Sieci komputerowe – konwersatorium 5

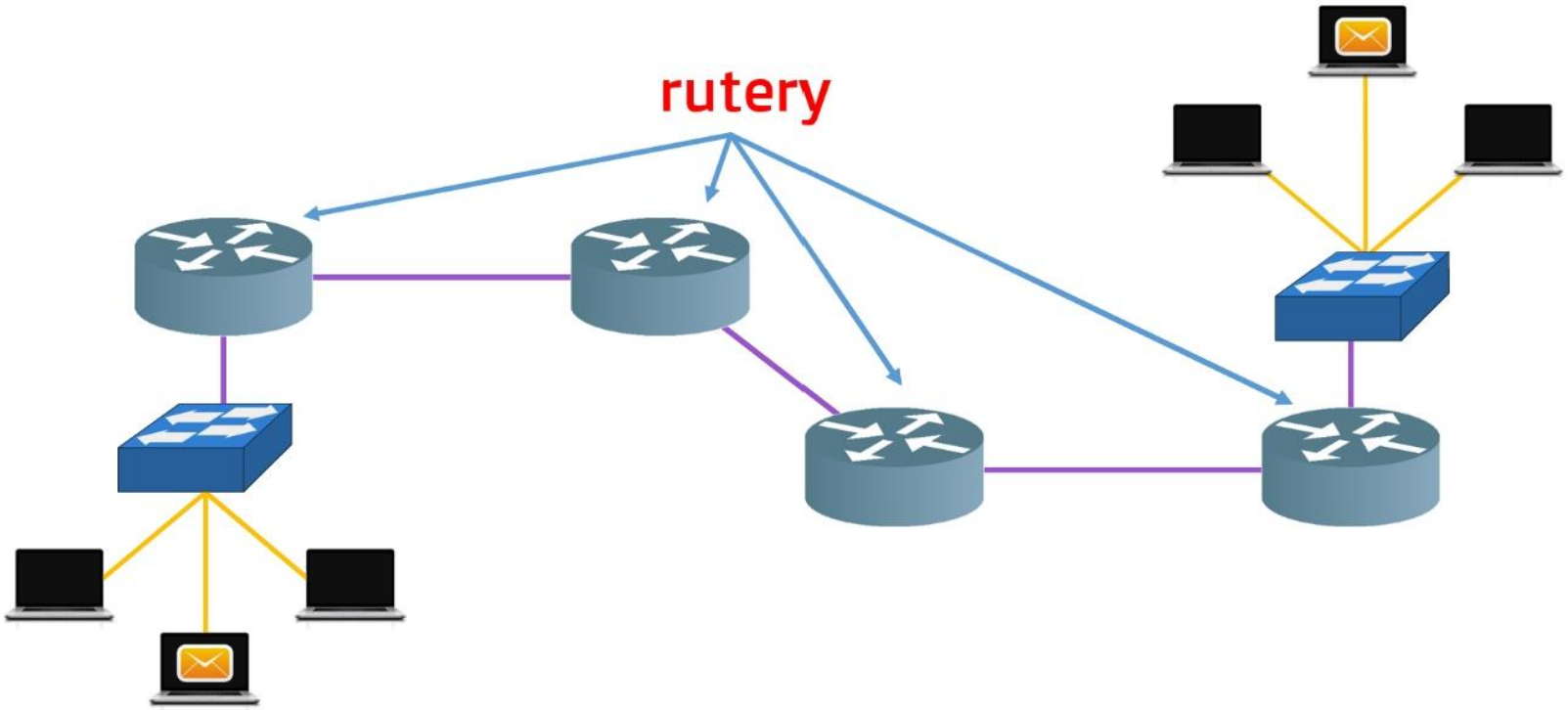
Jarosław Szkoła

Routing IP

Wprowadzenie

- Routing jest ustalony zestawem sposobów jak przesłać pakiety z jednej sieci do drugiej. Jest to jedna z podstawowych własności routerów umożliwiających przesyłanie danych w Internecie.
- oryginalne określenia (angielskojęzyczne) użyte do tych zagadnień mają wiele tłumaczeń. Stąd może się pojawić wrażenie pewnego braku standardu w języku polskim. I tak: ang. routing - pl. trasowanie, ruting, rutowanie
- W dalszej części wykładu zostanie przyjęta najbardziej rozpowszechniona nazwa – routing

Przykładowa sieć



Sieć komputerowa złożona z wielu routerów

Funkcja routera w procesie przesyłania pakietów

- Router jest specjalistycznym komputerem, którego podstawowym zadaniem jest właściwe przesyłanie pakietów, które przychodzą na kolejne interfejsy sieciowe.
- Dzięki temu możliwa jest niezawodna komunikacja pomiędzy poszczególnymi sieciami komputerowymi.
- Każdy komputer wyposażony w system operacyjny może pełnić rolę routera.
- Ze względów bezpieczeństwa funkcja ta jest wyłączana w przypadku zwykłych hostów.

Funkcja routera w procesie przesyłania pakietów

- W praktyce najczęściej stosuje się do celu przesyłania pakietów specjalistyczne urządzenia, które mają zbliżoną budowę do standardowych jednostek obliczeniowych
- Ze względu na specjalistyczne funkcje, które muszą pełnić są też wyposażone w odpowiedni system operacyjny typowy dla producenta tych urządzeń
- Router dzięki wpisom w tablicy routingu obsługuje ruch pakietów w warstwie L3 modelu ISO/OSI
- Wbudowane mechanizmy umożliwiają również filtrowanie pakietów zwiększając tym samym poziom bezpieczeństwa sieci, które są obsługiwane przez te urządzenia
- Dodatkowo odpowiednie algorytmy doboru optymalnych ścieżek umożliwiają efektywne i niezawodne przesyłanie pakietów w sieci. Router korzysta przy tym z informacji wymienianych z urządzeniami sąsiednimi.

Routing w protokole IP

- Protokół IP jest przykładem protokołu routowalnego
- Protokół IP jest protokołem bezpołączeniowym, co oznacza, że do przesłania danych nie potrzebne jest zestawienie połączenia pomiędzy nadawcą i odbiorcą. Jest to protokół, który został opracowany aby był maksymalnie skuteczny
- Protokół IP wykorzystuje wszystkie posiadane mechanizmy, aby dostarczyć pakiet do celu. Protokół ten nie dba o potwierdzenie, czy dane dotarły do adresata, stąd też często jest określany jako zawodny. Określenie „zawodny” jest trochę nieprecyzyjne, ponieważ pakiety wysyłane są wszelkimi możliwymi trasami. Za potwierdzenie właściwego przesłania odpowiadają protokoły wyższych warstw.

Rodzaje routingu

- W zależności od sposobu zdobywania informacji na temat dróg przesyłania poszczególnych pakietów dzieli się routing na statyczny i dynamiczny. W przypadku tego pierwszego wpisy dokonywane są ręcznie przez administratora systemu. To administrator musi znać topologię sieci i na jej podstawie dokonuje wyznaczenia optymalnych tras przesyłania pakietów.
- W przypadku routingu dynamicznego za wymianę informacji na temat topologii sieci i zachodzących zamianach w połączeniu routerów odpowiadają protokoły routingu.

Tablice routingu

- Tablice routingu są tworzone w celu wyboru optymalnej ścieżki przesyłania pakietów.
- W przypadku routingu statycznego wpisów do tych tablic dokonuje administrator.
- W przypadku routngu dynamicznego tworzeniem tablic zajmują się protokoły routingu, na podstawie informacji od innych routerów.
- Wymiana informacji umożliwia protokołom utrzymanie poprawnych tras. Część z protokołów wysyła cyklicznie informacje dotyczące topologii sieci. Powoduje to niepotrzebne obciążanie łączy.
- Lepszym rozwiązaniem wykorzystywanym przez niektóre protokoły dynamicznego routingu jest wysyłanie uaktualnień w momencie, gdy nastąpią zmiany w topologii sieci.
- Innym rozwiązaniem poprawiającym efektywność przesyłania uaktualnień jest przesyłanie tylko tej części tablicy routingu, której dotyczą zmiany.

Tablice routingu - pozycje

- Wśród danych, które mogą występować w tablicach routingu są następujące elementy:
  - typ protokołu - wpis, który z protokołów routingu dostarczył informacji na temat danej trasy odniesienie do punktu docelowego/następnego przeskoku - informacja o tym, gdzie znajduje się punkt docelowy lub jak (przez który router) do niego dotrzeć.
  - metryka routingu - informacja o metryce routingu dla danego protokołu
  - interfejs wyjściowy - interfejs, przez który należy wysłać pakiet, aby trafił do sieci docelowej.

Tablice routingu - przykład

- Na rysunku została pokazana przykładowa tablica routingu uzyskana na stacji roboczej pod kontrolą systemu operacyjnego UNIX, za pomocą polecenia: netstat -4 –r -n.
  - W pierwszej kolumnie pokazane są sieci i hosty docelowe.
  - Kolumna „Gateway” informuje, przez jaką bramę następuje komunikacja do wymienionej w poprzedniej kolumnie lokalizacji.
  - Kolejna kolumna „Flags” podaje następujące informacje:
    - U - trasa działająca (ang. up)
    - G - trasa prowadzi przez bramę
    - H - trasa zdefiniowana do hosta docelowego, a nie do sieci (pierwszy i ostatni wiersz).
    - Ostatnia kolumna informuje o tym, przez który interfejs odbywa się komunikacja.

```
root@webserver:/ # netstat -4 -r -n
Routing tables

Internet:
Destination        Gateway            Flags     Refs      Use  Netif Expire
default            192.168.1.254      UGS          0    12167 epair0
127.0.0.1          link#1             UH           0        0    lo0
192.168.1.0/24     link#2             U            1     2182 epair0
192.168.1.30       link#2             UHS          0        0    lo0
root@webserver:/ #
```

Routing statyczny

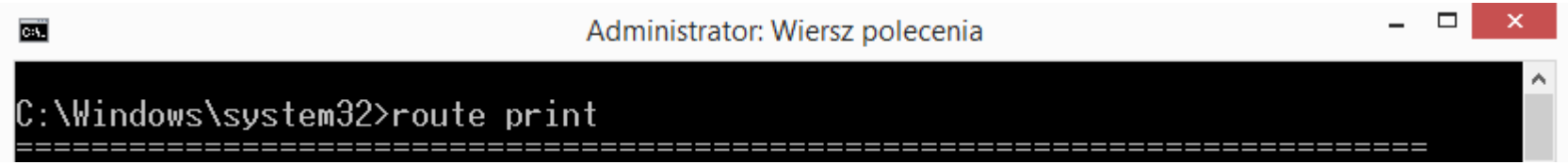
- Określenie routing statyczny odnosi się do przypadku, gdy informacje na temat topologii sieci i tras przesyłania pakietów są wpisane na stałe przez administratora systemu.
- Administrator w oparciu o wiedzę, którą posiada, dokonuje wpisów, które są następnie podstawą do kierowania przez router pakietów. Ten sposób konfiguracji routera sprawdza się w sytuacjach, gdy obsługiwana sieć ma nieskomplikowany schemat połączeń. Ewentualne błędy przy przesyłaniu pakietów są wynikiem błędnych wpisów.
- Administrator ma możliwość zdefiniowania dystansu administracyjnego. Dzięki takiemu dodatkowemu wpisowi można ustawiać ścieżki zapasowe na wypadek uszkodzenia jednej z tras.
- Routing statyczny można mieszać z routingiem dynamicznym wtedy zwykle trasy zdefiniowane statycznie są trasami zapasowymi. W takich przypadkach należy użyć wyższej wartości dystansu administracyjnego dla trasy zdefiniowanej w sposób statyczny niż dla trasy wyznaczonej przez protokół routingu.

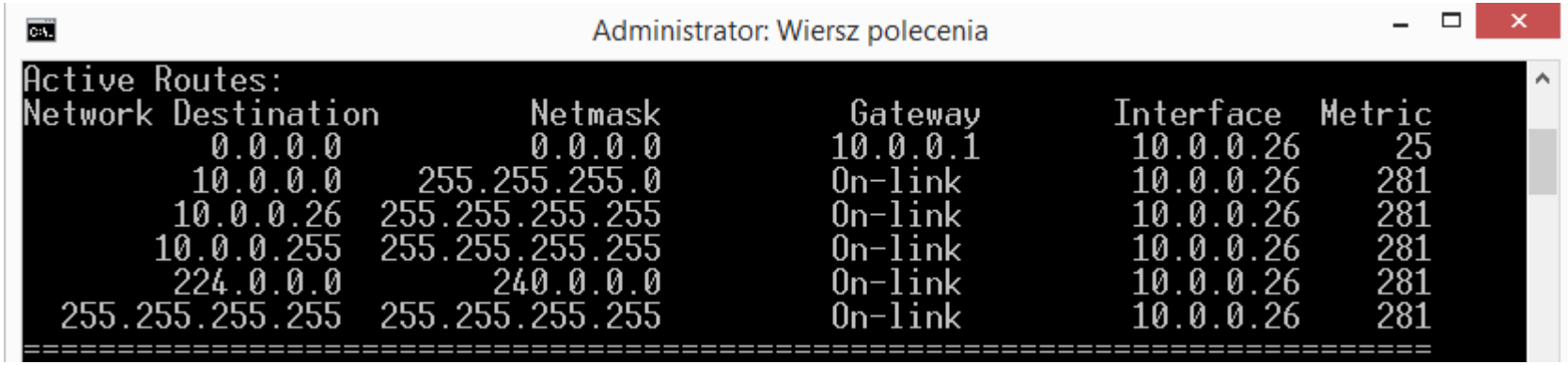
Routing statyczny

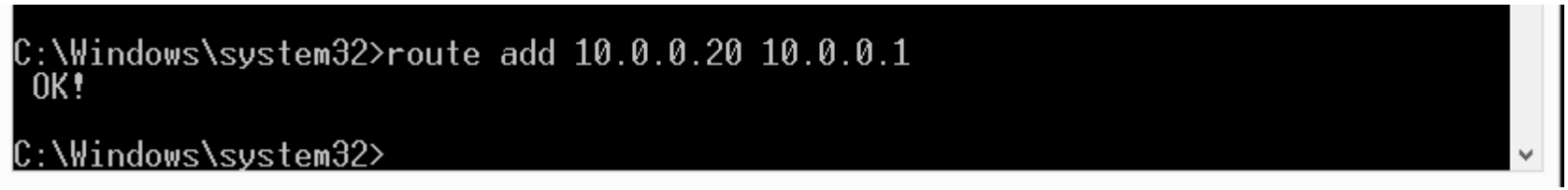
- Zaletą routingu statycznego jest fakt nie obciążania sieci dodatkowymi pakietami z informacjami o topologii (lub jej zmianach), które są przesyłane w przypadku stosowania routingu dynamicznego.
- Wadą takiego rozwiązania jest potrzeba ręcznej ingerencji w przypadku awarii któregoś z łączy pośrednich oraz trudność przy definiowaniu połączeń redundantnych na wypadek awarii.
- Na kolejnym slajdzie zostanie podana składnia polecenia ustawienia routingu statycznego.

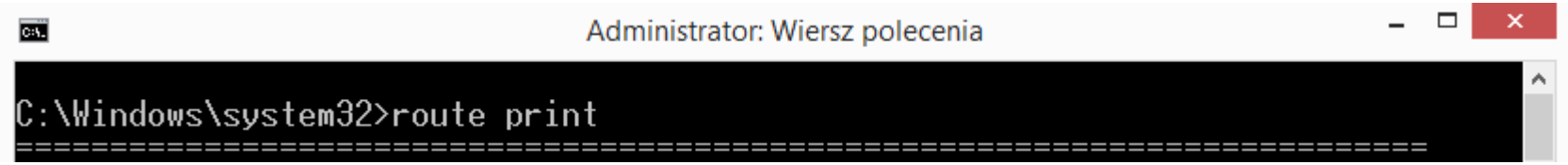
Routing statyczny

Składnia polecenia: route add <cel> <adres hosta>

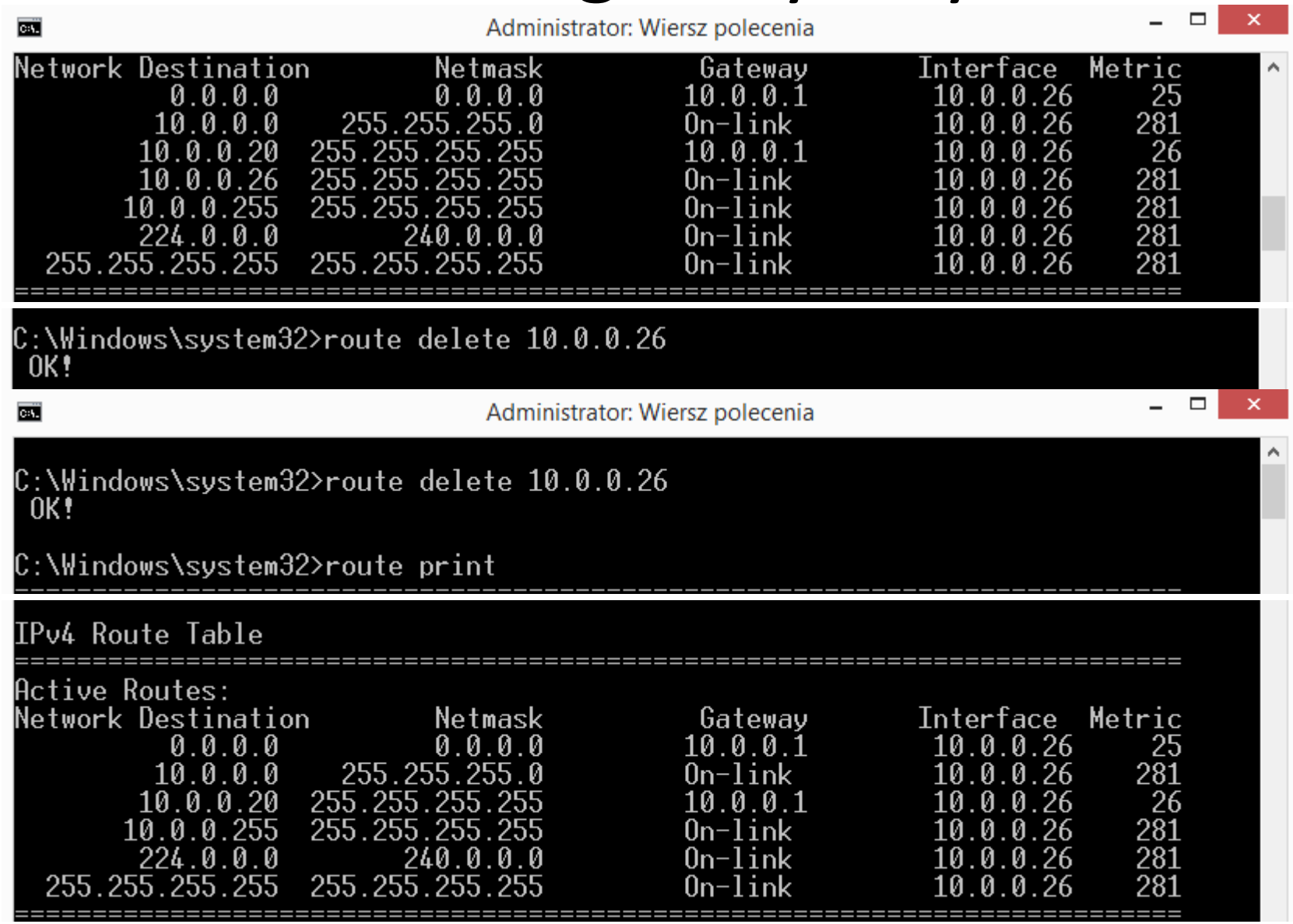








Routing statyczny



Routing – domyślna trasa

- Często zachodzi potrzeba wpisania tzw. tras domyślnych (ang. default route).
- Są to wpisy w tabeli routingu, które umożliwiają określenie ścieżki przesyłania pakietów, dla których nie zadeklarowano lub nie została określona w sposób dynamiczny ścieżka.
- W ten sposób wszystkie te pakiety zostaną automatycznie skierowane do określonego routera. Na kolejnym slajdzie zostanie pokazana przykład deklaracji domyślnej ścieżki.

Routing – domyślna trasa

Domyślna trasa w systemie Windows:

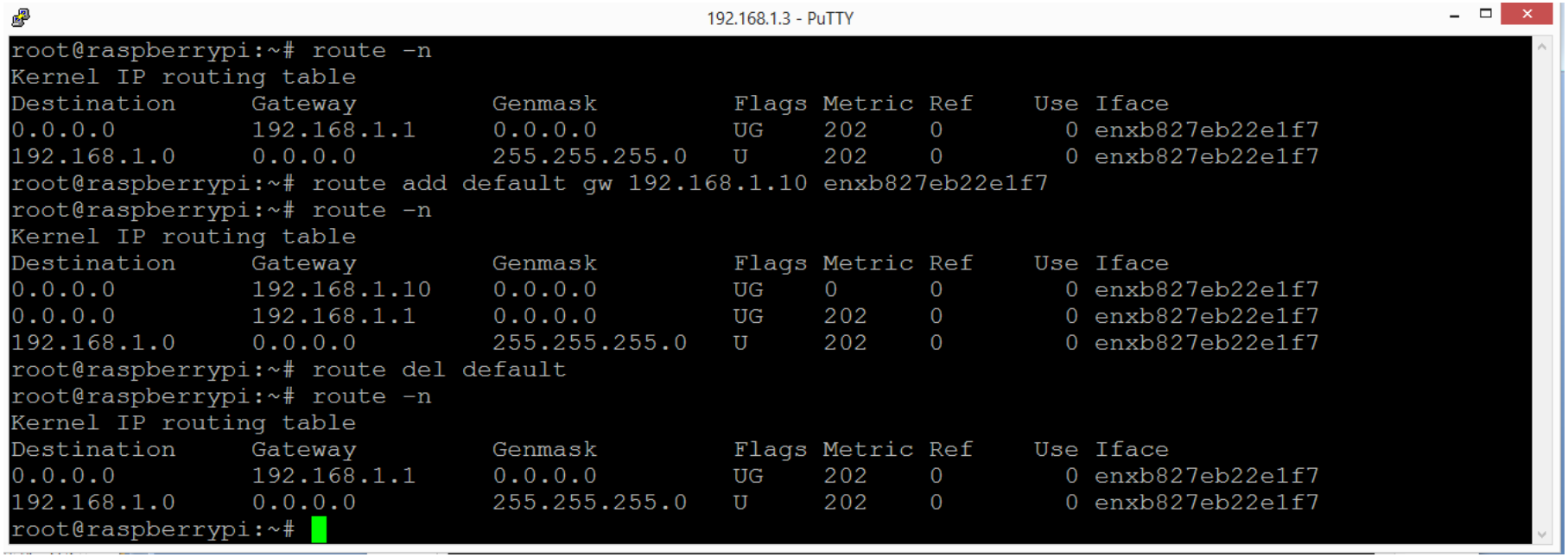
```
C:\Windows\system32>route add 0.0.0.0 mask 0.0.0.0 192.168.1.1 metric 25
 OK!

C:\Windows\system32>_
```

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1        10.0.0.26     25
          0.0.0.0          0.0.0.0      192.168.1.1        10.0.0.26     50
         10.0.0.0    255.255.255.0         On-link        10.0.0.26    281
        10.0.0.20  255.255.255.255         10.0.0.1        10.0.0.26     26
       10.0.0.255  255.255.255.255         On-link        10.0.0.26    281
        224.0.0.0        240.0.0.0         On-link        10.0.0.26    281
  255.255.255.255  255.255.255.255         On-link        10.0.0.26    281
===========================================================================
```

Routing – domyślna trasa

Domyślna trasa w systemie Linux:



Routing dynamiczny – rodzaje

- Podział ze względu na sposób wyznaczania trasy wynika z odmiennego podejścia do tworzenia informacji na temat routingu.
- W przypadku protokołów wektora odległości (ang. distance vector) wyznaczenie trasy routingu oparte jest o znalezienie kierunku, w którym należy przesłać pakiety oraz określeniu odległości (ilości skoków - routerów) do sieci przeznaczenia pakietów.
- Taki sposób podejścia skutkuje tym, że każdy router widzi sieć przez pryzmat routerów sąsiednich.

Routing dynamiczny – rodzaje

- Protokoły tego typu są dosyć proste algorytmicznie i nie wymagają dużych nakładów obliczeniowych. Niestety ze względu na stosowaną metrykę (liczbę skoków) protokoły te wyznaczają najkrótszą trasę, która nie zawsze musi być najszybsza.
- W protokołach, które analizują stan łącza tworzona jest jednolita mapa topologii całej sieci.
- Do tworzenia topologii sieci używany jest m.in. algorytm Dijkstry. Algorytmy protokołów stan-łącze lepiej wyznaczają optymalną trasę przesyłania pakietów niż protokołu wektora odległości.

Routing dynamiczny – wybrane protokoły

- Przykładami używanych protokołów routingu są:
  - RIP (ang. Routing Information Protocol) w wersji 1 i 2.
  - OSPF (ang. Open Shortest Path First)
  - BGP (ang. Border Gateway Protoco)
  - IGRP (ang. Interior Gateway Routing Protocol)
  - EIGRP (ang. Enhanced IGRP)
- Pierwsze trzy protokoły są zdefiniowane jako otwarte standardy. Dwa ostatnie z wymienionych są protokołami zaproponowanymi przez firmę Cisco.

Routing dynamiczny – wymagania

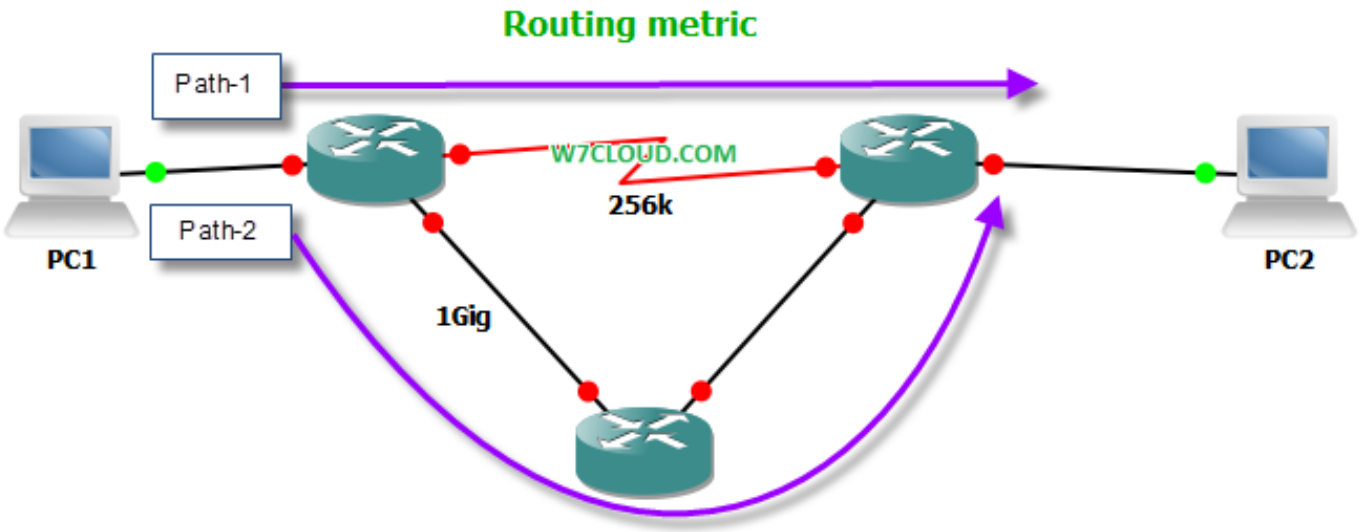
- Protokoły routingu były oraz są projektowane z myślą o zapewnieniu skutecznego i szybkiego rouingu.
- Istnieją pewne ogólne cechy, które (część lub wszystkie) każdy z zaimplementowanych protokołów powinien spełniać:
  - Optymalizacja - pod tym wymaganiem kryje się zdolność algorytmu do wyboru ścieżek o najlepszych metrykach.
  - Odporność na błędy i stabilność - zdolność protokołu do radzenia sobie w przypadku nieprzewidzianych awarii.
  - Szybka zbieżność - w przypadku zmiany dostępnych tras następuje przesyłanie informacji na temat zmian do wszystkich routerów, które obsługują routing dynamiczny. Szybka zbieżność gwarantuje, że po zmianie topologii połączeń informacja na temat zmian zostanie możliwie szybko rozpropagowana wśród pozostałych routerów.

Routing dynamiczny – wymagania

- Elastyczność - cecha, która pozwala na zastosowanie w sieci urządzeń o różnych parametrach. Dotyczy ona również zmiennych warunków pracy w sieci, np. zmiana szerokości pasma, zmiany opóźnień występujących w sieci.
- Prostota i niski narzut - protokół routingu jest implementowany jako program komputerowy na poszczególnych routerach. Proste algorytmy routingu, które nie wymagają dużych narzutów obliczeniowych w niewielkim stopniu obciążają zasoby sprzętowe urządzenia. Ma to szczególnie istotne znaczenie przy dużych tablicach routingu i rozbudowaniu sieci komputerowych.

Routing - metryki

- Zadaniem protokołu routingu jest wybór optymalnej trasy dla przesyłanych pakietów. Pakiety mogą być wysłane krótszą trasą (przez mniejszą liczbę routerów) lub też trasą dłuższą. Optymalność obu tych tras może być wyznaczana na podstawie kilku cech, tak jak na poniższym rysunku.



Routing – przykłady metryk

- Do porównania kilku różnych alternatywnych tras przesyłania pakietów potrzebna jest jakaś miara.
- Podobnie jak w przypadku porównywania cech różnych obiektów, dystansu pomiędzy miastami, podobieństwa obiektów, itd. w przypadku określania optymalności danej trasy należy posłużyć się jakimiś wartościami poprzez zdefiniowanie metryki routingu.
- Różne protokoły routingu mogą wykorzystywać odrębne wartości. W skład wartości, które mogą być wykorzystywane przy definiowaniu metryki mogą wchodzić następujące parametry:
  - szerokość pasma - zwykle im szybsze łącze, tym bardziej preferowane, np. łącze 1Gb/s będzie bardziej preferowane niż łącze modemowe o prędkości 56kb/s
  - Opóźnienie - jest czasem potrzebnym do przesłanie pakietów w pojedynczym łączu danych. Im czas opóźnienia mniejszy tym lepsze własności łącza

Routing – przykłady metryk

- Obciążenie - intensywność wykorzystanie danego łącza przez innych użytkowników. Im mniejsza tym więcej zasobów może być przeznaczone na przesyłane dane.
- Niezawodność - liczba awarii w danym łączu. Im mniejsza tym łącze bardziej niezawodne.
- Liczba przeskoków [ang. hoop count] - określa liczbę pośrednich routerów przez, które będzie przesyłany pakiet. W niektórych protokołach, np. w RIP, jest to jedyna miara. Im mniejsza liczba przeskoków (pośrednich routerów), przez które musi być przesłany pakiet do miejsca przeznaczenia, tym lepiej.
- Impulsy zegarowe - czas opóźnienia łącza jest liczony impulsami zegara komputera IBM PC (ok. 1/18 s)
- Koszt - wartość oszacowania opłat przypadających na koszt przesłania danych przez łącze.

- Wymienione cechy są użyteczne przy definiowaniu metryki routingu jednak w praktyce stosowane protokoły wykorzystują tylko wybrane z nich. Warto zauważyć, że wymienione parametry w sposób naturalny opisują właściwości sieci komputerowych.

RIP v1

- Protokół RIPv1 został zaprojektowany jako protokół typu IGP (Interior Gateway Protocol) wykorzystywany w ramach jednego systemu autonomicznego (AS).
- Standard ten został opisany w dokumencie RFC 1058.
- Protokół ten bada wektor odległości (ang. distance vector) i został zaprojektowany z myślą o małych sieciach o nieskomplikowanej topologii.
- Protokół obsługuje tylko adresację z podziałem na klasy, stąd nie nadaje się do obsługi sieci z zastosowaną adresacją VLSM.
- Protokół ten wysyła aktualizację w formie rozgłaszania na adres broadcastowy 255.255.255.255.
- Aktualizacja tras wysyłana jest co 30 s.
- Metryka stosowana w tym protokole to liczba przeskoków. Maksymalna liczba przeskoków w danej trasie to 15. Zatem jeśli licznik przeskoków osiągnie wartość 16 to dany adres docelowy zaznaczany jest jako nieosiągalny.
- Protokół ten umożliwia zrównoważenie obciążenia na maksymalnie 6 ścieżkach, przy czym muszą mieć one równe koszty przesyłania.

RIP v1 – format pakietu

- Informacje przenoszone przez ten protokół wysyłane są na adres rozgłoszeniowy.
- Sam pakiet zawiera następujące pola:
  - command - (1B) pole określające funkcje pakietu.

    Pole to może zawierać następujące wartości:
    - request (1) - żądanie przesłania tablicy routingu
    - response (2) - odpowiedź na żądanie
    - traceon (3) - pakiety z taką wartością pola powinny być ignorowane
    - traceoff (4) - pakiety z taką wartością pola powinny być ignorowane
    - reserverd (5) - pakiety z taką wartością pola powinny być ignorowane - pole zarezerwowane dla SUN Microsystems.
  - version - (1B) pole numeru wersji protokołu RIP
  - AFI (ang. Address Family Identyfier) (2B) - określa, który protokół jest routowany. Dla protokołu IP wartość tego pola wynosi 2.
  - IP address - (4B) Adres sieci
  - must be zero – (2B lub 4B) pole wypełnione zerami.
  - metric (4B) - metryka

RIP v1 – format pakietu

Command (1)	**Version (1)**	**Must be zero (2)**
Address family identifier (2)		Must be zero (2)
IP Address (4)		
Must be zero (4)		
Must be zero (4)		
Metric (4)		

RIP v1 vs RIP v2

- Format RIPv2 został opracowany na początku lat 90-tych XX w jako modyfikacja szeroko stosowanego protokołu RIPv1.
- Wersja 1 protokołu posiadała kilka wad, które ograniczały jego zastosowanie. Poprawiona wersja protokołu usuwa te ograniczenia.
- Specyfikacja protokołu w wersji 2 została podana w dokumencie RFC 1723.
- Protokół ten korzysta z tego samego algorytmu wyznaczania tras co jego poprzednik. Z tego względu nie nadaje się on do bardziej skomplikowanych topologii sieciowych.
- Cechami charakteryzującymi ten protokół są:
  - Wysyłanie razem z informacją o trasie również maski podsieci - możliwe jest dzięki temu stosowanie metody VLSM.
  - Wprowadza uwierzytelnienie - możliwe jest przesyłanie informacji uwierzytelniających zarówno tekstem jawnym jak i szyfrowanych.
  - Umieszcza adres IP routera następnego przeskoku w wysyłanych przez siebie aktualizacjach tras - dzięki temu inne routery, wiedzą przez który router prowadzi lepsza trasa.
  - Korzysta ze znaczników tras zewnętrznych - przenosi informacje uzyskane przy pomocy innych protokołów do sieci wewnętrznej, zaznaczając jednocześnie, że jest to informacja ze źródła zewnętrzenego
  - Wysyła aktualizacje tras na adres multicastowy - korzysta z rozsyłania grupowego na adres z klasy D o numerze IP 224.0.0.9

RIP v2 vs RIP v1

- Jedną z dosyć istotnych niedogodności wersji 1 protokołu był brak możliwości obsługi sieci z adresacją bezklasową. W obliczu wyczerpujących się adresów IPv4 jest to dosyć duże ograniczenie. Stąd poprawienie tej niedoskonałości było istotne.
- Wysyłanie informacji o masce podsieci umożliwia zastosowanie techniki VLSM. Dzięki temu wysyłana informacja o trasie jest pełna.
- W odróżnieniu od wersji 1 RIP w wersji 2 możliwe jest stosowanie uwierzytelniania przy przesyłaniu informacji o topologii sieci. Podnosi to znacznie bezpieczeństwo.
- Kolejną zmianą poprawiającą efektywność przesyłania uaktualnień jest wysyłanie ich na adres rozsyłania grupowego: 224.0.0.9. Dzięki temu tylko routery, do których jest adresowane uaktualnienie muszą przetworzyć pakiet.
- W wersji 1 RIP informacje o routingu były rozsyłane na adres rozgłoszeniowy (255.255.255.255) w związku z tym wszystkie maszyny musiały przetworzyć otrzymane pakiety. To w znacznym stopniu obciążało routery i całą sieć.

RIP v2 – format pakietu

- W wersji protokołu RIPv2 poszczególne pola mają następujące znaczenie:
  - command - (1B) pole komendy
  - version - (1B) wersja protokołu RIP
  - AFI (ang. address family identyfier) - (2B) pole identyfikujące jaki protokół będzie przesyłany. W przypadku IP wpisana jest tam wartość 2. Gdy pole ma ustawioną wartość 0xFFFF, to pakiet niesie informację o autoryzacji.
  - route tag (2B) - określa czy trasa jest wysłana z lokalnego routera obsługującego protokół RIP (trasa wewnętrzna) czy też innego routera obsługującego inne protokoły (trasa zewnętrzna).
  - IP address - (4B) jeśli w polu AFI jest wartość 2, to pole to przechowuje adres IP
  - subnet mask - (4B) maska podsieci
  - next hop - (4B) adres następnego routera na trasie (następnego skoku)
  - metric - (4B) metryka

RIP v2 – format pakietu

Command (1)	**Version (1)**	**Must be zero (2)**
Address family identifier (2)		Routing tab (2)
IP Address (4)		
Subnet mask (4)		
Next hop (4)		
Metric (4)		

RIP v2 – format pakietu z autoryzacją

- Jedną z cech odróżniających wersję 2 od wersji 1 protokołu RIP jest możliwość autoryzacji, która została wprowadzona do wersji 2.
- Uzyskuje się ją dzięki zapisaniu w polu AFI wartości 0xFFFF. Wtedy oktety 7 i 8 pakietu zawierają informację na temat typu autentykacji.
- Zaś w dwubajtowym polu authentication może być zawarte hasło pisane jawnym tekstem (nie zalecane). Dlatego zaleca się stosowanie szyfrowania metodą Message-Digest 5 (MD5). Jeśli na routerach zostanie aktywowana funkcja autoryzacji w protokole RIPv2, to pakiety nie zawierające nagłówka autoryzacyjnego będą odrzucane przez routery .

RIP v2 – format pakietu z autoryzacją

Command (1)	**Version (1)**	**Must be zero (2)**
0xFFFF (2)		Authentication type (2)
Authentication (16)		

Routing – sposoby unikania zapętleń

- W przypadku występowania alternatywnych tras może dojść do zapętlenia tras routingu objawiającego się nieprzesyłaniem pakietów.
- Aby zapobiec temu negatywnemu zjawisku stosuje się różne metody niwelujące takie zdarzenia.
- Problem ten dotyczy szczególnie protokołu RIP.
- Jedną z nich jest metoda podzielonego horyzontu (ang. split horizon). Metoda ta nie pozwala routerowi, który wysłał informację o danej sieci na przyjmowanie informacji o tej sieci od innych routerów.
- Inną metodą eliminującą zapętlenia jest blokowanie (zatruwanie) trasy (ang. route poisoning). Router, który wykrył, że sieć do niego przylegająca jest niedostępna zapisuje trasę w swojej tablicy routingu jako niedostępną (metryka = 16) i wysyła uaktualnienia do sąsiednich routerów. Blokuje („zatruwa”) w ten sposób trasę do tej sieci dla innych routerów.

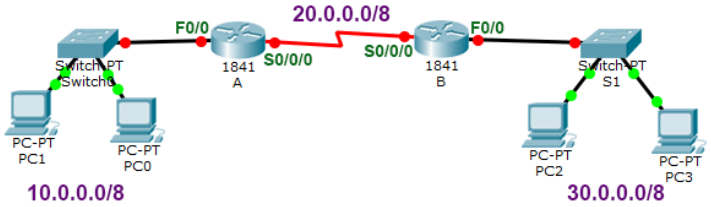
Routing – sposoby unikania zapętleń

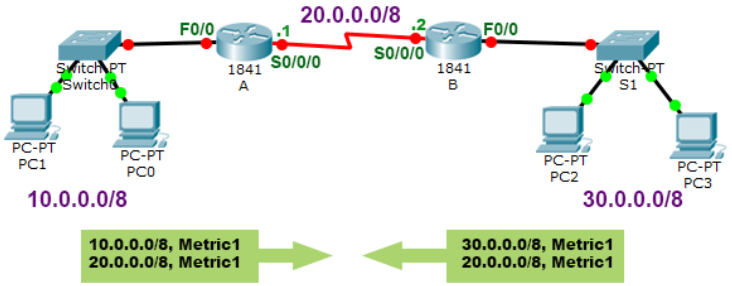
Routing table of router A

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	10.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0

Routing table of router B

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	30.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0



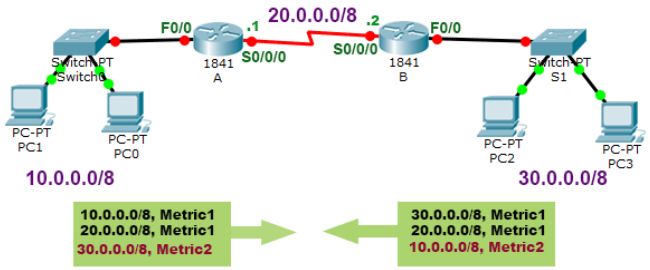


Routing table of router A

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	10.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0
RIP	30.0.0.0/8	20.0.0.2	S0/0/0	1

Routing table of router B

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	30.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0
RIP	10.0.0.0/8	20.0.0.1	S0/0/0	1



Split Horizontal

Routing table of router A

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	10.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0
RIP	30.0.0.0/8	20.0.0.2	S0/0/0	1

Routing table of router B

Source	Network	Next-Hop-IP	Out Int.	Metric
Conn.	30.0.0.0/8	N/a	F0/0	0
Conn.	20.0.0.0/8	N/a	S0/0/0	0
RIP	10.0.0.0/8	20.0.0.1	S0/0/0	1

Protokół OSPF

- Protokół OSPF (ang. Open Shortest Path First) jest protokołem typu stanu łącza (link-state). Został on zaprojektowany przez Internet Engineering Task Force w 1988 roku.
- Protokół ten został opracowany na przełomie lat 80-tych i 90-tych XX w. jako protokół otwarty niezależny od producenta.
- Jednak najszerzej stosowana specyfikacja tego protokołu została zdefiniowana w dokumencie RFC 2178 dopiero pod koniec lat 90-tych XX w.
- Specyfikacja ta pozwoliła na szerokie wykorzystanie tego protokołu.
- Protokół ten posiada wiele cech, które wyróżniają go w stosunku do wcześniej opisywanego protokołu RIPv1 jak również kilka ulepszeń w stosunku do wersji 2 RIP
- Nie ma ograniczeń dotyczących liczby przeskoków, obsługuje VLSM, wykorzystuje adres rozsyłania grupowego, szybsza zbieżność, bardziej skuteczna metryka, możliwość równoważenia obciążenia, możliwość uwierzytelnienia, podział sieci na obszary.

OSPF – format nagłówka

- W związku z tym, że protokół OSPF pozwala na podzielenie obsługiwanej domeny na obszary, w polu nagłówka pojawia się informacja o identyfikatorze obszaru do jakiego został przypisany router.
- Nagłówek pakietu zawiera również wpisy dotyczące uwierzytelnienia (typ uwierzytelnienia) oraz same dane uwierzytelniające.
- W momencie uruchomienia protokołu na routerze zaczyna on wymieniać dane na temat tablic routingu z sąsiednimi routerami.
- Każdy router posiada takie samo odzwierciedlenie topologii sieci, dzięki temu trasy, które są wyliczane przez poszczególne routery są zgodne.
- Komunikacja pomiędzy routerami odbywa się poprzez przesłanie pakietu hello. Pakiet taki jest wyróżniany poprzez wpis o wartości 1 w polu „Typ”. Pakiet taki jest wysyłany na adres rozsyłania grupowego 224.0.0.5, który jest dedykowany dla wszystkich routerów OSPF. Po rozesłaniu informacji inicjujących, pakiety „Hello” są przesyłane co 10s lub 30 s w celu potwierdzania właściwej pracy urządzeń.

OSPF – format nagłówka

- Po nawiązaniu komunikacji routery wymieniają się informacjami na temat topologii za pomocą komunikatów LSA (ang. Link State Advertisement).
- Przy dużej liczbie routerów w danym segmencie przesłanie informacji LSA wymagałoby przesłania NxN komunikatów. Stąd w celu zmniejszenia liczby wysyłanych pakietów wybiera się dwa routery:
  - router desygnowany DR (ang. Designated Router) oraz,
  - router zapasowy desygnowany BDR (ang. Back-up Designated Router).
- Wszystkie routery w danym segmencie wysyłają informacje o stanie łącz do routera DR (lub w momencie uszkodzenia DR do BDR). Router desygnowany rozsyła potem te komunikaty do wszystkich routerów w segmencie. Dzięki temu ilość wysyłanych komunikatów wynosi 2xN.

OSPF – struktura nagłówka

Wersja	**Typ**	**Długość pakietu**
Identyfikator routera		
Identyfikator obszaru		
Suma kontrolna		Typ uwierzytelniania
Dane uwierzytelniające		

OSPF – pakiet hello

- Gdy w polu „Typ” nagłówka pakietu OSPF wpisana jest wartość 1, to jest to informacja, że będzie przesyłany pakiet „Hello”.
- Pakiet ten zawiera wszelkie informacje niezbędne do przeprowadzenia procesu uzgadniania pomiędzy routerami.

OSPF – struktura pakietu hello

Maska sieci		
Czas pomiędzy pakietami Hello	Opcje	Priorytet routera
Interwał czasu nieaktywności		
Router desygnowany		
Zapasowy router desygnowany		
Identyfikator routera sąsiedniego		
Identyfikator routera sąsiedniego		
Dodatkowe pola identyfikatorów routerów sąsiednich mogą być – w razie potrzeby – dane na końcu nagłówka		

EIGRP

- Innym przykładem protokołu routingu jest EIGRP (ang. Enhanced Interior Gateway Routing Protocol).
- Protokół ten został wprowadzony w 1994 r przez firmę Cisco.
- Jest on następcą protokołu IGRP, który działał w oparciu o wektor odległości.
- Ze względu na fakt, że protokół EIGRP ustanawia relacje z sąsiednimi urządzeniami budując w ten sposób spójną topologię sieci protokół ten posiada również cechy typowe dla protokołów typu stan łącza.

EIGRP

- Wykrywanie sąsiednich urządzeń i usuwanie skutków awarii związanych z tymi urządzeniami.
- Używa protokołu transportu gwarantowanego RTP (ang. Reliable Transport Protocol).
- Korzysta z algorytmu automatu skończonego DUAL

BGP

- Protokół BGP (ang. Border Gateway Protocol) jest protokołem wykorzystywanym do wymiany informacji pomiędzy różnymi systemami autonomicznymi (AS).
- Jego specyfikacje znajdują się dokumentach RFC:
  - RFC 1771 - opis protokołu BGP4
  - RFC 1772 - informacje nt. BGP Application
  - RFC 1773 - Informacje nt. BGP Experience
  - RFC 1774 - Informacje nt. BGP Protocol Analysis
  - RFC 1655 - Informacje nt. BGP MIB
- Protokół ten jest obecnie najczęściej wykorzystywanym protokołem do wymiany tablic routingu pomiędzy różnymi systemami autonomicznymi.

BGP – zasada działania

- Protokół BGP uruchomiony na routerach nawiązuje połączenie pomiędzy sąsiednimi urządzeniami. W zależności od przypisania poszczególnych maszyn do określonych systemów autonomicznych może to być:
  - relacja wewnętrzna (Internal BGP) - gdy routery należą do tego samego systemu autonomicznego
  - relacja zewnętrzna (External BGP), gdy routery należą do różnych systemów autonomicznych
- Wymiana komunikatów pomiędzy routerami odbywa się na porcie 179 protokołu TCP.
- W celu otwarcia sesji routery wysyłają komunikat OPEN, w którym określają parametry sesji.
- Komunikat UPDATE umożliwia wymianę informacji na temat tablic routingu.
- Przy pierwszym połączeniu wysyłane są pełne tablice routingu, przy kolejnych tylko te które uległy zmianom.
- Gdy nie ma zmian, to wysyłany jest komunikat KEEPALIVE sygnalizujący poprawne działanie obu routerów i łącza.

Dziękuję za uwagę