Основи на проектирането на корпоративни мрежи

MikroTik Net Camp 2017

Трявна

Петър Димитров

За мен:

- Име: Петър Димитров
- Опит в областта на компютърните мрежи: от 2002 г.
- Опит с MikroTik: от 2005 г.
- MikroTik Trainer: от 2013 г.
- Предлагани MikroTik обучения:

MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME, MTCIPv6E, MTCINE

Проектиране на мрежи

- Целта на тази презентация е систематизиране на някои основни стъпки при проектирането на корпоративни мрежи.
- Дизайна на една мрежа обикновено е по-сложен и трудоемък процес от техническата реализация.
- Добрия проект улеснява бъдещите поддръжка и развитие на мрежата.

От къде да започнем?

- На първо място трябва да бъдат ясно определени нуждите на организацията, чиято мрежа планирате:
  - Обхват/размер на мрежата
  - Текущо състояние
  - Мрежови услуги
  - Вътрешна организация и политики

Обхват/размер на мрежата

- Тук трябва да определите компонентите и размерите на IT инфраструктурата:
  - Централен офис
  - Филиали
  - Data центрове
  - Отдалечен достъп на служители

Текущо състояние

- Ако съществува изградена инфраструктура:
  - Запознайте се с наличната документация.
  - Направете одит на мрежовите устройства (и информацията за трафика, ако има такава).
  - Преценете дали (част от) изградената мрежа/устройства могат да се използват.

Мрежови услуги

- Идентифицирайте видовете и обемите трафик, които трябва да се пренасят.
- Уточнете нивото на критичност на услугите, за да можете да планирате адекватни решения за виока надеждност.
- Обърнете внимание на особености като интеграция с други системи (например автентикация на безжичен достъп или отдалечен достъп от активна директория), multicast трафик и др.

Вътрешна организация и политики

- Запознайте се със структурата на организацията и изискванията по отношение на достъп до мрежови услуги.
- Проверете правилата и политиките, които ще трябва да реализирате.
- Не забравяйте, че освен сървъри и потребители, мрежата ще осигурява услуги и за други системи - например система за сигурност, контрол на достъп, видеонаблюдение...

Йерархичен модел

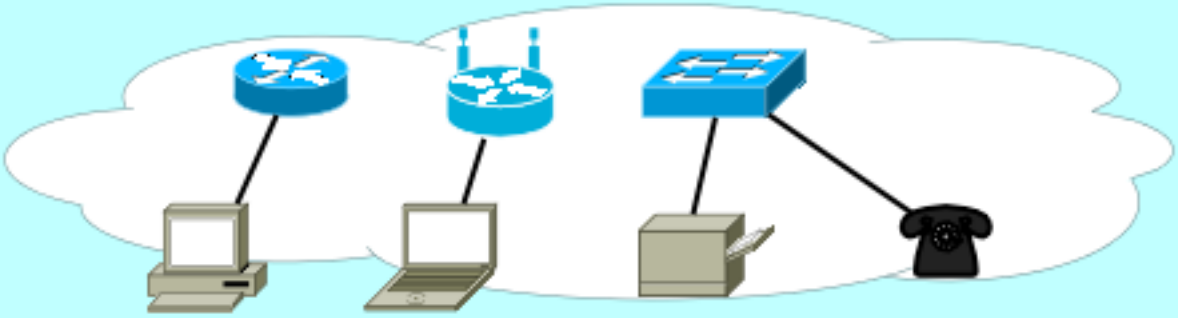
- Често подхода при реализация на корпоративни мрежи следва трислоен модел с обособени:
  - Слой за достъп (Access)
  - Разпределителен слой (Distribution)
  - Ядро (Core)
- При по-малки мрежи разпределителния слой и ядрото са обединени.

Йерархичен модел

Ядро
(Core)

Разпределителен
слой
(Distribution)

Слой за достъп
(Access)



Слой за достъп

- Устройствата тук осигуряват свързването на крайни устройства в мрежата. Обикновено поддържат OSI Layer2 (при някои имплементации Layer3) функционалност, не са резервирани и водеща при избора е цена на порт (свързан клиент). Такива са:
  - Комутатори (switch-ове) или маршрутизатори (рутери), към които са свързани крайни устройства.
  - Безжични точки за достъп (AP).

Слой за достъп

- При планиране на комутатори от слоя за достъп, обърнете внимание на:
  - Необходимия брой портове (оставяйте и запас).
  - Необходимост от поддръжка на PoE и необходимия стандарт.
  - При резервирана топология може да имате нужда от поддръжка на (R)STP.
  - Ако е необходимо увеличаване на надеждността - възможност за 2 захранвания.

Слой за достъп

- За увеличаване на капацитет може да имате нужда от поддръжка на Link Aggregation.
- За имплементиране на защити може да имате нужда от DHCP snooping, различни видове port security и/или ACL.
- Може да ви е необходима поддръжка на QoS.
- За оптимизация при Multicast ви е необходима поддръжка на IGMP snooping.

Разпределителен слой

- Устройствата тук осигуряват мрежови услуги към слоя за достъп съгласно приложените политики:
  - Тук се извършва маршрутизацията.
  - Тук се филтрира трафика.
  - Тук се прилага QoS.

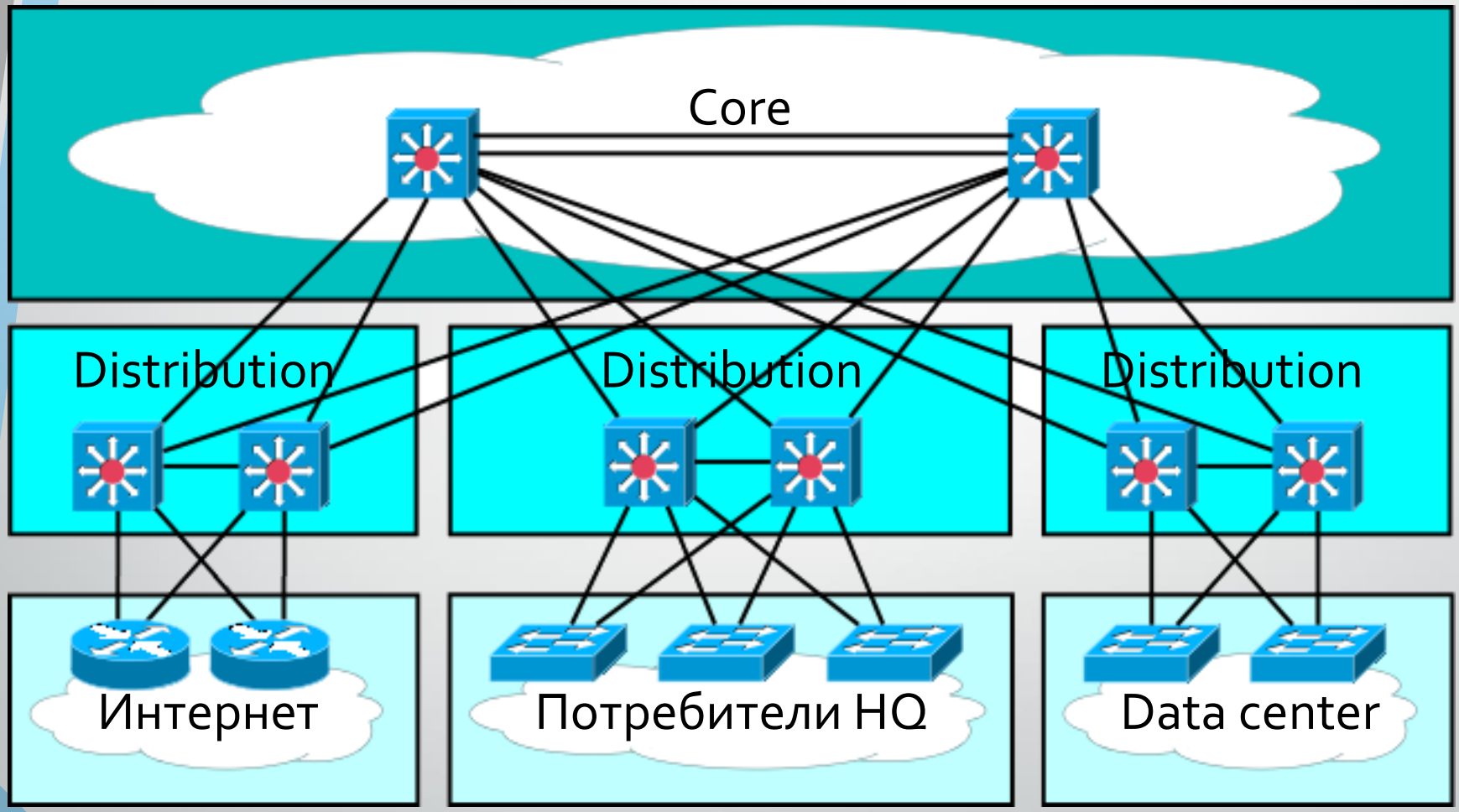
Разпределителен слой

- Планирайте висока надеждност, като използвате:
  - Дублирани връзки към разпределителния слой и ядрото
  - Дублирани шлюзове (gateway) за крайните устройства (чрез VRRP)
  - Устройства с дублирано захранване

Ядро

- Осъществява връзка между отделните възли на разпределителния слой.
- Изисква максимално висока надеждност.
- Поради големия обем трафик за максимална ефективност тук не се планират филтриране и QoS, единствено маршрутизация.

Обща топология трислоен модел

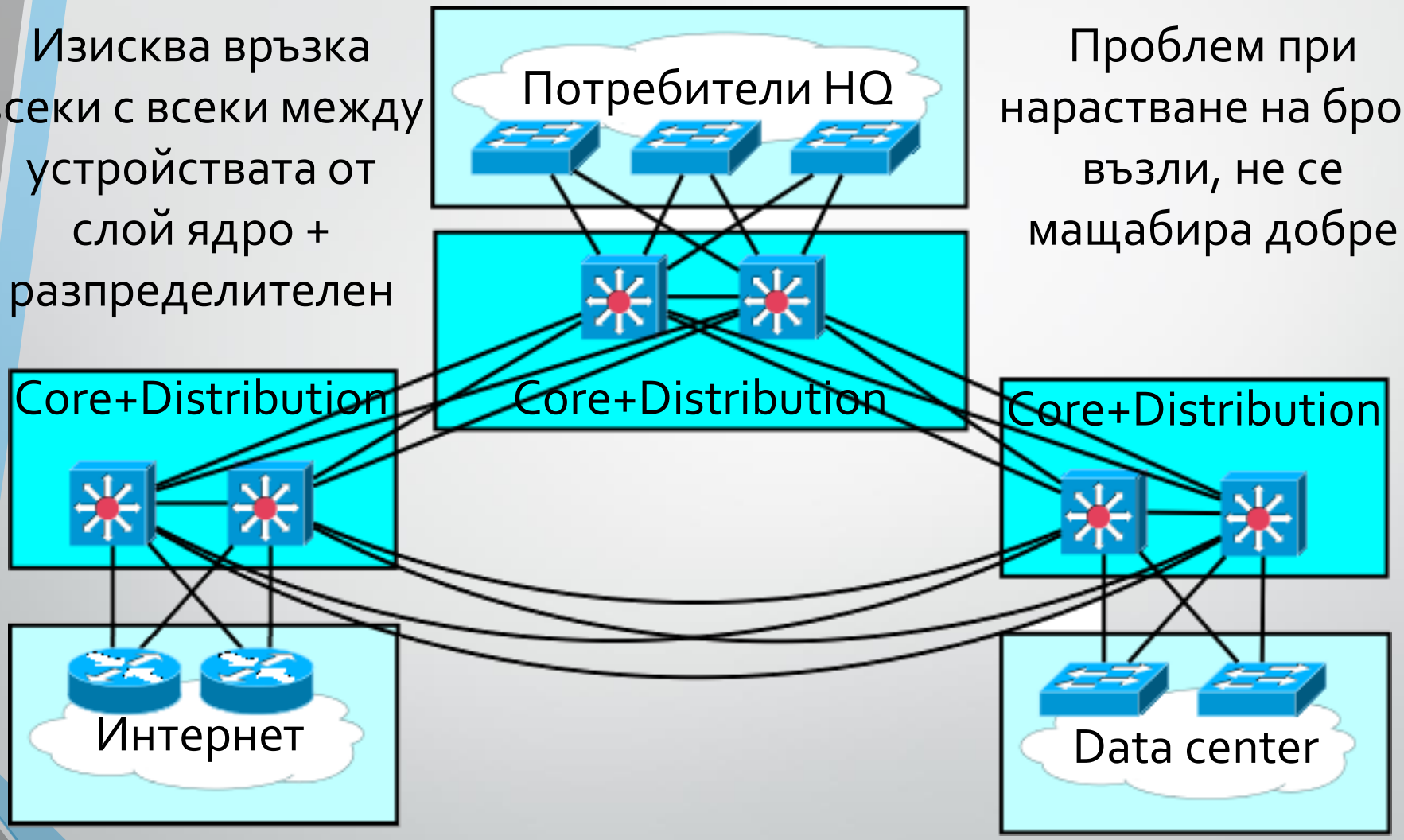


Основи на проектирането на корпоративни мрежи, Петър Димитров

Обща топология двуслоен модел

Изисква връзка всеки с всеки между устройствата от слой ядро + разпределителен

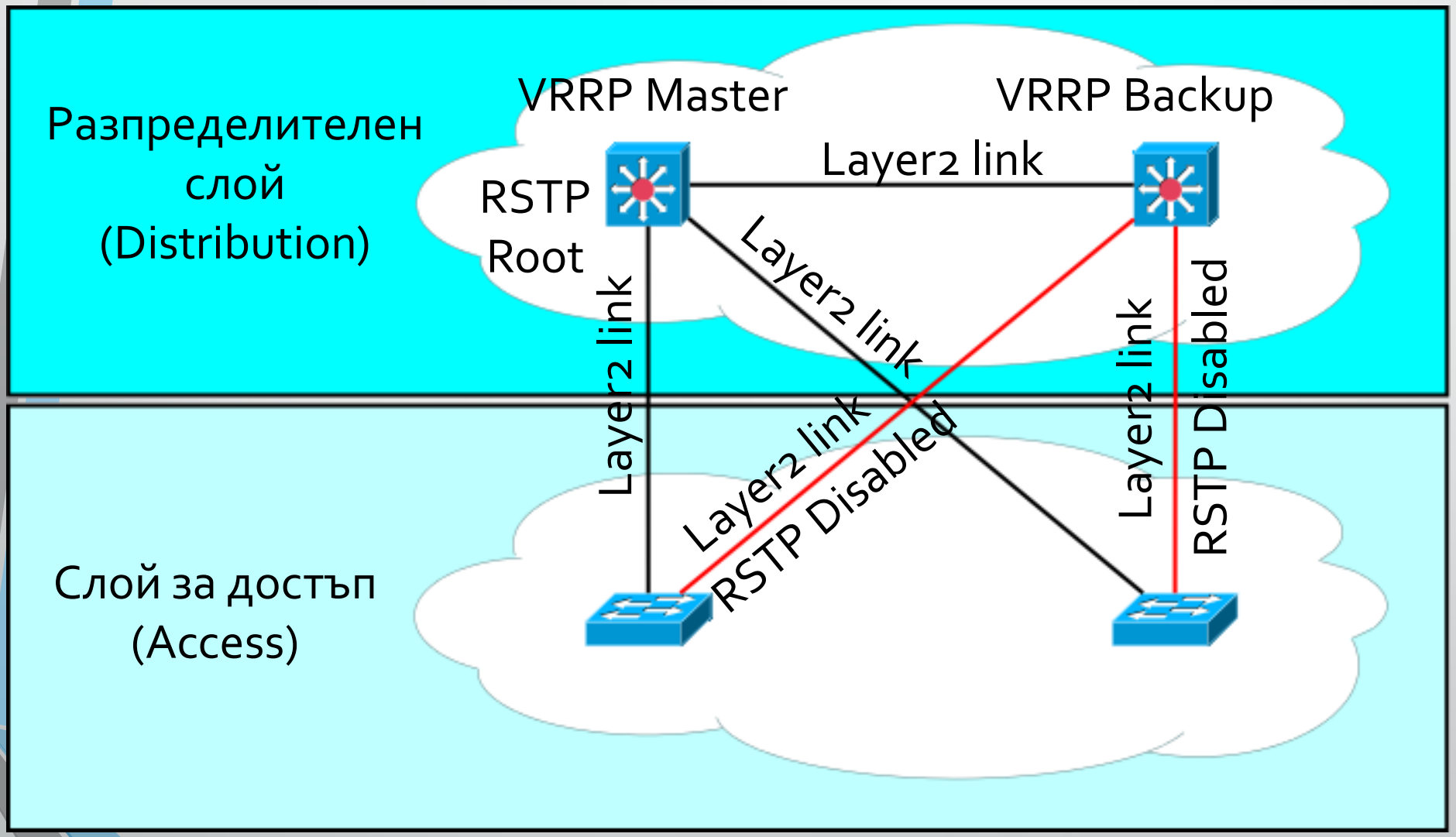
Проблем при нарастване на броя възли, не се мащабира добре



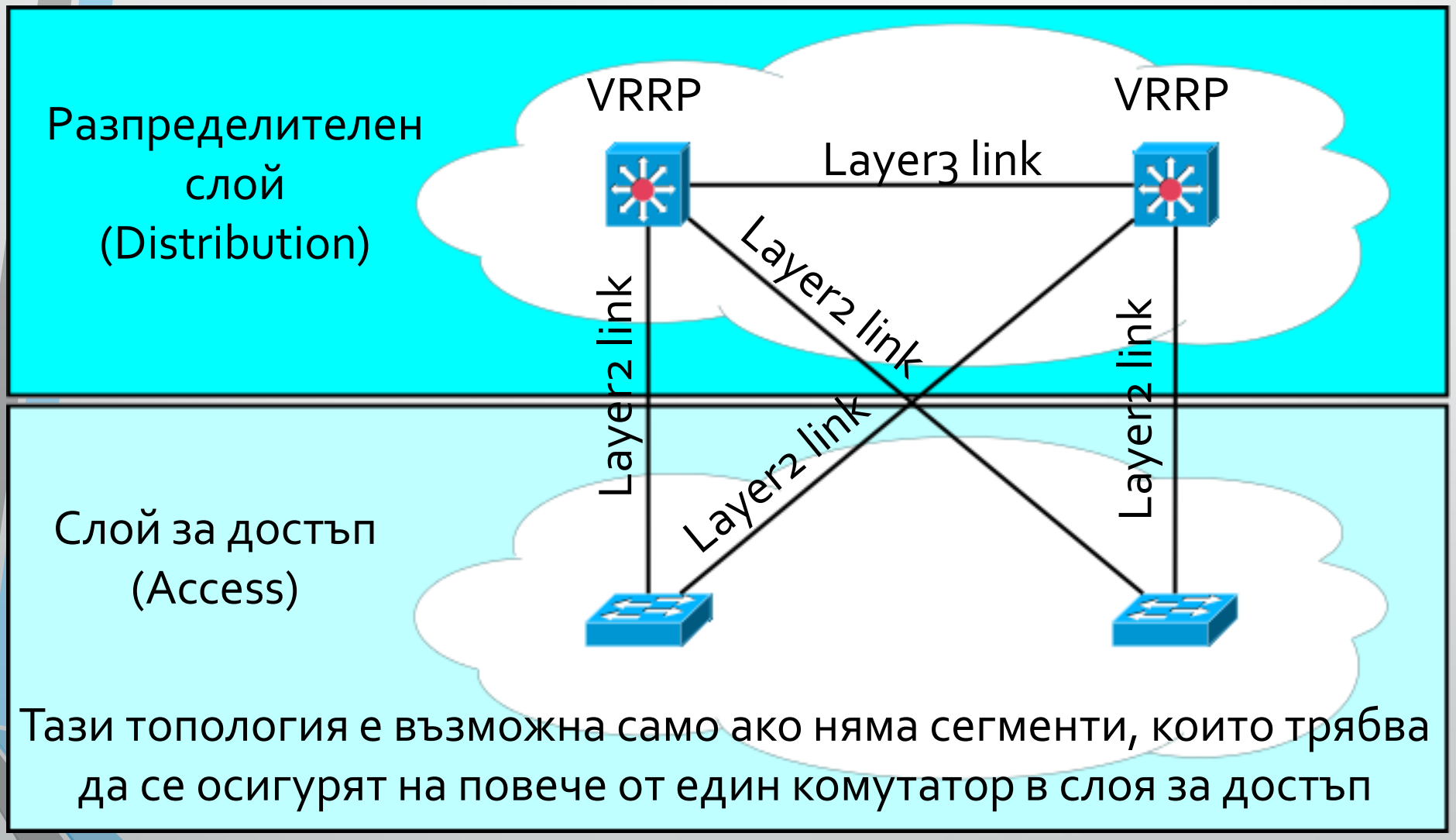
Връзки между слоевете/топология

- За изграждане на резервирани връзки могат да се използват различни топологии и протоколи:
  - За резервиране на Layer2 могат да се използват RSTP и някои режими на Bonding
  - За резервиране на Layer3 могат да се използват OSPF и/или статична маршрутизация и други помощни средства
  - За резервиране на шлюз (gateway) за крайните устройства може да се използва VRRP

Примерна топология с RSTP



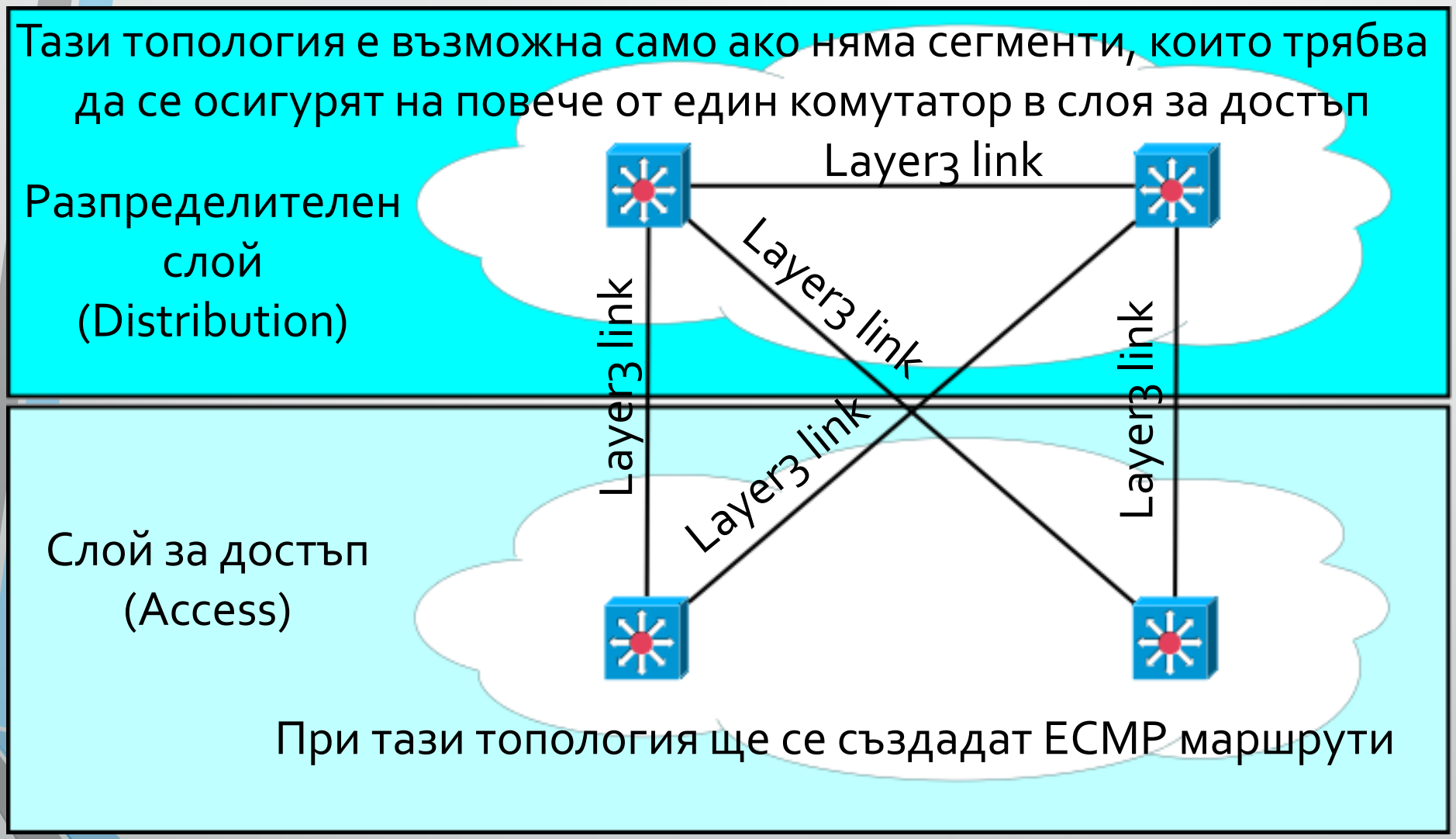
Примерна топология без RSTP



Тази топология е възможна само ако няма сегменти, които трябва да се осигурят на повече от един комутатор в слоя за достъп

Примерна топология с маршрутизация

Тази топология е възможна само ако няма сегменти, които трябва да се осигурят на повече от един комутатор в слоя за достъп



При тази топология ще се създадат ECMP маршрути

Сегментиране на мрежата

- Съобразно обхвата/размера на мрежата и вътрешна организация и политики, разделете мрежата на сегменти, като:
  - Планирате отделни сегменти за различните услуги, например VoIP, потребители, видеонаблюдение и т.н. Така ще улесните прилагането на политики за сигурност, имплементацията на QoS и ще ограничите влиянието на възникнали инциденти.

Сегментиране на мрежата

- Не пренасяйте даден сегмент между отдалечени офиси, планирайте отделни сегменти. Например вместо да осигурите един сегмент за IP телефони във всички офиси на фирмата, осигурете отделен сегмент във всеки офис. В идеалния случай даже в рамките на една сграда не планирайте сегмент, който да се достъпва от различни комутатори в слоя за достъп (в практиката рядко е възможно, но има предимства).

Сегментиране на мрежата

- Добрите практики са да нямате сегменти с повече от 250 устройства и да изолирате на ниво точка за достъп (AP) комуникацията между безжични клиенти. По възможност разделете сегментите за жичен и безжичен достъп.

IP адресиране

- Създаването на добра IP адресна схема е основна част от правилното проектиране на корпоративни мрежи.
- Без добро планиране за IP адресите не е възможно обобщаване на маршрути, затруднява се филтрирането, както и NAT.
- Разумната адресна схема улеснява поддръжката и диагностиката на мрежата.

Обобщаване на маршрути

- Намалява работата на динамичните маршрутизиращи протоколи:
  - По-малко натоварване на маршрутизаторите.
  - По-бърза реакция на промени.
  - По-малко промени в маршрутната информация като цяло.
- Улеснява диагностиката и проследяването на работата на мрежата.

IP адресиране и адресни листи

- Улеснява се описването на мрежи в адресни листи и правила, което улеснява:
  - Конфигурацията на филтрири
  - Конфигурацията на QoS
  - Конфигурацията на NAT

Планиране на адреси

- Не избирайте произволни пространства, използвайте лесна логика, като включите например:
  - Физическа локация - идентификатор на офис, или номер на шкаф или устройство
  - Логическо приложение - лесен и полезен подход е включването на vlan id в IP адресното пространство

Например ако даден офис в Плевен е с вътрешнофирмен идентификатор 32 и за сегмента с IP телефоните се използва vlan-id=107, може да се предвиди пространство 10.32.107.0/24 за този сегмент.

Планиране на адреси

- Планирайте адресни пространства с 50% излишък на адреси спрямо текущите нужди.
- Не забравяйте да пердвидите /30 адресните пространства, които ще използвате в съответната локация за връзки между устройства.
- Вземете под внимание нуждите от адресни пространства за VPN-и.

QoS

- Общия капацитет на връзките на крайните устройства към слоя за достъп надхвърля многократно капацитета на връзките от слоя за достъп към разпределителния слой, както и връзките от разпределителния слой към ядрото са с по-малък капацитет от общия за разпределителния слой.

QoS

- Капацитета на връзките между отделните офиси, към външни мрежи и Интернет също е по-малък от вътрешните капацитети в разпределителния слой и ядрото.
- Това може да доведе до ситуации, в които поради недостатъчен капацитет се изхвърлят (или забавят твърде много) данни.
- Решението е имплементиране на QoS.

QoS

- Разпознавайте вида трафик максимално близо до точката на възникване.
- Осигурете достатъчно гарантирани ресурси за критичните приложения.
- Имплементирайте подходящи опашки навсякъде, където имате промяна на капацитет (възможно получаване на повече данни, от колкото могат да се предават за единица време).

Управление и наблюдение на мрежата

- Важна част от мрежата са системите за нейното управление и наблюдение. Осигурете:
  - Съхранение на журнали (log-ове).
  - Наблюдение на параметрите на мрежовите устройства (Monitoring).
  - Наблюдение на трафика чрез ipfix/netflow.

Изграждане и поддръжка

- След като проекта е готов, тествайте в лабораторна или реална среда преди да го реализирате.
- Важно е изграждането и поддръжката да се извършват от квалифициран персонал.
- Винаги поддържайте документацията актуална!

Благодаря за вниманието!