Piotr Kowalski
KAiTI

Sieci komputerowe
- Protokoły wspierające IPv4

Plan i problematyka wykładu

1. Odwzorowanie adresów IP na sprzętowe i odwrotnie – protokoły ARP i RARP.
2. Routing IP
   - Tablice routingu, routing dynamiczny
   - Protokół RIP-2
   - Protokół OSPF
   - Inne protokoły routingu dynamicznego
3. Nadzór nad pracą sieci – protokół ICMP.

Odwzorowanie adresów

Adresy protokołowe – abstrakcja realizowana przez oprogramowanie, a nie sprzęt sieciowy który nie jest w stanie na ich podstawie zlokalizować komputera.

Adres protokołowy następnego etapu na drodze datagramu należy „przetłumaczyć" na odpowiadający mu adres fizyczny.

Ustalanie adresów sprzętowych na podstawie protokołowych (i odwrotnie) nosi nazwę odwzorowywania adresów.

Węzeł lub router odwzorowuje adres IP gdy wysyła pakiet do innego komputera/routera przyłączonego do tej samej sieci fizycznej. Odwzorowanie to nie ma miejsca gdy adresat datagramu jest przyłączony do innej sieci!

Metody odwzorowywania adresów

Tablicowa – odwzorowania są przechowywane w tablicy (zwykle tworzonej dynamicznie), która w razie potrzeby jest przeszukiwana przez oprogramowanie

Obliczeniowe – adres protokołowy przydzielony komputerowi jest wybrany w taki sposób, żeby można było go przekształcić w adres sprzętowy za pomocą ciągu operacji arytmetycznych i logicznych

Sieciowe – w celu odwzorowania adresów komputery przesyłają w sieci komunikaty z zapytaniami (o adres sieciowy węzła) i odpowiedziami (ten adres zawierający)

ARP (Address Resolution Protocol)

- ARP to sieciowa metoda odwzorowywania adresów, opracowana pierwotnie dla sieci Ethernet w latach 80-tych XX wieku.
- Klient ARP poza przesyłaniem komunikatów przechowuje tabelę odwzorowywania adresów, z której wpisy usuwane są automatycznie po pewnym, zależnym od implementacji protokołu czasie.
- ARP definiuje 2 rodzaje komunikatów:
  - żądanie (ang. request) – rozgłaszane w sieci lokalnej
  - odpowiedź (ang. reply) – węzła o adresie w żądaniu
- W obu przypadkach wiadomość protokołu ARP zawiera adres sprzętowy i IP, zarówno nadawcy, jak i odbiorcy, co pozwala na obustronną aktualizację tablic.

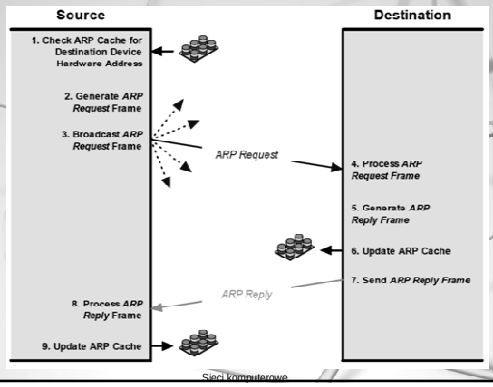
Format wiadomości ARP

Bity / Bajty	0-7	8-15	16-23	24-31
1	Typ adresu sprzętowego		Typ adresu protokołowego	
2	Długość adresu sprzętowego	Długość adresu protokołowego	Typ operacji	
3	Adres sprzętowy nadawcy			
4	Adres sprzętowy nadawcy (cd.)		Adres protokołowy nadawcy	
5	Adres protokołowy nadawcy (cd.)		Adres sprzętowy adresata	
6	Adres sprzętowy adresata (cd.)			
7	Adres protokołowy adresata			

Pola wiadomości ARP

- Typ adresu sprzętowego – np. 1 dla Ethernet
- Typ adresu protokołowego - np. 0800h dla IPv4
- Długość adresów: sprzętowego i protokołowego – w bajtach (dla Ethernet 6, dla IPv4 – 4)
- Typ operacji – np.
  1 – żądanie ARP,
  2 – odpowiedź ARP,
  3 – żądanie RARP
  4 – odpowiedź RARP
- Adresy sprzętowe i protokołowe nadawcy i odbiorcy

Działanie protokołu



RARP – czyli Reverse ARP

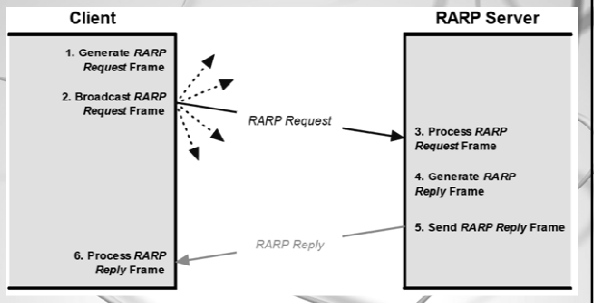
Po co nam w ogóle RARP?

Niektóre węzły, takie jak bezdyskowe stacje robocze nie znają swojego adresu IP. Wysłanie zapytania RARP pozwala im ten adres ustalić.

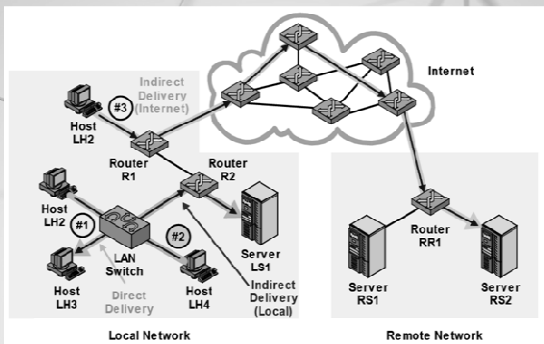
Adresatem zapytania RARP jest umieszczony w sieci lokalnej serwer do tego dedykowany. Komunikaty przesyłane w ramach protokołu są zgodne z komunikatami ARP (kod operacji: 3).

Obecnie w celu przyznania adresów IP stosuje się częściej protokoły bazujące na UDP – tj. DHCP i BOOTP.

RARP – zasada działania



Wprowadzenie do przekazywania pakietów



Routing

- Jeśli punkt przeznaczenia informacji dołączony jest bezpośrednio do hosta (np. łącze punkt - punkt) lub jest nim wydzielona sieć LAN (np. Ethernet), to wtedy datagram wysyłany jest bezpośrednio do tego punktu.
- W innym przypadku host wysyła informacje do rutera domyślnego (ang. default), którego zadaniem jest dostarczenie tego datagramu do punktu przeznaczenia
- Warstwa IP ma w pamięci tablicę rutowania, która jest przeszukiwana za każdym razem, gdy nadejdzie nowy datagram. Jeśli datagram nie jest skierowany do tej warstwy IP, to wtedy:
  1) jeśli warstwa IP skonfigurowana jest do pracy jako ruter, pakiet jest przesyłany dalej
  2) jeśli warstwa nie pracuje jako ruter to datagram jest odrzucany

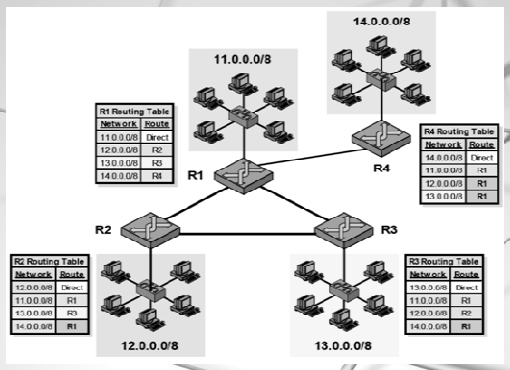
Algorytm routingu IP (next-hop routing)

1. Przeszukać tablicę rutingu w poszukiwaniu rekordu, który odpowiada adresowi przeznaczenia IP. Jeśli taki adres został znaleziony – wyślij pakiet do wskazanego rutera będącego ruterem następnego przejścia lub do bezpośrednio dołączonego interfejsu.
2. Przeszukać tablicę rutingu w poszukiwaniu rekordu, który odpowiada adresowi sieci. Jeśli taki adres został znaleziony – wyślij pakiet do wskazanego rutera będącego ruterem następnego przejścia lub do bezpośrednio dołączonego interfejsu.
3. Przeszukać tablicę rutingu w poszukiwaniu rekordu oznaczonego jako "domyślny" (ang. default). Jeśli zostanie znaleziony, wyślij pakiet do wskazanego rutera następnego przejścia.

Jeśli żaden z tych trzech kroków nie przyniesie rezultatu, datagram zostaje uznany jako taki, którego nie można dostarczyć a do aplikacji wysyłającej datagram wysyłany jest komunikat o błędzie.

Uwaga: w procesie przekazywania pakietów adres adresata pozostaje niezmieniony!

Rola tablicy routingu



Protokoły routingu dynamicznego

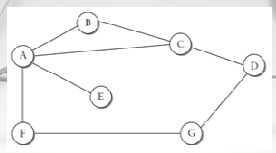
Tablice routingu musza być nieustannie uaktualniane (dostosowywane do bieżącego stanu sieci), w sposób zapewniający efektywne jej wykorzystanie. W tym celu opracowano protokoły routingu dynamicznego, pozwalające na wymianę informacji między routerami.

Podstawowe metody routingu dynamicznego:

- Metoda wektora odległości (ang. distance vector routing), nazywana często algorytmem Bellmana-Forda
- Metoda stanu łącza (ang. link-state routing) nazywana też często algorytmem najkrótszej ścieżki

Metody wektora odległości

Każdy router przesyła wektor zawierający znane mu odległości do innych węzłów.



Start

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Stop

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	?	?	?
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

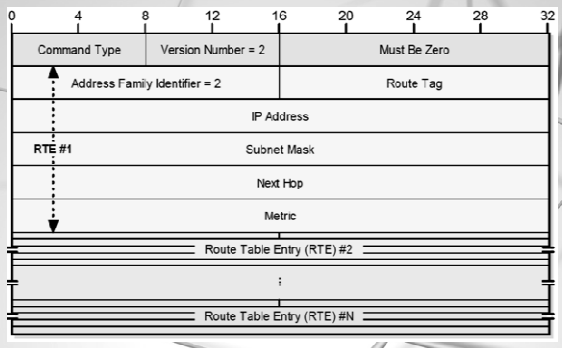
Przykład: RIP

RIP (Routing Information Protocol) to najbardziej znany protokół routingu dynamicznego oparty o metody wektora odległości. Najnowsze odmiany tego protokoły to RIP-2 i RIPng opracowany dla IPv6.

Główne cechy:

- Odległość mierzona w skokach (ang. hops), maksymalna długość trasy to 16 węzłów (odp. Destination unreachable)
- Dwa typy komunikatów
  - zapytanie (ang. request) – wysyłane przez router np. przy jego włączeniu, może dotyczyć całej tabeli bądź jej części
  - odpowiedź (ang. response) – wysyłana w odpowiedzi na zapytanie i stale, co 30 sekund
- Dodatkowe timery usuwające dawno nieuktualniane wpisy
- Wsparcie domyślnej trasy (oznaczonej 0.0.0.0) i multicasting (w RIP-2)

Ramka RIP-2



Metody stanu łącza

W metodach stanu łącza każdy router przesyła jedynie dostępne mu informacje dotyczące połączeń do najbliższych mu węzłów tzw. Link-State Packet (LSP). Wybór trasy polega na składaniu tego typu informacji w spójną całość.

Każdy z routerów rozsyła tzw. link-state packet zawierający identyfikator oraz listę węzłów do niego przyłączonych wraz z kosztem tych połączeń.

Trasa obliczana jest na podstawie grafowego algorytmu Dijkstry.

Algorytm Dijkstry

M – lista węzłów dodanych do zbioru tras
N – zbiór węzłów sieci
l(i, j) – koszt połączenia (i,j)
M = {s}

for każdy n **w** N− {s}
  C(n) = l(s, n)
while (N != M)
  M = M ∪ {w} **taki że** C(w) jest **minimum** dla wszystkich w **w** (N− M)
  for każdy n **w** (N− M)
  C(n) = MIN(C(n), C(w) + l(w, n))

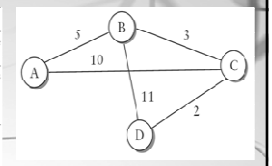
Algorytm Dijkstry w routingu

Dwie listy: potwierdzonych LP (ang. Confirmed list) i oczekujących LO (ang. Tentative list) każda zawierająca wpisy postaci <cel, koszt, następny węzeł>

1. Zainicjalizuj LP z wpisem dla samego siebie (i kosztem 0).
2. Węzeł dodany do LP nazwij następnym (NEXT) i analizuj jego LSP
3. Dla każdego sąsiada (NEIGHBOR) węzła NEXT policz koszt liczony jako koszt dotarcia od bieżącego węzła do NEXT i od NEXT do NEIGHBOR
   (a) Jeżeli NEIGHBOR nie jest na żadnej z list dodaj do LO <NEIGHBOR, KOSZT, NEXTHOP> gdzie NEXTHOP jest kierunkiem na drodze do NEXT
   (b) Jeżeli NIEIGHBOR jest na liście LO i koszt jest większy niż aktualny to zmień wpis LO <NEIGHBOR, KOSZT, NEXTHOP>
4. Jeżeli LO jest pusta – STOP. W przeciwnym wypadku wybierz wpis o najmniejszym koszcie z LO, przenieś do LP i wróć do kroku 2.

Przykład wyznaczania tablicy routingu

Step	Confirmed	Tentative	Comments
1	(D,0,-)		Since D is the only new member of the confirmed list, look at its LSP.
2	(D,0,-)	(B,11,B) (C,2,C)	D's LSP says we can reach B through B at cost 11, which is better than anything else on either list, so put it on Tentative list; same for C.
3	(D,0,-) (C,2,C)	(B,11,B)	Put lowest-cost member of Tentative (C) onto Confirmed list. Next, examine LSP of newly confirmed member (C).
4	(D,0,-) (C,2,C)	(B,5,C) (A,12,C)	Cost to reach B through C is 5, so replace (B,11,B). C's LSP tells us that we can reach A at cost 12.
5	(D,0,-) (C,2,C) (B,5,C)	(A,12,C)	Move lowest-cost member of Tentative (B) to Confirmed, then look at its LSP.
6	(D,0,-) (C,2,C) (B,5,C)	(A,10,C)	Since we can reach A at cost 5 through B, replace the Tentative entry.
7	(D,0,-) (C,2,C) (B,5,C) (A,10,C)		Move lowest-cost member of Tentative (A) to Confirmed, and we are all done.



Przykład: OSPF (ang. Open Shortest Path First)

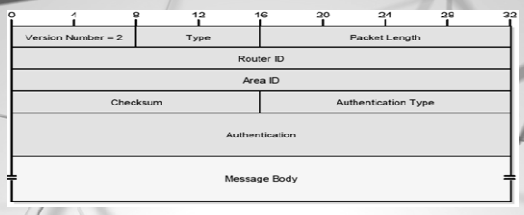
Protokół OSPF używa hierarchicznej struktury sieci z podziałem na obszary z centralnie umieszczonym obszarem zerowym (ang. area *0*).

OSPF jest protokołem typu link-state jedynie wewnątrz obszaru. Oznacza to, że w ramach pojedynczego obszaru wszystkie routery znają całą jego topologię i wymieniają się między sobą informacjami o stanie łączy, a każdy z nich przelicza trasy samodzielnie (algorytm Dijkstry).

Między obszarami OSPF działa jak protokół typu distance-vector, co oznacza, że routery brzegowe obszarów wymieniają się między sobą gotowymi trasami.

OSPF zapewnia ponadto dodatkowe uwierzytelnianie wysyłanych komunikatów.

Ramka OSPF



Typy wiadomości:

- Hello – nawiązywanie i utrzymywanie relacji z sąsiednimi węzłami,
- Database description – opis przechowywanych baz danych,
- Request link-state – żądanie informacji na temat stanów połączeń,
- Update link-state – aktualizacja stanów połączeń,
- Acknowledgment links-state – potwierdzenia stanów połączeń.

Inne metody routingu dynamicznego

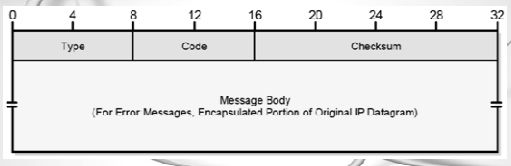
System autonomiczny (ang. *Autonomous System*, AS) to sieć lub grupa sieci opartych na protokole IP pod wspólną administracyjną kontrolą, w której utrzymywany jest spójny schemat trasowania (ang. *routing policy*). Protokoły używane w ramach systemów autonomicznych to wymienione już RIP, OSPF, a także EIGRP (Enhanced Interior Gateway Routing Protocol) firmy Cisco.

Zewnętrzne protokoły trasowania (zwane również protokołami bramy zewnętrznej – EGP, ang. Exterior Gateway Protocol) – używane do wymiany informacji o trasach pomiędzy różnymi systemami autonomicznymi. Podstawowym protokołem z tej grupy jest BGP (ang. Border Gateway Protocol). BGPv4 jest podstawą działania współczesnego Internetu.

Protokół ICMP

Protokół ICMP (ang. Internet Control Message Protocol) został opracowany jako uzupełnienie protokołu IP w zakresie niezawodności i jakości transmisji. Nie zapewnia on jej bezpośrednio, natomiast pozwala na przesyłanie komunikatów kontrolnych.

Protokół ICMP pracuje w warstwie internetu, a do przekazywania wiadomości wykorzystuje datagramy IP.



Funkcje protokołu ICMP

Wykrywanie nieosiągalnych miejsc przeznaczenia

Jeśli komputer docelowy nie odpowiada system, który wykrył problem wysyła do nadawcy komunikat *Destination Unreachable* (typ 3). Jeśli komunikat ten jest wysyłany przez router, oznacza, że router nie może wysyłać pakietów do danego komputera. Może to nastąpić w dwóch przypadkach:

- adres docelowy IP nie istnieje
- router nie może dostarczyć datagramu do tej sieci

W momencie, gdy komunikat ten jest wysyłany przez host, może to oznaczać, że:

- dany komputer nie posiada wsparcia dla któregoś z protokołów warstw wyższych lub port protokołu TCP jest nieosiągalny.

Destination unreachable

Code Value	Message Subtype	Description
0	*Network Unreachable*	The datagram could not be delivered to the network specified in the network ID portion of the IP address. Usually means a problem with routing but could also be caused by a bad address.
1	*Host Unreachable*	The datagram was delivered to the network specified in the network ID portion of the IP address but could not be sent to the specific host indicated in the address. Again, this usually implies a routing issue.
2	*Protocol Unreachable*	The protocol specified in the Protocol field was invalid for the host to which the datagram was delivered.
3	*Port Unreachable*	The destination port specified in the UDP or TCP header was invalid.
4	*Fragmentation Needed and DF Set*	This is one of those "leaders" rules. :) Normally, an IPv4 router will automatically fragment a datagram that it receives if it is too large for the maximum transmission unit (MTU) of the next physical network link. However, if the Don't Fragment (DF) bit in the Flags field of the IP header is set, this means the sender of the datagram does not want the datagram ever to be fragmented. This puts the router between the proverbial rock and hard place, and it will be forced to drop the datagram and send an error message. (We'll see this message type is most often used in a "clever" way, by intentionally sending messages of increasing size to discover the maximum transmission size that a link can handle. This process is called MTU path discovery.)
5	*Source Route Failed*	Generated if a source route was specified for the datagram in an option, but a router could not forward the datagram to the next step in the route.
6	*Destination Network Unknown*	Not used. Code 0 is used instead.
7	*Destination Host Unknown*	The host specified is not known. This is usually generated by a router local to the destination host and usually means a bad address.
8	*Source Host Isolated*	Obsolete, no longer used.
9	*Destination Network is Administratively Prohibited*	The source device is not allowed to send to the network where the destination device is located.
10	*Communication with Destination Host is Administratively Prohibited*	The source device is allowed to send to the network where the destination device is located, but not that particular device.
11	*Destination Network Unreachable for Type of Service*	The network specified in the IP address cannot be reached due to inability to provide service specified in the Type Of Service field of the datagram header.
12	*Destination Host Unreachable for Type of Service*	The destination host specified in the IP address cannot be reached due to inability to provide service specified in the datagram's Type Of Service field.
13	*Communication Administratively Prohibited*	The datagram could not be forwarded due to filtering that forces the message based on its contents.
14	*Host Precedence Violation*	Sent by a first-hop router (the first router to handle a sent datagram) when the Precedence value in the Type Of Service field is not permitted.
15	*Precedence Cutoff in Effect*	Sent by a router when receiving a datagram whose Precedence value (priority) is lower than the minimum allowed for the network at that time.

Inne funkcje ICMP

Informowanie o „zaginionych datagramach”

Jeśli jakiś datagram, podczas przechodzenia przez ruter osiągnie zerowy limit „czasu życia” (*Time-to-Live*) jest usuwany. Do komputera źródłowego danego datagramu wysyłany jest komunikat ICMP *Time-exceeded* (typ 11, kod 0).

Sprawdzanie zdalnego hosta

Odbywa się m.in. poprzez wywołanie komendy ping. Wysyłany jest komunikat ICMP *Echo Message* (typ 8, kod 0), po otrzymaniu którego komputer docelowy musi odpowiedzieć komunikatem *Echo Reply* (typ 0, kod 0). Jeśli tego nie zrobi, uznawany jest za nieosiągalny.

Dalsze możliwości zastosowania ICMP

Sterowanie przepływem danych

W przypadku, gdy komputer docelowy transmisji IP nie nadąża za obróbką przychodzących datagramów IP, ICMP wysyła komunikat *Source Quench* (typ 4, kod 0), po którym nadawca czasowo wstrzymuje transmisję.

Przekierowywanie ścieżek

Jeśli komputer, do którego dotarł datagram IP uzna, że właściwszą bramką będzie inny komputer z tej samej sieci, wysyła komunikat *Redirect* (typ 5, kody różnorakie) wskazujący na ten właśnie komputer (musi znajdować się w tej samej sieci). Po otrzymaniu takiego komunikatu nadawca aktualizuje swoją tablicę rutingu.

Inne przykłady: Rozgłaszanie routerów, maski podsieci itp.


DZIĘKUJĘ ZA UWAGĘ!
NASTĘPNY WYKŁAD:
TCP I UDP
Sieci komputerowe