Нов български университет

Проектиране на корпоративни мрежи

Част IV
Свързване на слоя за достъп с разпределителния слой на мрежата. Инфраструктурни услуги

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, април 2015

Съдържание

Този доклад е част от поредицата доклади посветени на изграждането на високо достъпни големи корпоративни мрежи. В него са разгледани главно два въпроса:

- С какви варианти разполагаме за свързване на слоя за достъп с разпределителния слой на мрежата и
- Как да осигурим поддръжката на инфраструктурните услуги.

1. Свързване на слоя за достъп с разпределителния слой на мрежата.

Когато разсъждаваме върху въпроса как да изградим връзката между слоя за достъп и разпределителния слой на мрежата трябва да имаме предвид, че разполагаме с няколко възможни модела.

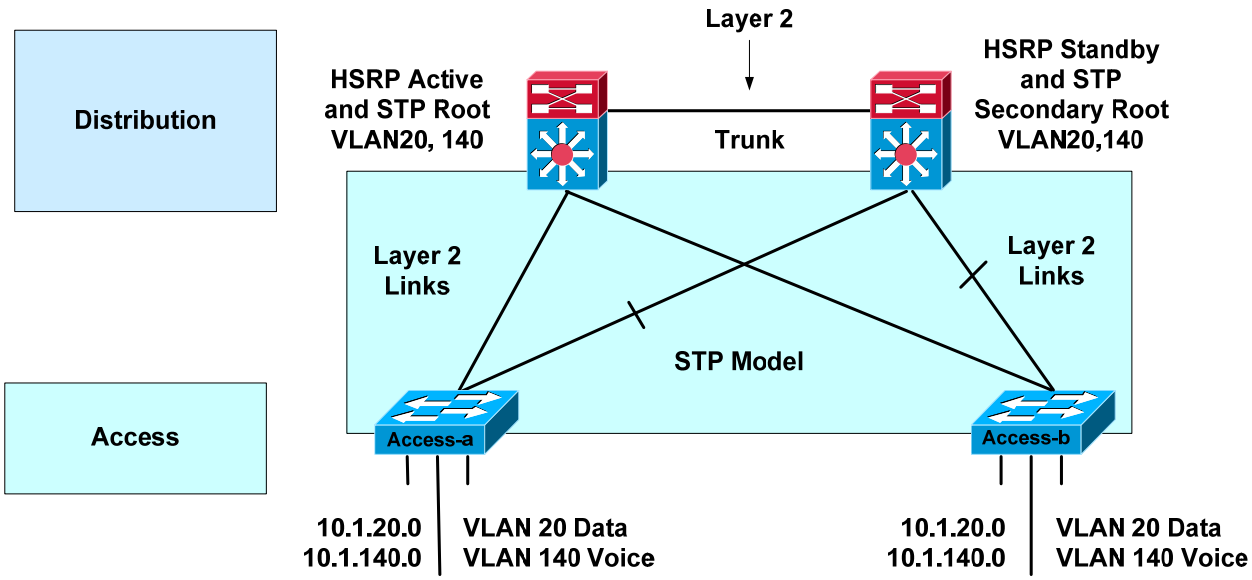
1.1 Модели на свързване

В този раздел последователно ще разгледаме различните архитектури на свързване в една корпоративна мрежа съгласно нейния йерархичен модел [1].

1.1.1 Използване на връзки от слой 2 за достъп към комутаторите в разпределителния слой

1.1.1.1 Връзки от слой 2 между комутаторите в разпределителния слой. STP модел

Ако в корпоративната мрежа трябва да се поддържат виртуални локални мрежи (VLAN), които се разпростират в няколко комутатора в слоя за достъп, подходящият модел трябва да използва връзки от слой 2 за свързване на комутаторите от разпределителния слой. Този дизайн е показан на Фигура 1. Той е значително по-усложнен в сравнение със свързването на комутаторите в разпределителния слой с връзки от слой 3. В тази схема задължително трябва да използваме STP протокола и да разгледаме неговата сходимост и възстановяването на мрежата при повреда във връзките от слоя за достъп към разпределителния слой.



Фигура 1 Свързване на комутаторите в разпределителния слой с връзки от слой 2

Тази, в известен смисъл неоптимална схема, може значително да се подобри, ако се водим от следните препоръки:

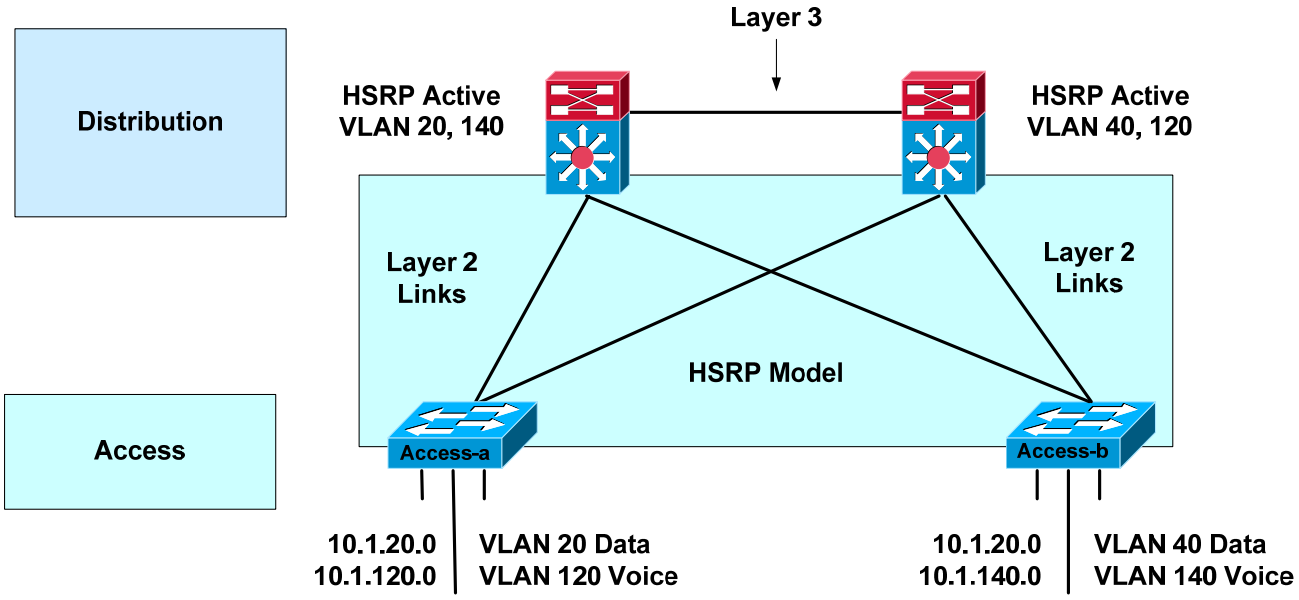
- Като протокол STP винаги използвайте неговата ускорена версия RSTP. В Cisco среда това е версията RPVST+, която представлява едно подобрение на RSTP използващо PVST+. Този протокол осигурява отделен екземпляр на 802.1W за всяка VLAN. Отделният екземпляр поддържа PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, и loop guard [2]. (RPVST+ е известен също и като PVRST+.)

- Създайте магистрална връзка (trunk) от слой 2 между двата комутатора на разпределителния слой за да избегнете неочаквани пътища на трафика и появата на множество различни събития свързани със сходимостта на протокола.

- Ако решите да използвате балансиране на натоварването за отделните VLAN по възходящите връзки, то не забравяйте да осигурите коренния мост на STP и основния шлюз на HSRP да се намират в един и същи комутатор на разпределителния слой, както е показано на Фигура 1. Това се прави с цел да се избягнат транзитните връзки и трафикът да преминава през няколко възела до шлюза по подразбиране [3] .

1.1.1.2 Връзки от слой 3 между комутаторите в разпределителния слой. HSRP модел

На Фигура 2 е показан модел при който се използват връзки от слой 3 между комутаторите в разпределителния слой. Като протокол за резервиране на първия скок [3] тук е възприет HSRP.



Фигура 2 Връзки от слой 3 между комутаторите в разпределителния слой (с HSRP)

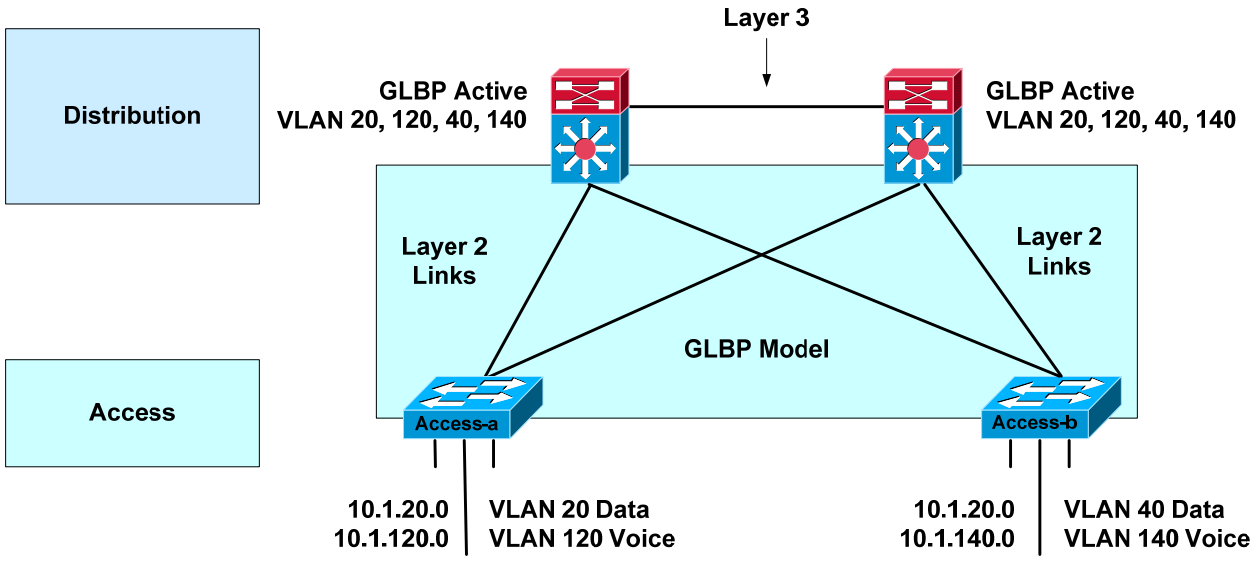
При тази доказана с течение на времето топология не съществува VLAN която да се разпростира в повече от един комутатор на слоя за достъп. Подмрежата всъщност е една VLAN, която се намира в един комутатор. Коренният мост на всяка VLAN съвпада с активния HSRP комутатор. От гледна точка на протокола STP и двете възходящи връзки са в режим на препредаване. Единствените неща, които засягат сходимостта при повреда са определяне на шлюза по подразбиране и избора на обратен път в разпределителния слой.

Този препоръчителен дизайн осигурява най-висока достъпност. При него връзката в разпределителния слой се изисква за обобщаване на маршрути. Препоръчителната

практика е номера на VLAN в слой 2 да съответства на подмрежата в слой 3 с цел по-лесно им управление.

1.1.1.3 Връзки от слой 3 между комутаторите в разпределителния слой. GLBP модел

Както е показано на Фигура 3, протоколът GLBP също може да се използва за резервиране на първия скок когато използваме връзки от слой 3 между комутаторите в разпределителния слой.

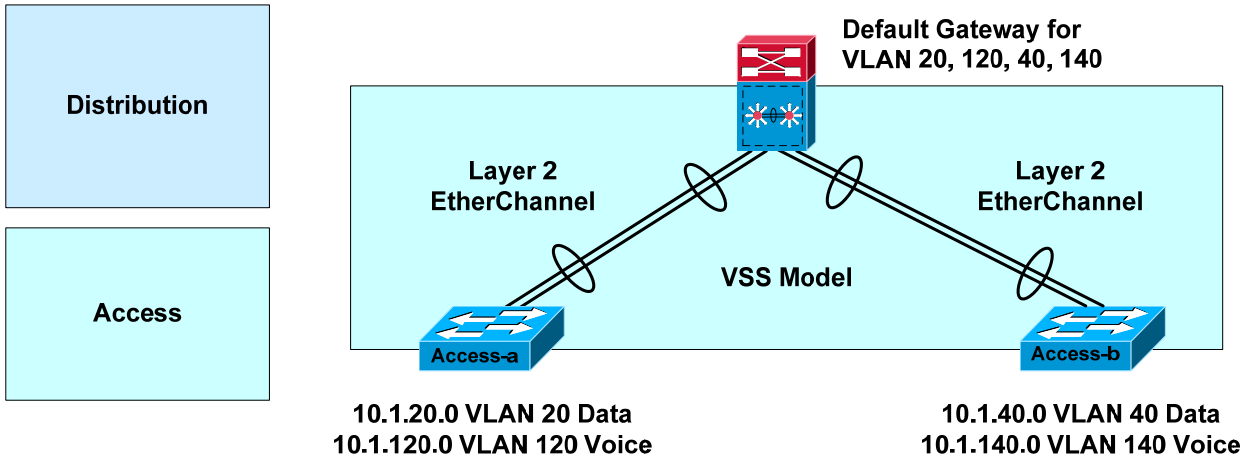


Фигура 3 Връзки от слой 3 между комутаторите в разпределителния слой (с GLBP)

GLBP позволява пълното използване на възходящите връзки от слоя за достъп. Въпреки това, понеже отговорът на ARP е случаен, то тази схема е по-малко детерминирана отколкото схемата с HSRP. Връзката между комутаторите в разпределителния слой, също както и при другата схема, е необходима за обобщаването на маршрутите. Понеже няма VLAN, която да се разпростира в повече от един комутатор за достъп, не се изисква сходимост на STP при повреда и възстановяване на възходящите връзки.

1.1.1.4 L3 комутатор с VSS възможности в разпределителния слой

Можем да използваме виртуална комутираща система (virtual switching system - VSS) за да изградим логическа топология тип „звезда” за достъп към разпределителния слой. При това целим да запазим пълна физическа редундантност. Тази схема е представена на Фигура 4.



Фигура 4 VSS модел на свързване

Разполагането на VSS в разпределителния слой значително опростява дизайна на връзките между слоя за достъп и разпределителния слой. VSS свежда топологията до логическа звезда, в която естествено няма затворени контури. От гледна точка на STP по всички връзки се предава потребителски трафик, а самият протокол STP не играе никаква роля при преконфигуриране на мрежата. Ако някой от комутаторите в разпределителния слой се повреди или връзките между слоя за достъп и разпределителния слой се прекъснат, това ще засегне само една от връзките между отделните шасита (MEC) [3]. Трафикът ще продължи да се препредава по останалата връзка на EtherChannel.

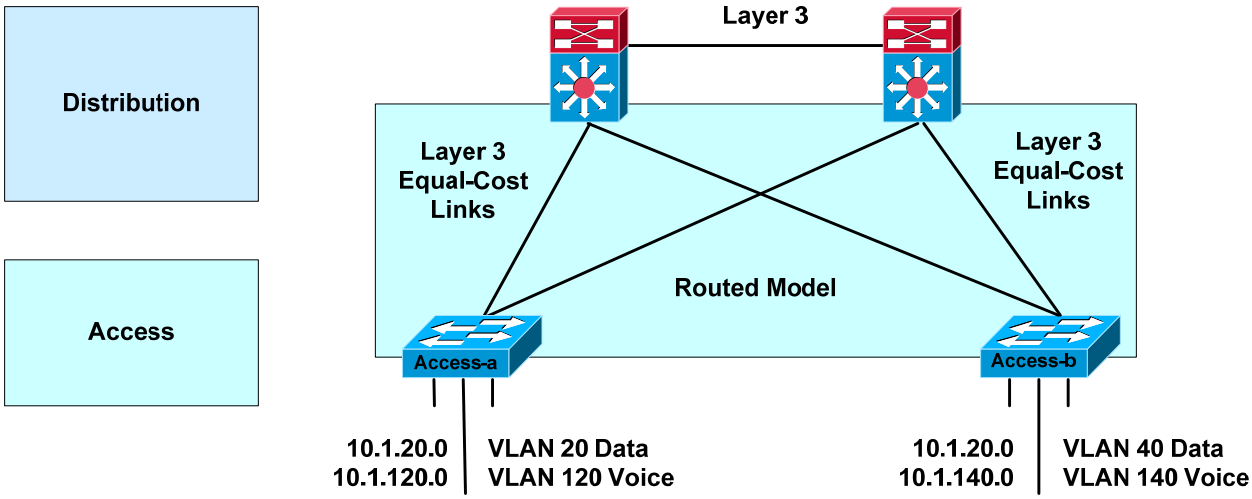
VSS свежда границата между слой 2 и слой 3 до едно логическо устройство. Това елиминира необходимостта от FHRP протокол. Само един маршрутизатор препредава трафика от VLAN в слоя за достъп към ядрото на мрежата. Високата достъпност на този единствен маршрутизатор се гарантира от механизмите за висока достъпност, които са вградени във VSS.

При този дизайн балансирането на натоварването между слоя за достъп и разпределителния слой не се основава на механизма използван в FHRP протокола. По-скоро тук се използва метода за балансиране използван в EtherChannel. Този метод позволява всички връзки от слоя за достъп към разпределителния слой да бъдат изцяло използвани.

Този дизайн позволява също дадена VLAN да се разпростира в множество комутатори на слоя за достъп, без това да оказва никакво влияние върху сходимостта. Да отбележим все пак, че съществуват определени ограничения за VSS дизайна. VSS комутаторите винаги се разполагат по двойки. Няма възможност да се добави трети комутатор към VSS системата с цел да се увеличи достъпността.

1.1.2 Използване на връзки от слой 3 за достъп към комутаторите в разпределителния слой

На Фигура 5 е показан дизайн, при който връзките от слой 3 стигат чак до слоя за достъп. Той осигурява най-бързата възможна сходимост на мрежата.



Фигура 5 Връзки от слой 3 между комутаторите в слоя за достъп и в разпределителния слой

С използването на маршрутизиращ протокол по тези връзки, като например добре настроен EIRGP, могат да се постигнат по-добри резултати за сходимост в сравнение с моделите които разчитат на STP да разреши събитията за сходимост. С маршрутизиращ протокол по тези връзки се постига дори по-добра сходимост, отколкото с изпитания дизайн преместващ границата между слой 2 и слой 3 в разпределителния слой. Този дизайн по-

лесно се имплементира отколкото да конфигурираме връзки от слой 2 в разпределителния слой, тъй като не е необходимо STP да се приведе в съответствие с HSRP или GLBP.

Тази схема поддържа връзки от слой 3 с равна цена между всички мрежови комутатори. Не е необходимо да конфигурирате HSRP или GLBP, тъй като комутаторът за достъп извършва маршрутизирането. Понеже този комутатор е многослоен комутатор, той служи и като шлюз по подразбиране за крайните потребители.

VLAN не могат да се разпростират в различните комутатори за достъп при този дизайн. Времето за сходимост, необходимо за пренасочване на трафика при повреда на връзка от слоя за достъп към разпределителния слой е под 200 ms в сравнение с 900 ms, когато границата между слой 2 и слой 3 е в разпределителния слой. Трафикът в обратна посока също се нормализира за време под 200 ms когато използваме например EIGRP.

Тъй като както при EIGRP, така и при OSPF, натоварването се разпределя по пътища с равни разходи (equal-cost paths), този дизайн осигурява сходимост на преходните процеси подобна на тази при GLBP. Около 50% от хостовете не са засегнати от преходния процес, тъй като техният трафик не преминава през повредените връзка или възел. Въпреки това се появяват някои допълнителни усложнения свързани с IP адресирането и разделянето на подмрежи, при което се губи определена гъвкавост.

Маршрутизация в слоя за достъп не се използва широко при корпоративните мрежи. Тя може да бъде забранена поради противоречие със съществуващата архитектура, заради високите цени на многослойните комутатори или по изрични изисквания на някои приложения и услуги.

1.1.2.1 Препоръки за използване на EIGRP

Когато използваме EIGRP за маршрутизиращ протокол в слоя за достъп при подходящи настройки може да се постигне сходимост на възстановяване на мрежата под 200 ms. Оптимизиране за бърза сходимост може да се постигне като се придържаме към следните правила:

- Ограничете обхвата на заявките към един съсед.

- Използвайте обобщаване на информацията от разпределителния слой към ядрото. Това става по същия начин, както ако границата между слой 2 и слой 3 се намираше в разпределителния слой. С обобщаването се ограничава въздействието на повреда на връзка за достъп, тъй като се спират запитванията на EIGRP да преминават през ядрото на мрежата. Когато в разпределителния слой се извършва обобщаване към ядрото, запитванията се ограничават само до един скок напред от комутаторите в разпределителния слой, а това води до намаляване на времето за сходимост на EIGRP.

- Конфигурирайте всички комутатори от слоя за достъп като EIGRP крайни възли (stub nodes), така че устройствата за достъп да не бъдат запитвани от комутаторите в разпределителния слой за маршрути. Крайните възли на EIGRP не са транзитни възли, и следователно не участват при EIGRP запитванията. Когато един възел в разпределителния слой научи с помощта на hello пакетите, че разговаря с краен възел, той не изпраща запитвания към този възел.

- Контролирайте разпространението на маршрути като използвате списъци (distribution lists). Комутаторите в слоя за достъп имат нужда само от маршрут по подразбиране към комутаторите в разпределителния слой. Следователно за всички интерфейси на комутаторите в разпределителния слой, които са свързани със слоя за достъп, могат

да се създадат изходящи списъци. Използването на такива списъци води до намаление на използваната памет и до оптимизиране на работата на слоя за достъп.

- Задайте на hello и dead таймерите стойности в съотношение 1 към 3 като вторичен механизъм за ускоряване на сходимостта. Повреда във връзка или възел би трябвало да предизвика определени събития от процеса за сходимост. Такава настройка на таймерите ще ви предпази от леки повреди, при която физическите връзки остават активни, но обработката на маршрутите е спряна.

Един пример на фрагмент от EIGRP оптимизирана конфигурация е показан по-долу:

```
interface GigabitEthernet1/1 ip hello-interval eigrp 100 2 ip hold-time
eigrp 100 6
router eigrp 100 eigrp stub connected
```

1.1.2.2 Препоръки за използване на OSPF

Когато използваме OSPF като маршрутизиращ протокол, при подходяща настройка, също може да се постигне сходимост на възстановяването на мрежата под 200 ms.

При OSPF обобщаването и ограничаването на диаметъра на разпространение на LSA рекламиранията се постига с използването на гранични маршрутизатори на област (Area Border Router - ABR). Използвайте следните правила за да контролирате боя на маршрутите и на маршрутизаторите във всяка област:

- Конфигурирайте всеки комутатор в слоя за достъп в отделна OSPF област от вида totally stubby. Комутаторите в разпределителния слой стават ABR, като техните интерфейси към ядрото са връзки с област 0, Не разпростирайте област 0 до комутаторите за достъп, тъй като те не се използват като транзитни области в корпоративната мрежа. При такова конфигуриране LSA рекламиранията са изолирани в комутатора от слоя за достъп и не се предават по-нататък от разпределителния слой.

- Настройте OSPF таймерите hello, dead-interval, SPF и LSA throttle като вторичен механизъм за подобряване на сходимостта. Понеже в корпоративната среда процесорните ресурси не са така ограничени както в глобалната мрежа, OSPF таймерите могат безопасно да бъдат настроени както е показано във фрагмента от конфигурация представен тук:

```
interface GigabitEthernet1/1 ip ospf dead-interval minimal
hello-multiplier 4
router ospf 100 area 120 stub no-summary timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000 timers lsa arrival 80
```

1.2 Възможни проблеми при проектирането

В следващите раздели ще разгледаме някои проблеми, които се появяват при определяне на мястото на границата между слой 2 и слой 3 в корпоративната мрежа.

1.2.1 Последователно свързване на комутаторите от слоя за достъп

Ако свържете последователно (daisy chain) няколко комутатора с фиксирана конфигурация в слоя за достъп на мрежата, вие рискувате да се появят черни дупки при повреда на връзка или възел.

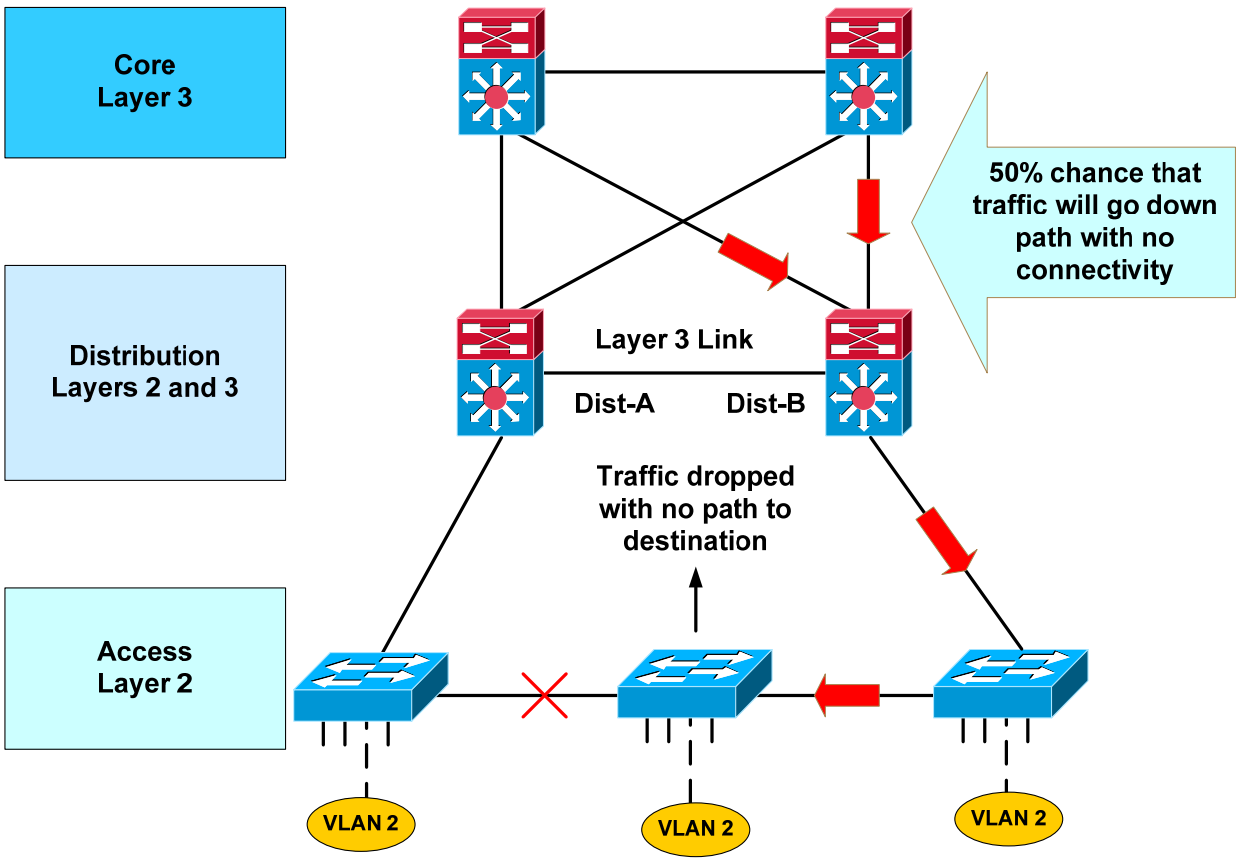
В топологията представена на Фигура 6, преди повредата няма блокирани връзки от STP или RSTP, така че и двете възходящи връзки са достъпни и по тях активно се изпраща и получава трафик. И двата разпределителни възела могат да препредават обратен трафик от останалата част на мрежата към устройствата свързани към комутаторите в слоя за достъп.

При повреда на връзка или възел в средата на веригата (или на стека) трябва да се разгледат два случая: какво става с изходящия трафик и какво става с обратния трафик.

В първия случай изчакващият в готовност (вторичният) HSRP възел става активен (тъй като е изгубил връзката с първичния HSRP възел) и започва да препредава изходящия трафик на устройствата, които все още са свързани с него. Първичният HSRP възел остава активен и също препредава изходящ трафик от устройствата намиращи се в неговата половина на стека. Въпреки че това не е оптимална ситуация, тя не е вредна от гледна точка на изходящия трафик.

Проблемът е във втория случай. 50% от обратния трафик е вероятно да попадне в комутатора от разпределителния слой, който няма физическа връзка с половината от устройствата за които трафика е предназначен. Този трафик, когато пристигне в грешния комутатор, бива отстраняван. Решението на този проблем в тази конфигурация е да се осигури алтернативна свързаност през стека, като се използва кабел свързващ върха с дъното на стека. Тази връзка трябва да се направи много внимателно, така че да се осигури едно подходящо поведение на STP в слоя за достъп.

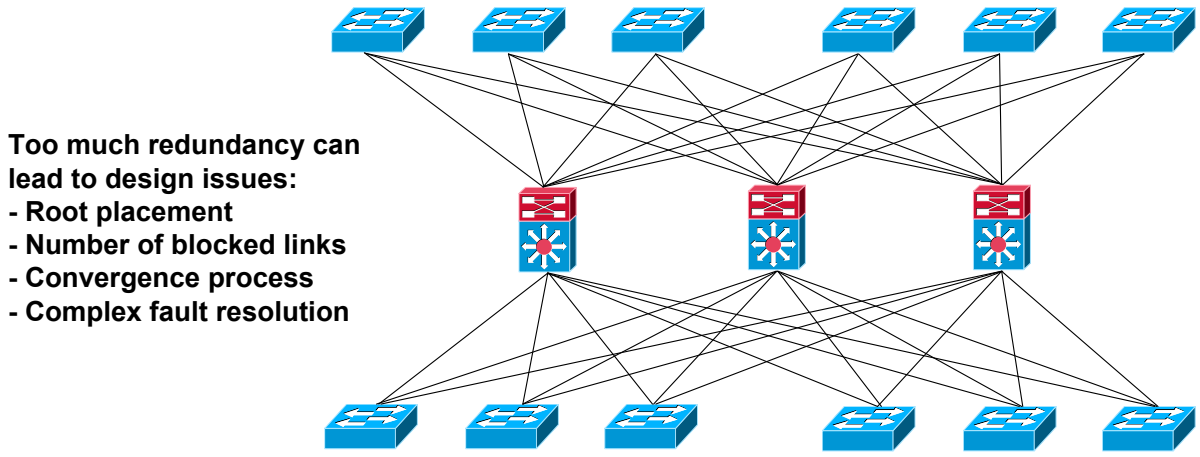
Алтернативата на това е да се използва връзка от слой 2 между комутаторите в разпределителния слой.



Фигура 6 Комутатори в слоя за достъп свързани последователно (daisy chain)

1.2.2 Твърде много резервиране

Имайте предвид, че е добре да се използват резервни връзки, но при използването на повече резервни връзки не е задължително да е по-добре. На Фигура 7 е добавен трети комутатор в разпределителния слой.



Фигура 7 Твърде много резервираност

Този комутатор добавя ненужна сложност на проекта и с него неминуемо възникват следните въпроси:

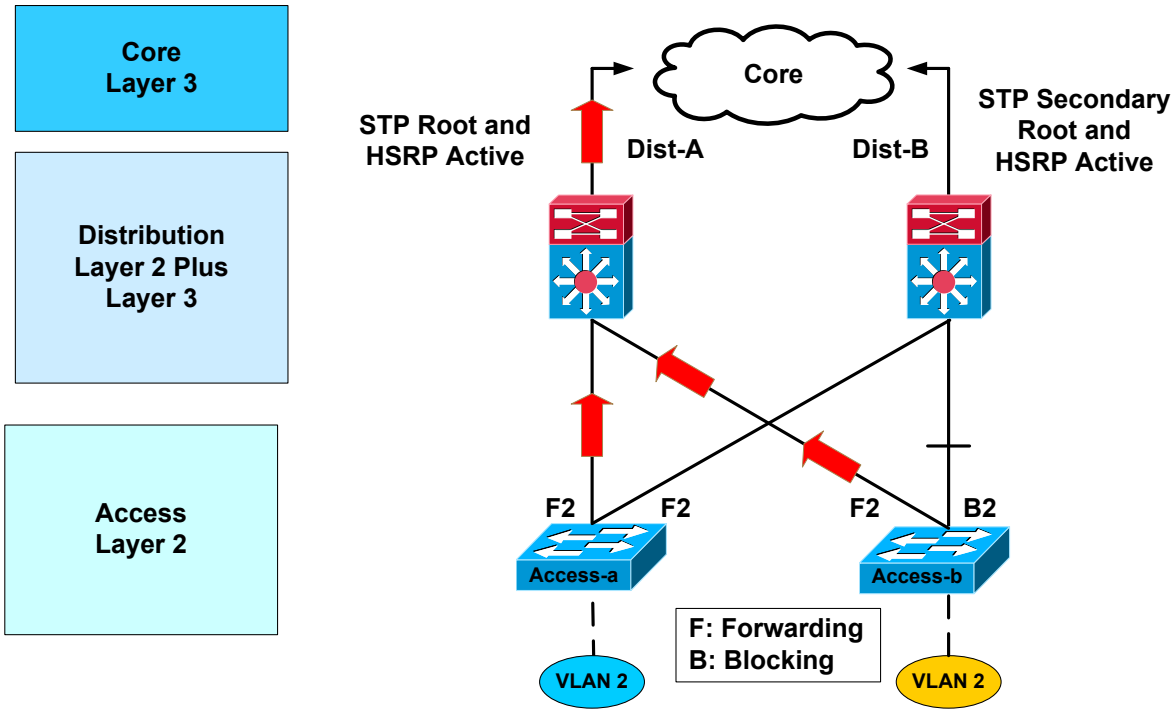
- Къде трябва да бъде поставен коренния комутатор? При този дизайн съвсем не е лесно да се определи неговото местоположение.
- Кои връзки трябва да бъдат блокирани? Много трудно е да се определи колко порта ще бъдат в блокирано състояние.
- Какви са изводите за STP и RSTP сходимостта? Сходимостта на възстановяването на мрежата определено не е детерминирана.
- Когато нещата се объркат, как ще намерите източника на проблема? Откриването и отстраняването на повреди в такава топология много трудно.

1.2.3 Твърде малко резервиране

При повечето конструкции се изискват резервни връзки между комутаторите в разпределителния слой.

На Фигура 8 е показана схема при която на VLAN се разпростира в няколко комутатора за достъп. Без връзката от слой 2 между комутаторите в разпределителния слой схемата представлява затворен контур във формата на осмица. Едната възходяща връзка за достъп ще бъде блокирана. Пакетите hello на HSRP се обменят транзитно през комутаторите в слоя за достъп.

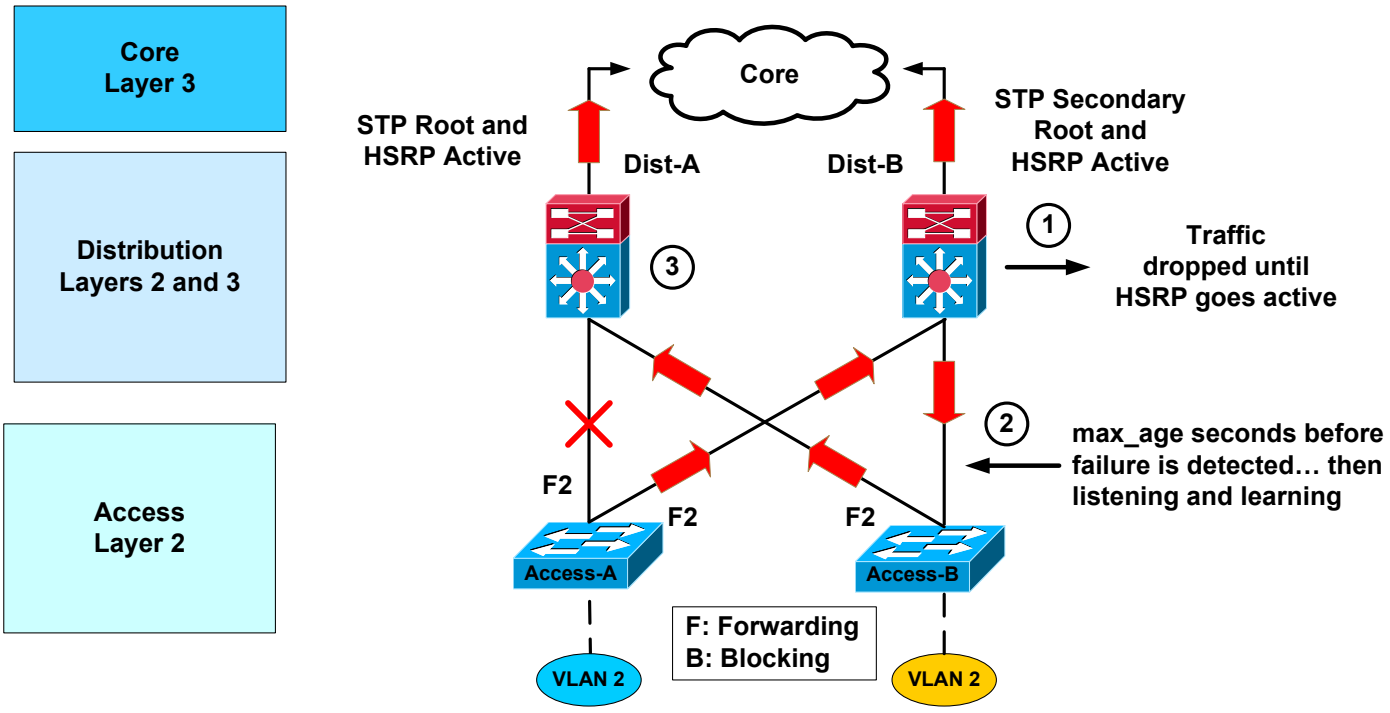
Първоначално трафикът се предава от двата комутатора в слоя за достъп към разпределителния комутатор Dist-A, който е коренен за STP и първичен или активен възел на HSRP за VLAN 2. Въпреки това, този дизайн се влияе от множество събития свързани със сходимостта при единична мрежова повреда и се явява като черна дупка за трафика.



Фигура 8 Твърде малко резервираност

1.2.3.1 Влияние на повредата върху възходящия трафик

На фигура 9 е разгледан случая когато имаме повреда във възходяща връзка и комутаторите в разпределителния слой не са директно свързани.



Фигура 9 Влияние на повредата върху възходящия трафик

При повреда във връзката между комутаторите Access-A и Dist-A се появяват три събития свързани със сходимостта:

1. Комутаторът Access-A изпраща трафик по активната си възходяща връзка към комутатор Dist-B за достъп към своя шлюз по подразбиране. Този трафик се отхвърля от Dist-B, тъй като този комутатор първоначално няма път към първичния или активен HSRP възел в Dist-A, понеже този път е блокиран от STP. Трафикът се отхвърля,

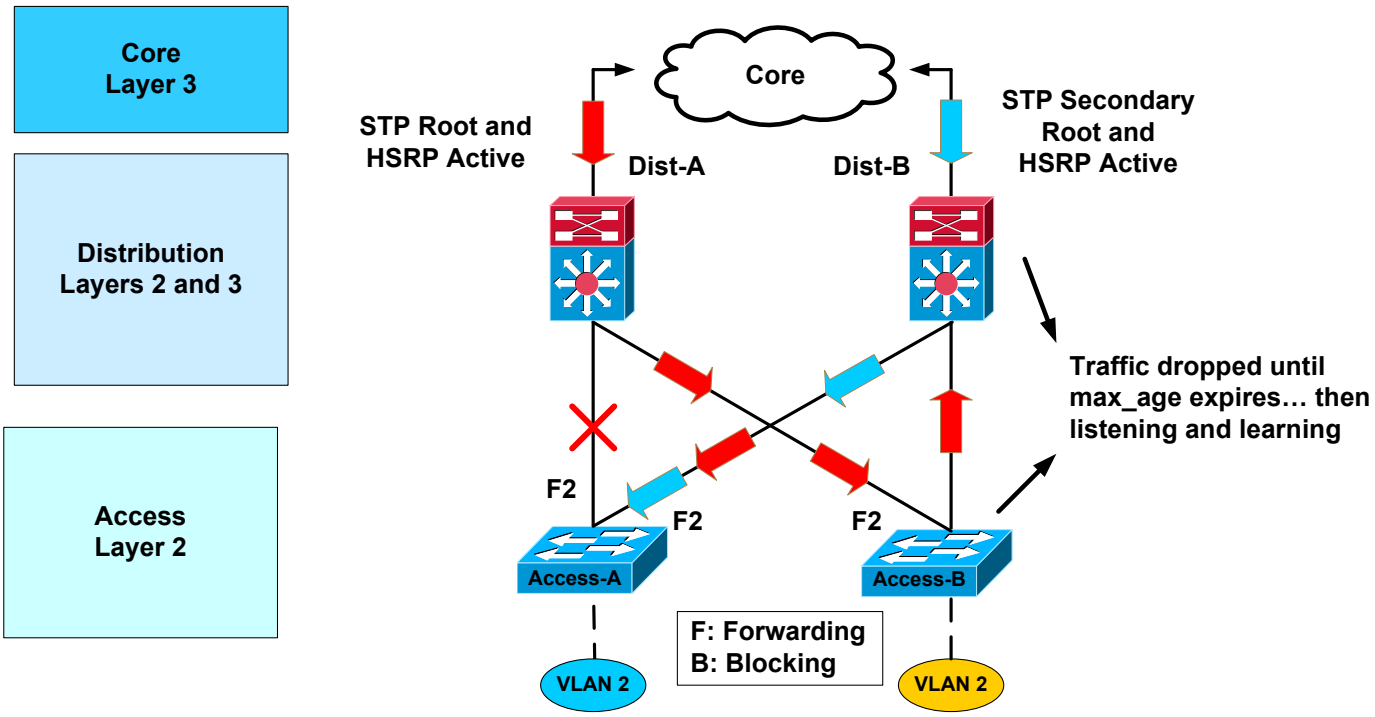
докато резервният HSRP възел не започне да функционира като шлюз по подразбиране следствие на това, че не получава пакети hello от Dist-A. Да отбележим, че с използването на агресивни HSRP таймери можете да сведете този период на загуба на трафик до около 900 ms.

2. Индиректната повреда се открива в крайна сметка от комутатор Access-B след изтичане на таймера *max_age* и Access-B преустановява блокирането на възходящата връзка към Dist-B. Когато използваме стандартен протокол STP, времето за преминаване в състояние на препредаване на порта е 50 секунди. Ако разрешим функцията BackboneFast и протокол PVST+, това време може да бъде намалено до 30 секунди, а с RSTP да се сведе до 1 секунда.

3. След осъществяване на сходимост на STP или RSTP, комутаторите в разпределителния слой възстановяват своите HSRP взаимоотношения и Dist-A (първоначалният HSRP възел) се възстановява. Тук имаме ново събитие свързано със сходимостта. Неочакваният страничен ефект е, че трафикът от комутатора Access-A преминава през комутатора Access-B за да достигне своя шлюз по подразбиране. Сега връзката между Access-B и Dist-B става транзитна връзка за трафика на Access-A. По възходящата връзка между комутаторите Access-B и Dist-A преминава трафика и на двата комутатора от слоя за достъп.

1.2.3.2 Влияние на повредата върху обратния трафик

Тъй като в разпределителния слой на Фигура 10 се извършва маршрутизиране с балансиране на натоварването по пътища с равни разходи, до 50% от обратния трафик ще пристигне в комутатора Dist-A и трябва да се препрати към Access-B. Комутаторът Access-B отхвърля този трафик докато връзката към Dist-B не започне да го препредава. Сходимостта при тази индиректна повреда ще отнеме 50 секунди. Ако използваме PVST+ с функцията UplinkFast това време е между 3 и 5 секунди, а при RSTP продължава да бъде 1 секунда. След като се установи връзката между Access-B и Dist-B, тя се използва като транзитна връзка за обратния трафик към комутатора Access-A.



Фигура 10 Влияние на повредата върху обратния трафик

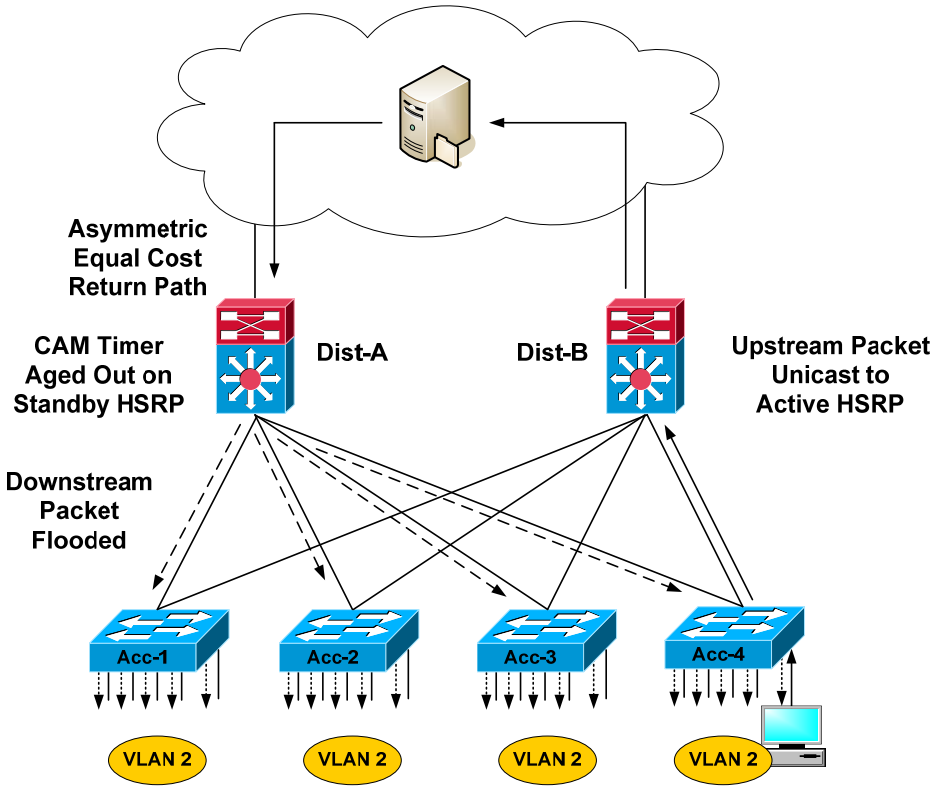
Тези значителни прекъсвания на трафика могат да повлияят на изпълнението на критични приложения, като предаване на гласов или видео трафик.

Управлението на трафика и планирането на капацитета на връзките в двете посоки е трудно и сложно и трябва да се предвиди преминаването на трафика най-малко през един допълнителен комутатор в слоя за достъп. Изводът е, че ако VLAN се разпростира в повече от един комутатор в слоя за достъп, то трябва да предвидим допълнителна връзка от слой 2 между комутаторите в разпределителния слой (или в слоя за достъп).

1.2.4 Асиметрично маршрутизиране (Unicast Flooding)

Когато една VLAN се разпростира в повече комутатори от слоя за достъп се получава ситуация на асиметрично маршрутизиране, тъй като използваме балансиране на натоварването по пътища с равни разходи между разпределителния слой и ядрото на мрежата. До 50% от обратния трафик в този случай пристига в резервния HSRP, VRRP или в алтернативния, непрепредаващ GLBP възел. Ако времето на един вход в таблицата CAM (content-addressable memory) изтече преди да се възстанови от протокола ARP за крайния потребител, то трафикът трябва да бъде изпратен до всички комутатори и крайни потребители за дадената VLAN.

На Фигура 11 времето на вход в CAM таблицата на резервния HSRP маршрутизатор изтича, тъй като таймерите по подразбиране на ARP протокола са настроени за 4 часа, а таймерите на CAM са с интервал от 5 минути. Таймерът в CAM изтича, понеже няма изпратен трафик от крайния потребител към резервния HSRP възел след като потребителят е използвал ARP за да определи своя шлюз по подразбиране. Когато таймерът за даден вход в CAM таблицата изтече, то дадения вход се изтрива от таблицата и резервният HSRP възел трябва да изпрати обратния трафик до всички негови портове на тази VLAN. По-голямата част от комутаторите в слоя за достъп нямат вход в CAM за MAC адреса на получателя и те ще изпратят обратния трафик бродкастно до всички портове на общата VLAN. Това наводнение от трафик оказва значително влияние върху производителността на свързаните крайни станции, тъй като те получават голямо количество трафик, който не е предназначен за тях.



Фигура 11 Асиметрично маршрутизиране

1.2.5 Избягване на асиметричното маршрутизиране

Горният вид асиметрично маршрутизиране може лесно да бъде избягнато, като не позволим VLAN да се разпростира в множество комутатори от слоя за достъп.

Наводненията с unicast пакети не са проблем когато VLAN се ограничава до един комутатор. В този случай трафика се разпространява само до един VLAN интерфейс на комутатора в разпределителния слой. Това е интерфейса по който нормално трафика се изпраща към съответния комутатор в слоя за достъп. Този пък комутатор в слоя за достъп има в своята таблица CAM вход за дадения хост, тъй като той е директно свързан към него. Следователно трафикът се изпраща само на този единствен хост, а останалите станции не са засегнати от такова наводнение с такъв вид трафик.

Ако все пак ви се наложи да използвате топология при която една VLAN се разпростира в повече от един комутатор, препоръчителното решение е да заобиколите проблема като настроите таймера на ARP така, че неговата стойност да е равна или по-малка от aging таймера на CAM. Малката стойност на ARP таймера принуждава резервният HSRP възел да използва ARP преди да изтече CAM таймера и MAC входа да бъде изтрит. Това премахва възможността от поява на наводнение следствие на асиметричното маршрутизиране на обратния трафик. Можете също да разсъждавате и върху промяна на маршрутизиращите метрики така, че да премахнете пътищата с равни разходи.

2. Поддръжка на инфраструктурните услуги

В този раздел е направен преглед на съображенията за поддръжка на инфраструктурните услуги във високо достъпните корпоративни мрежи. Разглеждат се въпросите на изграждане на единна мрежа поддържаща IP телефония. Описани са атрибутите на QoS и някои аспекти на функциите на Catalyst за вградена сигурност (Cisco Catalyst Integrated Security features).

2.1 IP телефонни услуги

IP телефонните услуги се поддържат във всеки слой на корпоративната мрежа. Те изискват висока достъпност, резервираност и бърза сходимост в цялата корпоративна мрежа. В мрежата трябва да се изпълняват QoS функциите. Реализирането на тази политика обикновено се възлага на разпределителния слой.

Въпреки това, понеже IP телефонните услуги се разпростират до границите на мрежата, тези услуги оказват влияние в най-голяма степен върху слоя за достъп. Този слой трябва да поддържа свързването на телефоните и тяхното откриване от мрежата, захранване на тези устройства, QoS функциите, включително тяхната класификация и график.

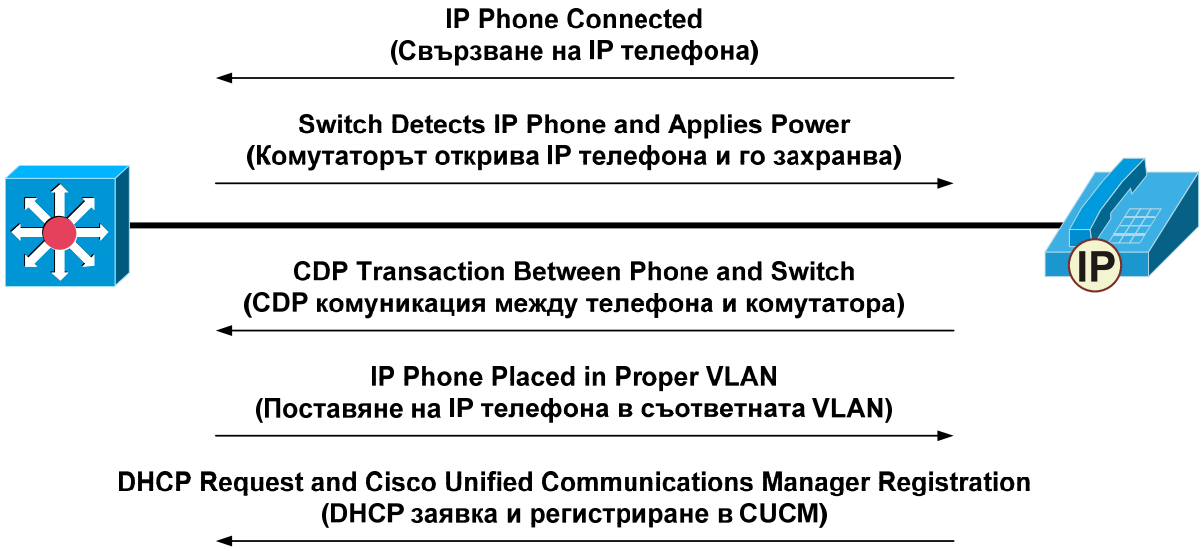
2.1.1 IP телефонията разширява границите на мрежата

Тъй като IP телефона представлява три портов комутатор, IP телефонните услуги всъщност разширяват границите на мрежата, както е показано на Фигура 12.

IP телефонът показан на тази фигура включва комутатор с три порта който се конфигурира заедно с комутатора в слоя за достъп от Мениджъра за унифицирани комуникации на Cisco (Cisco Unified Communications Manager - CUCM). Тази програма извършва следните функции:

- Договаряне на захранването
- Конфигуриране на VLAN

- Синхронизация съгласно 802.1X
- Конфигуриране на QoS и
- Регистриране на DHCP и CUCM.



Фигура 12 IP телефонията разширява границата на мрежата

Когато един Cisco IP телефон се свързва към мрежата, комутаторите Catalyst откриват и интегрират този телефон в нея. Комутаторите захранват IP телефоните по метода PoE (Power over Ethernet) като използват свързващите кабели. Комутаторите поставят IP телефоните в съответната VLAN като използват услугите на 802.1X. Те също така поддържат QoS конфигурацията необходима за IP телефоните и осъществяват свързването с DHCP сървърите и CUCM системата за регистриране.

Методът PoE отразява способността на комутиращата LAN инфраструктура да подава захранване на крайните устройства по меден Ethernet кабел. За да се осъществи захранването на едно устройство по Ethernet кабел, трябва да бъдат решени няколко проблема: откриване на телефоните, доставката на захранването, управлението на това захранване, както и управлението на кабела и на честотната лента.

2.1.2 Изисквания на PoE

Има две PoE реализации и два начина да се подаде захранване на IP телефоните:

- Контролери на Cisco, които поддържат предварителния стандарт за PoE, IEEE 802.3af, и набор от устройства. Характерното тук е, че устройствата, които поддържат само IEEE 802.3af не могат да договарят и да получат захранване от оригиналните PoE контролери на Cisco.

- Устройства на Cisco, които използват двупосочния протокол за откриване на Cisco (Cisco Discovery Protocol - CDP) за да договорят точните изисквания за захранването. Такова договаряне оптимизира консумацията, като в комутатора се резервира само толкова мощност, колкото е необходима на даденото устройство.

По-ранните устройства на Cisco, изградени по предварителния PoE стандарт, първоначално получаваха 6.3 вата (W), след което допълнително договаряха изискванията за мощност като използваха CDP. Тези устройства използваха реле за да отразят специалния FastLink

импулс, използван за откриване на устройството. Устройствата базирани на IEEE 802.3af (също известни като 802.3at тип 1) първоначално получават мощност 12.95 W, а устройствата 802.3at тип 2 получават 25.5 W, освен ако устройството изпращащо мощността (power-sourcing equipment - PSE) открие захранваното устройството в списъка на конкретна класификация на захранвани устройства. PSE устройството по 802.3af изпраща напрежение в обхвата от −2.8 до −10 волта по кабела, след което очаква да види съпротивление от 25 KΩ в захранваното устройство.

Мощността по IEEE 802.3af може да бъде доставена, като се използва Ethernet порт с възможност за PoE, известен също като крайна PSE точка. При него за захранване се използват или активните кабели за предаване на данни, или резервната (свободна) усукана двойка. Ако не разполагаме с комутатор с такива възможности, за захранване можем да използваме устройство наречено midspan PSE. При някои от тези устройства се използват само свободните усукани двойки и следователно те не могат да служат за захранване по Ethernet на 1000BASE-T връзки.

2.1.3 Планиране и управление на захранването

Необходимо е да се извърши планиране на захранването, за да се определи кои устройства могат да се поддържат в момента и кои в бъдеще.

Комутаторите управляват мощността според това за което са проектирани, а не според това което използваме в момента. Мощността, която консумират устройствата, не е константна:

- Телефонът Cisco Unified IP Phone 7960G изисква захранване от 7 W когато звъни с максимална мощност на звука.

- Същият Cisco Unified IP Phone 7960G изисква 5 W когато е включен или изключен.

Захранването по PoE съгласно класификацията по подразбиране на IEEE 802.3af може значително да увеличи изискванията за мощност на PSE комутатора и на захранващата инфраструктура. За да се извърши PoE захранване по ефективен начин, комутаторите Catalyst на Cisco поддържат освен класификацията по IEEE 802.3af, така и системата Cisco Intelligent Power Management (Cisco IPM). Това дава възможност захранваното устройство и PSE да договарят с каква мощност е необходимо устройството да бъде захранено, а също така и как комутаторът с PSE възможности да разпределя мощността между отделните захранвани устройства. Тези способности на Cisco IPM позволяват ефективно и икономично управление на мощностите в рамките на комуникационния шкаф.

Управлението на захранването е сложна задача. То може да има значителни последици за всички захранвани устройства и контролери, за разпределението на енергията в комутатора, и накрая за изискванията за мощност към комуникационния шкаф. Захранването трябва така да се проектира, че да има на разположение достатъчно мощност за крайните устройства, както и за контролерите в комутатора. Дори когато PSE и захранваните устройства поддържат стандартна класификация, то нейните изисквания са в широки граници и може да се получи значителна загуба на енергия. Ако нямаме достатъчно мощност в комутатора, то системата за управление на неговото захранване започва да деактивира контролери.

Можете да използвате Cisco Power Calculator за да изчислите изискванията за мощност. Този калкулатор ви позволява да установите необходимата захранваща мощност за всяка конкретна конфигурация на PoE и вграден контролер. Калкулаторът изисква потребителско име и парола. Инструментът позволява да изберете различни варианти на конфигурируеми продукти, и той показва изходящия ток, мощността и системата за разсейване на топлината за всяка конкретна конфигурация.

2.1.4 Порт за достъп към много VLAN

В корпоративните мрежи концепцията на порт за достъп беше разширена до порт за достъп към много VLAN. Многофункционалните комутатори имат нов параметър за поддръжка на IP телефония, който превръща порта за достъп в порт за достъп към много VLAN (multi-VLAN access port). Този нов параметър се нарича допълнителна (auxiliary) VLAN. Всеки Ethernet порт на комутатора е свързан с две VLAN:

- Родна (native) VLAN за предаване на данни, която се идентифицира с идентификатора на порта (PVID).

- Допълнителна (auxiliary) VLAN за гласова услуга, която се идентифицира с идентификатора за глас (VVID).

По време на първоначалния CDP обмен на съобщения между телефона и комутатора от слоя за достъп, IP телефона се конфигурира с VVID. Той също получава своята QoS конфигурация. Гласовия трафик е отделен от данните и за него имаме различни граници на разпространение.

Пакетите с данни между комутатора за достъп и работните станции преминават по родната VLAN. Всички пакети които се появяват в родната VLAN в един IEEE 802.1Q порт се изпращат немаркирани от комутатора за достъп. Работните станции свързани към IP телефоните обикновено изпращат маркирани пакети.

Гласовите пакети се маркират от IP телефона съгласно CDP информацията получена от комутатора за достъп.

Да отбележим, че портовете за достъп към много VLAN не са магистрални (trunk) портове, дори когато хардуерът е конфигуриран като dot1q магистрала. Хардуерната конфигурация се използва за предаване на данни за повече от една VLAN, но портът продължава да се разглежда като порт за достъп който обслужва една родна VLAN и една допълнителна VLAN. За порта за достъп към много VLAN в комутатора за достъп можем да използваме командата *`switchport host`*.

Да отбележим, че комутаторът свързва и двете VLAN (native, auxiliary) към телефона. IP телефонът маркира трафика в допълнителната VLAN като модифицира битовете за приоритет в 802.1Q/p етикета да отговарят на CoS 5 (двоично 111).

2.1.5 Софтуерни телефони и VLAN

Когато използваме софтуерни телефони (soft phones) вместо хардуерни телефони (hard phones), това се отразява на реализацията на QoS и на политиките за сигурност на гласовия трафик.

Понеже софтуерният телефон е просто едно приложение стартирано в персоналния компютър, гласовият трафик се смесва с трафика на данните в родната VLAN към която персоналният компютър е присъединен. Тук нямаме маркиране по 802.1Q и 802.1P между персоналния компютър и комутатора. Това оказва влияние върху разработването и прилагането на политики за сигурност и QoS на гласовия трафик. Тъй като в този случай нямаме разделяне на трафика между глас и данни, то в политиките по сигурността трябва да използват характеристиките на трафика от горните слоеве. VLAN или подмрежата не могат за се използват за класифициране на трафика като глас или данни.

2.2 Някои съображения за QoS

Обикновено корпоративните мрежи се изграждат с презапасяване. Мрежата има няколко възможни точки на задръстване, където важният трафик може да бъде изхвърлен, ако не използваме QoS.

Повечето връзки в корпоративната мрежа не се използват пълноценно. В някои изследвания се доказва, че 95 процента от връзките на фирмения комплекс в слоя за достъп използват по-малко от 5% от капацитета си. Следователно се използва свръх абонамент (oversubscription).

Препоръката за свръх абонамент в слоя за достъп е да бъде 20:1, т.е. такова да бъде съотношението на броя портовете за достъп до мрежата към броя на портовете за връзка към разпределителния слой. При връзките от разпределителния слой към ядрото, това съотношение на портовете се препоръчва да е 4:1. Когато използвате такива съотношения на свръх абонамент, може понякога да се появят задръствания. В този случай трябва да използвате QoS. Ако задръстването на връзките се случва често, то проектът не разполага с достатъчна честотна лента по връзките нагоре (към ядрото) [3].

2.2.1 Препоръчителни практики за QoS

QoS помага да управляваме свръх абонамента и използването на връзки с различни скорости в проекта. По-долу са представени най-добрите практики за QoS:

- Да се осигури критичните приложения да не се влияят от връзките и от натрупването на съобщения в опашките.

- Да се използват политики за QoS в точките на агрегиране и на промяна на скоростта на връзките.

- Да се предвидят много опашки с конфигурируеми критерии за тяхното използване и ефективно да се планира QoS от край до край за всеки слой.

Интернет червеите и атаките от вида отказ на услуга (DoS) могат да блокират връзките дори в една високоскоростна мрежа. Политиките на QoS защитават трафика от аудио, видео и критични данни като прехвърлят заподозрения трафик в по-нисък клас на обслужване.

В точките, в които се извършва агрегиране и промяна на скоростта на връзките, трябва да се прилагат политики на QoS за да се подкрепи приоритетния трафик и да се управляват задръстванията. В корпоративните мрежи в LAN портовете се използват множество опашки с конфигурируеми критерии и графици.

2.2.2 Задръствания в опашките за предаване

Видът на задръстванията, които най-често се срещат в корпоративната мрежа, се нарича глад за опашки за предаване (transmit-queue starvation или Tx-queue starvation).

И при LAN и при WAN се получават задръствания в опашките за предаване:

- По време на прехода от LAN към WAN, маршрутизаторът трябва да намали скоростта на предаване от 10 или 100 Mbps в Ethernet до скоростта използвана във WAN. Когато това се извършва, маршрутизаторът трябва да постави пакетите в опашки и да приложи QoS за да осигури първо да бъде предаден приоритетния трафик. Глад за опашки за предаване се получава, когато входящите пакети пристигат по-бързо,

отколкото изходящите пакети се предават. Пакетите се записват в опашките, тъй като очакват да бъдат изпратени по по-бавните серийни връзки.

- Същите проблеми се получават и в LAN инфраструктурата на корпоративната мрежа, където скоростите на предаване от 10 Gbps или 1Gbps в ядрото или в дистрибутивния слой трябва да бъдат съгласувани със скоростите от 10 или 100 Mbps в слоя за достъп.

От тази гледна точка разликата между WAN маршрутизатора и комутатора в корпоративната мрежа е в броя на интерфейсите и свързаната с всеки един от тях памет. В комутаторите имаме заделена по-малко памет, следователно вероятността за отхвърляне на трафик заради глад от опашки за предаване е по-голяма.

2.2.3 Роля на QoS в корпоративната мрежа

Функциите на QoS се използват за приоритизиране на трафика съгласно неговата относителна важност и за да се осигури преференциална обработка като се използват техники за управление на задръстванията. Независимо от това, мрежата трябва да осигури адекватно ниво на обслужване за целия мрежов трафик, включително и на този с по-нисък приоритет, в нормални условия.

Необходимо е, също така, QoS да идентифицира и потенциално да накаже трафика, който е извън профила на обичайния трафик, като например генерирания от различни червеи и разпределени DoS атаки. Този трафик се поставя в дезактивиращ клас и се маркира с различен код за обслужване. В периоди на задръстване този клас е първият, който усеща глада за опашки за предаване и пакетите му биват отстранявани. Когато изискванията нараснат или капацитета се намали, останалите класове трафик също биват засегнати. Минималната цел на високо достъпната корпоративна мрежа е да осигури преминаването на високоскоростния аудио и видео трафик, както и данните на критично важните приложения. Техния трафик не трябва да бъде ограничаван по никакъв начин в случаите на мрежови задръствания.

2.2.4 Обсъждане на QoS дизайна

Дизайнът на QoS в корпоративната мрежа е преди всичко свързан с класифицирането, маркирането и използваната политика.

Опашките трябва да бъдат активирани във всеки възел, в който може да настъпи задръстване. Схемата за класифициране на трафика трябва да съответства на конфигурацията на опашките. Приложенията трябва да бъдат класифицирани и маркирани колкото е възможно по-близо до техния източник, веднага след като това е технически и административно осъществимо. Върху различния вид трафик трябва да се налага определена политика колкото е възможно по-близо да източника на този трафик.

Използването на различни опашки е единствения начин да се гарантира качеството на гласа и картината, както и да се защитят данните на критичните приложения или да се отстранят данните от необичайни източници:

- Пакетите с гласова информация трябва да бъдат насочени към хардуерната приоритетна опашка. Внедряването на VoIP изисква приоритетно обслужване на този трафик с гарантирана честотна лента. Опашката с най-висок приоритет обикновено е ограничена до 33% от капацитета на връзката.

- Най-малко 25% от честотната лента на връзката трябва да бъде заделена за класовете на обичайния трафик, който в същност е класът по подразбиране за

предаване на данни. При нормални обстоятелства мрежата трябва да осигури адекватно ниво на обслужване на този трафик.

- За трафика извън профила на обичайния трафик трябва да бъде заделена отделна опашка с нисък праг на задействане на механизма за отстраняване на пакетите. Приложенията, които са свързани с такъв клас, имат малък или никакъв принос за реализиране на целите на фирмата. Заделянето на минимална честотна лента за тази опашка позволява през нея почти да не преминават съобщения в период на задръстване, но тя все пак е достъпна когато имаме достатъчна честотна лента за целите на бизнеса, например в часовете, когато мрежата не е натоварена.

2.3 Характеристики на вградената в Catalyst сигурност

Функциите на системата за вградена сигурност в комутаторите Catalyst (Cisco Catalyst Integrated Security) засилват защитата на корпоративната мрежа. В тази система се използват следните интегрирани инструменти:

- Port security - Предотвратява атаки предизвикващи наводнения с MAC адреси.
- Подслушване на DHCP (DHCP snooping) - Предпазва от атаки срещу DHCP сървъра и комутатора.
- Динамичната ARP проверка (Dynamic ARP inspection) - Добавя сигурност към ARP като използва таблицата за подслушване на DHCP за да минимизира влиянието на такива действия като отравяне на ARP и имитационни (spoofing) атаки.
- IP source guard - Предпазва от използването на подправени (spoofing) IP адреси, като си служи с таблицата за подслушване на DHCP.

2.3.1 Port Security предотвратява атаки с MAC адреси

Атаките с MAC адреси се появяват, когато атакуващият изпраща наводнение от MAC адреси към комутатора с цел да запълни неговата CAM таблица. Когато CAM се запълни, комутаторът вече не може да следи за легитимност на адресите и започва да разпространява цялата информация по всички портове.

Функцията Port Security позволява на мрежовия администратор да ограничи MAC адресите за определен порт. Позволените MAC адреси за даден порт могат да бъдат или статично конфигурирани от администратора, или динамично да бъдат научени от комутатора. Нарушението на сигурността е налице, когато се прекрачи максимално допустимия брой MAC адреси за даден порт, или когато се забележи рамка с непозволен MAC адрес на източника в този порт. В този случай портът преминава в изключено състояние (shutdown) или се генерира съобщение на протокола SNMP от вида капан (trap). За порта могат да бъдат зададени и временни интервали за неактивност.

Когато се забележи нарушение на сигурността на порта, той може да предприеме три действия, в зависимост от това как е конфигуриран. Портът може да бъде блокиран (Shutdown), рамките просто да бъдат игнорирани (Protect), или рамките да бъдат игнорирани и броячът за нарушения да бъде увеличен (Restrict).

2.3.2 DHCP подслушване като защита от атаки срещу DHCP сървъра

Подслушването на DHCP може да се използва за защита срещу измамници и злонамерени действия срещу DHCP сървъра.

В някои случаи, един нарушител се опитва да се присъедини свой DHCP сървър към мрежата и да поеме тези функции в дадения сегмент. Това дава възможност на нарушителя да раздава фалшива DHCP информация за шлюза по подразбиране, за имената на домейн сървърите, които от своя страна насочват клиентите към машината на хакера. Тази заблуда позволява на хакера да поеме ролята на „човек в средата" ("man in the middle") и да получи достъп до секретна информация, като потребителски имена и пароли. Подслушването на DHCP може да предотврати това. Подслушването на DHCP е механизъм за сигурност на порт, който се използва за различаване на един ненадежден порт свързан с крайния потребител от един надежден порт свързан с DHCP сървър или друг комутатор.

Този механизъм се разрешава за всеки VLAN поотделно. Подслушването на DHCP позволява само авторизирани DHCP сървъри да отговарят на DHCP заявките и да разпространяват мрежова информация към клиентите. Той също дава възможност да поставите лимит на DHCP заявките от клиентските портове, като по този начин се намалява въздействието на DHCP DoS атаките от индивидуален клиент или порт за достъп.

2.3.3 Динамична ARP проверка защитава от ARP отравяне

При протокола ARP нямаме никакво удостоверяване (автентикация). Много лесно е злонамерен потребител да използва подправени (spoof) адреси с помощта на инструменти като ettercap, dsniff и arpspoof и да промени (отрови) ARP таблиците на други хостове от същата VLAN. При една типична атака, злонамереният потребител изпраща непоискани ARP отговори към други хостове в подмрежата със своя MAC адрес и своя IP адрес като шлюз по подразбиране. Пакетите предназначени за шлюза по подразбиране се изпращат от тези хостове с отровени ARP таблици към хакерската машина (където могат да бъдат подслушвани), или към недостъпен хост, който се използва за DoS атака. Отравянето на ARP води до различни „човек в средата" атаки, които са заплаха за сигурността в мрежата.

Динамичната ARP проверка помага за предотвратяване на атаки от вида „човек в средата", като не препредава непоисканите ARP отговори към другите портове в същата VLAN. Проверката прихваща всички ARP заявки и отговори от несигурните портове. Всеки прихванат пакет се проверява за валидни IP към MAC връзки, които се събират с DHCP подслушване. Отказаните ARP пакети или се отхвърлят или се регистрират в комутатора за целите на одита. Входящите ARP пакети в сигурните портове не се проверяват. Динамичната ARP проверка може също да ограничи броя на ARP заявките за даден клиентски порт с цел минимизиране на механизмите за сканиране на портовете.

2.3.4 IP Source Guard защитава от подменени IP адреси

IP source guard е уникална функция на операционната система на Cisco за комутаторите Catalyst която помага за намаляване на измамите с IP подменени адреси.

IP source guard предотвратява един злонамерен хост да атакува мрежата като отмъкне IP адреса на своя съсед. Тази функция за всеки порт филтрира IP трафика за присвоени IP адреси на източника. Тя динамично поддържа списък за контролиране на достъпа (ACL) за всеки порт на дадена VLAN. Този списък обвързва IP адреса и MAC адреса с порта. Списъкът се създава или чрез DHCP подслушване, или чрез статично конфигуриране. IP source guard обикновено се използва за несигурните портове на комутаторите в слоя за достъп.

2.3.5 Пример за конфигуриране на вградената в Catalyst сигурност

Този фрагмент от конфигурационна програма показва командите използвани за активиране на Catalyst Integrated Security:

```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fastethernet3/1
switchport port-security
switchport port-security max 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
ip verify source port-security
!
interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```

3. Литература

[1] Стоилов Емил, Проектиране на корпоративни мрежи. Част I Архитектура, Technical Report, Научен електронен архив на НБУ, 2014, http://eprints.nbu.bg/2219/

[2] Стоилов Емил, Проектиране на корпоративни мрежи. Част II Оптимизиране на слой 2, Technical Report, Научен електронен архив на НБУ, 2014, http://eprints.nbu.bg/2231/

[3] Стоилов Емил, Проектиране на корпоративни мрежи. Част III Препоръки за използване на VSS и EtherChannel, Technical Report, Научен електронен архив на НБУ, 2014, http://eprints.nbu.bg/2512/