sieci w systemie Windows® Seven™ 1

Narzędzia do diagnostyki sieci 3

Zajęcia 2 5

Adresacja IP v4 5

Wstęp 5

Wyznaczanie adresu sieci i rozgłoszeniowego 6

Podział na podsieci 7

Zajęcia 3 9

Adresacja IP v4 - ćwiczenia 9

Wskazówki 9

Rozwiązania zadań 10

Zajęcia 4 11

Warstwa fizyczna modelu OSI – okablowanie 11

Wykonanie kabla typu patchcord 12

Konfiguracja routera SOHO 12

Panele konfiguracyjne 12

Konfiguracja interfejsów 13

Konfiguracja usług – przekierowanie portów 14

Zajęcia 5 16

Routing w sieciach lokalnych 16

Routing statyczny 16

Routing dynamiczny 16

Przykład 17

Zajęcia 6 19

Protokoły warstwy aplikacji modelu TCP/IP 19

Przykładowa sesja protokołu POP3 19

Przykładowa sesja protokołu FTP 20