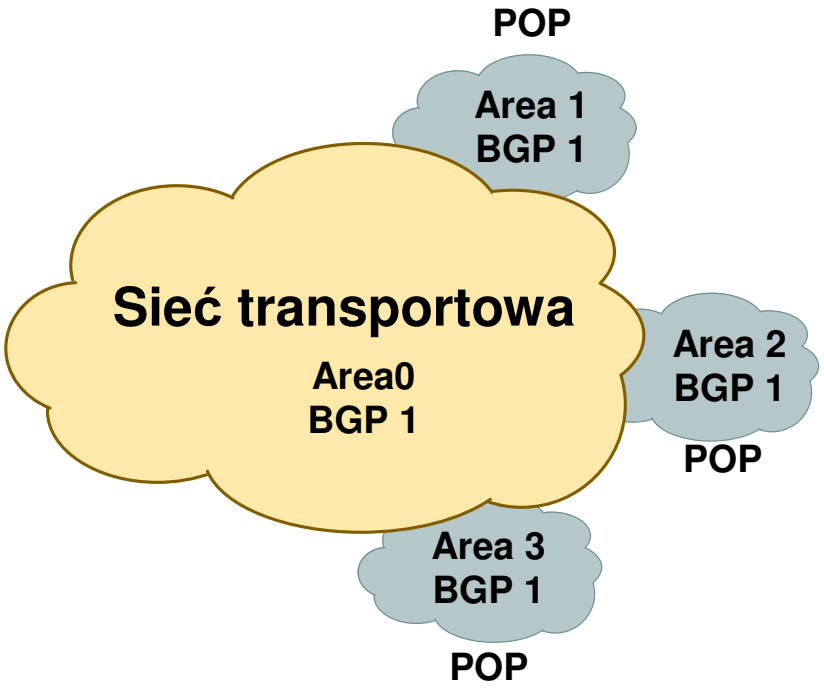
Praktyczne aspekty implementacji IGP

Piotr Jabłoński
pijablon@cisco.com

Ogólne rekomendacje

- Jeden proces IGP w całej sieci.
- Idealnie jeden obszar.
- Wiele obszarów w całej sieci w zależności od ilości oraz rodzaju użytego sprzętu oraz od możliwości innych protokołów.
- BGP przenosi prefiksy zewnętrzne, IGP wskazuje next-hop do tych tras.



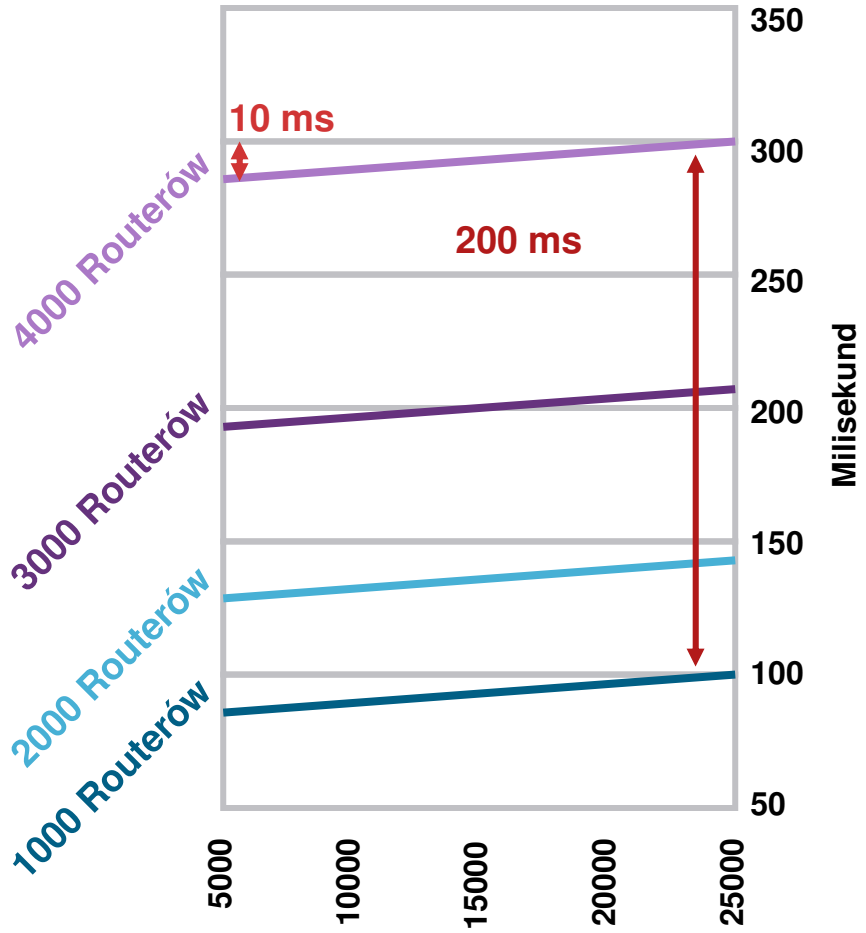
Wybór protokołu IGP

- Najważniejsze czynniki: koszty migracji, architektura sieci, znajomość protokołu.
- ISIS jest mniej podatny na ataki z zewnątrz np. DoS.
- ISIS jest prostszym protokołem w budowie, niż OSPF. Wszystkie LSP korzystają z TLV. Szybciej pojawiają się rozszerzenia wspomagające nowe funkcjonalności.
- ISIS wyróżnia się priorytetyzacją instalacji prefiksów w tablicy RIB oraz szerszymi możliwościami znakowania prefiksów.
- Niewielkie różnice w przeliczeniu SPF na korzyść ISIS.
- Więcej urządzeń wspiera OSPF.

Przeliczenie SPF

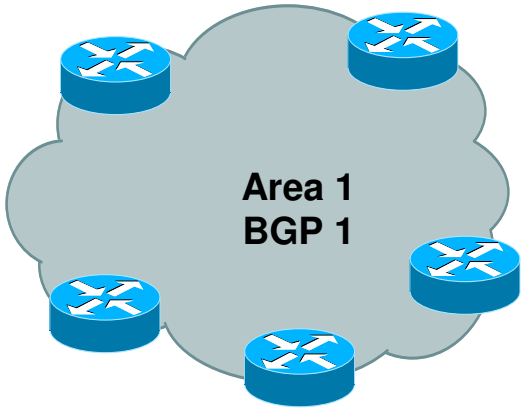
Co ma większy wpływ?
Ilość routerów, czy ilość prefiksów?

- Zmiana liczby prefiksów o 20 tys. spowodowała wzrost czasu przeliczenia SPF o 10 ms.
- Zmiana liczby routerów o 3000 spowodowała wzrost czasu przeliczenia SPF o 200 ms.
- Liczba routerów w sieci IPv4/IPv6 jest głównym czynnikiem wpływającym na konwergencję.

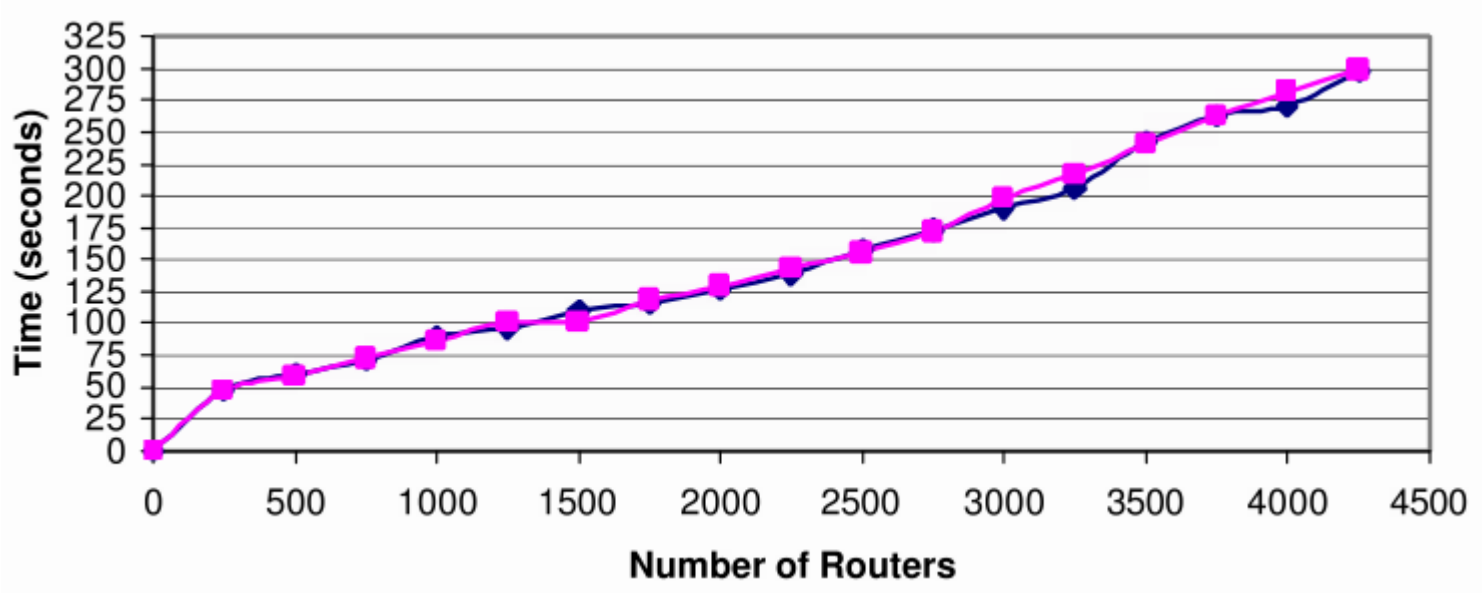


Ilość routerów w obszarze

- Obszar Area 0, Level-2 nie musi pokrywać się z faktyczną topologią routerów P.
- Limit ilości routerów zależny od akceptowalnej konwergencji.

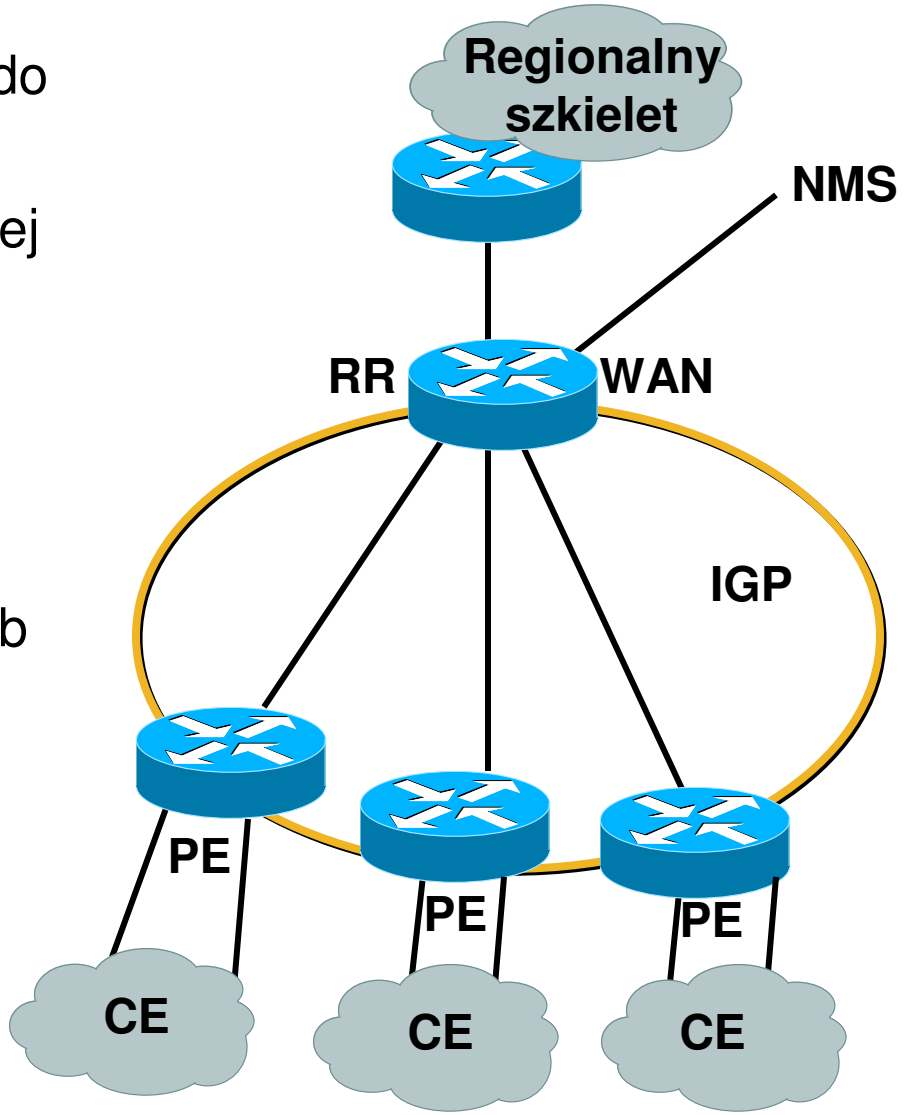


Test konwergencji dla ISIS:



Ilość tras w IGP

- Redukcja rozmiar tablicy IGP do ilości Loopbacków.
- Większe bezpieczeństwo, mniej rozgłoszeń.
- Dodatkowy zysk do konwergencji.
- Ostrożnie z agregacją tras.
- Prefix-suppression w OSPF lub advertise passive-only w ISIS



Limity skalowalności

- Nieaktualne ograniczenia

  OSPF: Odświeżenie bazy z LSA maksymalnie co 60 minut.
  Rozwiązanie: DoNotAge bit - ip ospf flood-reduction

  ISIS: Maks. ilość fragmentów LSP = 255, ok. 30tys. Prefiksów
  Rozwiązanie: IS Alias ID TLV, uruchomione domyślnie

- Aktualne ograniczenia

  Wymagany czas konwergencji, ilość sąsiadów w obszarze.

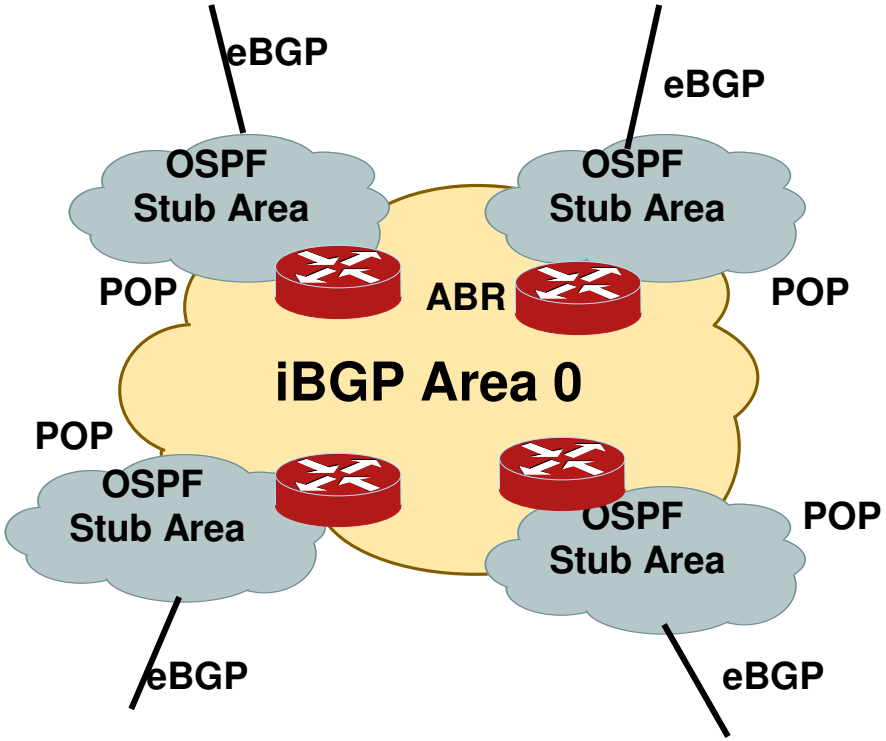
  OSPF: jedno LSA typu 3, 4, 5, 7 może zawierać informację tylko o jednym prefiksie. ISIS nie ma takich obostrzeń.

Redystrybucja

- Nie wykonuj redystrybucji między IGP, a BGP.
- IGP nie powinno przenosić zewnętrznych informacji.
- BGP ma zapewnić widoczność do zewnętrznych tras.
- IGP rozgłasza adresy next-hop dla BGP, czyli np. adresy Loopback.

Ochrona przed redystrybucja (OSPF)

- Zdefiniowanie obszarów jako stub.
- Filtrowanie LSA Type 3 na routerach ABR. Leaking adresów Loopback do sieci szkieletowej.
- Adresy Loopback z osobnej, łatwo agregowalnej puli adresów.
- Domyślnie trasy iBGP nie sa redystrybuowane do IGP.
- NMS znajduje się w Area0.



Konwergencja sieci

Mechanizmy przyspieszające konwergencję

- Carrier Delay
- Event Dampening na interfejsie
- Liczniki Hello/dead
- Bi-Directional Forwarding Detection—(BFD)
- Liczniki czasu generowania LSA oraz przeliczenia SPF
- Incremental SPF
- Przeliczenie części tras (Partial SPF)
- LSA packet pacing
- Licznik MinLSArrival

Mechanizmy zwiększające niezawodność

- Stub router
- Graceful Restart/NSF
- NSR

Przeliczenie SPF

Przykład dla OSPF

- Konfiguracja Cisco:

```
spf-interval <spf-max> <spf-start> <spf-hold>
```

<spf-max> Maksymalny czas między kalkulacjami SPF (sek)

<spf-start> Czas do pierwszego przeliczenia (msek)

<spf-hold> Czas między pierwszym i drugim SPF (msek)

- Konfiguracja Juniper:

```
set spf-options delay <> holddown <> rapid-runs <>
```

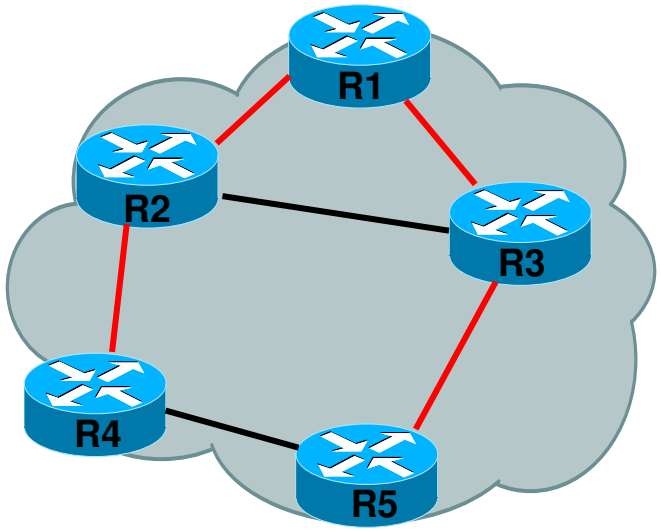
<delay> Czas odliczany w ‘fast mode’ (msek)

<holddown> Czas odliczany w ‘slow mode’ (msek)

<rapid-runs> Ilość szybkich update’ów, po których nastąpi przełączenie w ‘slow mode’ (numer)

Przeliczenie inkrementalne SPF

- Incremental SPF
  - Zmodyfikowany algorytm Dijkstry
  - Utrzymuje niezmienioną część drzewa
  - Przbudowuje zmienioną część drzewa SPF
  - Dołącza ponownie usunięte segmenty do niezmienionej reszty drzewa



Wpływ Inkrementalnego SPF

- Zawsze są węzły, które są bliżej zmian w topologii oraz węzły, które są dalej.
- Rozgłoszenie informacji o zmianie zabiera czas proporcjonalnie do odległośc – najdalsze węzły są informowane najpóźniej.
- Jeżeli pełny SPF jest uruchamiany na wszystkich węzłach, wówczas najdalsze routery zbiegną się najpóźniej.
- Wraz z iSPF dalsze węzły przetwarzają coraz mniej, w krótszym czasie. Rezultatem jest szybsza konwergencja całej sieci.

Przeliczenie części tras

Partial SPF

- Pełny SPF

  Wywoływany przez zmianę dotyczącą węzła lub prefiksów.

  Całe drzewo SPT jest przeliczane.

  Wszystkie typy LSA (Type-1/2/3/4/5/7) są brane pod uwagę.

- Częściowy SPF

  Wywoływany przez zmianę pochodzącą od LSA Type-3/4/5/7.

  Jeżeli jest to Type-3, wszystkie LSA Type-3 do prefiksu są przeliczane.

  Jeżeli jest to Type-5/7, wszystkie LSA Type-5/7 LSA do prefiksu są przeliczane.

  Jeżeli jest to Type-4, wszystkie LSA Type-4 LSA do określonego ASBR oraz wszystkie LSA Type-5/7 LSA są przeliczane.

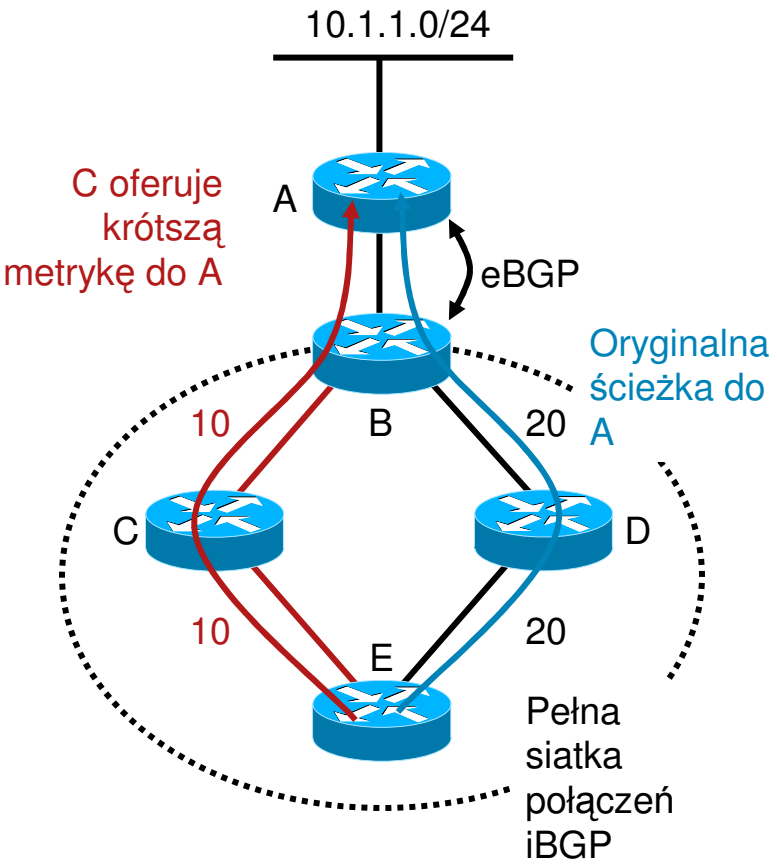
Przeliczenie części tras

Partial SPF

- Czas przeliczenia SPF
  - Pełny SPF:
    - Zależy od:
      - Ilości węzłów/linków w obszarze
      - Ilości LSA Type-3/4/5/7
    - Przykład przeliczenia SPF (12k)
      - 50 węzłów ~ 10ms
      - 100 węzłów ~ 25ms
      - 500 węzłów ~ 50 ms
      - 1000 węzłów ~ 100 ms
  - Częściowy SPF:
    - Szybkie przeliczenie – od 0,5 do 10 ms.

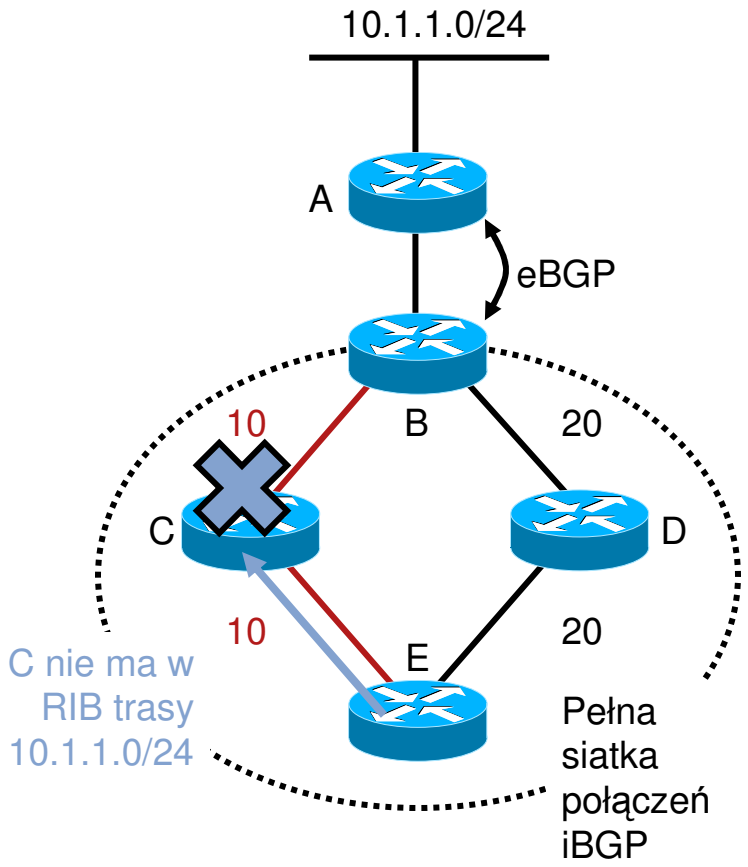
Interakcja BGP z IGP

- E uczy się trasy 10.1.1.0/24 poprzez iBGP od węzła D z next-hop = A
- E sprawdza ścieżkę do A i znajduje ją w IGP poprzez router D. E instaluje trasę BGP w RIB.
- Wraz z uruchomieniem C pojawia się nowa ścieżka. E zmienia ścieżkę do A wybierając C, jako najlepszą ścieżkę.



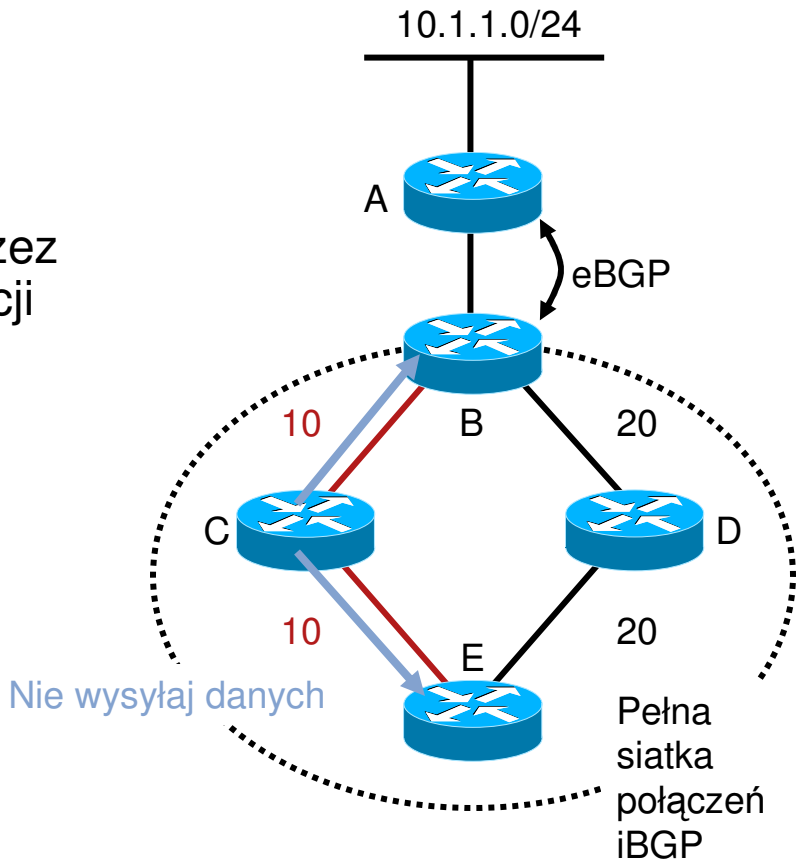
Interakcja BGP z IGP

- Jednak BGP na C jest jeszcze nie gotowe. Konwergencja 340 tys. prefiksów zabiera więcej czasu.
- Jeżeli E wysyła pakiety pod 10.1.1.1 węzeł C nie wie, gdzie je wysłać dalej w sieci.
- C odrzuca pakiety.



Odczekanie na BGP

- Rozwiązaniem jest, by C zasygnalizował sąsiadom, że nie powinni korzystać z niego, jako tranzytu.
- Router E będzie przesyłał ruch poprzez D do czasu zakończenia konwergencji na C.
- W OSPF czekanie na BGP sygnalizowane jest za pomocą maksymalnej metryki.
- W ISIS jest opcja ustawienia bitu overload (Cisco) lub maksymalnej metryki (Juniper).



Bezpieczeństwo

- Włączenie uwierzytelniania w IGP.
- TTL-security w OSPF.
- Ochrona przed przepełnieniem bazy LSA.
- Nie rozgłaszanie adresów połączeniowych. Loopbacki urządzeń osiągalne poprzez serwer pośredni.
- ISIS działa bezpośrednio w warstwie 2. Nie można zaatakować za pomocą IP.

Pytania i odpowiedzi