Protokół ARP (Address Resolution Protocol)

Służy do ustalania nieznanego adresu sprzętowego (ang. MAC address) maszyny o znanym adresie IP znajdującej się w tej samej sieci. Znajomość samego adresu IP jest bowiem niewystarczająca do realizowania komunikacji wewnątrzsieciowej, która wykorzystuje adresy MAC. Protokół ARP może być stosowany w sieciach umożliwiających transmisję w trybie broadcast (Ethernet, Token Ring, FDDI). Jego działanie przebiega następująco:

1 etap: Stacja A wysyła w trybie rozgłoszeniowym (ang. broadcast), czyli na adres sprzętowy FF:FF:FF:FF:FF:FF, żądanie (ang. ARP request), aby stacja o danym adresie IP odpowiedziała swoim adresem MAC. Pakiet z tym żądaniem zawiera adres MAC i adres IP stacji A.

2 etap: Jeśli stacja o danym adresie IP jest aktywna - nazwijmy ją B, wówczas wysyła do stacji A odpowiedź (ang. ARP reply) zawierającą własny adres MAC i własny adres IP. Uzupełnia przy tym swoją tablicę ARP (ang. ARP cache) znajdującą się w pamięci podręcznej o wpis z odwzorowaniem adresu IP stacji A na jej adres MAC. Może to zrobić, ponieważ informacje te są zawarte w pakiecie z żądaniem ARP wysłanym w 1 etapie przez stację A.

3 etap: Po otrzymaniu odpowiedzi od stacji B, stacja A wpisuje do swojej tablicy ARP odwzorowanie adresu IP stacji B na jej adres MAC. Wpis w pamięci podręcznej ARP jest przechowywany przez określony czas (zależny od systemu operacyjnego i konfiguracji odpowiedniego parametru), a po upływie tego czasu jest usuwany.

W systemie Linux czas ten jest określany w sekundach parametrem jądra *net.ipv4.neigh.default.gc_stale_time* i można go ustawiać poleceniem *sysctl*, np.

sysctl –w net.ipv4.neigh.default.gc_stale_time=1800

Protokół ARP jest uruchamiany zawsze wtedy, kiedy stacja źródłowa ma wysłać dane na określony adres IP **w tej samej sieci**, ale nie ma w swojej tablicy ARP wpisu odwzorowującego adres IP stacji docelowej na jej adres MAC. Po uzyskaniu adresu MAC stacji docelowej, stacja źródłowa umieszcza ten adres w odpowiednim polu adresowym ramki z danymi i przystępuje do ich wysyłania.

W systemie operacyjnym Linux protokół ARP jest zaimplementowany jako jeden ze składników jądra. Dostępne jest również polecenie *arp* służące do zarządzania pamięcią podręczną ARP. Oto niektóre opcje tego polecenia:

arp –a : Wypisuje zawartość tablicy ARP, podaje nazwy hostów. Użycie dodatkowo opcji –n powoduje wypisanie adresów IP zamiast nazw.

arp –a –i <nazwa interfejsu> : Wypisuje zawartość tablicy ARP dla wskazanego interfejsu. **W przypadku, gdy maszyna ma wiele interfejsów, dla każdego z nich istnieje osobna tablica ARP**.

arp –d <nazwa lub adres hosta> : Usuwa z tablicy ARP wpis dla wskazanego hosta

*arp –d ** : Usuwa wszystkie wpisy z tablicy ARP (* zastępuje dowolny ciąg znaków)

arp –s <nazwa lub adres IP> <adres MAC> : Dodaje wpis do tablicy ARP odwzorowujący nazwę lub adres IP wskazanego hosta na jego adres MAC. Wpis taki nie jest automatycznie usuwany z pamięci podręcznej ARP, można go usunąć tylko ręcznie.

ifconfig eth0 –arp : Wyłącza ARP na lokalnym interfejsie eth0, który przestaje wysyłać i odpowiadać na zapytania ARP.

ifconfig eth0 arp : Włącza ARP na lokalnym interfejsie eth0

W nowszych wersjach systemu Linux jest instalowany pakiet *iproute*, udostępniający polecenie „*/sbin/ip*" służące do konfigurowania protokołu IP. Rolę polecenia *arp* spełnia polecenie „*ip neighbor*", dające więcej możliwości. Oto kilka przykładów:

ip neighbor show : wypisuje zawartość tablicy ARP

ip neighbor add <adres IP> lladdr <adres MAC> dev eth0 : dodaje wpis do tablicy ARP odwzorowujący adres IP wskazanego hosta na jego adres MAC. Jeśli chcemy, aby wpis nie był usuwany automatycznie, należy dodać opcję „*nud permanent*".

ip neighbor del <adres IP> dev eth0 : usuwa wpis dla hosta o podanym adresie IP z tablicy ARP interfejsu eth0

Uwaga: zamiast „*ip neighbor*" wystarczy pisać „*ip neigh*".

Działanie protokołu ARP można „wymusić" wydając polecenie *arping*:

arping <adres IP> : wysyła nieskończoną liczbę zapytań ARP ze wskazanym adresem IP. Można to przerwać wciskając Ctrl-C (jeśli polecenie *arping* działa w pierwszym planie). Użycie opcji –f powoduje wysłanie tylko jednego zapytania.

Śledzenie działania protokołu ARP umożliwia polecenie *arpwatch* . Nie jest ono dostępne w standardowych wersjach znanych dystrybucji systemu Linux. Wymaga instalacji ręcznej (np. poleceniem *yum* w dystrybucji Fedora, albo *apt-get* w dystrybucjach Ubuntu czy Debian).

Protokół DHCP (Dynamic Host Configuration Protocol)

Służy do automatycznej konfiguracji parametrów sieciowych na komputerze-kliencie. Serwer DHCP zazwyczaj znajduje się w tej samej sieci co komputer-klient. Protokół ten jest realizowany w następujących etapach:
1. Klient wysyła w sieć komunikat DHCP Discover (broadcast MAC, czyli ff:ff:ff:ff:ff:ff)
2. Serwer odpowiada komunikatem DHCP Offer, w którym są m.in. adres IP, maska, adres routera, adres serwera DNS.
3. Klient akceptuje proponowane parametry wysyłając komunikat DHCP Request
4. Serwer potwierdza przydzielenie parametrów komunikatem DHCP Ack
Parametry są dzierżawione na pewien czas zwany okresem dzierżawy. Po upływie połowy tego okresu klient wysyła do serwera żądanie odnowienia dzierżawy.

Trasowanie (Routing)

Przed wysłaniem pakietu na określony adres IP, host źródłowy sprawdza, czy maszyna docelowa znajduje się w sieci lokalnej, czy też poza nią. Sprawdzenie to polega na nałożeniu maski, będącej lokalnym parametrem konfiguracyjnym maszyny źródłowej, na adres IP maszyny docelowej. Jeśli w wyniku tej operacji otrzymany zostanie adres sieci lokalnej, host źródłowy umieszcza w odpowiednim polu wysyłanej ramki adres MAC maszyny docelowej, a następnie wysyła ramkę bezpośrednio do niej. **Jeśli docelowy adres MAC jest nieznany (nie ma go w tablicy ARP), to do jego ustalenia stosowany jest protokół ARP**. Jeśli po nałożeniu maski na docelowy adres IP otrzymany zostanie adres inny niż sieci lokalnej, to pakiet kierowany jest do jednego z routerów znajdujących się w sieci lokalnej. Wybór routera dokonywany jest na podstawie adresu docelowego. Jeśli w sieci znajduje się tylko jeden router, to jego adres IP jest konfigurowany na hostach w tej sieci jako adres tzw. routera domyślnego (ang. default gateway). Router domyślny może być też skonfigurowany na hostach w sieci z więcej niż jednym routerem, ale wtedy niektóre pakiety będą przesyłane między routerami przed opuszczeniem sieci lokalnej. Adresy IP routerów są, podobnie jak własny adres IP i maska, lokalnymi parametrami konfiguracyjnymi każdego hosta działającego w oparciu o protokół IP. **Adresy MAC interfejsów routerów, tak samo jak adresy MAC wszystkich hostów z sieci lokalnej, ustalane są za pomocą protokołu ARP**.

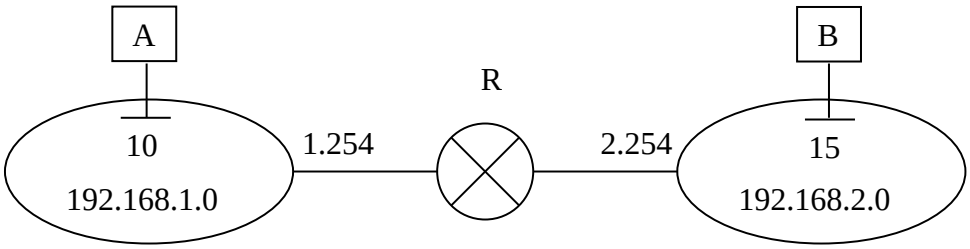
Proces przekazywania pakietów między sieciami nazywa się trasowaniem (ang. routing). Jest ono realizowane przez urządzenia trasujące (ang. router) w oparciu o docelowy adres sieciowy pakietu, oraz informacje zapisane w tablicy trasowania (ang. routing table). Po otrzymaniu pakietu router sprawdza zgodność adresu docelowego z kolejnymi wierszami tablicy i na tej podstawie przesyła pakiet do kolejnego routera albo bezpośrednio do komputera docelowego. Należy podkreślić, że tablice trasowania mają również hosty (w oparciu o nią host decyduje czy pakiet z danym adresem docelowym ma wysyłać bezpośrednio do odbiorcy w sieci lokalnej czy do routera).

Tabela trasowania routera może być konfigurowana ręcznie przez administratora – jest to tzw. routing statyczny, albo automatycznie w wyniku działania protokołu routingu – tzw. routing dynamiczny. Istnieje kilka podstawowych protokołów routingu różniących się pod względem kryterium wyboru trasy pakietów, czy obszaru działania. Jednak wszystkie te protokoły maja jedną wspólną cechę – router konfiguruje (automatycznie) swoją tablicę trasowania bazując na informacji uzyskiwanej od routerów sąsiednich, czyli znajdujących się w tych sieciach, do których jest on bezpośrednio przyłączony.

Uwaga: Przy zwykłym trasowaniu źródłowy i docelowy adres logiczny nie ulegają zmianie na całej trasie pakietu. Routery zmieniają natomiast adresy MAC. Podczas przekazywania pakietu router zmienia docelowy adres MAC (MAC interfejsu, na którym router odebrał pakiet) na adres MAC interfejsu następnego routera albo adres MAC interfejsu stacji docelowej. Natomiast źródłowy adres MAC (MAC interfejsu, z którego pakiet był wysłany do routera) jest zmieniany na adres MAC wyjściowego interfejsu routera.

Przykład ilustrujący zmianę adresów MAC przez router

W sieci klasy C o adresie 192.168.1.0 znajduje się host A o adresie 192.168.1.10, natomiast w sieci klasy C o adresie 192.168.2.0 – host B o adresie 192.168.2.15. A wysyła do B pakiet danych.



Adresy IP na całej trasie z A do B:
źródłowy: 192.168.1.10
docelowy: 192.168.2.15

Adresy MAC na trasie z A do interfejsu 192.168.1.254 routera R:
źródłowy: MAC hosta A
docelowy: MAC interfejsu 192.168.1.254

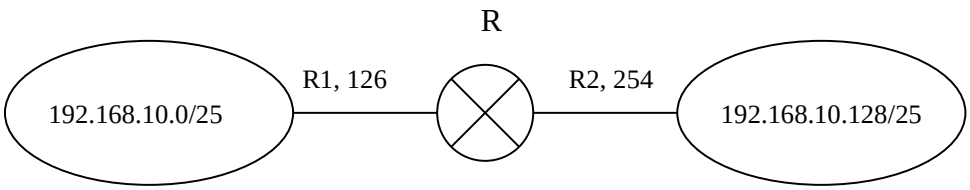
Adresy MAC na trasie z interfejsu 192.168.2.254 routera R do B:
źródłowy: MAC interfejsu 192.168.2.254
docelowy: MAC hosta B

Router R nie zmienia adresów IP – pozostają one stałe na całej trasie pakietu, natomiast musi zmienić adresy MAC, ponieważ pakiet jest przekazywany z jednej sieci do drugiej.

Uwaga: adresy IP nie ulegają zmianie przy zwykłym routingu, ale zmieniają się przy przechodzeniu pakietu z sieci prywatnej do publicznej albo z publicznej do prywatnej. Jest to tzw. mechanizm translacji adresów. Router, który realizuje ten mechanizm jest bramą (ang. gateway) między siecią prywatną a publiczną częścią internetu.

Przykłady ilustrujące routing IPv4

Przykład 1: Sieć klasy C o adresie 192.168.10.0 jest podzielona na dwie równe podsieci maską 25 bitową, czyli 255.255.255.128. Fizyczne interfejsy routera R do pierwszej i drugiej podsieci mają nazwy systemowe R1 i R2.



Tablica routingu routera R:

Sieć (host) przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.0	255.255.255.128	0.0.0.0	R1
192.168.10.128	255.255.255.128	0.0.0.0	R2

Wpisy dla sieci, do których router jest bezpośrednio przyłączony, są dodawane do jego tablicy trasowania automatycznie, w wyniku skonfigurowania interfejsów łączących go z tymi sieciami. Bieżący przykład przedstawia taką właśnie sytuację.

Tablica routingu przykładowego hosta z pierwszej podsieci, z interfejsem o nazwie eth0:

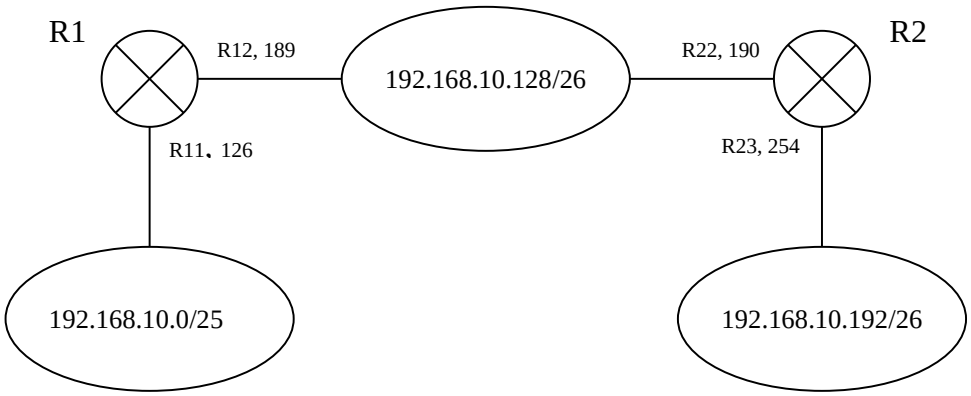
Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
127.0.0.0	255.0.0.0	0.0.0.0	lo (loopback)
0.0.0.0	0.0.0.0	192.168.10.126	eth0
192.168.10.0	255.255.255.128	0.0.0.0	eth0

Tablica routingu przykładowego hosta z drugiej podsieci, z interfejsem o nazwie eth0:

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
127.0.0.0	255.0.0.0	0.0.0.0	lo (loopback)
0.0.0.0	0.0.0.0	192.168.10.254	eth0
192.168.10.128	255.255.255.128	0.0.0.0	eth0

Przykład 2.

Sieć klasy C o adresie 192.168.10.0 jest podzielona metodą VLSM na trzy podsieci:



Maska pierwszej podsieci ma 25 bitów, drugiej i trzeciej – 26 bitów. Odpowiednie zakresy adresów unicast są następujące: 1 – 126, 129 – 190, 193 – 254 (ostatni bajt adresu), natomiast adresy broadcast (ostatni bajt adresu) to 127, 191 i 255. R11 i R12 to nazwy interfejsów routera R1 do pierwszej i drugiej podsieci; R21, R22 to nazwy interfejsów routera R2 do drugiej i trzeciej podsieci.

Tablica routingu R1:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.0	255.255.255.128	0.0.0.0	R11
192.168.10.128	255.255.255.192	0.0.0.0	R12
192.168.10.192	255.255.255.192	192.168.10.190	R12

Tablica routingu R2:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.0	255.255.255.128	192.168.10.189	R22
192.168.10.128	255.255.255.192	0.0.0.0	R22
192.168.10.192	255.255.255.192	0.0.0.0	R23

Przykładowy host z interfejsem o nazwie eth0 i adresie 192.168.10.130, znajdujący się w drugiej podsieci, powinien mieć w swojej tablicy routingu następujące wpisy:

Tabela trasowania hosta z podsieci 192.168.10.128

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.0	255.255.255.128	192.168.10.189	eth0
192.168.10.128	255.255.255.192	0.0.0.0	eth0
192.168.10.192	255.255.255.192	192.168.10.190	eth0

Gdyby rozważany host wszystkie pakiety adresowane poza sieć lokalną wysyłał do routera domyślnego, na przykład do R2, zgodnie z następującym wpisem:

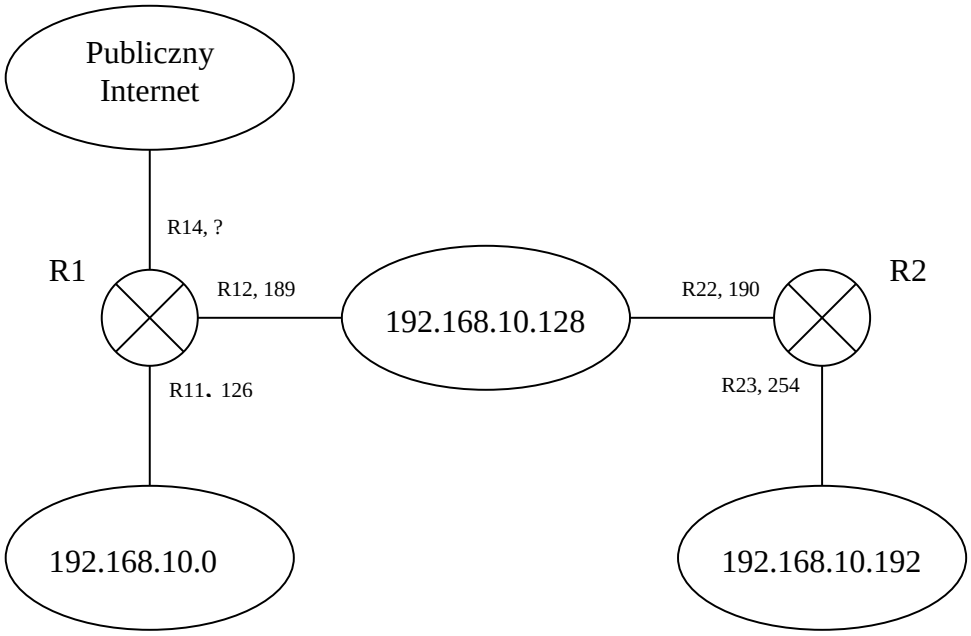
Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
0.0.0.0	0.0.0.0	192.168.10.190	eth0

wówczas pakiet do sieci 192.168.10.0, przykładowo do hosta o adresie 192.168.10.1, byłby najpierw skierowany do R2, stamtąd zgodnie z jego tablicą routingu – do R1, który wysłałby pakiet bezpośrednio do 192.168.10.1. W takim przypadku pakiet niepotrzebnie trafia do R2, zamiast od razu do R1.

Uwaga: R2 otrzymując od 192.168.10.130 pakiet skierowany do sieci 192.168.10.0 wysyła ten pakiet do R1, oprócz tego informuje hosta 192.168.10.130 (przy pomocy specjalnego komunikatu ICMP), że pakiety do sieci 192.168.10.0 powinien kierować bezpośrednio do R1.

Przykład 3.

Sieć klasy C o adresie 192.168.10.0 jest podzielona tak jak w przykładzie 2. Dodatkowo, router R1 ma połączenie z Internetem – przez interfejs R14 o nieznanym publicznym IP.



Tablica routingu R1:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.0	255.255.255.128	0.0.0.0	R11
192.168.10.128	255.255.255.192	0.0.0.0	R12
192.168.10.192	255.255.255.192	192.168.10.190	R12
0.0.0.0	0.0.0.0	Nieznany, publiczny IP (np. IP routera dostawcy Internetu)	R14

Uwaga: Sieć 192.168.10.0 (podzielona na 3 podsieci) jest siecią adresów prywatnych. W związku z tym w pakiecie wysyłanym np. z podsieci 192.168.10.128/26 do publicznego Internetu, przy przejściu przez router R1 źródłowy adres IP zmieni się na adres IP interfejsu R14, natomiast nie zmieni się adres docelowy. Z kolei w pakiecie wysyłanym z Internetu publicznego, a przeznaczonym np. dla hosta 192.168.10.150, docelowy adres IP (adres interfejsu R14) zmieni się na adres 192.168.10.150, natomiast nie zmieni się adres źródłowy.

Tablica routingu R2:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.128	255.255.255.192	0.0.0.0	R22
192.168.10.192	255.255.255.192	0.0.0.0	R23
0.0.0.0	0.0.0.0	192.168.10.189	R22

Zauważmy, że tabeli trasowania R2, oprócz wpisów dla sieci do niego przyłączonych, jest jeszcze tylko trasa domyślna. Wynika to z tego, że jeśli pakiet ma trafić z R2 do sieci 192.168.10.0 albo do Internetu, to w obu przypadkach R2 musi wysłać ten pakiet do R1.

Przykładowy host z interfejsem o nazwie eth0 i adresie 192.168.10.130, znajdujący się w drugiej podsieci, powinien mieć w swojej tablicy routingu następujące wpisy:

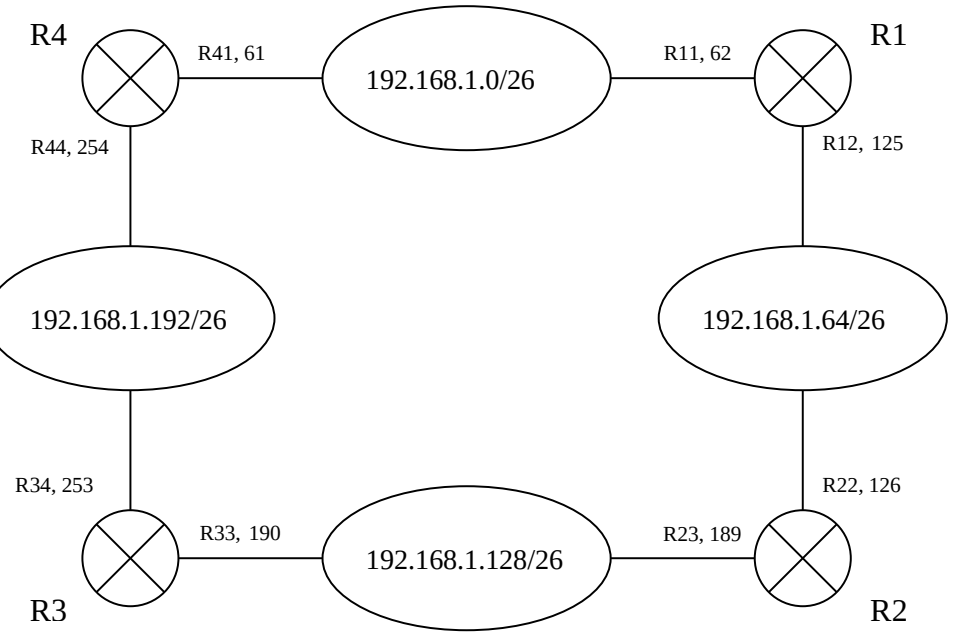
Tabela trasowania hosta z podsieci 192.168.10.128

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
192.168.10.128	255.255.255.192	0.0.0.0	eth0
0.0.0.0	0.0.0.0	192.168.10.189	eth0
192.168.10.192	255.255.255.192	192.168.10.190	eth0

W odróżnieniu od przykładu 2, trasa domyślna jest w tym przypadku konieczna, przy czym uzasadnienie jest takie samo, jak dla trasy domyślnej routera R2.

Przykład 4.

Sieć klasy C o adresie 192.168.1.0 jest podzielona na 4 równe podsieci maską 26 bitową.
Nazwy interfejsów routera R1 do pierwszej i drugiej podsieci: R11, R12;
nazwy interfejsów routera R2 do drugiej i trzeciej podsieci: R22, R23;
nazwy interfejsów routera R3 do trzeciej i czwartej podsieci: R33, R34;
nazwy interfejsów routera R4 do czwartej i pierwszej podsieci: R44, R41.



Tablica routingu R1:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.0	255.255.255.192	0.0.0.0	R11
192.168.1.64	255.255.255.192	0.0.0.0	R12
192.168.1.128	255.255.255.192	192.168.1.126	R12
192.168.1.192	255.255.255.192	192.168.1.61	R11
192.168.1.200	255.255.255.255	192.168.1.126	R12

Uwaga 1: Wpis w piątym wierszu określa trasę do pojedynczej stacji, a nie do sieci. Zgodnie z zasadą dłuższej maski, R1 wybierze trasę do 192.168.10.200 prowadzącą przez R2, a nie przez R4, ponieważ dla trasy przez R2 maska jest 32 bitowa, a dla trasy przez R4 – 26 bitowa.

Uwaga 2: Załóżmy, że działają wszystkie routery i rozważmy następującą sytuację:

Przykładowy host z interfejsem o nazwie eth0 i adresie 192.168.1.70, znajdujący się w drugiej podsieci, ma w swojej tablicy routingu następujące wpisy (routerem domyślnym jest R2):

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.64	255.255.255.192	0.0.0.0	eth0
0.0.0.0	0.0.0.0	192.168.1.126	eth0

czyli R2 jest routerem domyślnym dla 192.168.1.70, natomiast R2 ma w swojej tablicy routingu następujący wpis (trasa do czwartej sieci przez R1):

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.192	255.255.255.192	192.168.1.125	R22

Przy tak skonfigurowanych tablicach pakiety wysłane przez 192.168.1.70, przeznaczone dla 192.168.1.200, będą „odbijane" między routerami R1 i R2 (ściślej – między interfejsami R12 i R22), bo zgodnie z 5 wierszem swojej tabeli R1 kieruje do R2 pakiety przeznaczone dla 192.168.1.200). W rezultacie pakiety te nigdy nie trafią do adresata. Można temu zaradzić dodając do tablicy routingu R2 następujący wpis:

Sieć/host przeznaczenia	Maska	Adres następnego routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.200	255.255.255.255	192.168.1.190	R23

Uwaga 3: W protokole IP istnieje mechanizm (wykorzystujący pole TTL nagłówka IP) zapobiegający krążeniu pakietów w pętli, co może być efektem niepoprawnej konfiguracji tablic trasowania, m.in. takiej jak w powyższym przykładzie.

Mechanizm Proxy ARP

Mechanizm ten służy do ukrycia przed hostami faktu, że znajdują się one w różnych sieciach IP (np. rozdzielonych tunelem VPN). Jest konfigurowany na routerach i działa w ten sposób, że router odpowiada własnym adresem MAC na żądania ARP wysłane na adres IP z innej sieci. Ilustruje to następujący przykład. W środowisku przedstawionym na poniższym rysunku hosty w podsieciach 192.168.1.0/25 i 192.168.1.128/25 są skonfigurowane z maską 255.255.255.0, tak jakby znajdowały się w jednej sieci. Jeśli host o adresie 192.168.10.10 wyśle żądanie ARP na adres 192.168.10.150, to router R1 odpowie mu adresem MAC interfejsu R11. W rezultacie host ten wyśle do R1 pakiet przeznaczony dla 192.168.10.150, tak jakby wysyłał pakiet bezpośrednio do stacji docelowej, a nie do routera. Zgodnie z tabelami trasowania routerów, pakiet zostanie przesłany z R1 do R2, a następnie do hosta 192.168.1.150

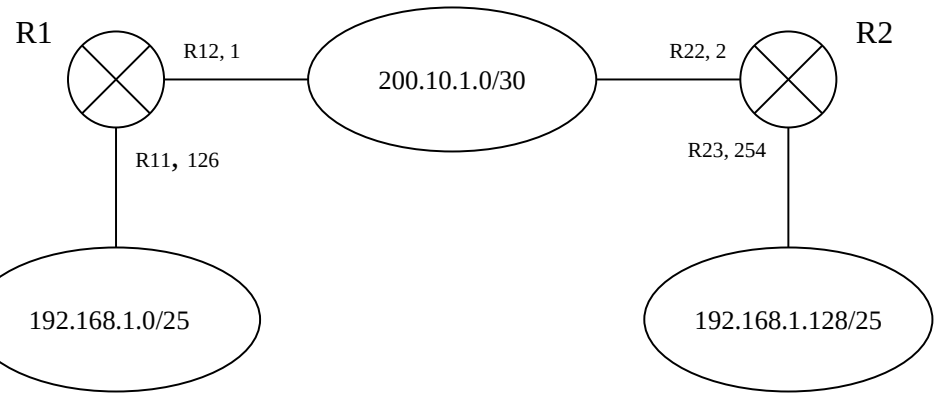


Tabela routingu R1

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.0	255.255.255.128	0.0.0.0	R11
200.10.1.0	255.255.255.252	0.0.0.0	R12
192.168.1.128	255.255.255.128	200.10.1.2	R12

Tabela routingu R2

Sieć/host przeznaczenia	Maska	Adres routera	Nazwa systemowa interfejsu wyjściowego
192.168.1.128	255.255.255.128	0.0.0.0	R23
200.10.1.0	255.255.255.252	0.0.0.0	R22
192.168.1.0	255.255.255.128	200.10.1.1	R22