



Система за динамична вътрешна маршрутизация на Софийския Университет “Св. Климент Охридски”, базирана на решения с отворен код

Веселин Колев, Николай Николов, Стефан Димитров
Университетски Изчислителен Център

Система за динамична вътрешна маршрутизация на СУ...

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
  network 62.44.127.244/30
  network 62.44.127.248/30
  neighbor AS112_BORDER_IPV4 remote-as 112
  neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
  neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
  neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```

КАКВА Е СИТУАЦИЯТА В СУ?



Система за динамична вътрешна маршрутизация на СУ...

Специфични условия за прилагане на решението в мрежата на СУ:

✓ Свързаност на AS5421 към Интернет:

- 2 международни канала
- 2 гранични маршрутизатора
- 7 peering партньора

✓ Топология на вътрешната маршрутизация в AS5421:

- Звездовидна топология
- Един Layer 2 (Ethernet) сегмент
- Един Layer 3 сегмент, с адресация както в IPv4 така и в IPv6

✓ Достъп до опорната мрежа:

- Граничните маршрутизатори
- Всички факултетски маршрутизатори
- През неконтролирана MAN среда

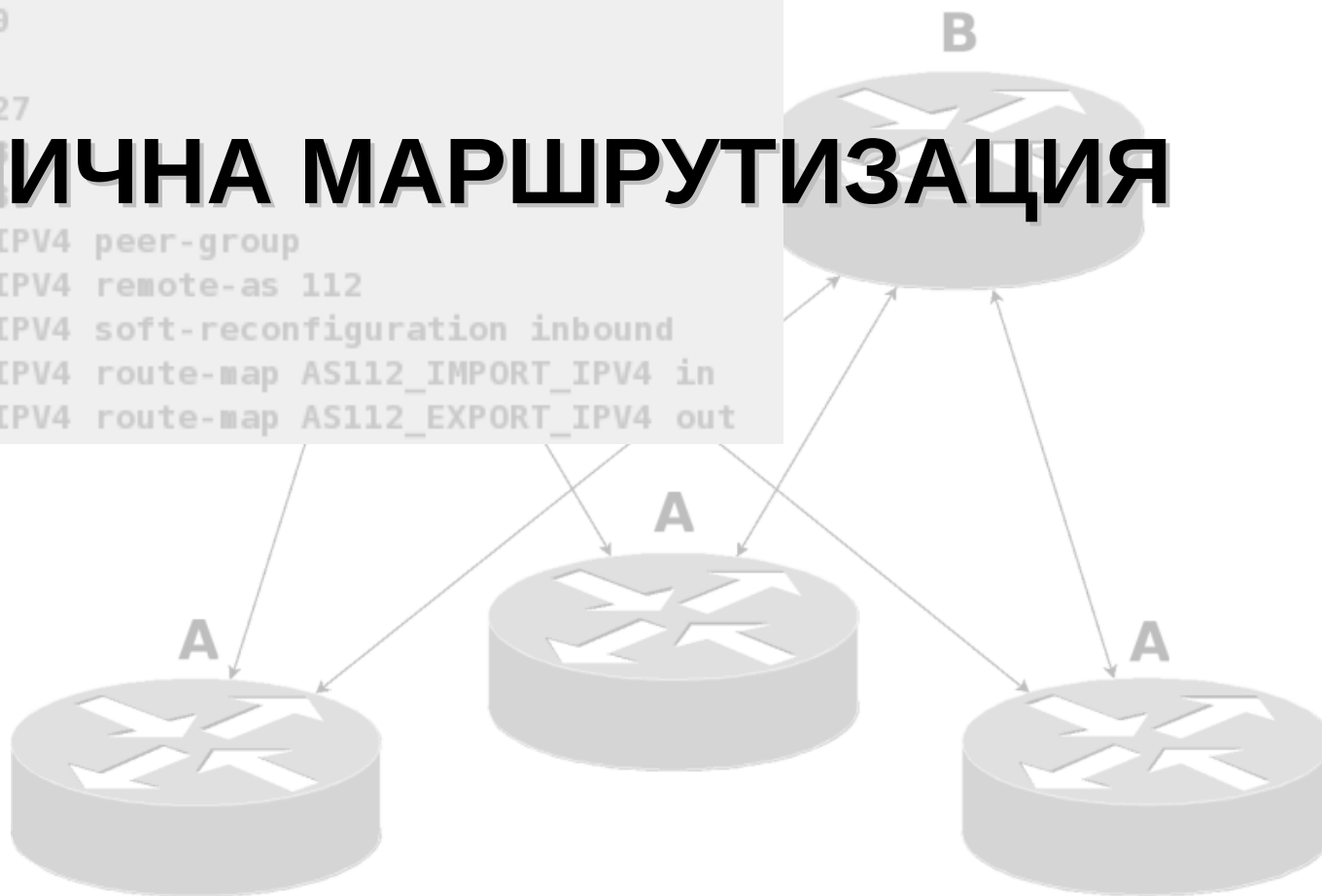
✓ Административен контрол върху маршрутизаторите:

- Наличие на автономни маршрутизатори

Система за динамична вътрешна маршрутизация на СУ...

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
  network 62.44.127.129/27
  network 62.44.127.130/27
  neighbor AS112_BORDER_IPV4 peer-group
  neighbor AS112_BORDER_IPV4 remote-as 112
  neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
  neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
  neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```

ДИНАМИЧНА МАРШРУТИЗАЦИЯ



Система за динамична вътрешна маршрутизация на СУ...

Схема на локална динамична маршрутизация с OSPF

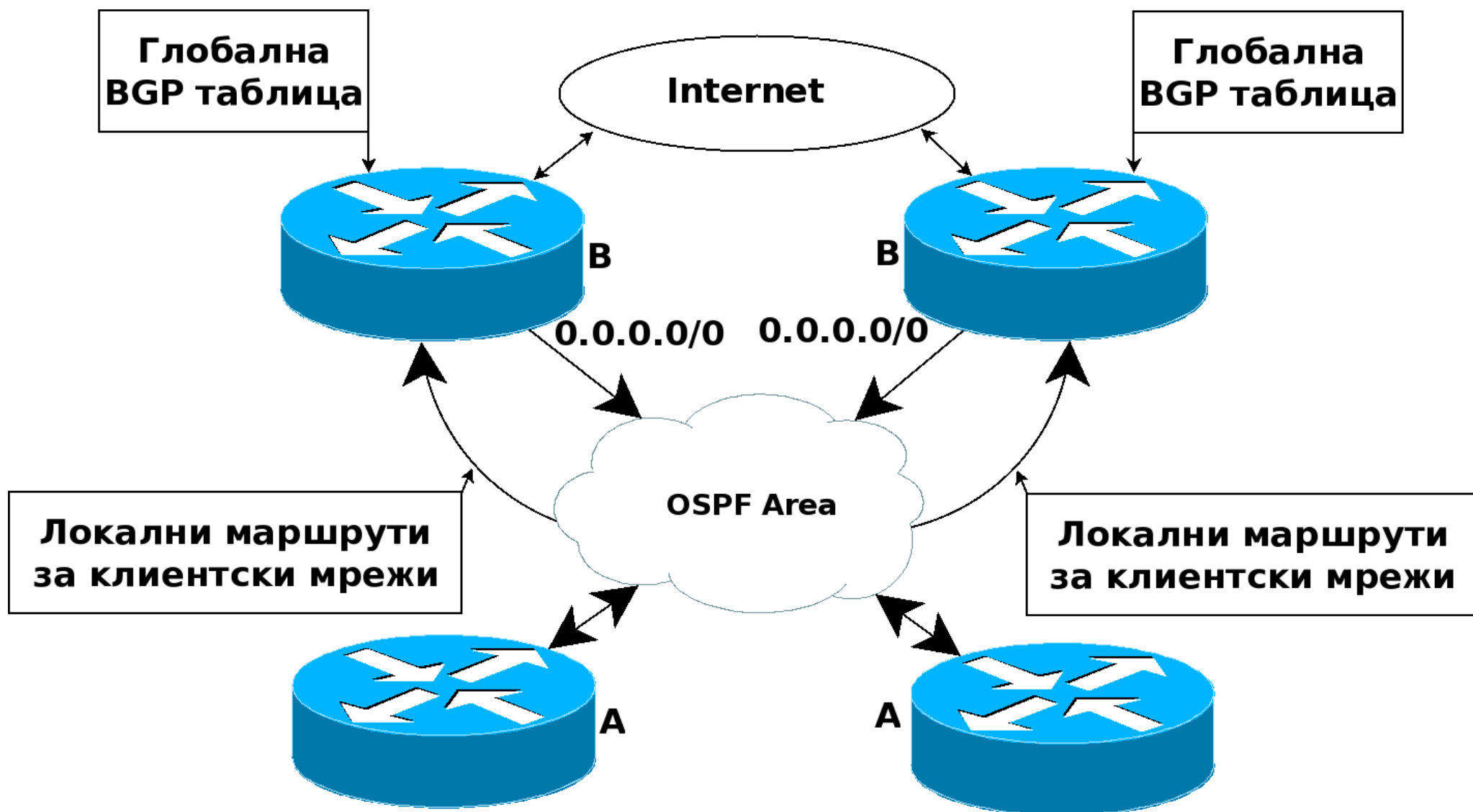


Схема на локална динамична маршрутизация с OSPF

+ Предимства:

- Бърза (“link-state”) вътрешна маршрутизация;
- Работи и с маршрутизатори с малко памет

– Недостатъци:

- Всички “access” маршрутизатори следва да са под единен оперативен контрол;
- Няма как пълната BGP таблица да се разпространи в OSPF;
- Няма как да се извърши специфична маршрутизация;
- Всяка грешка може да доведе до срив.

Система за динамична вътрешна маршрутизация на СУ...

Схема на локална динамична маршрутизация с BGP

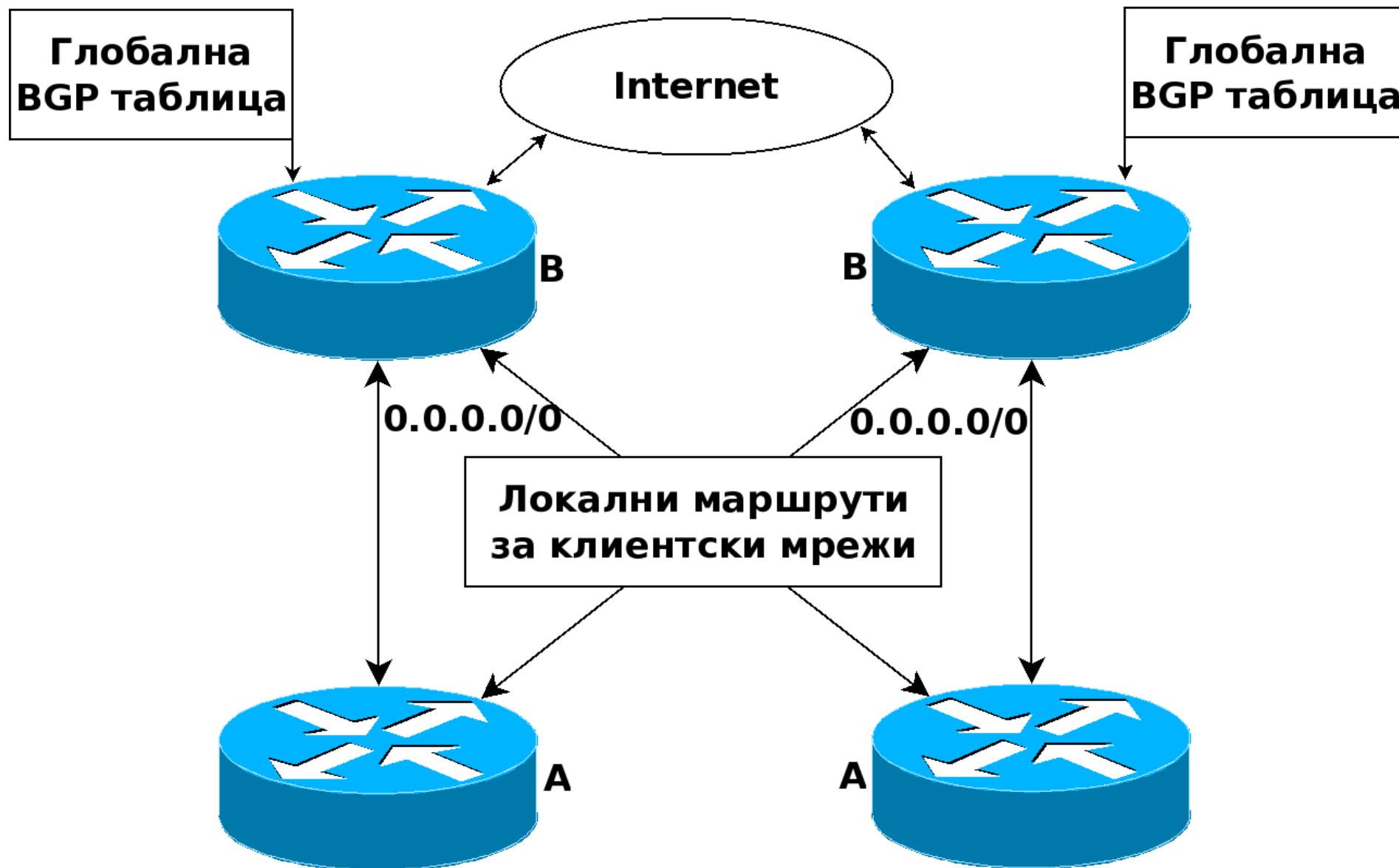


Схема на локална динамична маршрутизация с BGP

+ Предимства:

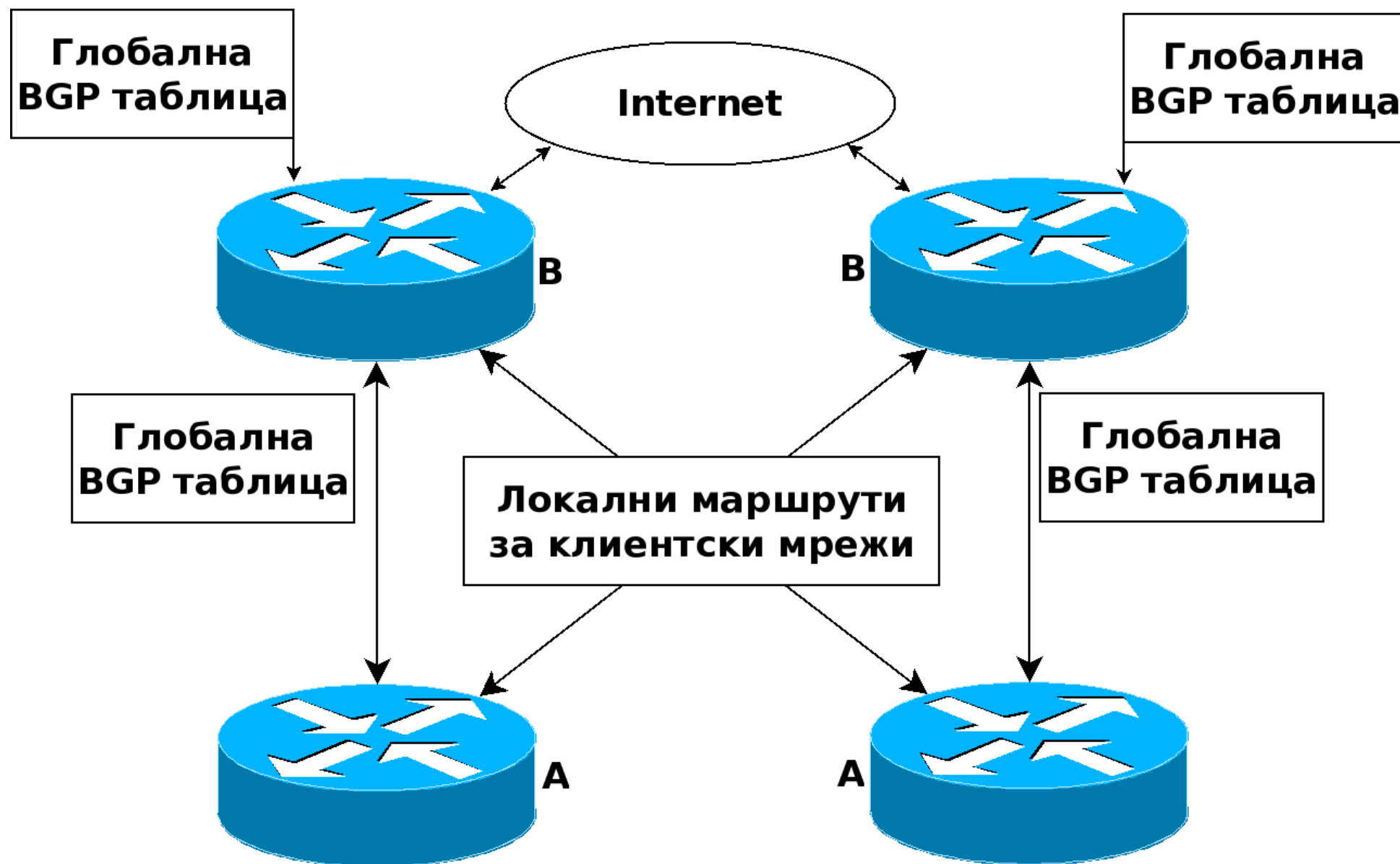
- Не е задължителен единния оперативен контрол върху “access” маршрутизаторите;
- Не изисква голямо количество свободна оперативна памет върху “access” маршрутизаторите.

– Недостатъци:

- Няма как да се извърши специфична маршрутизация;
- Паразитният трафик за неанонсирани мрежи стига до граничните маршрутизатори;
- Сравнително по-бавно разпространение на префиксите (на практика не е проблем).

Система за динамична вътрешна маршрутизация на СУ...

Пълна динамична маршрутизация в автономната система



Пълна динамична маршрутизация в автономната система

+ Предимства:

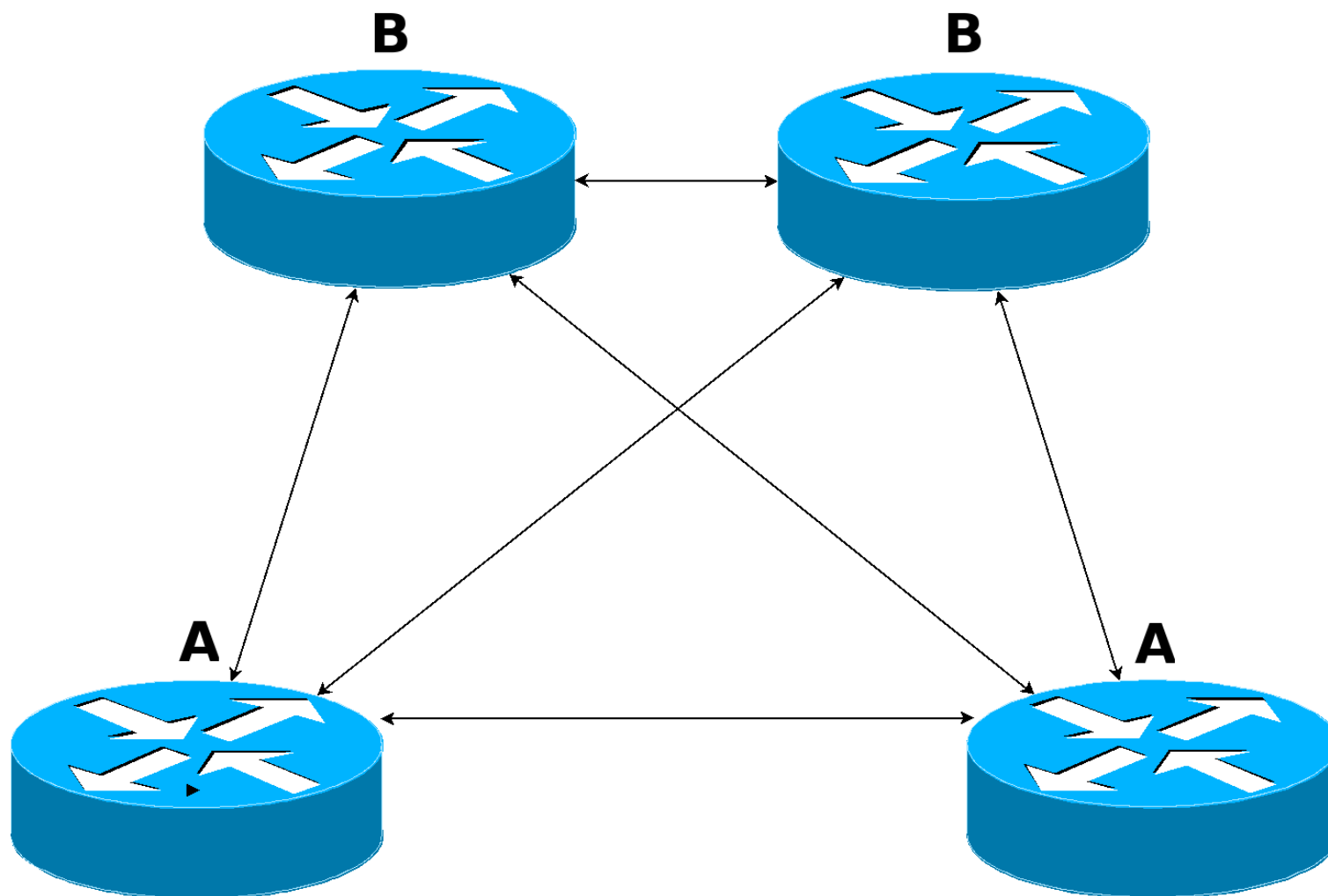
- Не е задължителен единния оперативен контрол върху “access” маршрутизаторите;
- Изходящият канал може да бъде много добре разпределен между потребителите;
- Паразитният трафик за неанонсирани мрежи не достига до граничните маршрутизатори.

– Недостатъци:

- Всички “access” маршрутизатори следва да имат достатъчно памет и производителен процесор;
- Сравнително по-бавно разпространение на префиксите (на практика не е проблем);
- Изисква се квалифициран персонал с опит и по-сложна конфигурация на BGP софтуера.

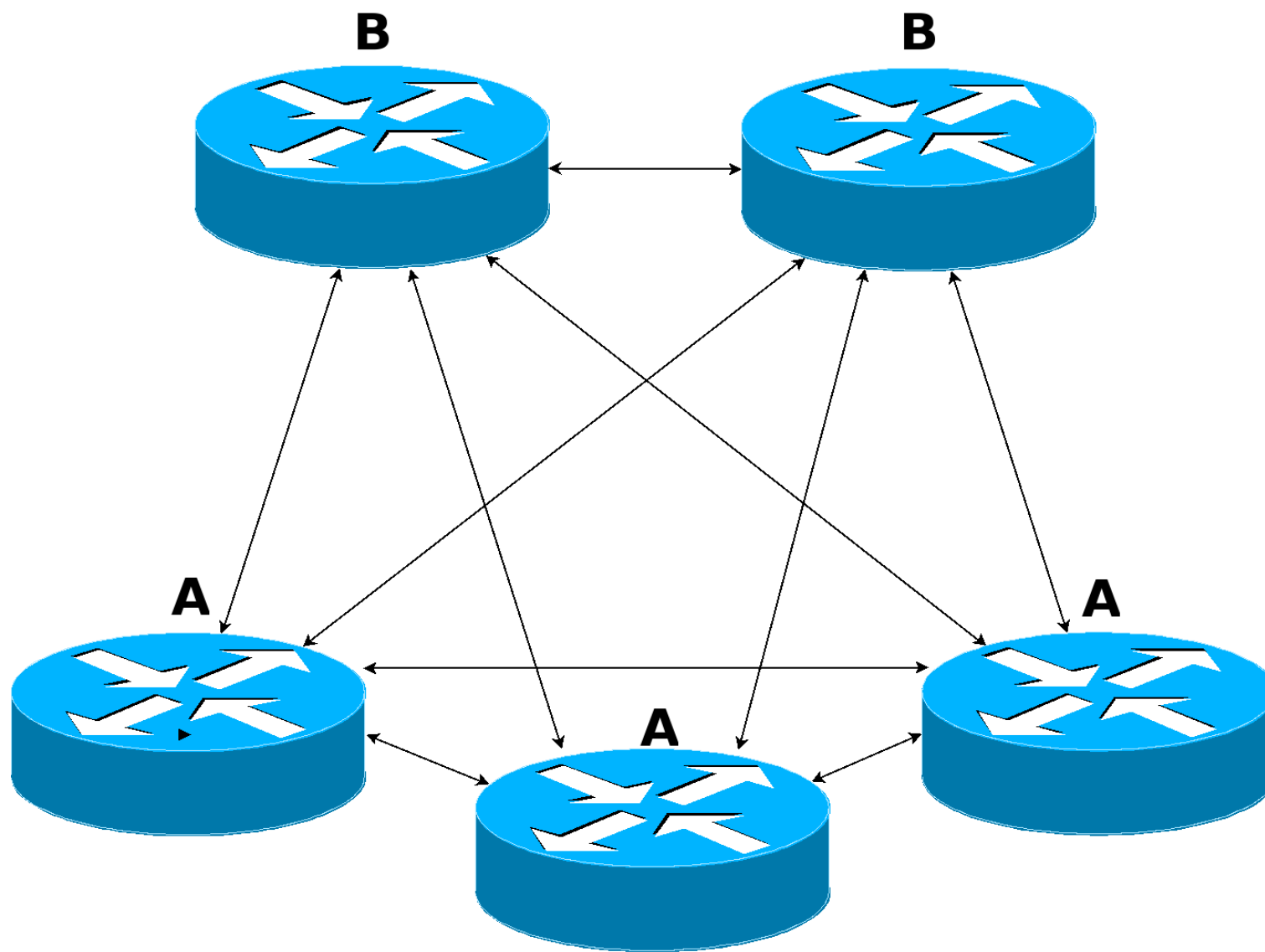
Проблем при изграждане на full-mesh

4 маршрутизатора => 6 вътрешни BGP сесии



Проблем при изграждане на full-mesh

5 маршрутизатора => 10 вътрешни BGP сесии



Система за динамична вътрешна маршрутизация на СУ...

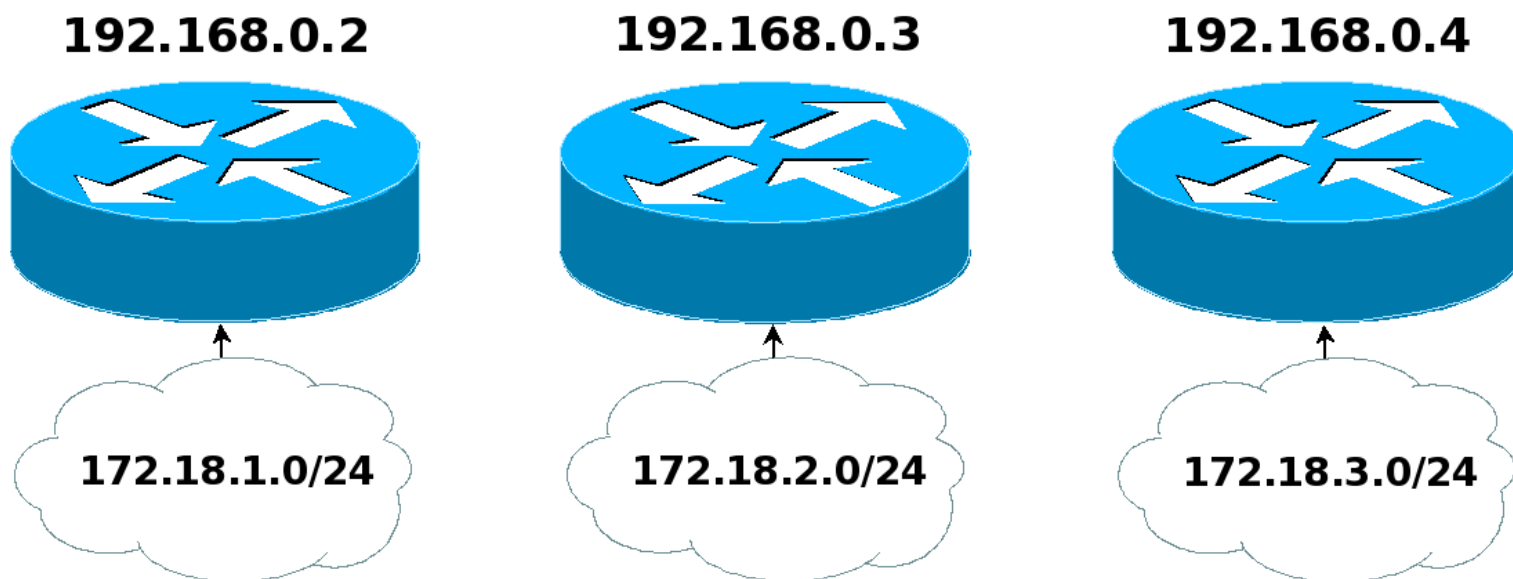
```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
  network 62.44.127.244/30
  network 62.44.127.248/30
  neighbor AS112_BORDER_IPV4 peer-group
  neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
  neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
  neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```

**ЩО Е ТО МАРШРУТЕН
РЕФЛЕКТОР (ОТРАЖАТЕЛ)?**



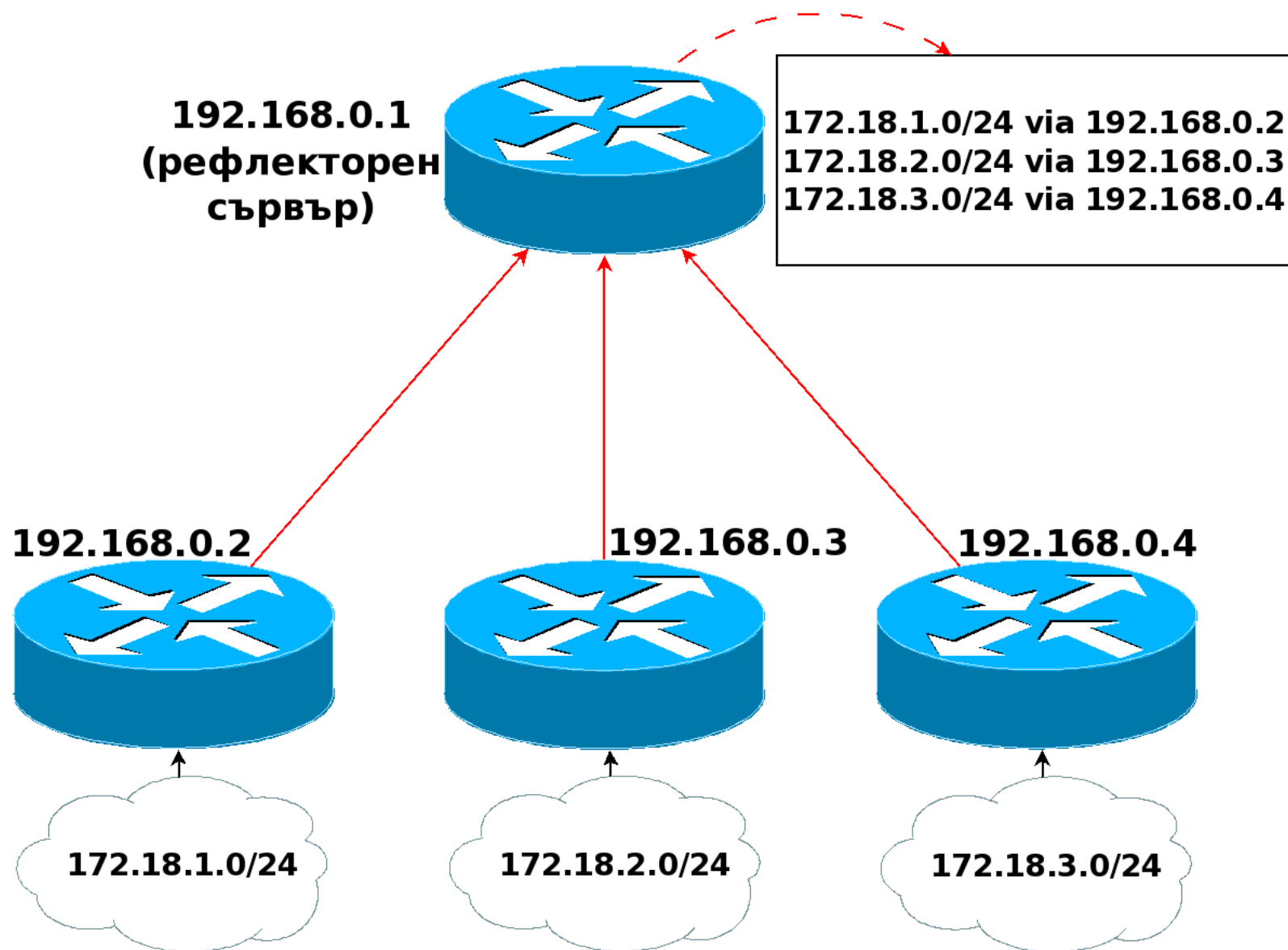
Роля на рефлекторния сървър при решаване на задачата

**КАК ДА СЕ ОБМЕНЯТ ЛОКАЛНИТЕ МАРШРУТИ, БЕЗ
ДИРЕКТНИ ВРЪЗКИ?**



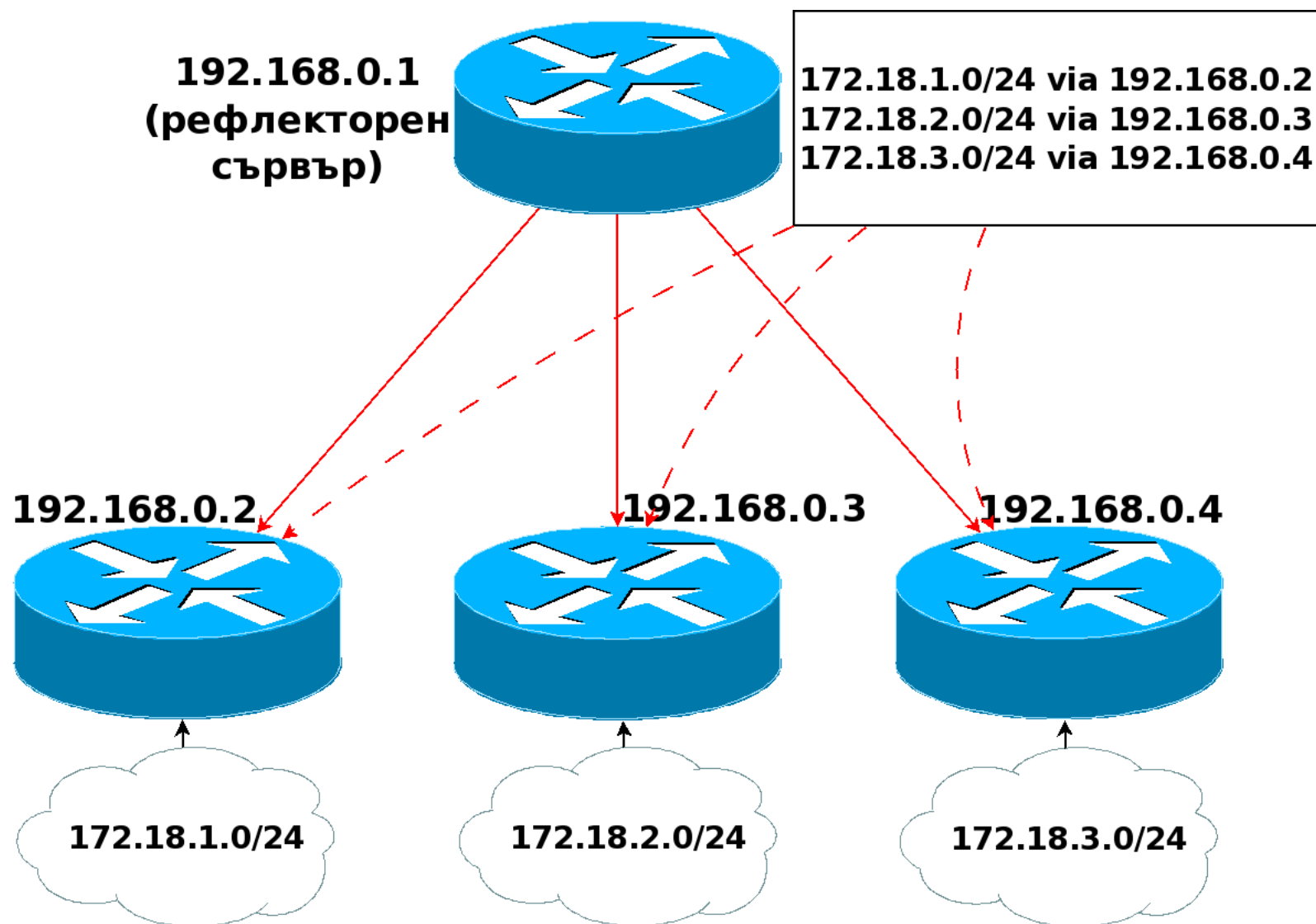
Система за динамична вътрешна маршрутизация на СУ...

Роля на рефлекторния сървър при решаване на задачата



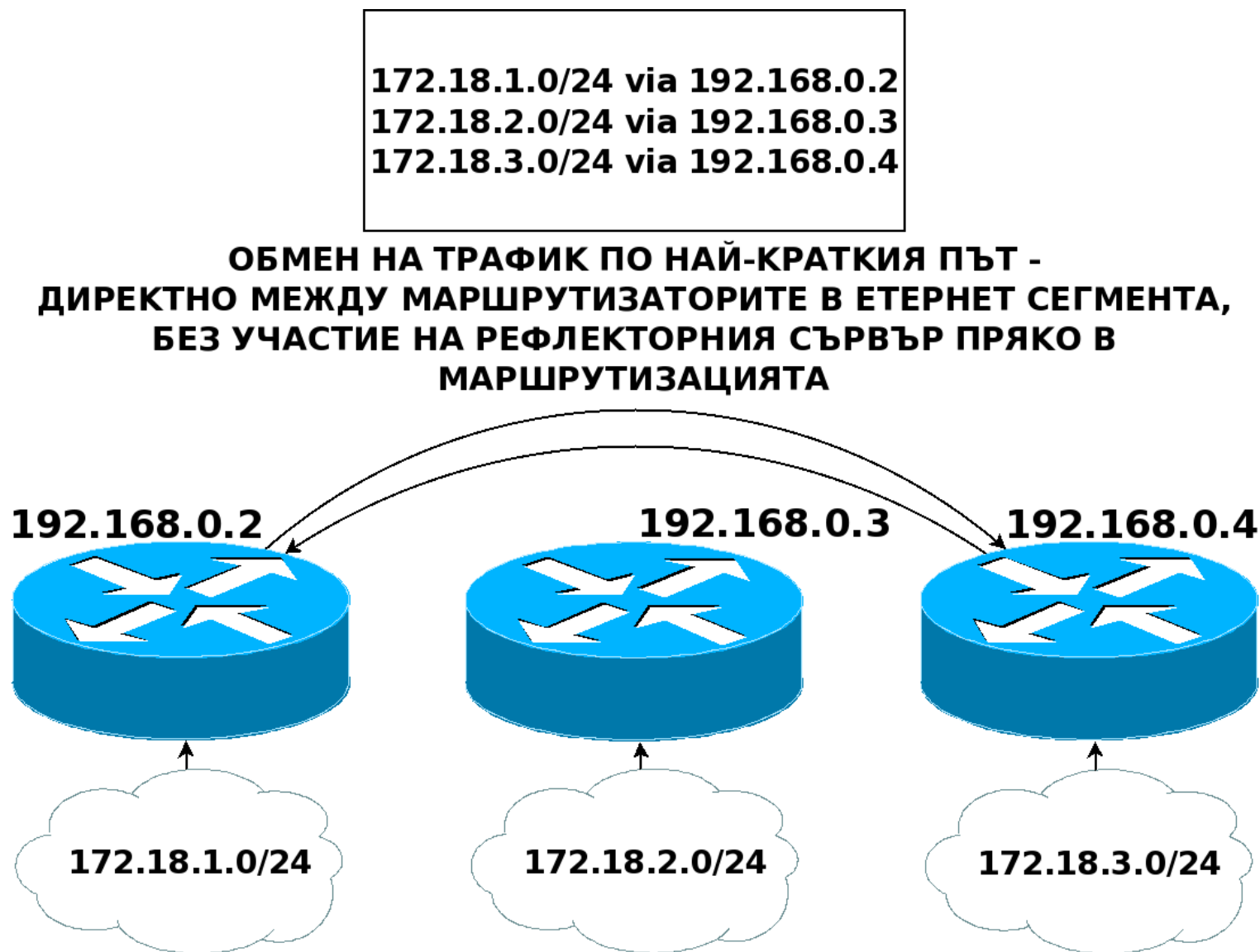
Система за динамична вътрешна маршрутизация на СУ...

Роля на рефлекторния сървър при решаване на задачата



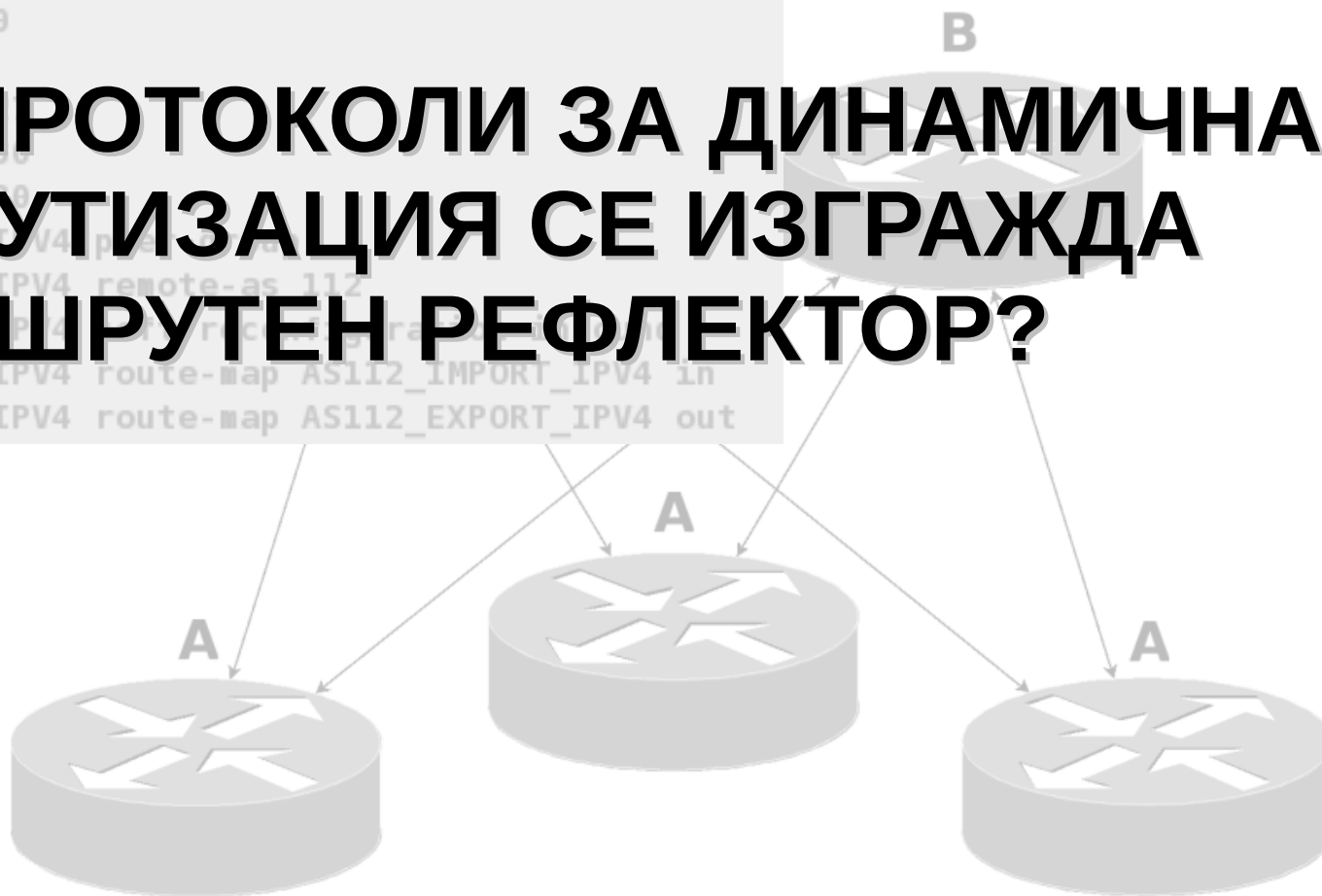
Система за динамична вътрешна маршрутизация на СУ...

Роля на рефлекторния сървър при решаване на задачата



```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
```

**С КАКВИ ПРОТОКОЛИ ЗА ДИНАМИЧНА
МАРШРУТИЗАЦИЯ СЕ ИЗГРАЖДА
МАРШРУТЕН РЕФЛЕКТОР?**



Използваеми в рефлектора протоколи за динамична маршрутизация

Маршрутен рефлектор може да се реализира чрез:

- ✓ BGPv4/4+
- ✓ OSPF (v2/v3) – само в “unicast” режим
- ✓ IS-IS – само в “unicast” режим, има ограниченията на OSPF
- ✓ EIGRP (непрепоръчителен – собственически на CISCO)
- ✓ RIPv2 – само в “unicast” режим
- ✓ RIPvng – само в “unicast” режим
- ✓ други протоколи за динамична маршрутизация, които не пренаписват “nexthop” стойността при обмен на маршрути в един адресен сегмент и поддържат “unicast” режим.

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
```

**С КАКЪВ СОФТУЕР С ОТВОРЕН КОД ЗА
ДИНАМИЧНА МАРШРУТИЗАЦИЯ СЕ
РЕАЛИЗИРА МАРШРУТЕН РЕФЛЕКТОР?**



Система за динамична вътрешна маршрутизация на СУ...

Използваем софтуер с отворен код за маршрутен рефлектор

Маршрутен рефлектор може да се реализира чрез:

✓ Quagga: <http://quagga.net/>

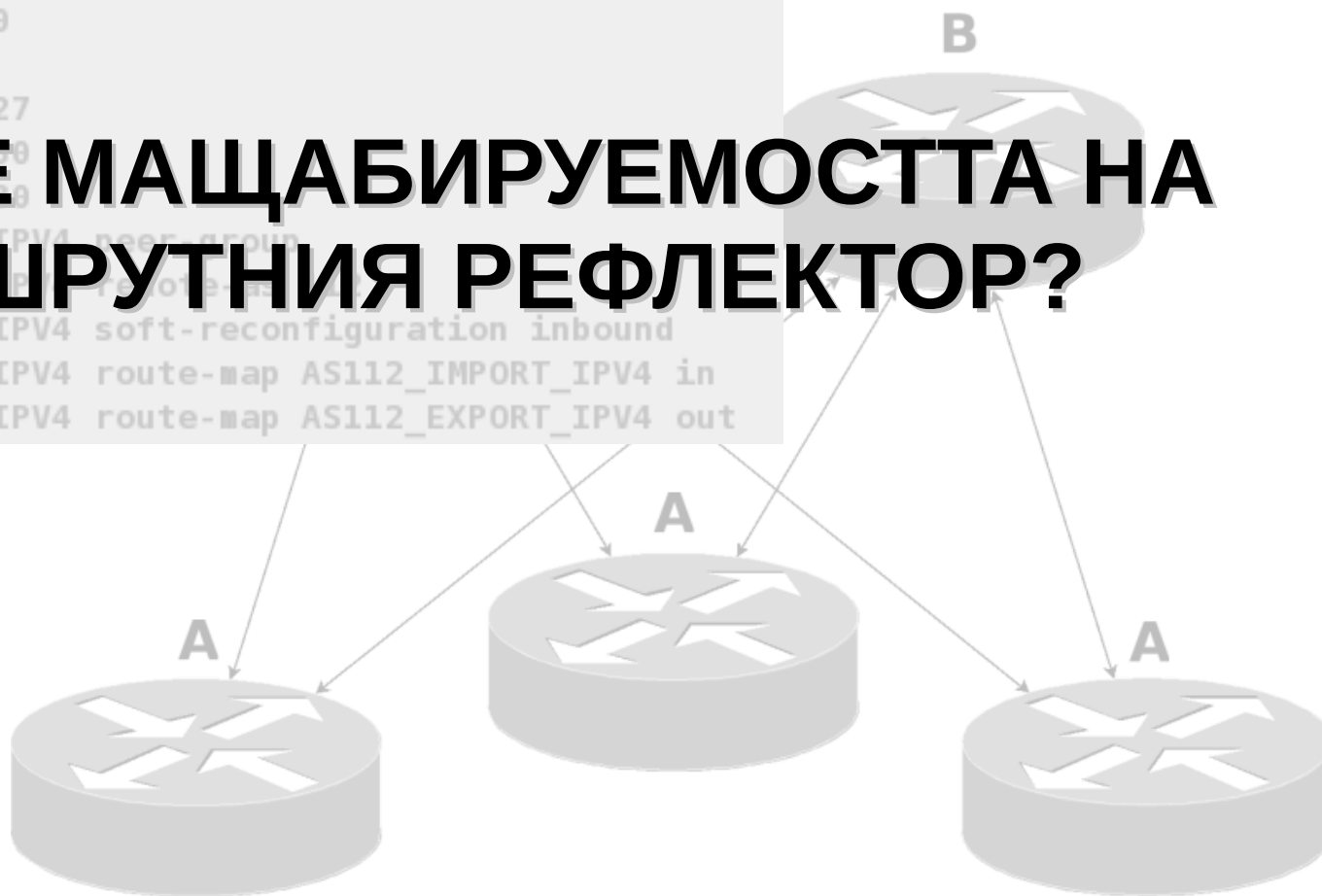
Използва IOS (Cisco) подобен синтаксис на конфигурациите, лесно се усвоява от преминали обучение в Cisco-академия.

✓ Xorp: <http://xorp.org/>

Използва JunOS (Juniper) подобен синтаксис на конфигурациите.

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
  network 62.44.127.129/24
  network 62.44.127.130/24
  neighbor AS112_BORDER_IPV4 peer-group
  neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
  neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
  neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```

**КАКВА Е МАЩАБИРУЕМОСТТА НА
МАРШРУТНИЯ РЕФЛЕКТОР?**



Мащабируемост на маршрутния рефлектор:

✓ Мащабируемост при добавяне на нов маршрутизатор:

Прибавянето на маршрутизатор в рефлекторната схема се отразява само в конфигурацията на рефлекторния сървър, но не и в конфигурациите на останалите маршрутизатори в рефлектора.

✓ Мащабируемост при филтрация на маршрути:

Филтрация за приемани/отхвърляни маршрути може да се прави както глобално, върху рефлекторния сървър, така и локално, върху всеки от маршрутизаторите.

✓ Мащабируемост при маршрутизация:

Доколкото рефлекторният сървър не маршрутизира никакви направления в рефлектора, неговото натоварване не зависи от количеството на обменяния трафик между маршрутизаторите.

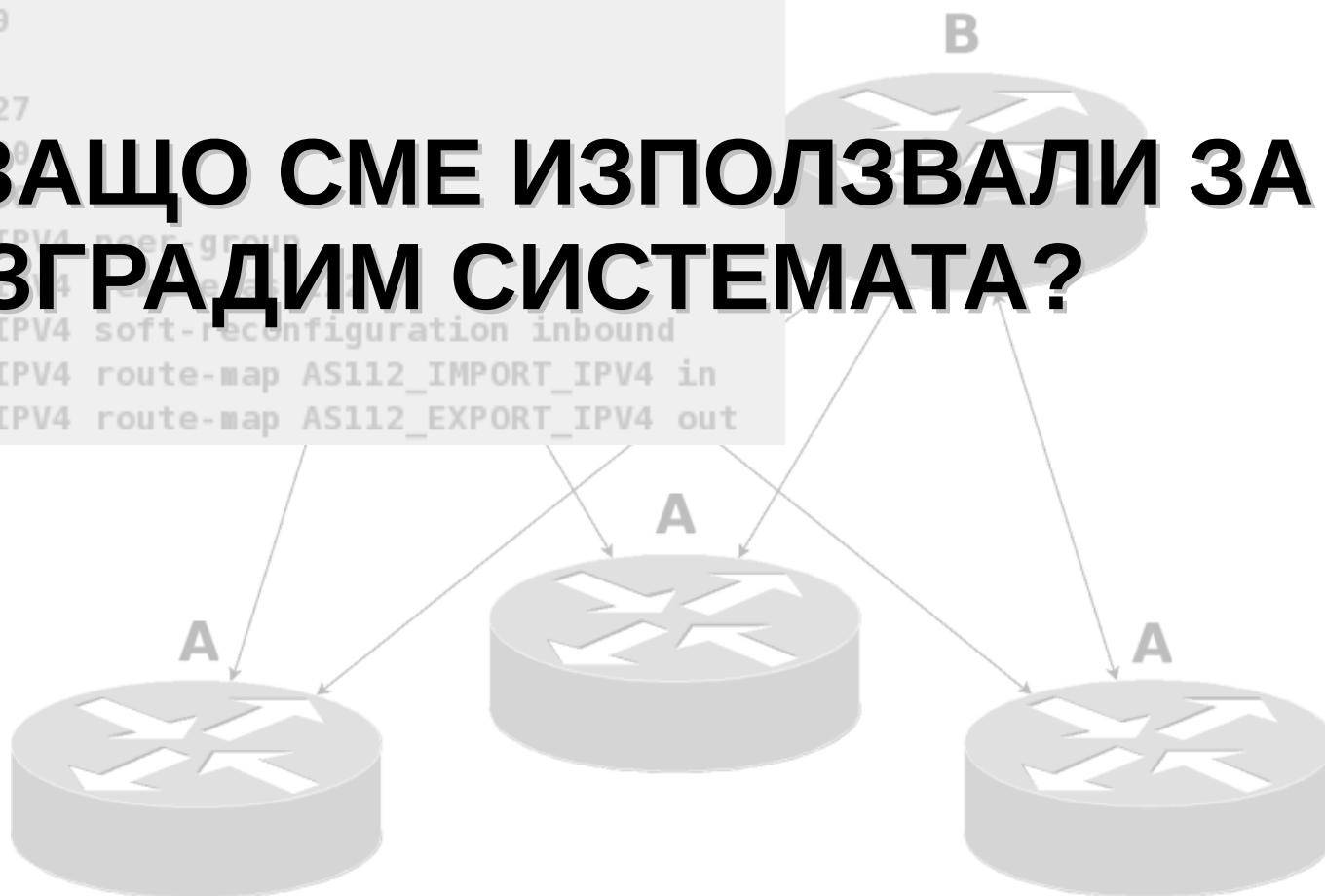
! Отказоустойчивост:

При отпадане на рефлекторния сървър се прекратява функционирането на рефлектора. Затова е наложително да има поне два рефлекторни сървъра!

Система за динамична вътрешна маршрутизация на СУ...

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
```

**КАКВО И ЗАЩО СМЕ ИЗПОЛЗВАЛИ ЗА
ДА ИЗГРАДИМ СИСТЕМАТА?**



Система за динамична вътрешна маршрутизация на СУ...

Софтуер с отворен код, използван за компоненти на системата:

✓ Linux дистрибуция:

CentOS 5 (<http://www.centos.org/>)

Дистрибуция производна на Red Hat Enterprise Linux, с много добра поддръжка, дълъг жизнен цикъл (7 години), позволяваща автоматична актуализация на пакетите (чрез yum-updatesd).

✓ Софтуер за динамична маршрутизация:

Quagga (<http://www.quagga.net/>)

За поддръжката на 32-битови номера на автономни системи е изграден RPM пакет за CentOS с версия на Quagga 0.99.14, публично достъпен на адрес <http://rpm.vesselin.org/redhat/daemons/>.

✓ IPsec реализация и инструментариум:

Използвана е вградената в Linux ядра 2.6 поддръжка на IPsec. Използваният IKEv1 демон (**racoon**) и инструментариума за управление на политиките (**setkey**) са от дистрибутивния пакет **ipsec-tools**.

Система за динамична вътрешна маршрутизация на СУ...

```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
```

КАК СМЕ РЕАЛИЗИРАЛИ МАРШРУТНИЯ РЕФЛЕКТОР В МРЕЖАТА НА СУ?

```
neighbor AS112_BORDER_IPV4 peer-group
neighbor AS112_BORDER_IPV4 peer-as 112
neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```



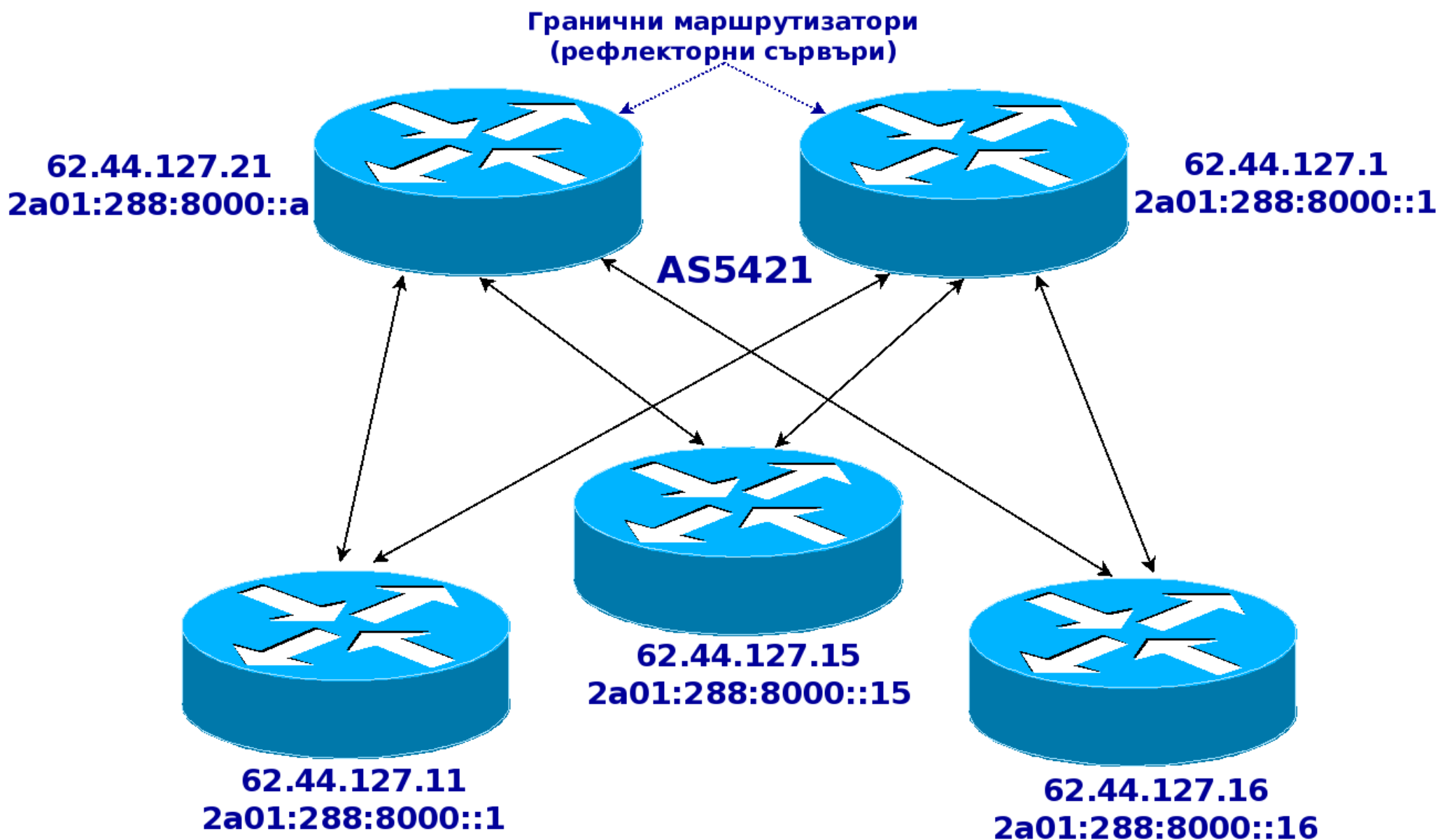
Система за динамична вътрешна маршрутизация на СУ...

Особености на изградения рефлексор:



Система за динамична вътрешна маршрутизация на СУ...

Особености на изградения рефлексор:



Особености на изградения рефлексор:

✓ Използване на BGP4/4+ за основен маршрутизиращ протокол:

Всеки маршрутизатор на факултет или самостоятелно звено получава пълните BGP таблици от двата гранични маршрутизатора и анонсира към тях префиксите на мрежите на своите клиенти (потребители).

✓ Роли в рефлексорна схема:

Граничните маршрутизатори на AS5421 са рефлексорни сървъри, а “access”-маршрутизаторите на факултерите са рефлексорни клиенти.

✓ Достъп до опорната мрежа:

Достъп до опорната мрежа имат само граничните маршрутизатори и маршрутизаторите на съответните факултети и самостоятелни звена.

✓ Административен контрол върху маршрутизаторите:

Някои от маршрутизаторите са под оперативния контрол на Университетския изчислителен център, а други под тази на администраторите на съответните факултети и самостоятелни звена.

Особености на изградения рефлексор:

✓ Напълно динамична маршрутизация:

Никъде в рефлексора няма маршрут по подразбиране (“default”). Поради обмена на пълната маршрутна BGP таблица, всеки “access”-маршрутизатор знае всички маршрути в Интернет.

✓ Еднозначна филтрация на префикси:

Граничните маршрутизатори на AS5421, в ролята си на рефлексорни сървъри, приемат от рефлексорните клиенти само тези префикси, които са описани чрез съответните филтри префикси.

✓ Оптимизация на вътрешния трафик в AS5421:

Обменът на трафик между факултетските мрежи става на максимално достижимата скорост в опорната мрежа, без да се транспортира вътрешен трафик през граничните маршрутизатори.

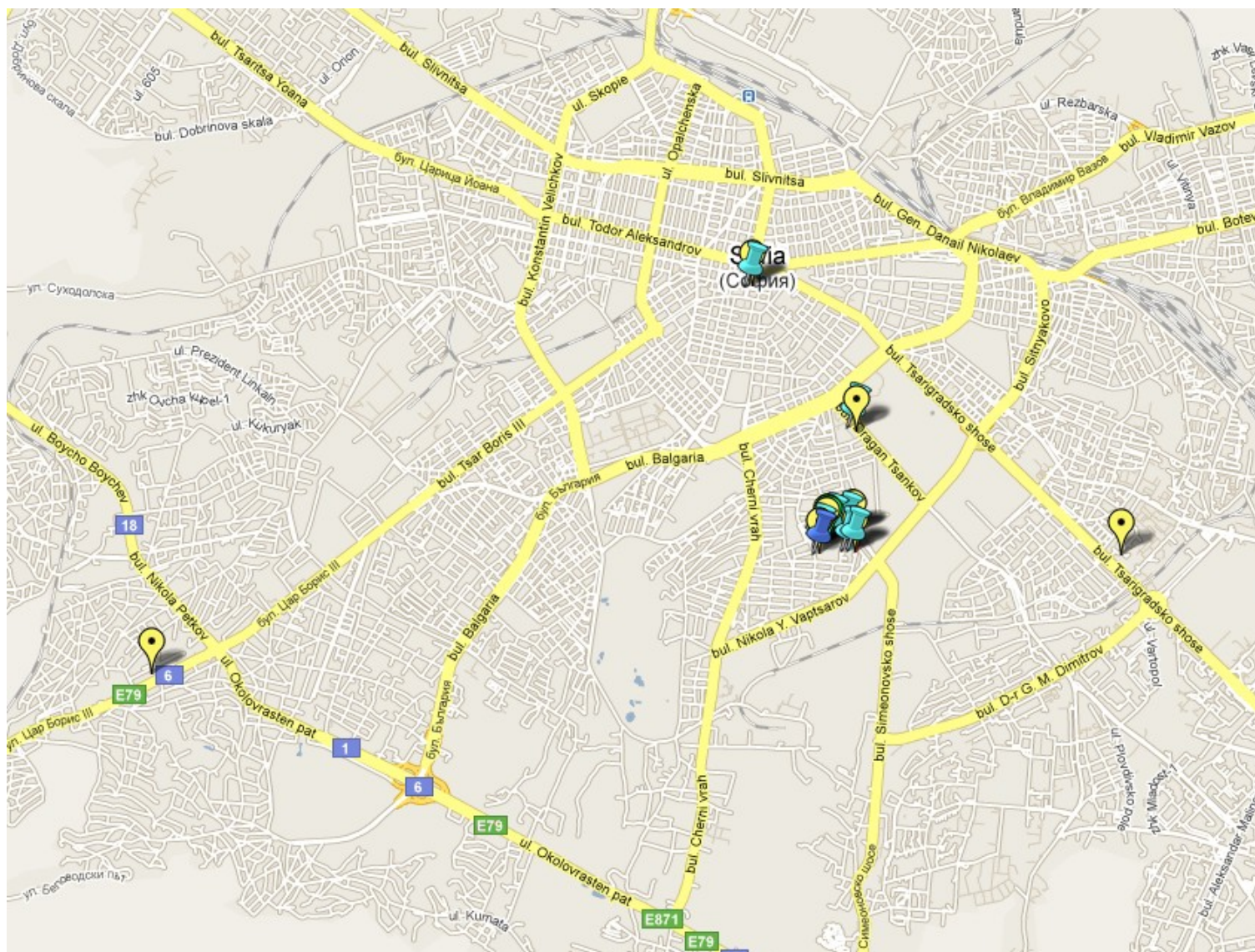
✓ Използване на Quagga за софтуер за динамична маршрутизация:

Използваната версия на Quagga е 0.99.14, компилирана специално за нуждите на AS5421, поддържаща 32-битови ASN.

Система за динамична вътрешна маршрутизация на СУ...



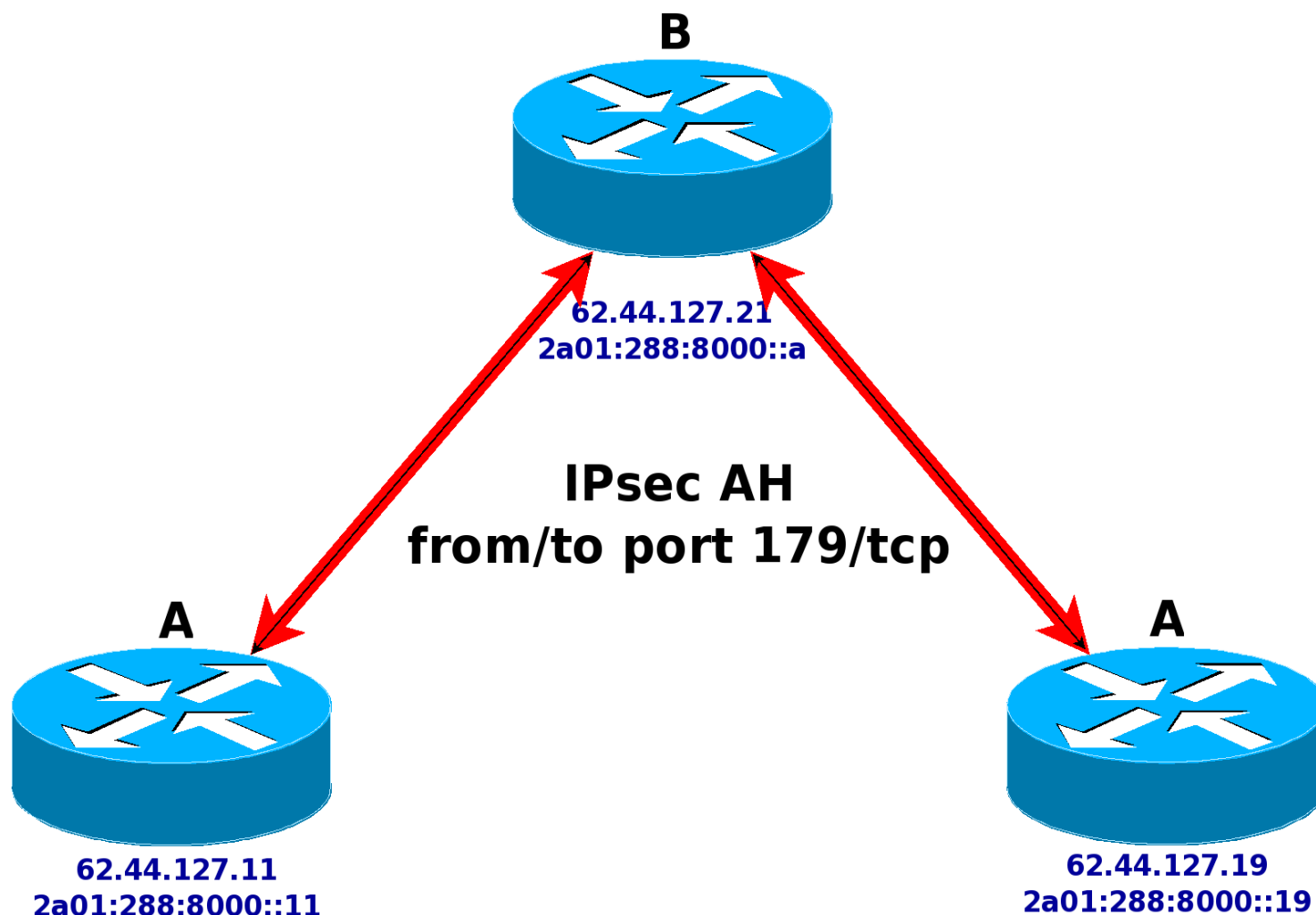
Нужно е да можем да идентифицираме еднозначно маршрутизаторите в опорната мрежа, които са разпръснати географски из град София и са свързани през MAN среда, която ние не контролираме!



ИЗПОЛЗВАНЕ НА IPsec/AH ЗА УДОСТОВЕРЯВАНЕ И ЗАЩИТА НА BGP СЕСИИ

Система за динамична вътрешна маршрутизация на СУ...

Защита на BGP услугата чрез “обвиването” на комуникацията по протокола в IPsec/AH



ЗАЩО IPsec/AH?

Система за динамична вътрешна маршрутизация на СУ...

Защо защитаваме TCP услуга като BGP чрез IPsec/AH?

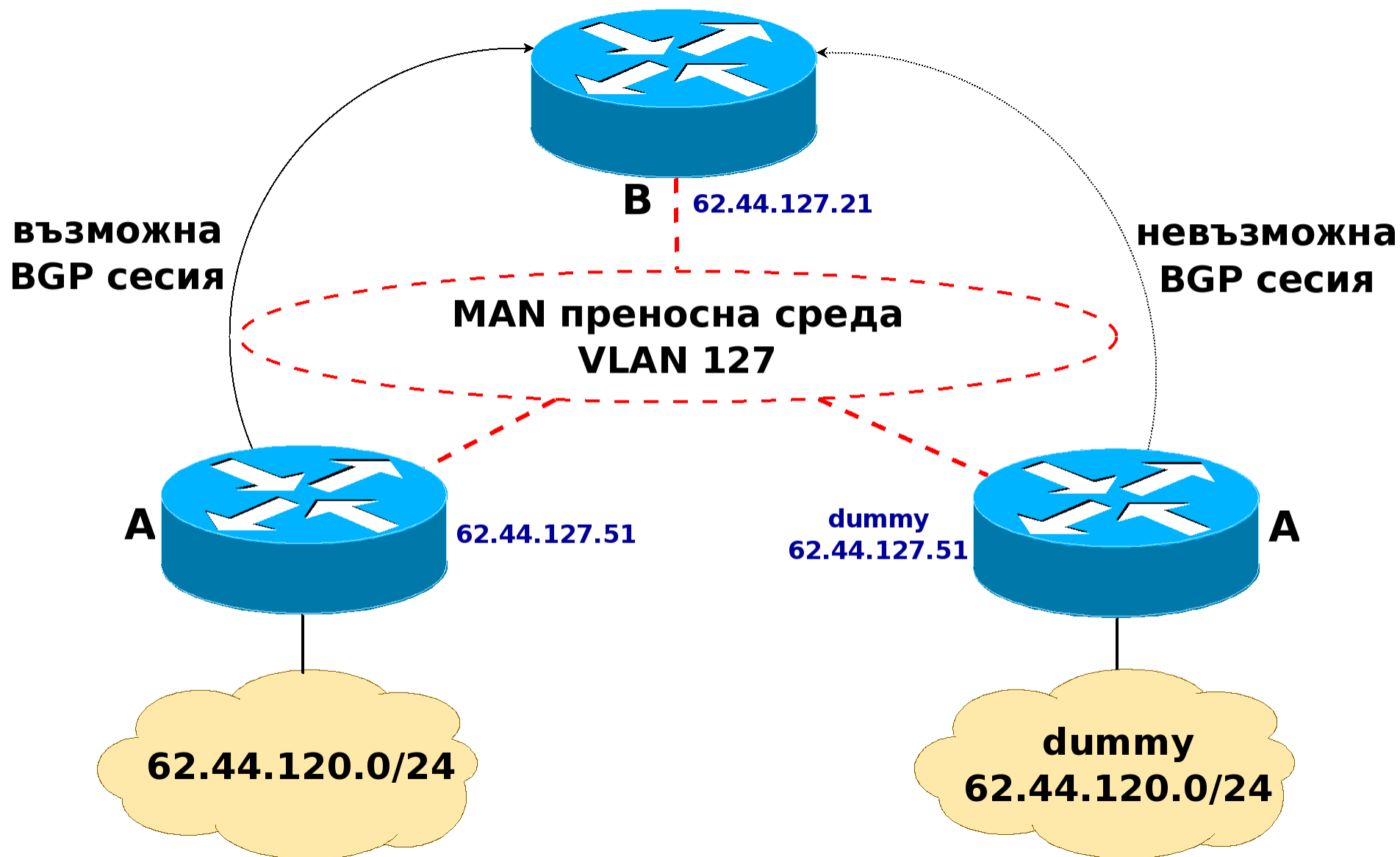
- ✓ Удостоверяването на съседа става чрез електронен подпис
- ✓ BGP сесия само с описаните в IPsec политиките източници
- ✓ Неописан източник не установява дори TCP сесия
- ✓ Предотвратяват се редица чисто TCP атаки
- ✓ IPsec се поддържа в ядрото => минимално натоварване
- ✓ IPsec е част от IPv6 протоколният стек

**КАКВО ПОСТИГА И КАКВО НЕ
УДОСТОВЕРЯВАНЕТО ПО ТОЗИ НАЧИН?**

Система за динамична вътрешна маршрутизация на СУ...



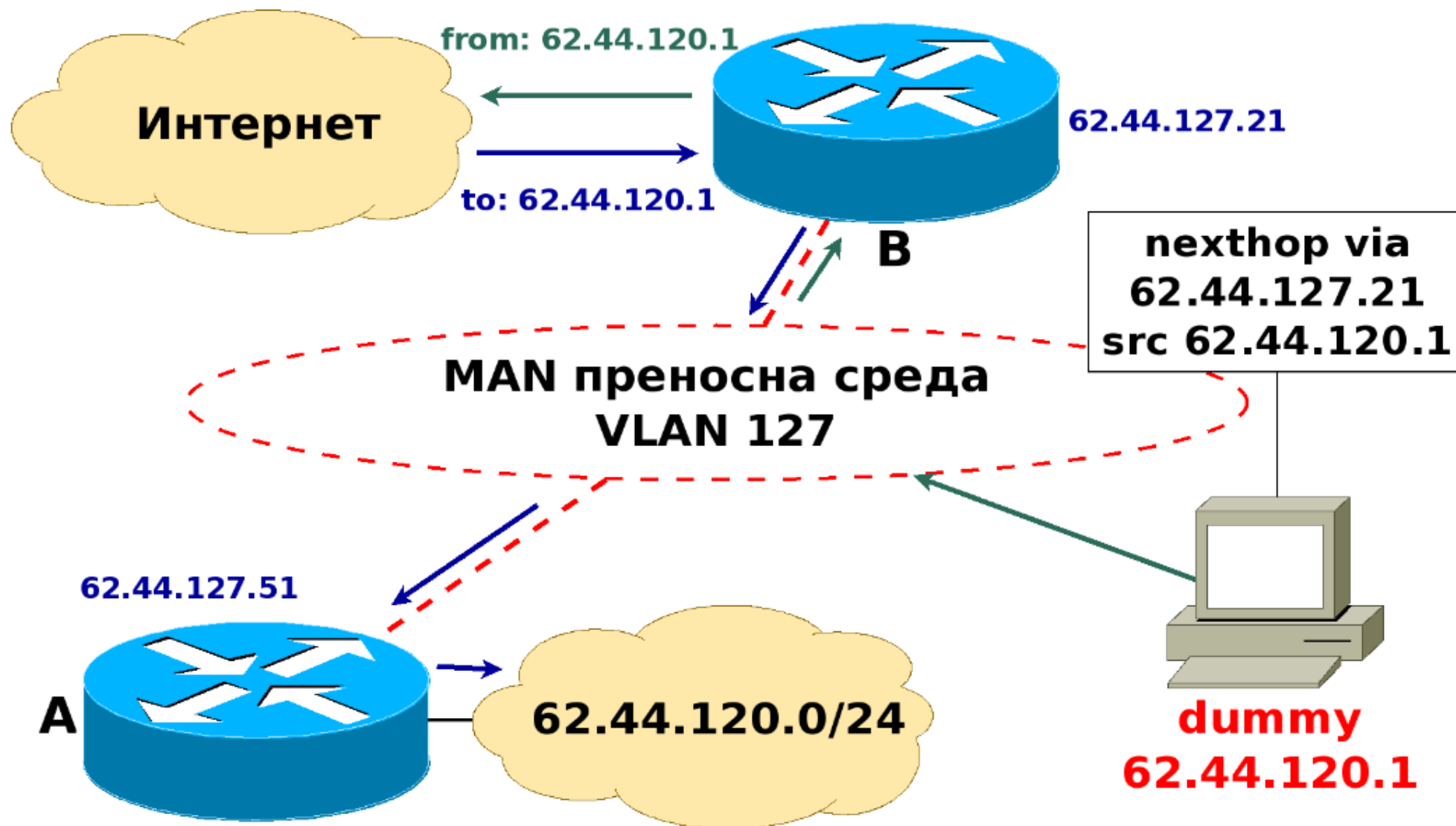
Отхвърляне на опит за установяване на BGP сесия след “изхвърляне” на оригиналния маршрутизатор от етернет сегмента на виртуалния LAN и заместването му с “фалшив”!



Система за динамична вътрешна маршрутизация на СУ...

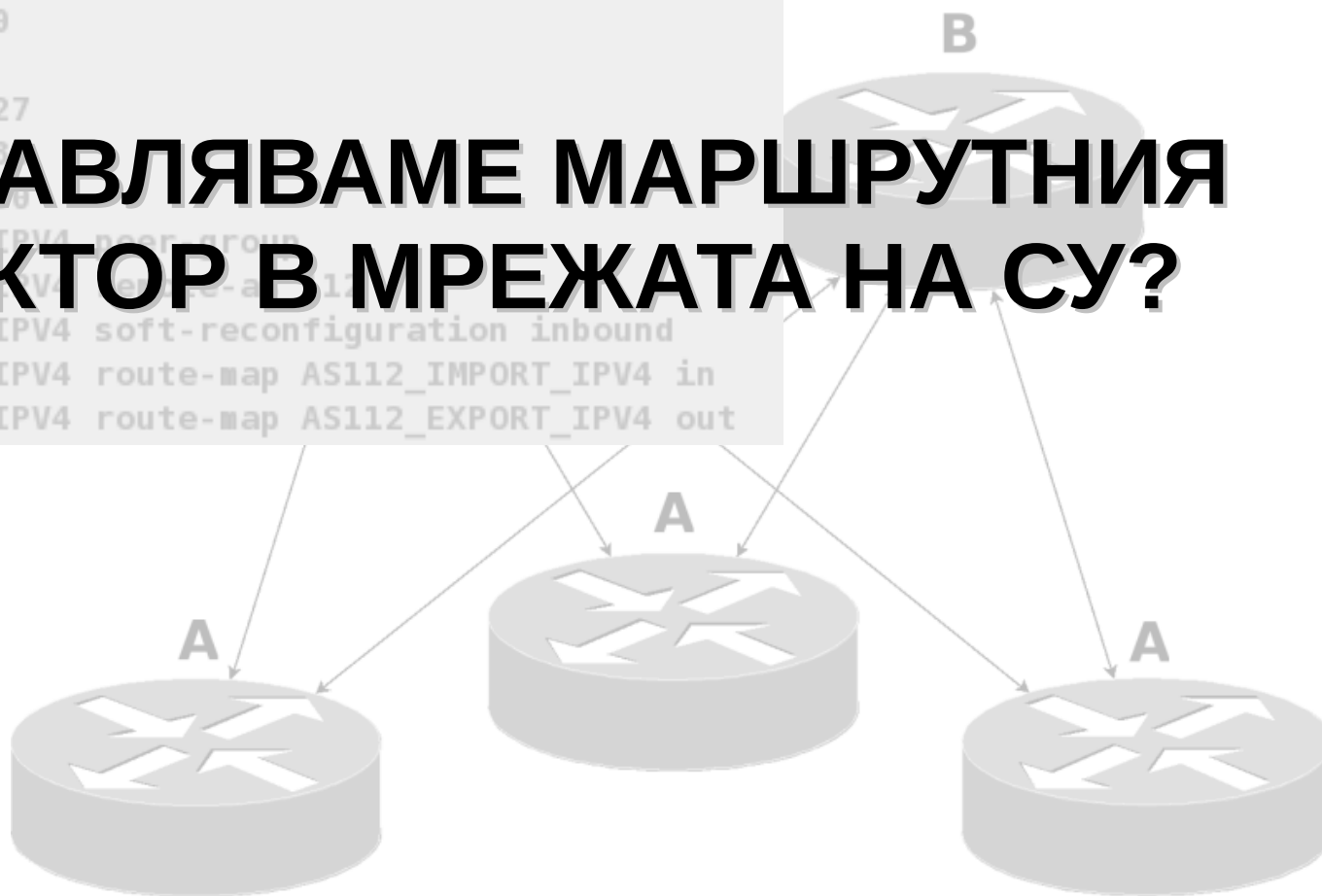


Не е възможно чрез IPsec/AH удостоверяване на BGP сесия, да се предотврати еднопосочното излъчване на пакети от името на IP адрес от мрежата на Университета!



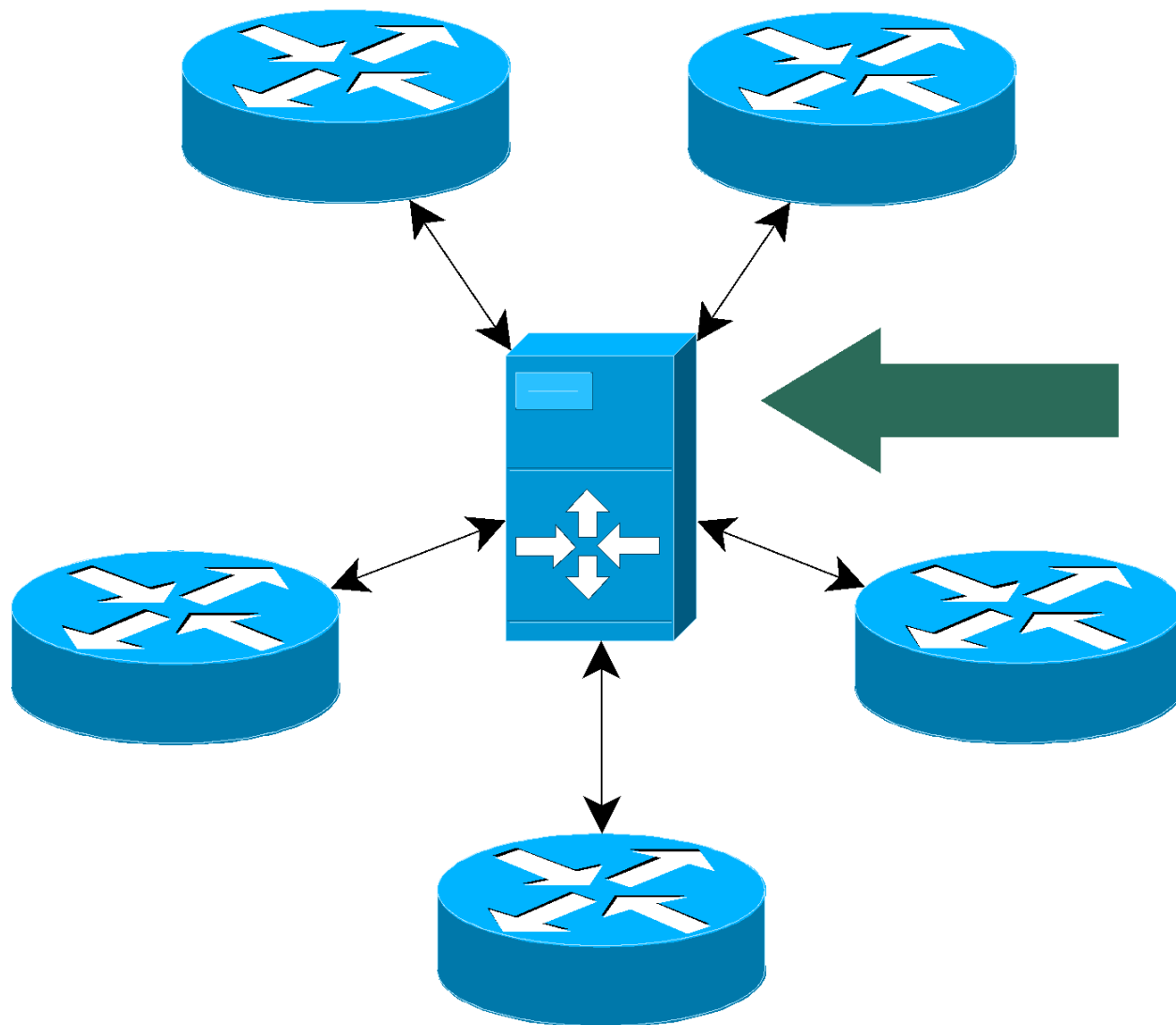
```
router bgp 5421
  bgp router-id 62.44.127.11
  network 62.44.96.0/25
  network 62.44.96.129/32
  network 62.44.96.228/30
  network 62.44.97.0/27
  network 62.44.97.192/27
  network 62.44.97.224/30
  network 62.44.97.232/30
  network 62.44.97.236/30
  network 62.44.109.0/24
  network 62.44.127.128/27
  network 62.44.127.129/32
  network 62.44.127.130/32
  neighbor AS112_BORDER_IPV4 peer-group
  neighbor AS112_BORDER_IPV4 peer-as 112
  neighbor AS112_BORDER_IPV4 soft-reconfiguration inbound
  neighbor AS112_BORDER_IPV4 route-map AS112_IMPORT_IPV4 in
  neighbor AS112_BORDER_IPV4 route-map AS112_EXPORT_IPV4 out
```

КАК УПРАВЛЯВАМЕ МАРШРУТНИЯ РЕФЛЕКТОР В МРЕЖАТА НА СУ?



Система за динамична вътрешна маршрутизация на СУ...

Сервизна станция за управление и поддръжка на рефлексора



Предоставяни услуги:

- NTPv4 (Stratum 1)
- Remote Syslog
- SVN (за конфигурации)
- система за статистика
- достъп през X.25

ОБОБЩЕНИЕ

Обобщение:

✓ Пълен контрол над вътрешната маршрутизация:

Вероятността да има грешен анонс (поради грешка или умишлено) и той да се приеме от маршрутизаторите е минимална, тъй като на всеки маршрутизатор има двупосочни префиксни филтри.

✓ Най-кратък път между факултетите с минимум сесии:

Рефлекторната схема дава гъвкавост и сигурност едновременно.

✓ Резервираност на външната и вътрешната маршрутизация:

Двата гранични маршрутизатора които работят и като два рефлекторни сървъра гарантират тази сигурност.

✓ BGP сесиите са удостоверени:

IPSec/АН асоциациите между маршрутизаторите дават максимално високо ниво на защита от злонамерно вмешателство в BGP анонсите.

✓ Аварийен достъп до всички опорни маршрутизатори:

Дори при отпадане и на двата външни канала, отдалеченият достъп до опорните маршрутизатори е възможен през сервисната станция.

БЛАГОДАРИМ ЗА ВНИМАНИЕТО
ВЪПРОСИ?



Съдържанието може да се използва и разпространява при
условията на **"Creative Commons - Признание 2.5"**