NAT

Tło historyczne

W 1983 roku wprowadzono do użycia w sieci ARPANET protokół IP (ang. Internet Protocol) w wersji 4, który do dzisiaj odpowiada za sterowanie większością ruchu w sieci Internet, mimo iż w użyciu od pewnego czasu jest stopniowo zastępowany przez protokół IPv6.
Protokół IPv4 oparty jest o adresy, które mają długość 32 bitów. W efekcie umożliwia to zaadresowanie 4294967296 (2^{32}) urządzeń. O ile na początku lat 80. taka liczba wydawała się wystarczająca to bardzo szybko zaczęto zdawać sobie sprawę z tego, że pula dostępnych adresów szybko się wyczerpie. Głównymi przyczynami rynkowymi, które odpowiadały za przyspieszone wyczerpywanie adresów IP były:

- Zwiększająca się liczba urządzeń będących ciągle podłączonych do sieci (np. modemy ADSL)
- Rosnąca liczba użytkowników Internetu
- Pojawienie się urządzeń mobilnych z dostępem do Internetu
- Nieefektywne wykorzystanie puli adresów

Zanim opracowano i wdrożono protokół IPv6, którego głównym założeniem było zwiększenie rozmiaru adresu do 128 bitów (w efekcie zwiększając pulę adresów do $2^{128} = 3{,}4 \times 10^{38}$), zdecydowano się wprowadzić inne rozwiązania takie jak: sieci bezklasowe, bezklasowa metoda przydzielania adresów (ang. Classless Inter-Domain Routing,CIDR), podział na adresy publiczne i prywatne, czy translacja adresów sieciowych (ang. Network Address Translation, NAT).

Sieć prywatna

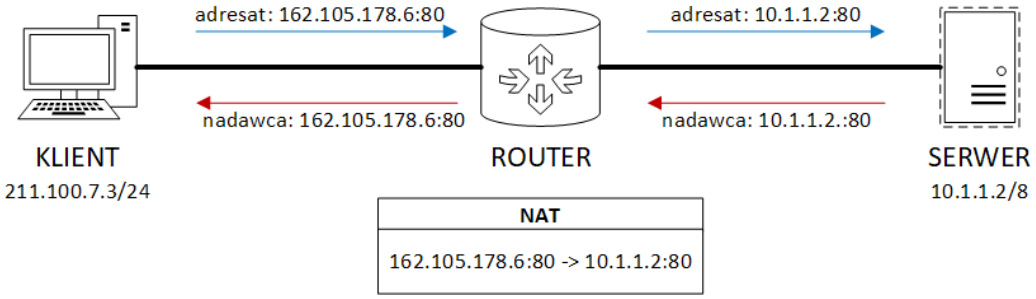
Jedną z metod mającą ograniczyć wyczerpywanie puli adresów IP było wprowadzenie do architektury sieci Internet pojęcia sieci prywatnej, czyli takiej która do adresacji urządzeń wykorzystuje adresy prywatne.
Pula adresów prywatnych została wydzielona przez Internet Assigned Numbers Authority (IANA) na zlecenie Internet Engineering Task Force (IETF). Zarezerwowane zakresy przedstawiono w poniższej tabeli:

Nazwa wg RFC1918	Zakres adresów IP	liczba adresów	liczba bitów hosta	liczba bitów maski
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	24	8
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	20	12
16-bit block	192.168.0.0 – 192.168.255.255	65 536	16	16

Łącznie daje to pulę ponad 17 milionów adresów. Cechą charakterystyczną adresu prywatnego jest to, że w odróżnieniu od publicznego nie jest on unikalny i może pojawiać się w wielu podsieciach lokalnych.

NAT

Usługa translacji adresów sieciowych (ang. Network Address Translation, NAT), zwana również maskaradą sieci, polega na zamianie adresów źródłowych i docelowych w pakietach IP podczas przechodzenia przez router. Głównym celem wykorzystania NAT jest umożliwienie dostępu do Internetu wielu urządzeniom z sieci lokalnej wykorzystując jeden publiczny adres IP.



Translacja adresów może odbywać się na dwóch poziomach:

1. na poziomie warstwy sieciowej przez zmianę adresu IP (NAT)
2. na poziomie warstwy transportowej poprzez zmianę adresu IP oraz numeru portu (NAPT – Network Address and Port Translation)

Obecnie powszechnie stosowane jest to drugie rozwiązanie i przez to jest traktowane jako synonim NAT.

Rodzaje zachowania NAT

Terminologia służąca do opisu zachowania NAT została ustandaryzowana w dokumencie RFC 4787. Definiuje on następnie terminy:

Endpoint-Independent Mapping: jeśli zdefiniowano mapowanie wewnętrznego adresu i portu (iAddr:iPort) na zewnętrzny adres i port (eAddr:ePort) to każdy pakiet z iAddr:iPort jest wysyłany przez eAddr:ePort niezależnie od adresu odbiorcy

Address- and Port-Dependent Mapping: jeśli z adresu wewnętrznego (iAddr:iPort) realizowane są żądania do różnych odbiorców to każde z tych żądań otrzymuje swoje mapowanie na zewnętrzny adres i port (eAddr:ePort)

Endpoint-Independent Filtering: zewnętrzny klient może wysłać pakiet na adres:port wewnętrzny tylko jeśli wcześniej otrzymał pakiet z tego adresu

Address-Dependent Filtering

Address and Port-Dependent Filtering

Oprócz wymienionych zachowań dokument RFC 4787 klasyfikuje również inne zachowania, takie jak na przykład sposób odświeżania mapowań.

Port forwarding

Przekierowanie portów (ang. port forwarding) jest jedną z metod translacji adresów sieciowych. Polega ona na przekierowaniu pakietów przychodzących na bramę sieciową (np router) na inne urządzenie. Technika ta umożliwia zdalnym urządzeniom nawiązanie połączenia z urządzeniami podłączonymi do sieci prywatej.

Wykorzystanie tej techniki umożliwia dostęp komunikację z hostem w prywatnej sieci z wykorzystaniem takich protokołów jak: HTTP, HTTPS, SSH, FTP, SFTP.

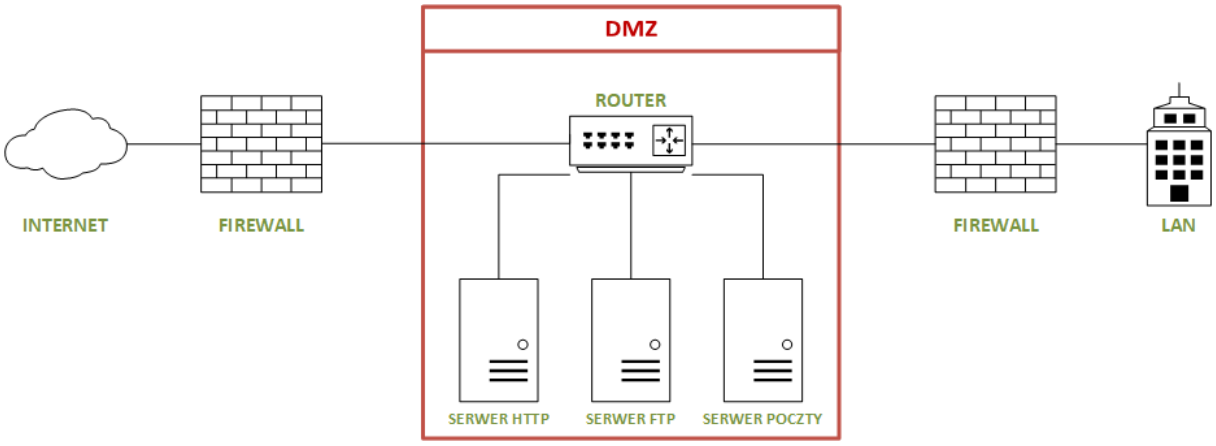
Poniżej przedstawiono wybrane „dobrze znane” (ang. well known) porty oraz usługi, które obsługują:

Numer portu	Usługa
20	FTP – Data
21	FTP – Control
22	SSH Remote Login Protocol
25	Simple Mail Transfer Protocol (SMTP)
80	HTTP
115	Simple File Transfer Protocol (SFTP)
443	HTTPS

DMZ

Serwery, które udostępniają swoje usługi na zewnątrz sieci lokalnej, bardzo często umieszczane są w tzw. strefie zdemilitaryzowanej (ang. demilitarized zone, DMZ). Jest to pewien obszar fizyczny lub logiczny sieci lokalnej, który z jednej strony jest dostępny z sieci zewnętrznej (np. sieci Internet), a z drugiej strony ma on ograniczony dostęp to pozostałej części sieci lokalnej. DMZ jest zarządzany przez jeden lub więcej firewalli. Przykładowe usługi, które umieszczane są w DMZ to:

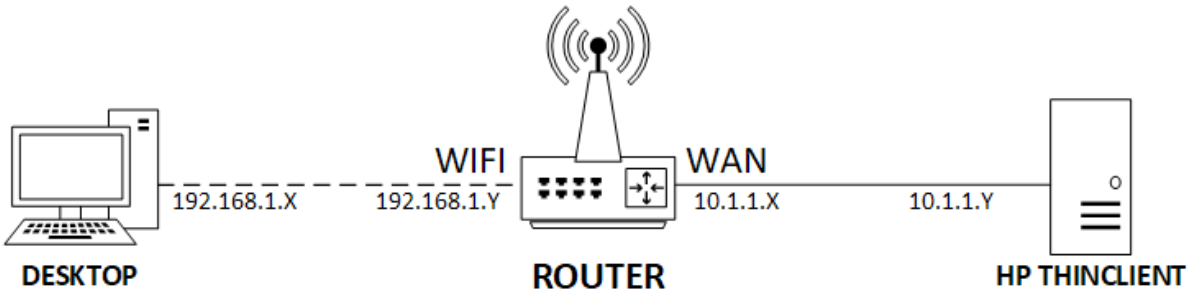
- serwery HTTP
- serwery FTP
- serwery poczty email
- serwery VoIP



Scenariusz nr 1

Sprzęt:
Router tp-link TL-MR3420
1x komputer PC
1x komputer HP ThinClient

Oprogramowanie:
XAMPP



SERWER HTTP		
adres IP		192.168.1. …
maska sieci		255.255.255. …
ZDALNY KLIENT		
nazwa interfejsu		
adres IP		
maska sieci		
ROUTER		
LAN	adres IP	192.168.1. …
	maska sieci	255.255.255. …
WAN	adres IP	
	maska sieci	
	brama domyślna	
Virtual Server	port zewnętrzny	
	port wewnętrzny	

TABELA DO UZUPEŁNIENIA PRZEZ STUDENTÓW!

Wykonanie ćwiczenia:

Przygotowanie

1. Podłącz terminal HP ThinClient do KVM
2. Podłącz terminal HP ThinClient do interfejsu WAN routera TP-Link przy pomocy kabla Ethernet

FAZA A: SERWER HTTP = HTTP

1. Uruchom program XAMPP
2. Do folderu htdoc w katalogu domowym programu XAMPP skopiuj plik test.html
3. Wykorzystując panel kontrolny XAMPP uruchom serwer Apache
4. Uruchom przeglądarkę i wpisz adres http://localhost:80/test.html. Przeglądarka powinna wyświetlić zawartość pliku.

FAZA B: ZDALNY KLIENT

1. Uruchom terminal a następnie sprawdź status interfejsów sieciowych przy pomocy polecenia `ifconfig`. Wyniki polecenia zapisz w formie zrzutu ekranu
2. Przejdź do trybu superuser przy pomocy polecenia `su` (hasło niewymagane)
3. Przypisz statyczny adres IP dla interfejsu ethernet przy pomocy polecenia:
   `ifconfig` **`nazwa_interfejsu adres_ip`** `netmask` **`maska`**
4. Uruchom terminal a następnie wykonaj polecenie ping do serwera HTTP:
   `ping` **`ip_serwera_http`**
5. Ping powinien zakończyć się niepowodzeniem. Zapisz wynik działania polecenia
6. Otwórz przeglądarkę i spróbuj uruchomić stronę udostępnioną przez serwer HTTP wpisując adres: http://ip_serwera:80/test.html
7. Zrób zrzut okna przeglądarki

FAZA C: ROUTER

1. Uruchom urządzenie
2. Z poziomu serwera HTTP połącz się z siecią WiFi nadawaną przez router
3. Przy pomocy polecenia ipconfig sprawdź adres IP przypisany dla karty WiFi
4. Wykorzystując serwer HTTP uruchom przeglądarkę a następnie uruchom panel administracyjny Routera wpisując adres: 192.168.1.1.
5. W przeglądarce pojawi się formularz szybkiej konfiguracji. W pierwszej kolejności należy ustalić hasło admina (np. admin). **UWAGA!** Słabe hasło może być wykorzystywane tylko na potrzeby wykonywanego zadania.
6. Po wciśnięciu „Let's Get Started" przechodzimy do widoku wyboru strefy czasowej. Możemy zostawić domyślną wartość, a następnie klikamy **Next**.
7. W kolejnym widoku wybieramy tryb pracy routera. Wybieramy **Wireless Router Mode** i klikamy **Next**.
8. Kolejny formularz służy do wyboru rodzaj połączenia WAN. Wybieramy **Static IP** i klikamy next.
9. Wyświetla się formularz, w którym podajemy dane związane z interfejsem WAN ustalone z prowadzącym.

10. Ostatni formularz jest związany z danymi sieci WiFi. Możemy podać dowolną nazwę sieci oraz dowolne hasło (należy je zapisać, aby możliwe było późniejsze połączenie się serwera http z routerem).
11. Po podaniu wszystkich danych następuję restart rutera.
12. Po restarcie należy zalogować się do panelu administratora a następnie w górnym menu wybrać zakładkę Advanced i przejść do menu Network->Internet
13. Zrobić zrzut ekranu przedstawiający konfiguracje interfejsu WAN rutera
14. W bocznym menu wybierz NAT Forwarding->Virtual Servers, wcisnij przycisk Add, a następnie w formularz podaj następujące dane:
    a. Interface Name: ewan_ipose_s
    b. Service type: dowolna nazwa (np. http)
    c. External port: port zewnętrzny ustalony z prowadzącym
    d. Internal IP: adres IP serwera HTTP
    e. Internal Port: port wewnętrzny ustalony z prowadzącym
    f. Protocol: TCP
    g. Zachowaj konfigurację wciskając przycisk Save
15. Zrób zrzut ekranu przedstawiający dodany serwer wirtualny

FAZA D: ZDALNY KLIENT

1. Potwórnie wykonaj ping do serwera HTTP (powinien zakończyć się niepowodzeniem), zapisz wyniki polecenia
2. W przeglądarce uruchom stronę udostępnioną przez serwer wpisując adres: http://adres_wan_routera:port_zewnętrzny/test.html

Wyniki pomiarów:

- Przedstaw opis poszczególnych faz wraz ze zrobionymi ilustracjami i wynikami pomiarów (np. ping)
- Wyjaśnij dlaczego polecenie ping ze zdalnego klienta do serwera HTTP zakończyło się niepowodzeniem
- Opisz co daje dodanie serwera wirtualnego w konfiguracji routera
- Przedstaw możliwości zastosowania funkcji wirutalnego serwera
- Wnioski