Akademickie
Centrum
Informatyki PS

Akademickie
Centrum Informatyki

Wydział Informatyki PS

Wydział Informatyki

Sieci komputerowe i Telekomunikacyjne

ADRESOWANIE IP WERSJA 4
Wyczerpanie adresów IP
CIDR, NAT

Krzysztof Bogusławski
tel. 449 41 82
kbogu@man.szczecin.pl

MENU

1. Problemy z ilością adresów IP
2. Routing oparty o klasy adresowe
3. CIDR – Classless InterDomain Routing
4. NAT – Network Adress Translation

Prezentacja ta dotyczy możliwym realizacjom rozwiązania problemu braku adresów IP w wersji 4

Klasy adresowe

4 bity	Klasa	maska	Dwójkowo				
0xxx	a	255.0.0.0	11111111	00000000	00000000	00000000	/8
10xx	b	255.255.0.0	11111111	11111111	00000000	00000000	/16
110x	c	255.255.255.0	11111111	11111111	11111111	00000000	/24

W latach 90 XX wieku stało się oczywistym, iż nastąpi w krótkim okresie czasu wyczerpanie adresów IP. Sieci klasy A jest 128, klasy B ok. 16 tysięcy a klasy C ok. 2 miliony.

Routing oparty o klasy adresowe (1)

4 bity	Klasa
0xxx	a
10xx	b
110x	c

Etapy	Dwójkowo
213.18.21.6	11010101.00010010.00010101.00000110
240.0.0.0	11111111.00000000.00000000.00000000
Klasa C	11010000.00000000.00000000.00000000
maska (C)	11111111.11111111.11111111.00000000
Adres sieci	11010101.00010010.00010101.00000000

Routing oparty o klasy adresowe przebiega następująco:

2. Z pakietu IP pobierany jest adres docelowy IP.
3. Na adresie tym dokonywana jest operacja AND z wartością 240.0.0.0 lub adres ten jest przesuwany w prawo o 28 w celu uzyskania wartości najstarszych czterech bitów.
4. Po wartości tych bitów poznajemy jaka jest klasa adresowa sieci docelowej.
5. Wykonywana jest operacja AND adresu docelowego IP i maski właściwej dla danej klasy.
6. Wynikiem operacji jest adres sieci docelowej i ta sieć jest poszukiwana w tablicy routingu.

Routing oparty o klasy adresowe (2)

Zalety:

- Prosty mechanizm określania klasy adresowej i adresu sieci docelowej
- Nieskomplikowane tablice routingu
- Możliwość szybkiej i prostej procedury routingu w celu określenia drogi do sieci docelowej

Wady:

- Marnotrawstwo przestrzeni adresowej
  - –Klasa B posiada 65.534 adresy hostów ale niewiele jest firm, które mogą tą ilość wykorzystać (nawet ISP).
- Niemożliwość przydziału puli adresów z pomiędzy klasy B i C

Powyżej zostały opisane wady i zalety routingu opartego o klasy adresowe..

CIDR – Classless InterDomain Routing (1)

Uczelnia	Pierwszy adres	Ostatni adres	Liczba adresów	Zapis
Politechnika	213.18.0.0	213.18.7.255	2048	213.18.0.0 / 21
Uniwersytet	213.18.8.0	213.18.11.255	1024	213.18.8.0 / 22
(wolne)	213.18.12.0	213.18.15.255	1024	213.18.12.0 / 22
Akademia	213.18.16.0	213.18.31.255	4096	213.18.16.0 / 20

Routing bezklasowy używa różnych długości maski dla różnych adresów sieci przydzielonych firmom. Wpisy w routerach teraz muszą zawierać oprócz adresu sieci maskę. Dla przykładu dla Politechniki wpis w tablicy routingu będzie wyglądał następująco.

CIDR – Classless InterDomain Routing (2)

Wpis w tablicy routingu dla Politechniki

pole	dziesiętnie	binarnie			
sieć	213.18.0.0	11010101	00010010	00000000	00000000
maska	255.255.248.0	11111111	11111111	11111000	00000000

Wpisy w routerach teraz muszą zawierać oprócz adresu sieci maskę. Dla przykładu dla Politechniki wpis w tablicy routingu będzie wyglądał następująco.:

CIDR – Classless InterDomain Routing (3)

Tablica routingu

Uczelnia	Adres sieci	maska	Zapis
Politechnika	213.18.0.0	255.255.248.0	213.18.0.0 / 21
Uniwersytet	213.18.8.0	255.255.252.0	213.18.8.0 / 22
Akademia	213.18.16.0	255.255.240.0	213.18.16.0 / 20

Routing bezklasowy przebiega następująco:

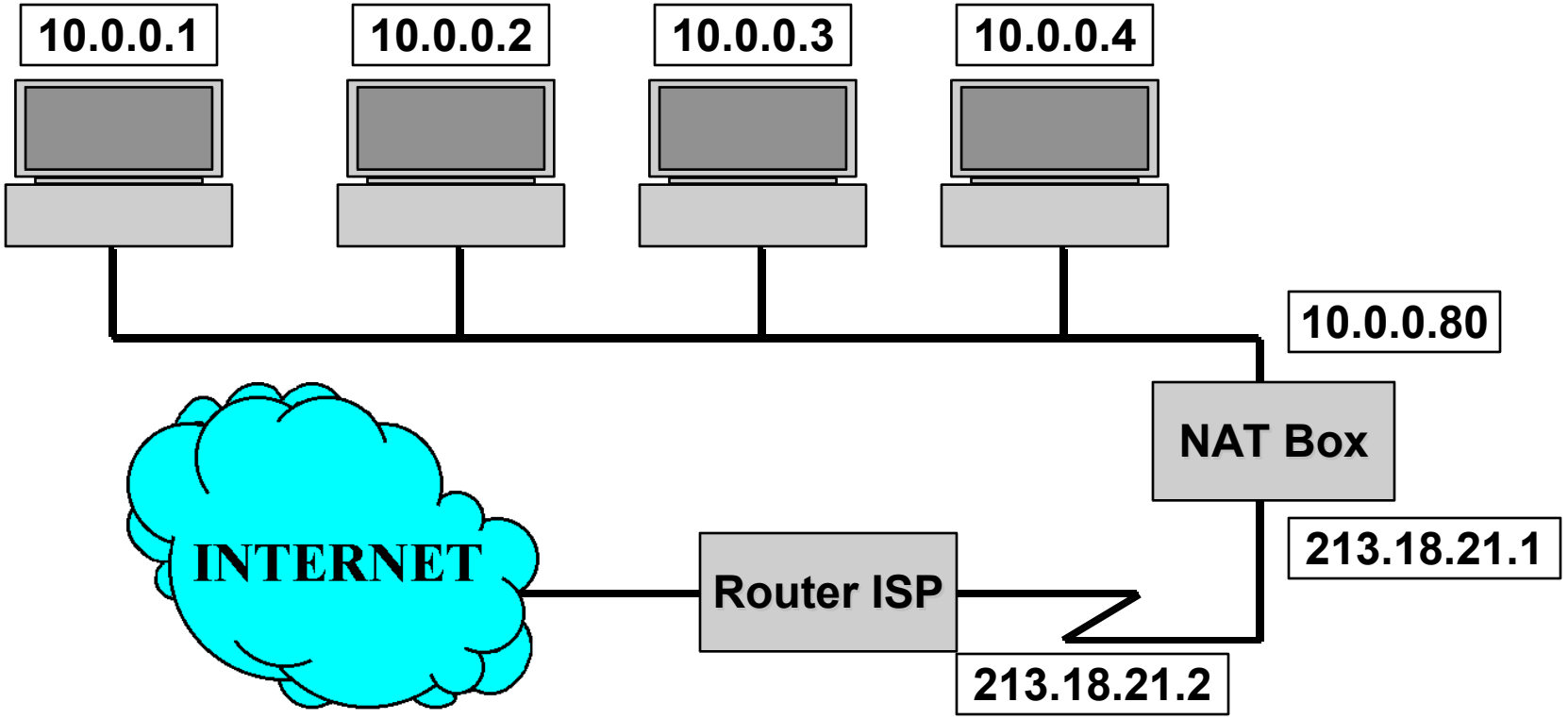
2. Z pakietu IP pobierany jest adres docelowy IP.
3. Dla każdego rekordu w tablicy wykonywana jest operacja AND adresu IP i maski określonej w tym rekordzie.
4. Wynik operacji AND porównywany jest z adresem sieci w tym rekordzie, W przypadku zgodności trasa określona w tym rekordzie jest trasą właściwą.
5. Spośród wszystkich tras właściwych wybiera się najlepszą.

NAT – Network Adress Translation (1)

Prywatne adresy IP			
Pierwszy adres	**Ostatni adres**	**Liczba adresów**	**Zapis**
10.0.0.0	10.255.255.255	16 777 216	10.0.0.0 / 8
172.16.0.0	172.31.255.255	1 048 576	172.16.0.0 / 12
192.168.0.0	192.168.255.255	65 536	192.168.0.0 / 16

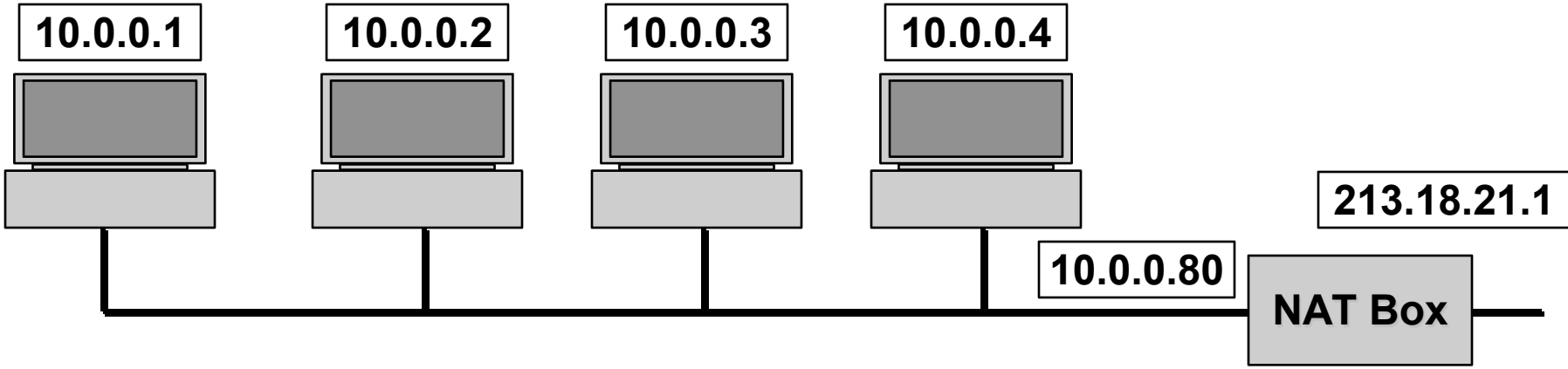
Z całkowitej puli adresów wydzielona została przestrzeń adresów prywatnych (pokazana powyżej). Został więc dokonany podział adresów na: (1) adresy publiczne – identyfikujące unikany numer hosta w sieci IP - adres ten może bez przeszkód być ujawniany w całej sieci Internet, (2) adresy prywatne, używane wewnątrz lokalnej sieci – adresy te ni mogą pojawić się w rozległej sieci IP (brak routingu międzydomenowego dla tych adresów).

NAT – Network Adress Translation (2)



Mechanizm NAT opisany jest w RFC 3022 i służy do zamiany wewnętrznych adresów prywatnych na adres publiczny. Na powyższym rysunku prywatne adresy 10.0.0.x zamieniane są na adres publiczny 213.18.21.1.

NAT – Network Adress Translation (3)



Sieć wewnętrzna	
Adres IP	Numer Portu
10.0.0.1	1020
10.0.0.2	1040
10.0.0.3	1020

Sieć wewnętrzna	
Adres IP	Numer Portu
213.18.21.1	5011
213.18.21.1	5012
213.18.21.1	5013

Zamiana adresów prywatnych na publiczne następuje przy użyciu specjalnej tablicy translacji. W każdym rekordzie tej tablicy znajdują się adresy IP i numery portów z warstwy transportowej dla sieci wewnętrznej i zewnętrznej.

NAT – Network Adress Translation – wady (4)

1. NAT narusza model architektury IP gdzie adres IP jednoznacznie identyfikuje komputer w sieci IP – adresy IP są używane wielokrotnie w sieci.

3. NAT zmienia sieć Internet z sieci bezpołączeniowej w sieć połączeniową. NAT box posiada informacje o połączeniach pomiędzy siecią wewnętrzną a zewnętrzną.
   1. Chwilowa awaria NAT Box'u powodująca utratę tablicy translacji powoduje zerwanie wszystkich aktywnych połączeń.
   2. Chwilowa awaria routera nie powoduje zerwanie połączeń w sieci tylko opóźnienia w przekazie ewentualnie retransmisje.

4. NAT narusza zasadę, iż warstwa ***n*** nie ingeruję w warstwę ***n+1***. NAT będąc mechanizmem warstwy sieciowej (trzeciej) zmienia numer portu warstwy transportowej (czwartej). Zmiana zasad w warstwie transportowej (np. przejście do wersji TCP – 2) spowoduje niedziałanie NAT.

NAT – Network Adress Translation – wady (5)

1. Procesy aplikacji nie muszą używać protokołów TCP i UDP tylko wprost IP i wtedy nie ma wiadomości warstwy transportowej i nie ma numerów portów. W takiej sytuacji procesy te nie mogą prowadzić transmisji w sieci

3. Niektóre aplikacje zapisują adresy IP do danych pakietu IP a NAT o tym nie ma informacji nie może dokonać translacji tego adresu. W wyniku tego te aplikacje nie mogą dokonać wymiany danych poprzez sieć (FTP, H.323). Aplikacje te wymagają „łatania” NAT. Powstanie nowej podobnej aplikacji wymaga „łatania” NAT.

5. Nr portu ma 16 bitów i po odjęciu zarezerwowanych numerów portów (4096) otrzymujemy 61 440 numerów portów, czyli jest to maksymalny rozmiar tablicy translacji
6. Te i inne wady zostały opisane w RFC 2993.

Koniec

Inne prezentacje znajdują się na stronie:

http://kbogu.man.szczecin.pl