Нов български университет

Проектиране на корпоративни мрежи

Част I
Архитектура

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, май 2014

Съдържание

1. Увод 3
2. Преглед на архитектурата на корпоративните мрежи 4
   2.1 Йерархичен модел 4
   2.2 Пример на йерархична мрежа 5
3. Разработени от Cisco архитектури за корпоративни мрежи 6
4. Интегриране на услугите и приложенията 9
   4.1 Мрежови услуги 10
   4.2 Мрежови приложения 11
   4.3 Модулност на архитектурите на корпоративните мрежи 12
5. Методология на проектирането 15
   5.1 Жизнен цикъл на мрежата 15
   5.2 Предимства на подхода на жизнения цикъл 17
   5.3 Използване на методологията за проектиране 19
      5.3.1 Идентифициране на изискванията на клиентите 19
      5.3.2 Характеризиране на съществуващата мрежа и на обектите 20
      5.3.3 Проектиране на топологията на мрежата и на отделните решения 21
      5.3.4 Разделяне на мрежата на отделни области 22
6. Литература 23

1. Увод

Този доклад е първият от серията доклади посветени на проектирането на корпоративни мрежи. В тях се разглеждат такива аспекти на проектирането като:

- Обща архитектура и методология на изграждането на мрежите
- Характерни особености на мрежите, изисквания за тяхната наличност и достъпност
- Топология на слой 2, използвани протоколи, конфигуриране и настройка
- Топология на слой 3, оптимизация на връзките
- Проектиране на границата между слоеве 2 и 3
- Поддържане на мрежовите услуги

В процеса на проектирането ще се опираме в голяма степен на методологията разработена от фирмата Cisco Systems Inc. Това не е случайно. Взети са предвид следните съображения:

- Фирмата е световен лидер в областта на мрежовите технологии.
- Документацията на нейните устройства и протоколи е много добре разработена и широко достъпна.
- Описаният процес на проектиране позволява използването на устройства и протоколи разработени от други фирми, т.е. в голяма степен той е универсален.

В този първи доклад е направен преглед на архитектурите срещани в корпоративните мрежи, дадени са предложения как тези архитектури да се използват в процеса на проектирането на мрежите, а също така е описана и методологията на Cisco състояща се от шест етапа: подготовка, планиране, проектиране, реализация, експлоатация и оптимизиране.

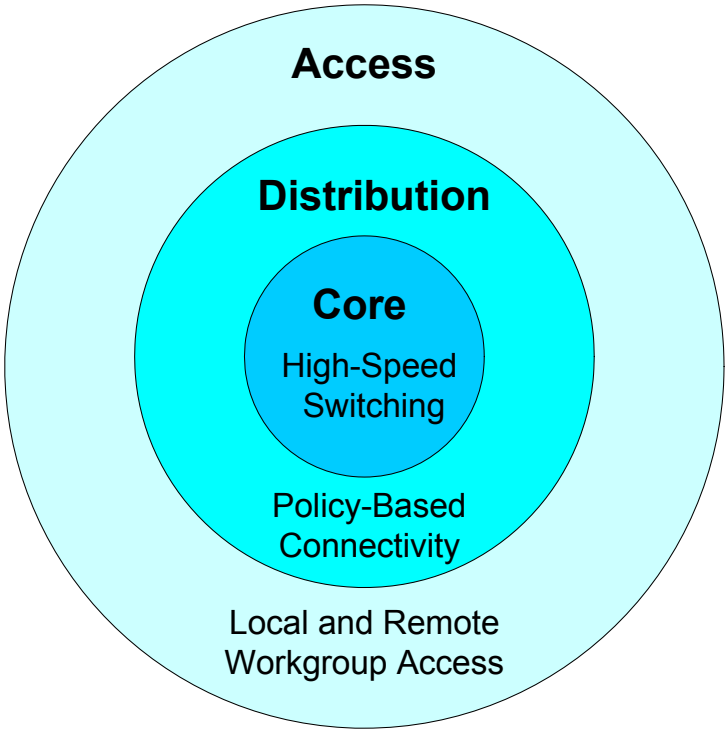
Архитектурата на корпоративната мрежа според Cisco е методология, която помага на мрежовите инженери да проектират стабилни инфраструктури за подпомагане на съвременните сложни бизнес приложения. Когато се прилага правилно, методологията може да служи за основа на изграждането на лесно мащабируеми мрежи, улесняващи както от тактическа, така и от стратегическа гледна точка прилагането на различни нововъзникващи бизнес приложения. Архитектурата включва не само проектиране и изпълнение на направените препоръки, но също така и принципи за наблюдение, измерване и документиране. Спазването на методологията осигурява пълен систематичен подход при проектирането и експлоатацията на мрежите.

2. Преглед на архитектурата на корпоративните мрежи

Богатото разнообразие от налични бизнес приложения, както и необходимостта от тяхното интегриране, е основния двигател за създаването на нови мрежови архитектури. В този раздел е представен един йерархически модел на компютърна мрежа. Разгледан е въпроса как в архитектурата на корпоративната мрежа са взети предвид новите тенденции в развитието на обкръжаващата фирмата среда, като например мобилността на работниците, сътрудничеството между отделите, както и виртуализацията на данните и компютрите. Описано е как мрежовите услуги могат да бъдат използвани за доставяне и съответно изпълнение на различни приложения и потребителски опит по корпоративната мрежа без граници (Borderless Network). Представено е също така и разделянето на архитектурата на отделни модули.

2.1 Йерархичен модел

В основите на архитектурата на Cisco лежи идеята за йерархична мрежа. Йерархичният модел включва освен локалната и глобална мрежи за данни на предприятието, също така и инфраструктурните модули на мрежата без граници, както и специализираните модули на мрежовата архитектура на Cisco. Фигура 1 показва отделните слоеве на този йерархичен модел.



Фигура 1 Слоеве в йерархичния модел

Йерархичният модел ни предлага един модулен поглед към мрежата, което ни позволява по-лесно да проектираме и изграждаме детерминирана мащабируема инфраструктура. Йерархичната мрежова структура е изградена от три слоя – слой за достъп (access layer), разпределителен слой (distribution layer) и слой на ядрото (core layer). Всеки слой има своите функции, които се използват при създаването на йерархичния дизайн. Моделът осигурява модулна рамка, която дава възможност за гъвкавост при проектирането,

улеснява изграждането на мрежата и не затруднява отстраняването на възникнали при нейното функциониране проблеми. Характеристиките на отделните слоеве са следните:

- **Слой за достъп (Access layer):** Чрез него се осъществява достъпът на потребителите да мрежовите устройства. В мрежите от тип campus слоят за достъп обикновено включва мрежовите устройства на локалната мрежа с техните портове свързани към работните станции (включително виртуални настолни компютри), IP телефони, сървъри и безжични точки за достъп. От страна на глобалната мрежа, през този слой се осъществява достъпът до корпоративната мрежа на мобилните служители и отдалечените офиси. В този случай естествено се използват технологии подходящи за глобална мрежа.

- **Разпределителен слой (Distribution layer):** Този слой обхваща комуникационните шкафове с опроводяването в тях, както и комутаторите служещи за разделяне на потребителите на работни групи и които комутатори спомагат възникналите проблеми да останат изолирани локално и да не се разпространяват в цялата мрежа. От страна на глобалната мрежа разпределителния слой агрегиран връзките на границата на корпоративната мрежа и предоставя определена свързаност като резултат от избрана политика (policy-based connectivity).

- **Слой на ядрото (Core layer):** Този слой представлява висикоскоростен гръбнак на мрежата, предназначен максимално бързо да комутира пакети. Тъй като ядрото е от решаващо значение за функционирането на мрежата, то трябва да бъде високонадеждно и да се адаптира бързо към различните промени. То осигурява мащабируемост, бърза сходимост и представлява интеграционна точка на виртуалния изчислителен център. В него се използват технологии за високоскоростно комутиране (High Speed Switching) [1].

2.2 Пример на йерархична мрежа

Фигура 2 показва една корпоративна мрежа в съответствие с йерархичния модел.

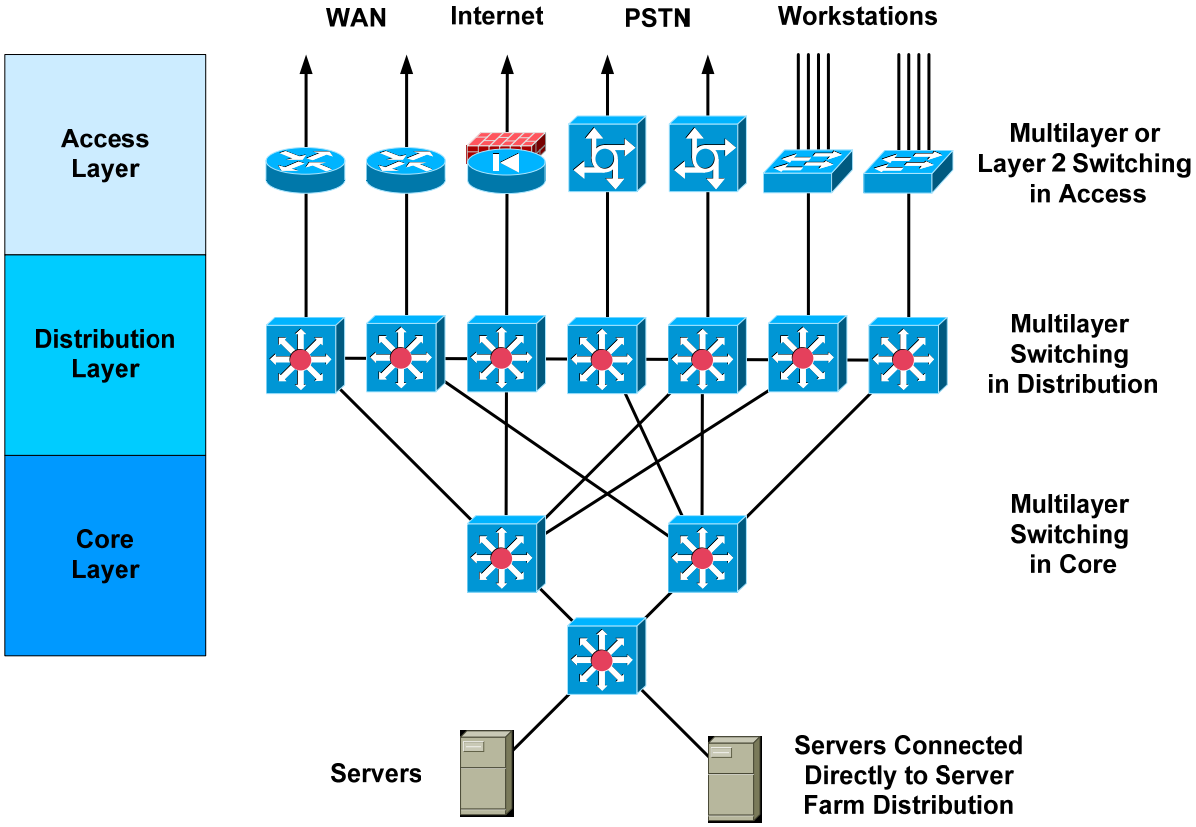
Слоестият йерархичен модел на корпоративната мрежа съдържа следните компоненти:

- **Слой за достъп:** Мрежовите устройства от този слой контролират трафика като локализират заявките за обслужване по медиите за достъп. Тези устройства също трябва да осигуряват необходимата свързаност без да се нарушава целостта на мрежата. Така например, те трябва да откриват с минимален брой проверки дали даден потребител на работна станция е легитимен. В този слой можем да срещнем такива устройства като маршрутизатори и защитни стени за връзка към глобалната мрежа (WAN), сървъри за отдалечен достъп за връзка към телефонната мрежа (PSTN), както и комутаторите (Switches) към които се свързват работните станции (Workstations).

- **Разпределителен слой:** Устройствата от този слой контролират достъпа до ресурсите, които са на разположение през ядрото, следователно трябва да осигурят ефективно използване на честотната лента. В допълнение те трябва да осигуряват необходимото качество на обслужване (Quality of Service - QoS) за различните протоколи, като прилагат контрол на трафика съгласно определена политика. Такъв контрол позволява да се въведат приоритети, и да се гарантира

максимална производителност за зависимите от времето критични приложения. Най-често тук се използват такива мрежови устройства като многослойни комутатори (Multilayer Switches).

- **Слой на ядрото:** Устройствата от този слой предоставят услуги, които оптимизират транспортните потоци в мрежата. В допълнение от тях се очаква да осигурят максимална наличност и надеждност с минимална обработка на пакетите. Устройствата от ядрото трябва да могат да поддържат връзката, дори когато някои от свързващите ги вериги са прекъснати. Следователно ядрото трябва да бъде проектирано като отказоустойчиво, което от своя страна да гарантира, че определени неизправности няма да окажат значително влияние върху мрежовата свързаност. Повече за изискванията към ядрото на мрежата можете да намерите в [1]. Към него понякога директно се свързва клъстерът от сървъри.



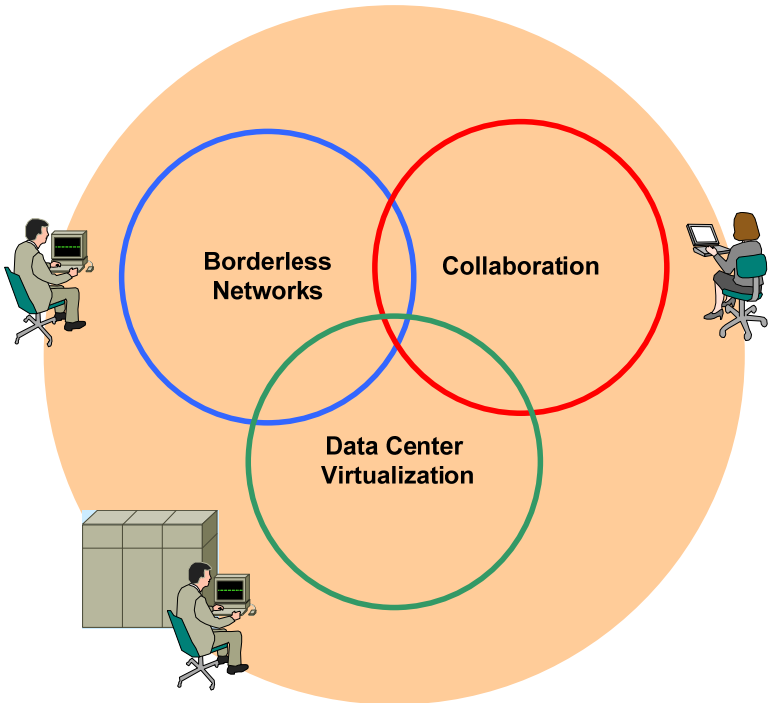
Фигура 2 Йерархична мрежа

3. Разработени от Cisco архитектури за корпоративни мрежи

Cisco разработи три припокриващи се архитектури като части от архитектурата и дизайна на корпоративната мрежа. Те са показани на Фигура 3: Архитектура за мрежа без граници (Borderless network), Архитектура за сътрудничеството (Collaboration) и Архитектура за виртуализация на изчислителния център (Data Center Virtualization). В този раздел са описани тези архитектури и развитието на корпоративната мрежа, което те представляват.

Дизайнът на корпоративната мрежа трябва да гарантира използването на натрупания потребителски опит и да удовлетворява бизнес целите, които са поставени. Производителността на едно предприятие зависи в голяма степен от различните приложения, които се използват в него. С малки изключения, повечето приложения използват компютърната мрежа и са поддържани от нея. За да изпълняват ежедневните си задачи, работниците имат нужда от достъп до мрежови инструменти и приложения. Ето защо очакванията на потребителите са за достъп до мрежата и ресурсите по всяко време на деня и от всяко едно място. Тези фактори оказват влияние върху мрежовия дизайн и архитектура.

Традиционно екипите, които поддържат една голяма корпоративна мрежа, са разделени от технологията и работят в различни области и на различни места . Например има отделни екипи за поддръжка на сървъра, на базата данни, на локалната мрежа в главната квартира, както и екип отговарящ за връзката с глобалната мрежа и отдалечените офиси. Въпреки че такова разделение може да бъде смислено от гледна точка на поддръжката на мрежата, то често води до дизайн, който е сегментиран. Всеки отделен екип проектира и внедрява нови решения, които да отговарят на неговите специфични предизвикателства. Рискът от разпространението и развитието на този подход е, че достъпността и производителността могат да се променят в зависимост от местоположението на потребителите и начинът по който те имат достъп до своите приложения. Ето защо Cisco възприе един по-цялостен подход към архитектурата на корпоративните мрежи. Вместо мрежата да се разделя по местоположение и технология, се определят три различни препокриващи се области. Всяка област се съсредоточава върху конкретно развитие на средата в предприятието. Чрез фокусиране върху тези три области (мрежа без граници, сътрудничество и виртуализация на изчислителния център) са разработени архитектури, които подпомагат високото качество на работа на потребителя в мрежата.



Фигура 3 Дизайн на корпоративна мрежа използващ архитектурите на Cisco

Мрежовият дизайн трябва да бъде такъв, че към него лесно да могат да се адаптират тенденциите и новите развития в околната среда на предприятието. Cisco идентифицира три основни тенденции и създаде архитектури за всяка една от тях:

- **Мрежа без граници:** Работниците стават все по-мобилни. Много от тях работят от различни места: в офиса, у дома, дори на пътя. Работното време също се измества. При това става все по-гъвкаво. Традиционните граници между работата и личния живот се размазват. Потребителите се свързват към мрежата с все по нови устройства, като например с персонални цифрови помощници (Personal Digital Assistant – PDA), таблети, смарт телефони и камери. Архитектурата за мрежа без граници е специално създадена за да се справи с това ново развитие и да спомогне за разпространението на потребителския опит до всички потребители - навсякъде, по всяко време и от всяко устройство.

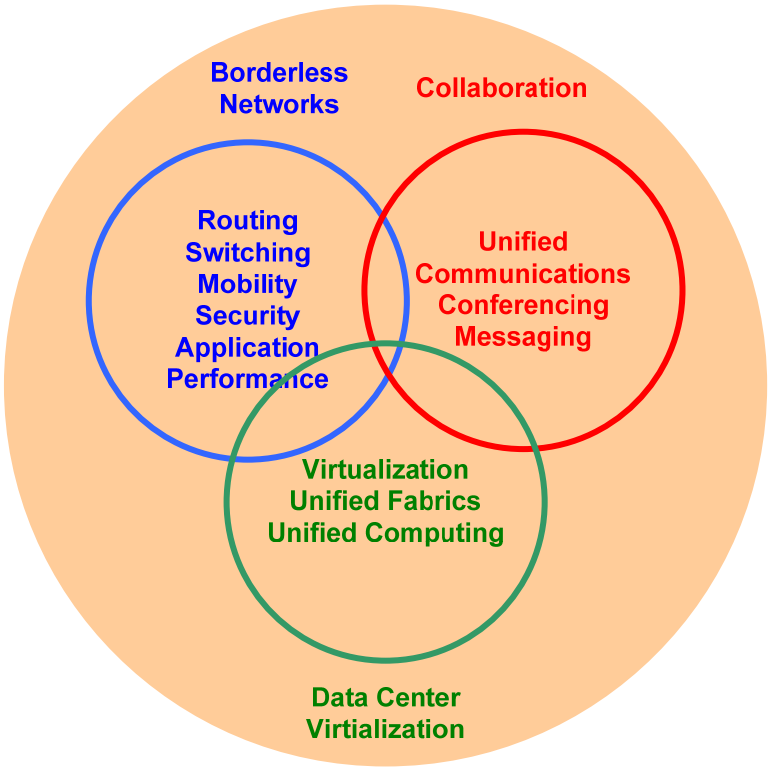
- **Сътрудничество:** Методите за комуникация постоянно се променят (например, кратки бързи съобщения, видео-конферентна връзка, IP телефония, социални мрежи). Работниците използват тези методи за комуникация като начин за общуване с колеги, партньори и клиенти и използват различните методи в зависимост от нуждите. Архитектурата за сътрудничество има за цел изграждането на мрежа, която обединява всички тези различни средства за комуникация и чиято инфраструктура е готова да подкрепи такава комбинация от мултимедийни приложения.

- **Виртуализация:** Архитектурите за мрежа без граници и сътрудничество се фокусират върху промените в стила на комуникация и в стила на работа. За разлика от тях архитектурата за виртуализация не се фокусира върху потребителя, а върху обезпечаването на приложения и услуги достъпни за него. Изчислителните центрове съдържат сървърни услуги и данни, които са достъпни за приложенията използвани в предприятието. За да се гарантира мащабираемостта на приложенията при промяна в търсенето, центровете за данни трябва да бъдат изградени по икономичен, енергийно ефективен, гъвкав и мащабируем начин. Това е, което архитектурата за виртуализация трябва да предостави.

Общото за трите архитектури е, че отправна точка за тях са ползите, които поддържаните приложения носят за бизнеса. Те създават цялостна архитектура, която гарантира потребителският опит да стигне до всички използвани приложения. Всяка от трите архитектури подсилва влиянието на различен набор от технологии за постигане на своите проектни цели. От друга страна няма строго разделение; съществува известно препокриване между трите области. Те работят заедно, за да доставят желания потребителски опит и свързаните с него ползи. Например технологиите за сигурност играят ключова роля в архитектурата за мрежа без граници поради фокусирането си върху свързаността от всяко място с помощта на всякакво устройство. Независимо от това сигурността се взема под внимание и в архитектурите за сътрудничество и виртуализация.

Както е показано на Фигура 4, всяка от архитектурите въздейства положително върху различен набор от технологии. Технологиите за мрежа без граници поставят акцент върху осигуряването на високопроизводителни, сигурни и мобилни връзки. Тук можете да срещнете технологии за маршрутизация (Routing), комутиране (Switching), мобилност

(Mobility), сигурност (Security), ефективност на приложенията (Application Performance) и други. Технологиите които се използват в архитектурата за сътрудничество са концентрирани върху интегрирането на много различни видове комуникационни методи и устройства. Тук можем да изброим използването на унифицирани комуникации (Unified Communications), на конферентни връзки (Conferencing), текстови съобщения (Messaging) и други. Технологиите в архитектурата за виртуализация се концентрират върху съхранението на информацията и обезпечаването на изчислителни ресурси за приложенията по начин, който е силно мащабируем и устойчив. Тук се използват такива технологии като унифицирани изчисления (Unified Fabrics, Unified Computing) и виртуализация (Virtualization).



Фигура 4 Дизайн на корпоративна мрежа използващ архитектурите на Cisco (продължение)

4. Интегриране на услугите и приложенията

Всичките три архитектури за корпоративната мрежа акцентират върху доставката на приложения. В допълнение към предоставянето на свързаност, мрежата трябва да предлага и различни приложения и услуги, за да гарантира постоянно високото качество на работата на потребителя. В крайна сметка всички корпоративни мрежи се изграждат за да работят приложенията, които поддържат първичните бизнес процеси в предприятието. Именно тези приложения водят до реални бизнес ползи. Потребителският опит стои в центъра на реализирането на потенциала на едно приложение. Ако очакваната производителност на приложенията не може да бъде гарантирана, бизнес ползите, свързани с тези приложения, се губят. Поради това проектирането на мрежата не трябва да се фокусира само върху предоставянето на свързаност и трафик, но и върху осигуряването на високо качество на работата на потребителя. Това става чрез оптимизиране на производителността на приложенията.

Ето защо архитектурите на Cisco за корпоративните мрежи включват в своите рамки някои общи мрежови услуги. Например архитектурите за мрежа без граници и сътрудничество са изградени върху идеята за Medianet мрежа. Medianet е интелигентна мрежа, която е оптимизирана за мултимедия, като глас и видео. Когато тези услуги са вградени в основата на мрежата, много различни мултимедийни приложения могат да използват един и същи набор от услуги, което улеснява цялостния дизайн и повишава оперативната съвместимост между различните приложения.

Даването на възможност на приложенията да споделят общи услуги, вместо отделни услуги за всяко приложение, води до по-бързо и ефективно внедряване на приложенията. Ето защо, проектирането на мрежови услуги е съществена част от дизайна на всяка мрежа.

4.1 Мрежови услуги

Този раздел описва мрежовите услуги, които се предоставят от архитектурата Medianet. Основната цел на тази архитектура е да прехвърли специфичните мултимедийни услуги към мрежата, и по този начин мрежата да предоставя услугите и ресурсите, които са необходими за модерните мултимедийни технологии.

Архитектурата Medianet на Cisco включва следните мрежови услуги:

- **Управление на мрежата (Network management):** Включва управлението на многослойните комутатори в локалната мрежа, управлението и наблюдението на маршрутизацията в глобалната мрежа, управлението на трафика, контрол на достъпа за администриране на пренасочващата инфраструктура в многофункционалните мрежи, администриране на сигурността и производителността на виртуалните частни мрежи (Virtual Private Networks – VPN) и т.н.

- **Висока надеждност:** Осигурява наличността на мрежата от край до край за услуги, клиенти и сесии. Реализацията включва използването на надеждни (reliable) и устойчиви на грешки (fault-tolerant) мрежови устройства, които автоматично да откриват и преодоляват неизправностите, както и гъвкави и устойчиви (resilient) мрежови технологии.

- **Качество на обслужване (QoS):** Управлява закъсненията, трептенето или с други думи вариациите в закъсненията (jitter), наличието на честотна лента, загубата на пакети, което е от съществено значение при предаването на глас, видео, данни и приложения. QoS предоставя допълнителна функционалност. Например мрежовата система за разпознаване на приложения (Network-Based Application Recognition - NBAR) класифицира трафика на базата на приложенията, агентът за осигуряване на услугата (Service Assurance Agent - SAA) извършва от край до край QoS измервания, протоколът за резервиране на ресурси (Resource Reservation Protocol - RSVP) сигнализира за контрол на достъпа и запазване на определени ресурси. Тук спадат и различните конфигурируеми системи за обслужване на опашките.

- **IP групово предаване (IP multicasting):** Предоставя технология със запазване на честотна лента, която технология намалява мрежовия трафик като осигурява

единен поток от информация предназначен за много корпоративни получатели в мрежата на предприятието. Груповото предаване позволява разпространението на видео-конферентна връзка, корпоративна комуникация, дистанционно обучение, разпространение на софтуер, както и много други приложения. Пакетите за групово предаване се репликират в мрежата само когато е необходимо от маршрутизатори и комутатори с активиран на тях независим протокол за групово предаване (Protocol Independent Multicast - PIM) или друг подобен протокол, в резултат на което се получава ефективно предаване на данни до множество приемащи потребители.

- **Прекодиране (Transcoding):** Цифровите сигнални процесори (Digital signal processors - DSP), които са вградени в маршрутизаторите за интегрирани услуги на Cisco могат да си използват за прекодиране (transcode) или промяна на скоростта (transrate) на гласови и видео потоци за да се адаптират към възможностите на устройствата на клиента и ограниченията на честотната лента. Чрез предоставяне на такива услуги мултимедийните приложения могат да бъдат оптимизирани с цел гарантиране на работата на потребителите в цялата мрежа без граници.

- **Удостоверяване на автентичността и криптиране (Authentication and encryption):** Системите за сигурност IP Security (IPsec) и Cisco IOS Secure Sockets Layer VPN (SSL VPN), които са вградени в мрежовите устройства, предлагат услуги за удостоверяване на автентичността и криптиране, осигуряващи целостта и поверителността на данните в мрежата.

4.2 Мрежови приложения

В този раздел са описани някои от приложенията, които могат да използват услугите предоставяни от Medianet. Крайната цел на Medianet всъщност е да предоставя услуги на мрежово ниво за приложенията използвани от потребителите. Тези приложения са следните:

- **Унифицирани комуникации (Unified Communications):** Включват глас, видео и уеб конферентни решения. Настолните решения за видео конферентна връзка, интегрирани с мултимедийните инструменти за сътрудничество, могат да доведат до по-висока ефективност на срещите. Тези приложения са с интерактивен характер, следователно са чувствителни на закъснения, трептене и загуба на пакети.

- **Системи за цифрова мултимедия на Cisco (Cisco Digital Media Systems):** Към тази група принадлежи приложението за обслужване на цифрови табла (Cisco Digital Signage), което доставя видео и приложна информация до множество големи монитори, разпръснати в цялото предприятие. Други такива системи са корпоративна телевизия (Cisco Enterprise TV), която позволява на крайните потребители да избират и да получават на живо върху големи екрани предварително записани видеофайлове, както и настолна телевизия (Cisco Desktop Video), при която потребителите получават на живо или предварително записано видео върху настолните си компютри. Тези приложения са в групата на поточната мултимедия и не са интерактивни по своята природа.

- **IP видео наблюдение (Cisco IP Video Surveillance):** Осигурява мониторинг в реално време на околната среда, хората и имуществото, и предоставя запис за

целите на разследването. Видео наблюдението е ключов момент в процедурите за безопасност и сигурност на много организации. Надеждността на решението, сигурността и поверителността на информацията, са основни съображения за този тип приложения.

4.3 Модулност на архитектурите на корпоративните мрежи

С цел оптимизирането на производителността на приложенията, мрежовите услуги трябва да бъдат проектирани от край до край, през цялата мрежа без граници. Работният проект трябва да бъде разделен на отделни модули, за да се улесни неговото постепенно прилагане, и да отговаря на специфичните изисквания на всяка отделна част на мрежата.

Един от начините да се раздели мрежата на отделни модули, е да се вземе предвид тяхното място в мрежата:

- **Комплекс от фирмени сгради (Campus):** Мрежата на този комплекс е от централно или регионално значение за фирмата. Тя е оперативен център за бизнеса. Този модул е мястото, където повечето потребители имат достъп до мрежата. В него е комбинирана инфраструктурата на ядрото, изградена от интелигентни маршрутизиращи и комутиращи устройства, със силно интегрираните технологии за повишаването на производителността, включително унифицираните комуникации, мобилността и повишената сигурност. Йерархичната структура на мрежата на този комплекс осигурява висока надеждност чрез гъвкав многослоен дизайн, дублирани хардуерни и софтуерни компоненти, както и автоматични процедури за преконфигуриране на мрежовите връзки, когато се появят повреди. Груповото предаване оптимизира консумацията на честотна лента, а QoS гарантира доставката на пакетите от критичния трафик (глас, видео и данни) в реално време, без те да бъдат отхвърляни или забавяни. Вградената сигурност защитава от появата на червеи, вируси и други атаки в мрежата (включително на ниво порт на комутатор). Архитектурата разширява удостоверяването на автентичността използвайки стандарти като IEEE 802.1X и Extensible Authentication Protocol (EAP). Тя предоставя също така определена гъвкавост, като поддържа протокола IPsec и частните виртуални мрежи в многопротоколното етикетно комутиране (Multiprotocol Label Switching Virtual Private Networks - MPLS VPN) [2], Достъпът до мрежата бива ограничаван от системата за управление на идентификацията, както и от използването на виртуални локални мрежи (Virtual Local Networks – VLANs). Всички тези добавки подобряват ефективността и сигурността на мрежата, като същевременно намаляват разходите.

- **Изчислителен център (Data Center):** Това е свързваща, адаптивна мрежова архитектура, която от една страна удовлетворява изискванията на старите, изпитани технологии, гарантиращи стабилност и сигурност на бизнеса, а от друга страна поддържа такива нови направления като виртуализация, изчисления по заявка, както и други нововъзникващи и ориентирани към услуги архитектури. Персоналът на IT департамента може лесно да осигури на служителите, доставчиците и клиентите защитен достъп до приложения и ресурси в изчислителния център. Тази възможност опростява и рационализира управлението, като значително намалява режийните разноски. Резервни изчислителни центрове осигуряват архивирането чрез синхронно и асинхронно копиране на данните и приложенията. Мрежата и устройствата предлагат балансиране на натоварването

за сървърите и приложенията, с което се постига максимална ефективност. Такова решение позволява на предприятието да се разраства без значителни промени в инфраструктурата. Изчислителният център обикновено се намира в комплекса от фирмени сгради, най-често е изграден като група от сървъри (server farm) и понякога е свързан директно с ядрото на мрежата. Но той може да бъде и отдалечен от главната квартира на корпорацията.

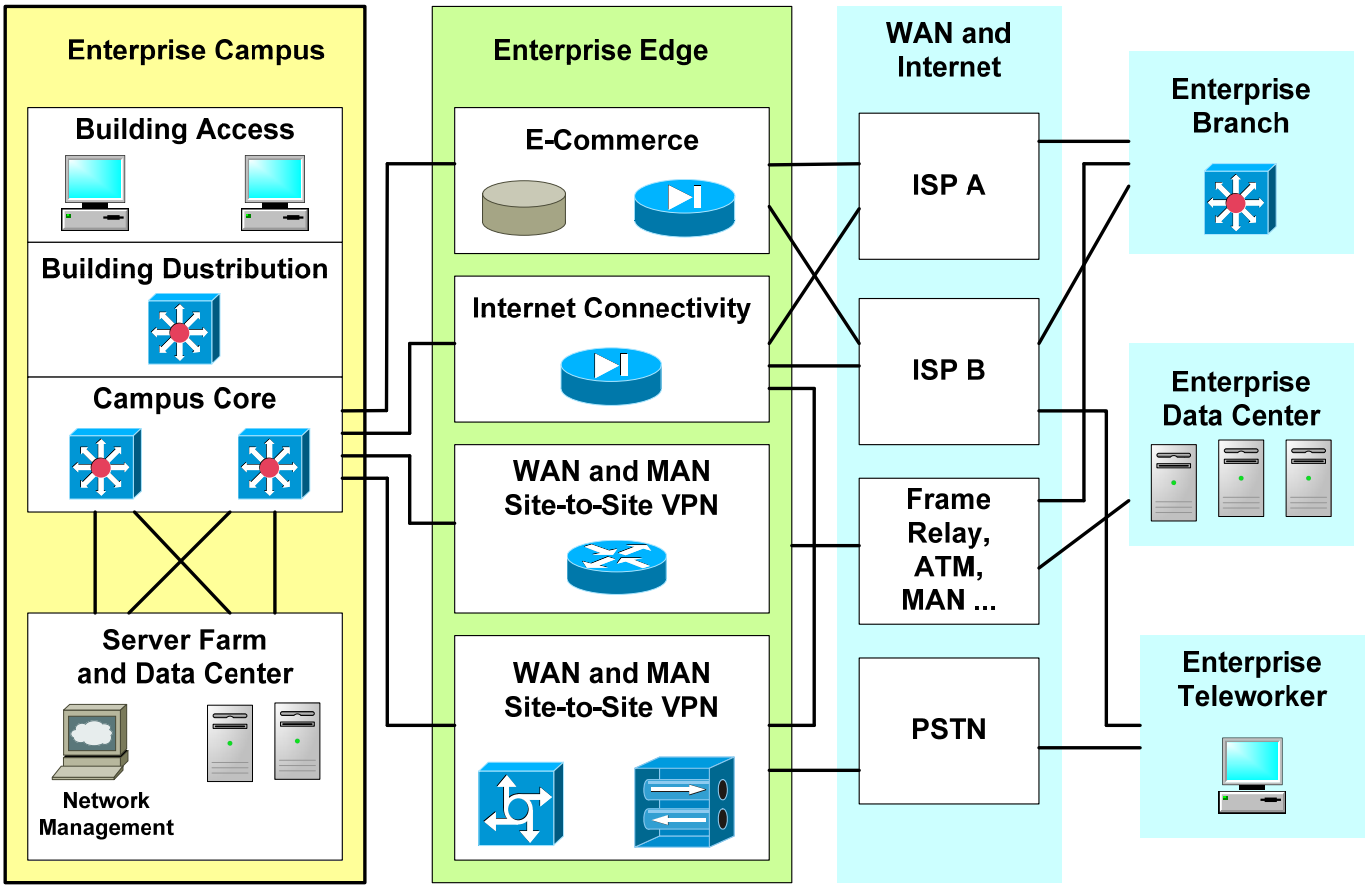
- **Глобална и локална мрежи (WAN and MAN):** Този модул предлага предаване на глас, видео и данни в проста мрежа от унифицирани комуникации на Cisco. Такова унифициране на предаването позволява на предприятието ефективно да се разпростре върху големи географски райони. Разделянето на обслужването на различни нива, гарантирането на качеството на обслужване (QoS), както и всеобхватните опции за криптиране, помагат за сигурната доставка на висококачествени корпоративни глас, видео, данни и ресурси до всички корпоративни сайтове. Това позволява на персонала да работи продуктивно и ефективно където и да се намира. Сигурността е осигурена от използването на такива технологии като VPN по IPSec и MPLS в слоеве 2 и 3 на глобалната мрежа [2], както и топологии с много пътища (full-mesh).

- **Филиал (Branch):** Този модул позволява на предприятието да разпростре приложенията и услугите, които се използват в главната квартира, до хиляди отдалечени места и потребители, както и до малка група от филиали и клонове. Интегрираните в главната квартира сигурност, комутиране, мрежови анализ, кеширане и конвергирани гласови и видео услуги се пренасят към филиалите под формата на серия от интегрирани услуги. Когато такава нова услуга е готова, тя се разпространява до филиалите. Мрежовите администратори на предприятието могат лесно централно да конфигурират, наблюдават и управляват устройствата, които са разположени в отдалечените обекти. Тук са включени такива инструменти като например Cisco AutoQoS, която система активно решава проблемите на трафика и задръстванията, преди те да се отразят на мрежата.

- **Отдалечен работник (Teleworker):** Модулът за отдалечен работник позволява на предприятията надеждно да доставят гласови услуги и данни до отдалечен малък офис (small office/home office - SOHO) като използват стандартната услуга за широколентов достъп. По този начин те осигуряват гъвкава работна среда за служителите. Централизираното управление намалява разходите за IT поддръжка, а надеждната комплексна безопасност смекчава уникалните предизвикателства пред сигурността в тази среда. Услугите за интегрирана сигурност и за установяване на автентичността помагат политиката за сигурност на главната квартира да се разпростре и върху отдалечения работник. Персоналът може да установи връзка с мрежата по винаги включената и надеждна VPN и да получи достъп до разрешените приложения и услуги от домашния си компютър. Производителността може допълнително да бъде подобрена чрез добавяне на IP телефон и осигуряване на икономически ефективен достъп до централизирана IP комуникационна система за предаване на съобщения и гласови услуги.

На Фигура 5 е показана една мрежа с модулен дизайн. На нея ясно е разграничен модулът на корпоративния Campus, изграден като йерархична мрежа. Към ядрото на тази мрежа са свързани Изчислителния център и мрежата за управление, в която работят мрежовите администратори (Network Management). Периферията на тази мрежа е

оформена като отделен модул за връзка с външния свят (Enterprise Edge). В този модул се осъществяват връзките към системата за електронна търговия (E-Commerce), към Inernet, към глобалните и градски мрежи (WAN and MAN), както и към външна телефонна мрежа (PSTN). Тук са и крайните точки на VPN каналите. На Фигура 5 са показани и мрежите на два Internet доставчика (ISP A и ISP B), телефонната мрежа, както и са сигнализирани различни технологии, които се използват в Internet. Най-вдясно са показани модулите на филиал (Enterprise Branch), на отдалечен изчислителен център, както и на отдалечен работник. Ясно се вижда, че някои от връзките са дублирани.



Фигура 5 Модулен дизайн на мрежа

Досега разглеждахме архитектурата на корпоративната мрежа така, както възнамеряваме да я проектираме. По-долу ще направим кратко резюме на изложеното до тук.

Йерархичният модел предвижда модулен поглед към мрежата, което води до по-лесно проектиране и изграждане на детерминирана мащабируема мрежа. Йерархичната структура на мрежата е изградена от слой за достъп, разпределителен слой и слой на ядрото. Фирмата Cisco Systems Inc е разработила три препокриващи се архитектури за корпоративна мрежа, като част от един цялостен подход към мрежовата архитектура и дизайн. Взети заедно, тези архитектури съставляват мрежовата архитектура на корпоративната мрежа. Архитектурите са фокусирани върху последните три насоки на развитие на околната среда на предприятието:

- Архитектурата на мрежа без граници е насочена към увеличаващата се мобилност на работниците и разглежда свързването на всеки, от всяко място, с всякакво

устройство, към всички ресурси, при това свързването да става сигурно, надеждно и безпроблемно.

- Архитектурата за сътрудничество е насочена към нарасналата необходимост от взаимодействие между различните фирми, партньори и доставчици. Решенията на проблема за сътрудничество се опират на тази модулна архитектура, която интегрира съществуващата среда и позволява въвеждането на нови възможности за общуване.

- Архитектурата за виртуализация разглежда три основни предизвикателства пред бизнеса: въвеждане на ред в бизнеса, разходи и енергийна ефективност, както и управление на риска и спазване на изискванията. Технологията на виртуализация позволява по-бързото разгръщане на приложенията и по-ефективно използване на ресурсите, което ви позволява да правите повече неща с едни и същи ресурси. Виртуализацията също така предлага по-добра защита срещу бедствия и прекъсвания.

- Инфраструктурните услуги добавят интелект на мрежовата инфраструктура, като подпомагат осведомеността на приложенията в рамките на мрежата. Интегрираните мрежови услуги предоставят общ набор от възможности, от които могат да се възползват много и различни приложения. Някои приложения активират мрежови услуги, които поддържат определени изисквания за трафика в цялата мрежа, от край до край.

5. Методология на проектирането

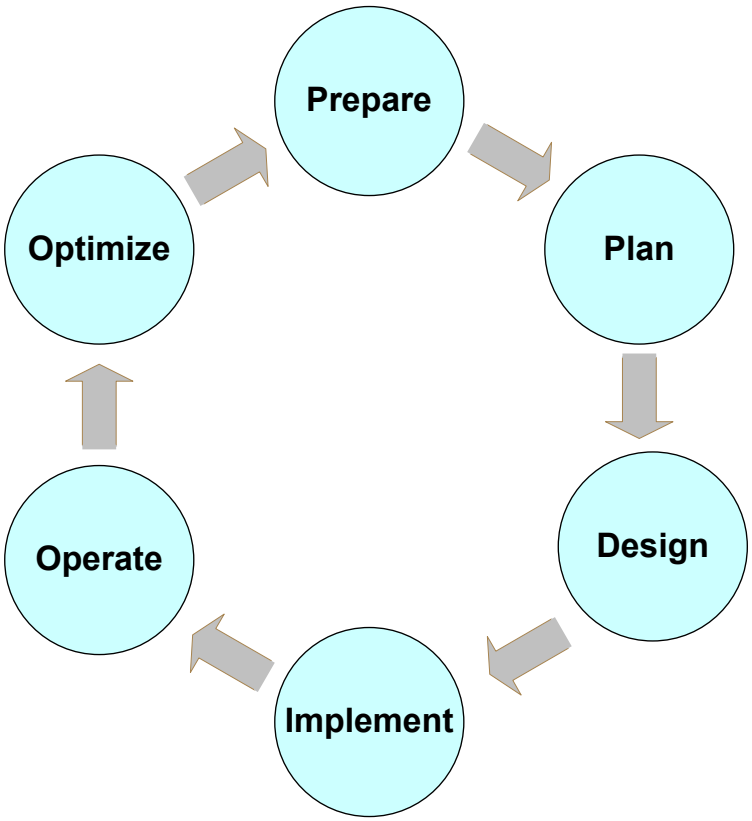
За да се проектира една мрежа, трябва да се определят [3]:

- нуждите на клиента,
- целите на организацията,
- организационните ограничения,
- техническите цели,
- техническите ограничения.

Cisco формализира жизнения цикъл на една мрежа в шест фази: подготовка, планиране, проектиране, изпълнение, експлоатация и оптимизация. Въз основа на този жизнен цикъл е разработена методология на проектирането, която накратко ще опишем в този раздел.

5.1 Жизнен цикъл на мрежата (Lifecycle of the network)

Жизненият цикъл на една мрежа е показан на Фигура 6.



Фигура 6 Жизнен цикъл на мрежата

По долу са описани фазите на жизнения цикъл:

- **Подготовка (Prepare):** Подготвителната фаза включва създаване на организационни изисквания, разработване на стратегия за мрежата, предлагане на концептуална архитектура на високо ниво, както и определяне на технологиите, които могат да подкрепят най-добре тази архитектура. В подготвителната фаза трябва да се направи финансова обосновка на мрежовата стратегия чрез оценка на икономическите аргументи за предложената архитектура.

- **Планиране (Plan):** Фазата на планиране включва определяне на първоначалните мрежови изисквания, които се основават на поставените цели, на наличните съоръжения, на нуждите на потребителите и т.н. Тази фаза включва характеризиране на обектите, оценяване на всички съществуващи мрежи, както и извършване на анализ на пропуските, за да се определи дали съществуващата системна инфраструктура, обектите и оперативната среда могат да подпомогнат предложената система. Проектният план улеснява управлението на задачите, отговорностите, критичните етапи и ресурсите необходими за изпълнението на промените в мрежата. Той трябва да се приведе в съответствие с обхвата, разходите и параметрите на ресурсите установени в първоначалните бизнес изисквания.

- **Проектиране (Design):** Първоначалните изисквания, които бяха установени във фазата на планирането трябва да се доведат да знанието на проектантите. Спецификацията на мрежовия дизайн трябва да бъде всеобхватна, детайлна и да покрива всички организационни и технически изисквания. Тя трябва да включва

спецификации за достъпност, надеждност, сигурност, скалируемост и производителност. Тези спецификации са в основата на дейностите по изпълнението.

- **Изпълнение (Implement):** След одобряването на проекта започва неговото изпълнение (и проверка). Изгражда се цялата мрежа или се добавят към съществуващата мрежа допълнителни компоненти според спецификациите на проекта, с цел интегриране на нови устройства, без нарушаване на работата на мрежата и без създаване на точки на уязвимост в нея.

- **Експлоатация (Operate):** Крайният тест за целесъобразността на един проект е дали той е работоспособен. Фазата на експлоатация включва поддържането на мрежата работоспособна чрез всекидневни операции за запазване на високата надеждност и намаляване на разходите. Откриването на грешки, корекциите, и мониторинга на резултатите от всекидневните операции служат като първоначални данни за фазата на оптимизация.

- **Оптимизация (Optimize):** Фазата на оптимизация включва активно управление на мрежата. Целта на това управление е да се открият и разрешат проблеми, преди те да са се отразили на организацията. Когато активното управление не може да предскаже и смекчи неуспехите, трябва да се приложи реактивно откриване на повреди и тяхното отстраняване (troubleshooting). Фазата на оптимизация може да подтикне към ново проектиране, ако възникнат твърде много мрежови проблеми и грешки, както и ако изпълнението не отговаря на очакванията, или ако нови приложения са открити удовлетворяващи организационните и технически изисквания.

Въпреки че проектирането е описано като една от шестте фази, то може да се появи като дейност и при другите.

5.2 Предимства на подхода на жизнения цикъл

Подходът на използване на жизнения цикъл на мрежата предоставя четири основни предимства. Той понижава общата цена на мрежата (за изграждане и експлоатация), увеличава нейната наличност във всеки момент, подобрява гъвкавостта на бизнеса и ускорява достъпа до приложенията и услугите. Следвайки тази методология, проектантите, инженерите и администраторите дават възможност на потребителите на мрежата ефективно да използват целия натрупан до момента опит. Сега ще опишем по-подробна стратегиите за постигането на тези предимства.

Общата стойност на мрежата се намалява чрез стратегии за:

- Идентифициране и утвърждаване на изискванията на използваната технология.

- Планиране на инфраструктурните промени и изискванията за ресурси.

- Разработване на мрежовия проект в съответствие с техническите изисквания и целите на бизнеса.

- Ускорено успешно внедряване

- Подобряване на ефективността на мрежата, както и на персонала нает за нейното обслужване.

- Намаляване на оперативните разходи чрез подобряване на ефективността на работните процеси и инструменти.

Наличността на мрежата и нейната достъпност се повишава чрез стратегии за:

- Оценка на състоянието на сигурността на мрежата и нейната адекватност към предложения дизайн

- Определяне на правилния набор и версии на хардуерните и софтуерни компоненти, както и поддържането на тяхната работоспособност във времето.

- Изработване на стабилен проект и въвеждане на мрежата в експлоатация.

- Разделяне на проекта на етапи и тестване на системата преди нейното внедряване.

- Подобряване на уменията на персонала.

- Активно наблюдение на системата и оценка на тенденциите в предупрежденията за наличност на мрежата.

- Активно откриване на нарушения в сигурността и изготвяне на планове за възстановяване.

Гъвкавостта на бизнеса се подобрява чрез стратегии за:

- Установяване на бизнес изискванията и на изискванията за технологично обновление.

- Подготовка на обектите, в които ще се разположи внедряваната система

- Интегриране на техническите изисквания и бизнес целите в подробен проект и доказване, че мрежата функционира съгласно направените спецификации.

- Експертно инсталиране, конфигуриране и интегриране на компонентите на системата.

- Непрекъснато подобряване на производителността.

Достъпът до приложенията и услугите се ускорява чрез стратегии за:

- Оценка и подобряване на оперативната готовност за подкрепа на текущи и планирани мрежови технологии и услуги.

- Подобряване на ефективността на доставката на услуги.

- Подобряване на наличността, надеждността и устойчивостта на мрежата и на приложенията, работещи в нея.

- Управление и разрешаване на проблеми свързани със системата, както и с наличните софтуерни приложения.

5.3 Използване на методологията за проектиране

Методологията за проектиране се състои от три главни стъпки, а именно:

- **Стъпка 1. Идентифициране на изискванията на клиентите.** В тази стъпка хората, упълномощени да вземат решения, определят първоначалните изисквания. Въз основа на тези изисквания, се предлага концептуална архитектура от високо ниво. Тази стъпка обикновено се прави в подготвителната фаза на жизнения цикъл.

- **Стъпка 2. Характеризиране на съществуващата мрежа и на обектите**. Фазата на планиране обхваща характеризиране на обектите, оценка на съществуващите мрежи, както и извършване на анализ на пропуските, за да се определи дали съществуващата инфраструктура, обектите и обкръжаващата среда са подходящи за предлаганата система. Характеризирането на съществуващата мрежа и на обектите включва техния одит, както и анализ на мрежата. При одита на мрежата се изследват главно нейната цялост и качеството, което тя предлага. При анализа на мрежата се изследва нейното поведение (трафик, задръствания и т.н.).

- **Стъпка 3. Проектиране на топологията на мрежата и на отделните решения.** В тази стъпка се създава работния проект. Тук се вземат решенията за мрежовата инфраструктура, интелигентните мрежови услуги, както и други решения засягащи мрежата (например VoIP, начина на работа в мрежата и т.н.). Може да бъде създаден и прототип на мрежата, за да се провери нейния дизайн. Изработва се подробна документация на работния проект.

5.3.1 Идентифициране на изискванията на клиентите

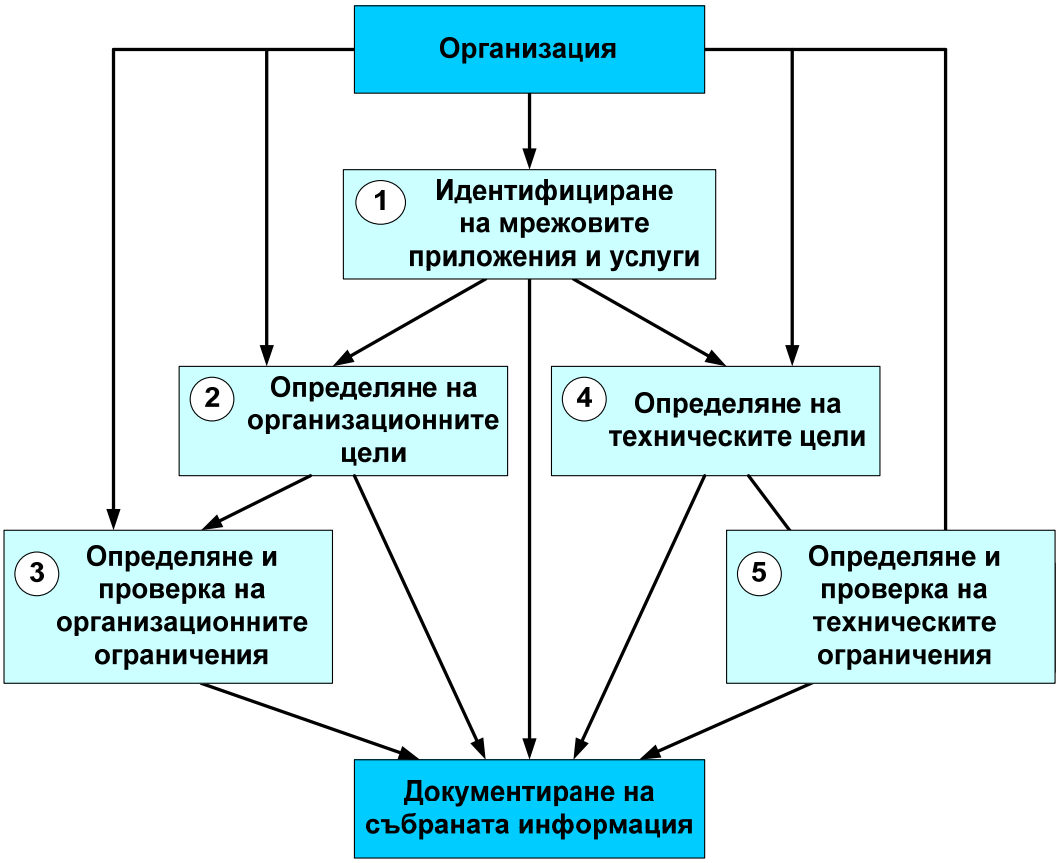
В този раздел се прави преглед на логическата последователност в процеса на изясняване на изискванията на клиентите към една корпоративна мрежа. Блок-схемата на процеса е представена на Фигура 7.

Процесът на изясняване на проектните изисквания на клиентите се състои от пет стъпки, които всъщност служат като цели за проектанта. Тези стъпки включват дискусии с членове на персонала, по време на които се събира информация и документация, необходими за да започне процеса на проектирането. Процесът на идентифициране на изискванията не е еднопосочен. Можете да се върнете към определена стъпка и да направите допълнителни запитвания относно проблеми, които са възникнали в процеса на проектиране. Стъпките за събиране на данни са както следва:

- **Стъпка 1.** Идентифициране на мрежовите приложения и услуги

- **Стъпка 2.** Определяне на организационните цели

- **Стъпка 3.** Определяне и проверка на всички възможни организационни ограничения.
- **Стъпка 4.** Дефиниране на техническите цели.
- **Стъпка 5.** Определяне и проверка на всички възможни технически ограничения.



Фигура 7 Определяне на изискванията на клиентите

След като завърши процеса на събиране на информация, проектантите са готови да анализират и тълкуват данните и да разработят предложение за мрежов дизайн.

5.3.2 Характеризиране на съществуващата мрежа и на обектите

Този раздел описва стъпките, които се необходими, за да се характеризират съществуващата мрежова инфраструктура и всички обекти. Процесът предполага три стъпки:

- **Стъпка 1.** Събиране на съществуващата документация за мрежата и запитвания към организацията за откриване на допълнителни данни. Необходимата ключова информация обикновено се съдържа в анализа на трафика и в документите на одита на мрежата. Имайте предвид, че съществуващата документация може да бъде неточна.

- **Стъпка 2.** Извършване на одит на мрежата, при който се правят допълнения и се създава едно ново нейно подробно описание. При възможност, да се използва информацията от анализа на трафика, за да се разшири наборът от протоколи и приложения използвани в мрежата.

- **Стъпка 3.** Използвайки характеризирането на мрежата трябва да се напише обобщен доклад за нейното състояние. Въз основа на този доклад вече може да се предложат хардуерни и софтуерни подобрения в подкрепа на мрежовите и организационни изисквания.

5.3.3 Проектиране на топологията на мрежата и на отделните решения

Проектирането на корпоративна мрежа е сложен процес. Използването на метод за проектиране от горе на долу (top-down design) [3], улеснява този процес, като го разделя на по-малки и по-лесно управляеми стъпки. Методът за проектиране от горе на долу изяснява целите на проектирането и стартира проектирането от гледна точка на необходимите приложения и мрежови решения. При оценяването на обхвата на проектирането трябва да се определи дали дизайнът е за напълно нова мрежа или е за модификация на мрежата, на един единствен сегмент или компонент, или пък на множество локални мрежи, на глобална мрежа или на мрежа за отдалечен достъп. Обхватът на проектирането може да засегне само една функция или всички слоеве на OSI модела. Практиките на такова структуриране се фокусират върху разделянето на задачата за проектиране на свързани, по-малко сложни компоненти и модули, като се използват следните стъпки:

- **Стъпка 1.** Идентифициране на приложенията, които са необходими за удовлетворяване на изискванията на клиента.

- **Стъпка 2.** Идентифициране на изискванията за логическа връзка между тези приложения с акцент върху необходимите мрежови решения и услуги. Като примери на инфраструктурни услуги можем да посочим предаване на глас, мрежи за съхранение на данни, наличност, управление, сигурност, QoS и IP групово предаване.

- **Стъпка 3.** В тази стъпка мрежата се разделя функционално, за да се развие нейната инфраструктура и изискванията на йерархията.

- **Стъпка 4.** Проектиране на всеки модул отделно от другите. Това е възможно, защото мрежовата инфраструктура и дизайна на мрежовите услуги са тясно свързани, тъй като се подчиняват на едни и същи логически и физически слоести модели.

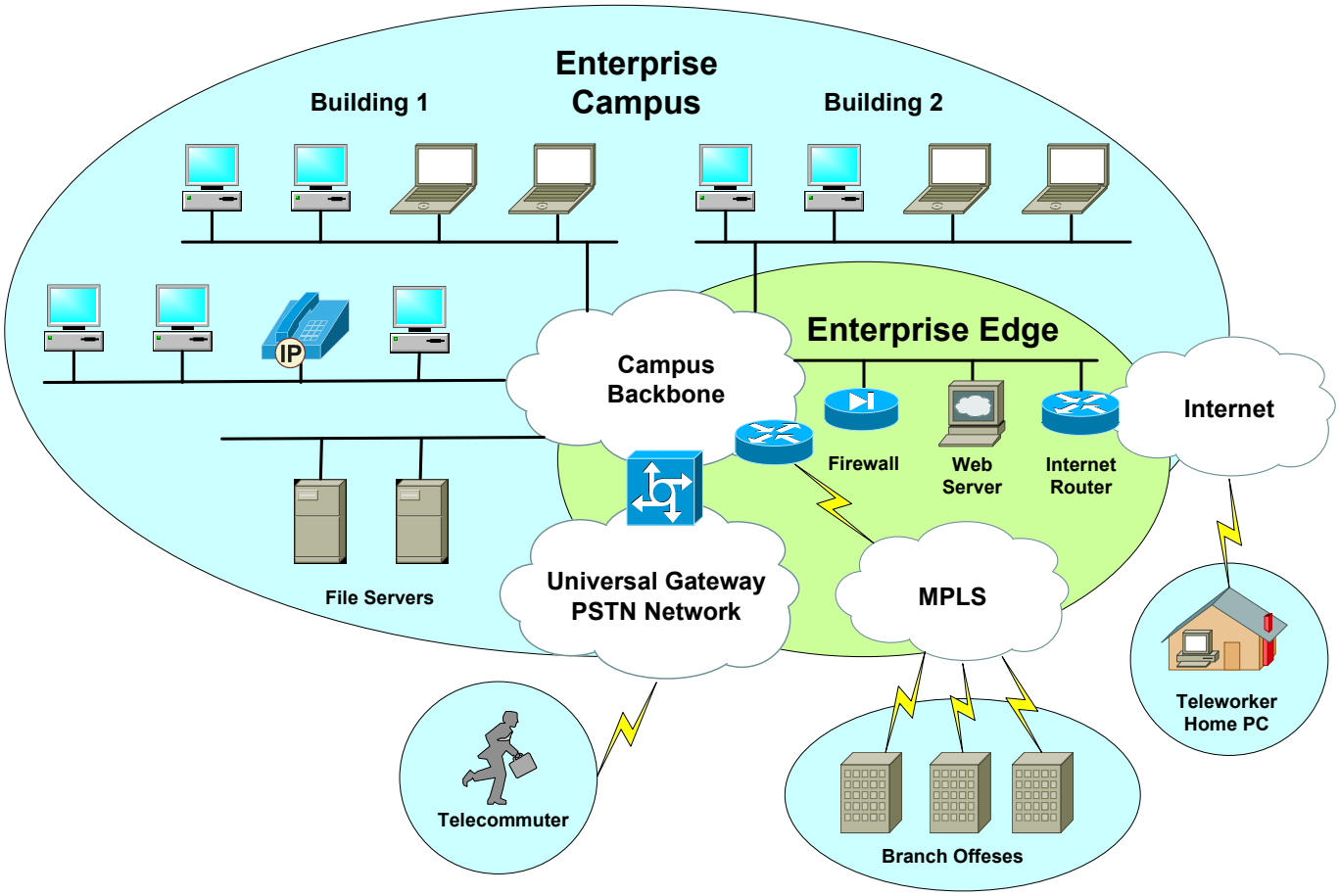
След завършване на проектирането, следващата стъпка е да се разработи и приложи план за изпълнение на проекта. Колкото е по-подробна документацията на този план, толкова изискванията към квалификацията на инженерите, които ще го прилагат, са по-малки.

Често е целесъобразно разработения дизайн на мрежата да бъде проверен. Можете да го тествате в съществуващата и работна мрежа (пилотно внедряване), или като се изгради

отделна мрежа (прототип). Във втория случай процеса на тестване не оказва влияние върху работещата мрежа.

5.3.4 Разделяне на мрежата на отделни области

Този раздел описва как да се раздели мрежата на отделни области, което е важна стъпка в процеса на проектирането. Фигура 8 илюстрира едно такова разделение.



Фигура 8 Разделяне на мрежата на области

При разделянето на мрежата на области се извършва следното:

- Определяне на модула на комплекса от фирмени сгради (campus). Той обхваща всички работни станции, сървъри и връзките между тях, включително ядрото или гръбнакът (backbone) на тази мрежа.

- Определяне на модула за неговата връзка с външния свят (Enterprise Edge). Проверка дали този модул включва всички комуникации към отдалечените обекти.

- Определяне на модула на отдалечените обекти. Той включва филиалите и клоновете на фирмата, служителите, които работят дистанционно, както и отдалечен изчислителен център, ако съществува такъв.

- Дефиниране точно на границите между тези три отделни модула.

6. Литература

[1] Стоилов Емил, Общи архитектурни концепции използвани в IP маршрутизаторите, Technical Report. Научен електронен архив на НБУ, 2013. http://eprints.nbu.bg/1770/

[2] Стоилов Емил, Технология за многопротоколно етикетно комутиране (MPLS), Technical Report. Научен електронен архив на НБУ, 2012. http://eprints.nbu.bg/1254/

[3] Oppenheimer Priscilla, Top-Down Network Design, Second Edition, Cisco Press, 2004.