ДОГОВОР

№ РД-08-57/10.05.2016г.

Днес, ... 2016 г. в гр. София, между:

1. НАЦИОНАЛЕН СТАТИСТИЧЕСКИ ИНСТИТУТ, гр. София, ул. „Панайот Волов" № 2, БУЛСТАТ 000695146, представляван от Сергей Цветарски – председател, наричан по-долу за краткост **ВЪЗЛОЖИТЕЛ,** от една страна

и

2. „Телелинк" ЕАД, ЕИК 130545438, със седалище и адрес на управление: гр. София, ул. „Лъчезар Станчев" № 3, ет. 4, телефон 02/970 40 40, факс 02/970 40 42, представлявано от Цветан Мутафчиев, на длъжност изпълнителен директор, наричан накратко **ИЗПЪЛНИТЕЛ** от друга страна,

на основание чл. 41, ал. 1 от Закона за обществените поръчки и Решение № ПД-23/05.04 2016 г. на председателя на Националния статистически институт за определяне на изпълнител, след проведена открита процедура за възлагане на обществена поръчка с предмет: **„Доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на Национален статистически институт"**, открита с Решение № ПД-6/29.01.2016 г., се сключи настоящият договор за следното:

I. ПРЕДМЕТ НА ДОГОВОРА:

1.1. Възложителят възлага, а Изпълнителят се задължава в съответствие с клаузите на договора да извърши срещу заплащане **доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на Национален статистически институт**.

1.2. Видът, количеството и характеристиките на комуникационното оборудване, както и обхвата на услугите по монтаж, конфигурация и интеграция, са подробно описани в Техническата спецификация, неразделна част от договора – Приложение № 1 и Техническо предложение на Изпълнителя, неразделна част от договора – Приложение № 2.

II. СРОК, МЯСТО И УСЛОВИЯ НА ДОСТАВКАТА:

2.1. Срокът за доставка на комуникационното оборудване е до 30 (тридесет) календарни дни, от датата на подписване на настоящия договор.

2.2. Оборудването, предмет на договора, се доставя в оригинална опаковка и с ненарушена цялост на адреса на Възложителя – гр. София, 1038, ул. „Панайот Волов" № 2, НСИ – Централно управление. Доставеното комуникационно оборудване трябва да бъде придружена с копие от сертификат за произход, гаранционни карти, технически брошури и маркировки. Приемането на доставката се удостоверява по реда, описан в настоящия договор.

2.3. Срокът за изпълнение на услугите по монтаж, конфигурация и интеграция на комуникационното оборудване е до 10 (десет) календарни дни, от датата на доставяне на оборудването, посочена в приемо-предавателния протокол за доставка. Приемането на изпълнението на услугите се удостоверява по реда, описан в настоящия договор.

2.4. При възникване на обективни пречки за нормалното изпълнение на доставките и услугите по договора, дължащи се на действия и/или бездействия на

чл. 2 от ЗЗЛД

Възложителя, предизвикани от трети лица или случайни събития, за които Изпълнителят няма вина, предвидените срокове за изпълнение се удължават съответно със срока на забавяне.

III. ЦЕНИ, УСЛОВИЯ И НАЧИН НА ПЛАЩАНЕ:

3.1. За доставката на комуникационното оборудване Възложителят дължи на Изпълнителя възнаграждение в размер на **411 351, 28 (четиристотин и единадесет хиляди, триста петдесет е един лева, двадесет и осем стотинки) лв.** без включен ДДС, съответно **493 621, 54 (четиристотин деветдесет и три хиляди, шестстотин двадесет и един лева, петдесет и четири стотинки) лв.** с включен ДДС съгласно единичните цени посочени в Приложение № 3 към договора – Ценово предложение на Изпълнителя.

3.2. За извършване на услугите по монтаж, конфигурация, интеграция и обучение Възложителят дължи на Изпълнителя възнаграждение в размер на **38 613, 14 (тридесет и осем хиляди, шестстотин и тринадесет лева и четиринадесет стотинки) лв.** без включен ДДС, съответно **46 335, 77 (четиридесет и шест хиляди, триста тридесет и пет лева, седемдесет и седем стотинки) лв.** с включен ДДС съгласно посоченото в Приложение № 3 към договора – Ценово предложение на Изпълнителя.

3.3. Възнаграждението по договора включва всички разходи на Изпълнителя за комплексното изпълнение на поръчката, в т.ч. данъци и такси, окончателно е и не подлежи на актуализация за срока на настоящия договор, освен при намаляване на договорените цени.

3.4. Възложителят заплаща възнаграждението по т. 3.1. и 3.2. изцяло авансово в срок до 10 дни от датата на подписване на настоящия договор срещу издадена проформа фактура за аванс и представена от Изпълнителя банкова гаранция за авансово плащане за 100% от стойността на дължимото възнаграждение със срок на валидност 30 дни след изтичане на срока на договора. Изпълнителят издава фактура дължимите плащания по т. 3.1. и 3.2. след подписване на съответния приемо-предавателен протокол за доставка и/или услуги.

3.5. В случай, че Изпълнителят не желае да получи авансово плащане на възнаграждението по т. 3.1. и 3.2., същите се заплащат от Възложителя както следва:

3.5.1. възнаграждението по т. 3.1. се заплаща в срок до 10 (десет) дни след представяне от Изпълнителя на оригинална данъчна фактура и подписан от двете страни приемо-предавателен протокол за доставка;

3.5.2. възнаграждението по т. 3.2. се заплаща в срок до 10 (десет) дни след представяне от Изпълнителя на оригинална данъчна фактура и подписан от двете страни приемо-предавателен протокол за услуги.

3.6. Всички плащания по договора се извършват в лева, чрез банков превод по сметка, посочена от Изпълнителя, както следва:

обслужваща банка: Уникредит Булбанк АД,
IBAN: BG16UNCR76301022595389,
BIC: UNCRBGSF.

3.7. В случай, че за изпълнението на договора има сключени договори за подизпълнение, Възложителят извършва окончателното плащане след като получи от изпълнителя доказателства, че е заплатил на подизпълнителите всички работи, приети по реда, предвиден в този договор.

3.8. Предходната клауза не се прилага, ако при приемането на работата Изпълнителят представи на Възложителя доказателства, че договорът за

чл. 2 от ЗЗЛД

подизпълнение е прекратен, или работата или част от нея не е извършена от подизпълнителя.

IV. РЕД И НАЧИН ЗА ПРИЕМАНЕ НА ДОСТАВКАТА И УСЛУГИТЕ:

4.1. Приемането на доставеното комуникационно оборудване се осъществява с подписан от двете страни приемо-предавателен протокол за доставка, след извършване на проверки и оглед. Протоколът се изготвя от Изпълнителя в два екземпляра и се подписва от упълномощените представители на двете страни.

4.2. Приемането на изпълнението на услугите се удостоверява с приемо-предавателен протокол за услуги, подписан от оправомощени представители на страните.

4.3. В случай, че по изпълнението на доставката или услугите бъдат констатирани липси, явни несъответствия или недостатъци, те се отбелязват в съответния приемо-предавателен протокол, а Изпълнителят е длъжен за своя сметка да достави липсващото оборудване или да поправи недостатъците. Срокът за отстраняване на констатираните липси, несъответствия и/или недостатъци се уговаря между страните. След отстраняване на липсите, несъответствията или недостатъците, се съставя нов приемо-предавателен протокол, който се подписва от упълномощените представители на двете страни.

4.4. В случай, че се приема работа, за която изпълнителят е сключил договор за подизпълнение, работата се приема в присъствието на изпълнителя и на подизпълнителя, като подизпълнителят подписва протокола за приемане на доставеното оборудване или извършените услуги.

4.6. При приемането на работата, Изпълнителят може да представи на Възложителя доказателства, че договорът за подизпълнение е прекратен, или работата или част от нея не е извършена от подизпълнителя.

4.7. Собствеността и рискът от погиване на оборудването преминава от Изпълнителя върху Възложителя от момента на подписване от двете страни на протокола за приемане на извършената доставка.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ:

5.1. Изпълнителят има право:

5.1.1. при добросъвестно, навременно и професионално изпълнение на договора, да получи уговореното възнаграждение в размера, срока и при условията, посочени в настоящия договор.

5.1.2. да получи необходимото съдействие от Възложителя за изпълнение на задълженията му по този договор.

5.2. Изпълнителят е длъжен:

5.2.1. да изпълни всички доставки и услуги по договора с грижата на добър търговец и в съответствие с приложимото законодателство, клаузите на договора и приложенията към него;

5.2.2. да сключи договор/и за подизпълнение с посочения/ите в офертата му подизпълнител/и при спазване разпоредбите на чл. 45а от ЗОП и в 3-дневен срок от сключване на настоящия договор, да предостави оригинален екземпляр от договорите за подизпълнение, на ВЪЗЛОЖИТЕЛЯ.

5.2.3. да достави на уговореното място ново и неупотребявано комуникационно оборудване.

чл. 2 от ЗЗЛД

5.2.4. да предостави оборудването, предмет на договора, със съответните инструкции за експлоатация от производителя, на български или английски език;

5.2.5. през времетраенето на гаранционния срок, да отстранява за своя сметка всякакви несъответствия на оборудването с изискванията по този договор или появили се през гаранционния срок недостатъци, за които е уведомен от Възложителя, съгласно клаузите на договора и приложенията към него. Изпълнителят отговаря дори и да не е знаел за несъответствието;

5.2.6. да не предоставя документи и информация относно изпълнението на поръчката, на трети лица, както и да не използва информация, станала му известна при изпълнението на задълженията му по настоящия договор. Това задължение важи и за неговите служители и подизпълнители;

5.2.7. да уведоми Възложителя за открито за него производство по ликвидация или за обявяване в несъстоятелност, в срок до 3 (три) дни от настъпване на съответното събитие;

5.3. Изпълнителят носи отговорност за действията на своите служители и подизпълнители (в случай, че използва такива), като за свои.

5.4. Изпълнителят отговаря за всички вреди, причинени на Възложителя и на трети лица в резултат на действия или бездействия на негови служители и подизпълнители (в случай, че използва такива), при или по повод изпълнението на договора.

5.5. Изпълнителят отговаря за всички вреди за околната среда, причинени при изпълнението на договора, в резултат на действия или бездействия на негови служители и/или подизпълнители (в случай, че използва такива).

5.6. При сключването на този договор Изпълнителят представя на Възложителя гаранция за изпълнение на договора в размер на 5 % (пет на сто) от стойността на поръчката без ДДС, под формата на **банкова гаранция** (парична сума или банкова гаранция), възлизаща на **22 498, 22 (двадесет и две хиляди, четиристотин деветдесет и осем лева, двадесет и две стотинки) лв.** със срок на валидност 30 дни след изтичане на срока на договора.

5.6.1. В случай че банката, издала гаранцията за изпълнение на договора, се обяви в несъстоятелност или изпадне в неплатежоспособност/свръхзадлъжнялост, или й се отнеме лиценза, или откаже да заплати предявената от Възложителя сума в 3-дневен срок, Възложителят има право да поиска, а Изпълнителят се задължава да предостави, в срок до 5 (пет) работни дни от направеното искане, съответната заместваща гаранция от друга банкова институция, съгласувана с Възложителя.

VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ:

6.1. Възложителят има право:

6.1.1. да получи изпълнение в съответствие с приложимото законодателство, клаузите на договора и приложенията към него;

6.1.2. да извърши проверка относно качеството, количествата и техническите параметри на доставеното оборудване и изпълнените от Изпълнителя услуги. Възложителят има право да откаже приемането на доставката и/или услугите, в случай че те не съответстват на уговореното в договора и приложенията към него;

6.1.3. да прави рекламации при установяване на некачествена гаранционна поддръжка на комуникационното оборудване по време на гаранционния срок и да изисква допълнително отстраняване на неизправностите за сметка на Изпълнителя;

чл. 2 от ЗЗЛД

6.1.4. да задържи съответна част от гаранцията за изпълнение, в случай на неизпълнение клаузите на договора от страна на Изпълнителя и да получи неустойката в размера, определен в този договор;

6.1.5. да изисква от Изпълнителя да сключи и да предостави договори за подизпълнение, с подизпълнителите, посочени в офертата (когато е приложимо).

6.2. Възложителят е длъжен:

6.2.1. при добросъвестно, навременно и професионално изпълнение на договора, да заплати на Изпълнителя договорената цена в размера, срока и при условията на настоящия договор;

6.2.2. да не разпространява под каквато и да е форма предоставената му от Изпълнителя информация, имаща характер на търговска тайна и изрично упомената от Изпълнителя като такава, в представената от него оферта;

6.2.3. да оказва необходимото съдействие на Изпълнителя за добросъвестно и точно изпълнение на договора;

6.2.4. при срочно и качествено изпълнение на задълженията за доставка от страна на Изпълнителя, в срок до 30 (тридесет) дни от датата на подписване протокола/ите по т. 4.2., а в хипотезата по т.4.3 – съответно от датата на подписване протокол/ите за приемане на отстраняване на недостатъците в изпълнението, Възложителят е длъжен:

а) да върне на Изпълнителя оригиналната банкова гаранция за авансово плащане, в случай, че Изпълнителят е предоставил такава и е получил авансовото плащане;

б) да възстанови 100% (сто процента) от гаранцията за изпълнение, в случаите, когато тя е парична сума, внесена по банковата сметка на НСИ, или

б) да върне на Изпълнителя оригиналната банкова гаранция за изпълнение, в случаите когато Изпълнителят е дал банкова гаранция за изпълнение на договора, и в двата случая без да дължи лихви за периода, през който средствата законно са престояли при него (или са били на негово разположение).

VII. ГАРАНЦИОННИ СРОКОВЕ И ЗАДЪЛЖЕНИЯ:

7.1. Гаранционният срок за доставеното комуникационно оборудване е съгласно Техническата спецификация на Възложителя от датата на приемане на оборудването с приемо-предавателен протокол.

7.2. Гаранционният срок започва да тече от датата на подписване на протокола за приемане на доставеното оборудването и се отнася до задължението на Изпълнителя да поправи (отстрани) несъответствия или недостатъци от всякакъв характер, вкл. фабрични дефекти, дефекти в материала, дефекти в изработката, механични дефекти, други недостатъци и/или повреди, освен ако същите са предизвикани от неправилно съхранение и/или експлоатация.

7.3. В случай, че в гаранционния срок се открият недостатъци и/или повреди, Възложителят отправя заявка до Изпълнителя за отстраняването им по факс, по пощата или по електронната поща за наличието и характера на повредата/ите.

7.4. Работата по отстраняване на повредата/несъответствието трябва да започне, както следва:

a. време за реакция при заявка от възложителя 1 час;
b. срок за подмяна на дефектирало оборудване и възстановяване на услугите – до 3 работни дни.

чл. 2 от ЗЗЛД

7.5. В случай, че Изпълнителят не отстрани недостатъците и/или повредите в договорения срок, Възложителят може да отстрани тези недостатъци и/или повреди за сметка на Изпълнителя.

7.6. Всички разходи за отстраняване на недостатъци и/или повреди по време на гаранционния срок са за сметка на Изпълнителя.

7.7. След изтичане на гаранционния срок, страните подписват двустранен протокол, с който удостоверяват приключването на своите взаимоотношения във връзка с гаранционните задължения на Изпълнителя.

VIII. ОТГОВОРНОСТИ И НЕУСТОЙКИ:

8.1. В случай, че Изпълнителят не спази задълженията си в сроковете, предвидени в този договор, същият дължи неустойка в размер на 0,2 % (нула цяло и две десети от процента) от стойността на неизпълнената част от доставката, без ДДС за всеки просрочен ден, но не повече от 20 (двадесет) процента от цената по т. 3.1.

8.2. В случай, че по вина на Възложителя не бъдат спазени договорените срокове за плащане, същият дължи обезщетение на Изпълнителя в размер на законната лихва върху просрочената сума от деня на забавата, но не повече от 20 (двадесет) процента от размера на забавеното плащане.

8.3. Плащането на неустойка не лишава изправната страна от правото да търси обезщетение за претърпени вреди и пропуснати ползи над размера на неустойката.

8.4. Възложителят има право да задържи представената гаранция за изпълнение на договора в пълен размер в случаите, в които едностранно и предсрочно прекрати договора, поради пълно неизпълнение от страна на Изпълнителя, поради частично или пълно неизпълнение на задълженията за доставка от Изпълнителя с повече от 30 дни, или поради откриване на производство за ликвидация или обявяване в несъстоятелност на Изпълнителя.

8.5. При забавено изпълнение на договора от Изпълнителя, Възложителят има право да задържи в пълен или частичен размер представената гаранция за изпълнение на договора или да извърши прихващане от стойността на дължимо плащане към Изпълнителя за покриване на дължимите от последния неустойки.

IX. НЕПРЕОДОЛИМА СИЛА:

9.1. Страните по настоящия договор не дължат обезщетение за претърпени вреди и загуби, в случай че последните са причинени от непреодолима сила, а именно обстоятелства, включително от извънреден характер, възникнали след сключване на договора, независимо от волята на страните, които не са могли да бъдат предвидени и правят невъзможно изпълнението при договорените условия.

9.2. В случай че страната, която е следвало да изпълни свое задължение по договора, е била в забава, тя не може да се позовава на непреодолима сила.

9.3. Страната, засегната от непреодолима сила, е длъжна да предприеме всички действия с грижата на добър стопанин, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна в срок до 15 (петнадесет) дни от настъпването на непреодолимата сила. При неуведомяване се дължи обезщетение за настъпилите от това вреди.

9.4. Докато трае непреодолимата сила, изпълнението на задълженията на страните и на свързаните с тях насрещни задължения се спира. След отпадане на непреодолимата сила страните са длъжни да подновят изпълнението на договорните си

чл. 2 от ЗЗЛД

задължения, като сроковете за изпълнение се увеличават съразмерно със срока на действие на непреодолимата сила.

X. ПРЕКРАТЯВАНЕ НА ДОГОВОРА:

10. Настоящият договор може да бъде прекратен предсрочно:

10.1. при виновно неизпълнение на задълженията на една от страните по договора с 14-дневно писмено предизвестие от изправната страна;

10.2. от Възложителя с едномесечно писмено предизвестие, ако в резултат на обстоятелства, възникнали след сключването му, не е в състояние да изпълни своите задължения;

10.3. от Възложителя без предизвестие в случай на частично или пълно неизпълнение на задълженията за доставка от Изпълнителя с повече от 20 дни;

10.4. от Възложителя с 14-дневно писмено предизвестие при открито производство за ликвидация или за обявяване в несъстоятелност на Изпълнителя.

XI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ:

11.1. Изменение на сключения договор за обществена поръчка се допуска по изключение, при условията на чл. 43, ал. 2 от Закона за обществените поръчки и с допълнително писмено споразумение между страните, което става неразделна част от настоящия договор.

11.2. Всички съобщения, предизвестия или нареждания, свързани с изпълнението на този договор, са валидни, когато са направени от страните в писмен вид по пощенски път (с обратна разписка), по факс или по електронен път, или предадени чрез куриер срещу подпис от приемащата страна, като сроковете текат от получаването им. Съобщения или уведомления, получени в неработен ден, ще се считат за получени на следващия работен ден.

11.2.1 Всяка от страните се задължава да уведоми писмено другата страна при промяна на адресна или друга регистрация, както и на лицата, упълномощени да подписват необходимите документи във връзка с изпълнение на договора.

11.2.2. Когато някоя от страните е променила адреса си, без да уведоми за новия адрес другата страна, съобщенията ще се считат за надлежно връчени и когато са изпратени на стария адрес.

11.4. Всички спорове, възникнали между страните при и по повод изпълнението на настоящия договор, се решават по пътя на преговорите, а при липса на съгласие – от компетентния съд в Република България.

11.5. Нито една от страните няма право да прехвърля правата и задълженията, произтичащи от този договор, на трета страна, освен в случаите по чл. 43, ал. 7 ЗОП.

11.6. За всички неуредени въпроси в настоящия договор ще се прилагат разпоредбите на действащото българско законодателство.

11.7. Страните определят свои служители, които имат право да подписват необходимите документи във връзка с изпълнението на договора, както следва:

За Възложителя: Веселин Раков - началник на отдел ИКИ, тел. 02/9857 510, електронна поща: VRakov@nsi.bg.

За Изпълнителя: Анна Момчилова - ръководител проект, тел: 0882980033, електронна поща: anna.momchilova@telelink.com

11.8. Неразделна част от този договор са следните приложения:

- Приложение № 1 – Техническо задание на Възложителя;
- Приложение № 2 – Техническо предложение на Изпълнителя;

чл. 2 от ЗЗЛД

- Приложение № 3 – Ценово предложение на Изпълнителя;

Настоящият договор се подписа в два еднообразни екземпляра, по един за всяка от страните, и влиза в сила от датата на подписването му.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

ВЪЗЛОЖИТЕЛ: ..
(Сергей Цветарски

ИЗПЪЛНИТЕЛ: .
(Цветан Мустафчи

чл. 2 от ЗЗЛД

Съгласували:

Д. Янчева - заместник-председател на НСИ ....

Цв. Нанов - главен секретар ....

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

Ю. Стаменов - директор на дирекция ИСИ ....

А. Фасулкова - началник на отдел ФСД .....

Г. Кунчева - началник на отдел ПД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

КОНТРОЛЕН ЛИСТ N: Д-РИ-77/10.05.2016 - 1

ЗА ИЗВЪРШВАНЕ НА ПРЕДВАРИТЕЛЕН КОНТРОЛ ОТ ФИНАНСОВИЯ КОНТРОЛЬОР

ПРЕДИ ПОЕМАНЕ НА ЗАДЪЛЖЕНИЕ

/Договор с "Телелинк" ЕАД/

Настоящият контролен лист се прилага към:

- ДОГОВОР N: .....
- Договор N: РД 08- / 10.05.2016г.

За сумата от 539957.31 лв.

Проверки преди поемане на задължението:

1. Съответства ли задължението с бюджетните параграфи?	ДА
2. Налице ли е бюджетен кредит?	ДА
3. Компетентно ли е лицето, което поема финансовото задължение?	ДА
4. Правилно ли са изчислени стойностите?	ДА
5. Спазени ли са тръжните процедури и други нормативни изисквания, свързани с поемане на задължението?	ДА
6. Необходимо ли е провеждане на процедура по ЗОП ?	ДА

В резултат от извършения предварителен контрол, считам:

1. Може да бъде поето задължение в размер на 539957.31 лв. Доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на НСИ. Общата стойност на доставката и договорените услуги е в размер 449 964.43 лв. без включен ДДС.
2. Необходимо е да се представят допълнително следните документи:

Забележка:

чл. 2 от ЗЗЛД

Извършил проверката - Финансов контрольор : /ВАЛЕНТИН НАЧЕВ/

Дата 10.05.2016г.

чл. 2 от ЗЗЛД

ОБРАЗЕЦ №9

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ
ЗА УЧАСТИЕ В ОТКРИТА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„Доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на НСИ“,

ДО: **Национален статистически институт,** гр. София, ул. "П. Волов" № 2,

От: **„Телелинк“ ЕАД**

с адрес: гр. София 1756, община Столична, район Изгрев, Бизнес център Литекс Тауър, ул. Лъчезар Станчев № 3, ет. 4, тел.: 02/970 40 40, факс: 02/970 40 42, e-mail: office@telelink.com, регистриран по ф.д. № 5699/2001 г. по описа на Софийски Градски съд, Булстат / ЕИК: 130545438,
Дата и място на регистрация по ДДС: на 30.07.2001 г. от Териториална данъчна дирекция – София, Данъчно подразделение „Средец“

УВАЖАЕМИ ДАМИ И ГОСПОДА,

След запознаване с настоящата документация за участие в открита процедура за възлагане на обществена поръчка с предмет: **„Доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на Национален статистически институт”**, предлагаме да изпълним поръчката съгласно техническите изисквания, неразделна част от документацията за участие при следните условия:

Срок за изпълнение на поръчката:

1. **Доставката ще извършим за срок до 30 (тридесет) календарни дни**, считано от датата на сключване на договора за възлагане на обществената поръчка
2. **Услугите ще извършим за срок от до 10 (десет) календарни дни** след доставка на оборудването.
3. Гаранционна подръжка на доставената техника за срок от 36 (тридесет и шест) месеца считано от датата на подписване на приемо-предавателния протокол.

Гаранционният период започва да тече от датата на подписване на протокола за приемане на доставеното оборудване и се отнася до задължението на Телелинк да поправи (отстрани) несъответствия или недостатъци от всякакъв характер, вкл. явни дефекти, дефекти в материала, дефекти в изработката, механични дефекти, други недостатъци и/или повреди, освен ако същите са предизвикани от неправилно съхранение и/или експлоатация.

Гаранционното обслужване включва:

- Единствена точка за контакт за услуги по гаранцията.

1

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

- Средствата, които се използват за приемане и обработване на сервизни заявки от оторизиран персонал на Клиента са:

Работно време за приемане на сервизни заявки: 24x7
Работно време за отработване на сервизни заявки: 8x5
Време за реакция (BP): 1 час
Време за отстраняване на повредата (BOП): 3 работни дни
Телефонни номера: +359 2 970 8888; +359 2 9704098
Мобилни телефони: +359 89 9980550; +359 87 8696909
E-mail адрес: support@telelink.bg
Уеб-базирано приложение: http://support.telelink.bg

- Разрешаване на проблеми, причинени от производствени дефекти на оборудването или несъвместимост на компонентите
- Хардуерна подмяна на дефектирало оборудване и възстановяване на услугите – до 3 работни дни.
- Дефектиралата част се връща на Телелинк до 3 работни дни от подмяната и възстановяването на услугите.
- Доставка, при заявка от страна на Клиента, на актуализирани версии на операционния софтуер (OS) на хардуера съгласно условията закупената версия.
- Ескалация към производителя, при необходимост

4. Техническа спецификация

Предоставяме техническото предложение за доставка на комуникационно оборудване. В техническото предложение за реализиране на комуникационната инфраструктура на територията на Национален статистически институт (НСИ) са описани и обосновани в пълнота и детайлност интеграцията на всички компоненти в наличната информационна среда, взаимовръзките, капацитетът и функционалността на техническата инфраструктура, имащи пряка връзка с проекта.

Предложената комуникационна инфраструктура гарантира постигане целите на проекта, като е избрана така, че да осигури изпълнение на специфичните изисквания към системата, както и да отговори на бъдещите нужди на НСИ за развитие.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

1. Предложен хардуер

В следващата таблица е представен списък на предложеното оборудване, което ще бъде използвано при изграждането на комуникационната инфраструктура:

Таблица 1: Комуникационно оборудване

Тип устройство	Описание	Брой
	Комутатор за център за данни	
N5K-C5672UP	Nexus 5672UP 1RU, 32x10G SFP+, 16pxUP SFP+, 6x40G QSFP+	2
N5672-ACC-KIT	Nexus 5672 Chassis Accessory Kit	2
SFP-10G-AOC5M	10GBASE Active Optical SFP+ Cable, 5M	16
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	4
N56-VMFEX9	Nexus 5600 VM-FEX license	2
N56-BASIK9	Nexus 5600 Series LAN Base License	2
NXA-PAC-1100W	Nexus 1100W Platinum PS, Port side Exhaust airflow	4
N6K-C6001-FAN-F	Nexus 6001 Fan for Port Side exhaust (Front to Back) airflow	6
N1K-VLCPU-96-ESSTL	Nexus 1000V Essential Edition Paper Delivery License Qty 96	2
N6KUK9-710N1.1B	Nexus 5600/6000 Base OS Software Rel 7.1(0)N1(1b)	2
N2K-C2232TM-E	N2K-C2232TM-E-10GE (32x1/10GT+8x10GE), airflow/power option	2
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	4
N2200-PAC-400W-SN	N2200-PAC-400W Power Supply - Service Specific	4
N2K-C2232-FAN-SN	N2K-C2232-FAN-SN - Service Specific	2
N2232TP-E-FA-BUN	Standard airflow/AC pack: N2K-C2232TM-E-10GE + Uplink Module	2
	Граничен комутатор	
WS-C2960X-24TD-L	Catalyst 2960-X 24 GigE, 2 x 10G SFP+, LAN Base	2
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	2
PWR-CLP	Power Retainer Clip For Cisco 3560-C and 2960-C Compact Swit	2
C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	2
CAB-STK-E-0.5M	Cisco FlexStack 50cm stacking cable	2
	Маршрутизатор	
ASR1001X-2.5G-VPN	ASR1001-X, 2.5G, VPN Bundle, K9, AES, Built-in 6x1G	2
SLASR1-AES	Cisco ASR 1000 Advanced Enterprise Services License	2
ASR1K-INTLRNET	ASR1K-Int Edge/Peering incl. BGP/NAT/ZBFW - tracking only	2
SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)	12
M-ASR1001X-8GB	Cisco ASR1001-X 8GB DRAM	2
SPA-BLANK	Blank Cover for regular SPA	2
NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	2
SASR1K1XUK9-313S	Cisco ASR1001-X IOS XE UNIVERSAL	2
ASR1001-X-PWR-AC	Cisco ASR1001-X AC Power Supply	4
FLSASR1-IPSEC	IPSEC License for ASR1000 Series	2
	Защитни стени	
ASA5525-FPWR-BUN	ASA 5525-X with FirePOWER Svcs, Chassis and Subs. Bundle	1
ASA5525-FPWR-K9	ASA 5525-X with FirePOWER Services, 8GE, AC, 3DES/AES, SSD	2
SF-FP5.3.1-K9	Cisco FirePOWER Software v5.3.1	2
ASA5525-CTRL-LIC	Cisco ASA5525 Control License	2
SF-ASA-X-9.2.2-K8	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	2
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	2
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA-IC-B-BLANK	ASA 5525-X Interface Card Blank Slot Cover	2
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client - Cisco Securily Desktop Software	2
ASA5500X-SSD120INC	ASA 5512-X through 5555-X 120GB MLC SED SSD (Incl.)	2
ASA5525-MB	ASA 5525 IPS Part Number with which PCB Serial is associated	2
L-ASA5525-TA=	Cisco ASA5525 FirePOWER IPS License	2
L-ASA5525-TA-3Y	Cisco ASA5525 FirePOWER IPS and Apps 3YR Subscription	2
FS-VMW-2-SW-K9	Cisco FireSIGHT Management Center,(VMWare) for 2 devices	1

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

SAN комутатор		
DS-C9148S-D12PSK9	MDS 9148S 16G FC switch, w/ 12 active ports + 16G SW SFPs	2
DS-SFP-FC16G-SW	16 Gbps Fibre Channel SW SFP+, LC	24
DS-9148S-KIT-CSCO	MDS 9148S Accessory Kit for Cisco	2
M91S5K9-6.2.9	MDS 9100 Supervisor/Fabric-5, NX-OS Software Release 6.2.9	2
M9148S-DPL12PSG	MDS 9148S 16G FC 12-port upgrade license + 16G SW SFPs	4
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	4
DS-SFP-FC16G-SW	16 Gbps Fibre Channel SW SFP+, LC	48
M9148S-PL12	MDS 9148S 16G FC 12-port upgrade license	4
Комутатор за ЮС сът		
WS-C2960X-48TS-L	Catalyst 2960-X 48 GigE, 4 x 1G SFP, LAN Base	15
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	15
PWR-CLP	Power Retainer Clip For Cisco 3560-C and 2960-C Compact Swit	15
GLC-SX-MMD	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	15
Опорен комутатор		
WS-C3850-12S-S	Cisco Catalyst 3850 12 Port GE SFP IP Base	2
S3850UK9-37E	CAT3850 Universal k9 image	2
CAB-TA-EU	Europe AC Type A Power Cable	2
STACK-T1-50CM	50CM Type 1 Stacking Cable	2
CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	2
C3850-NM-BLANK	Cisco Catalyst 3850 Network Module Blank	2
PWR-C1-350WAC	350W AC Config 1 Power Supply	2
PWR-C1-BLANK	Config 1 Power Supply Blank	2
GLC-SX-MMD	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	20
Комуникационен шкаф		
5509110	Сървърен шкаф TS 8 IT, 42U, 800x2000x1000мм - Комплекта включва: Завършена рамка TS 8, RAL 7035; Предна перфорирана (85%) врата с дръжка "Comfort handle" и секретен патрон, лява на отваряне 180°, RAL 7035; Задна двукрила перфорирана (85%) врата с дръжка "Comfort handle" и секретен патрон, дясна на отваряне 180°, RAL 7035; Предни 19" профили с маркировка за всяко U и възможност за настройка в дълбочина без инструменти, възможност за интегриране на кабелен организатор и/ис RFID dynamic rack control, RAL 9005; Задни 19" профили с маркировка за всяко U и възможност за настройка в дълбочина без инструменти, възможност за вертикално интегриране на резюметели от серията 7955.xxx, RAL 9005; Обща товароносимост на предни и задни 19" профили 1500кг; Покривна плоча с кабелни входове, защитени с четки и дълбочина - две и десет, възможност за монтиране на вентилаторен блок, RAL 7035; Без долна рамка и подови елени - налични като аксесоар; Заземителен комплект с централна заземителна точка; Инструкция за повече детайли покривна плоча 4 бр. в комплект Винт и гайка с винтаж с М5 за монтаж 19" оборудване - 500гр.	1
5502020	Вентилаторен покрив за TS IT с 2 вентилатора и термостат, възможност за добавяне на още 4бр. За шкафове с размери 800 x 800\1000\1200 мм	1
7980000	Испитатор 160 кв/час, 119x119x38 мм, 230 V, 15W	2
7824200	Странични 2000 x 1000 мм – 2 бр в к-т,бързосвалящи се. RAL 7035	1
7829110	Заземителен к-т за TS с размери до 800x2200x1000 мм. Комплекта включва: заземителна шина с 2 броя изолатори, кабели с определена дължина с надраснати и крепежни елементи за заземяване на всеки отделен елемент на рака	1
7159035	19" Аранжирен панел 1U с 5 бр. скоби 70x44 мм	8
7119400	Вентил 2U с дълбочина 400 мм.	2
4612000	Крака за нивелиране на шкаф (4 бр.в опак.)	1
7094100	Болт звезда M6x16мм с пластмасова шайба (50бр.) за монтаж на оборудване върху 19" профили	2
2092200	Плаваща гайка М6 (50 бр.), за монтаж на оборудване върху 19"	2

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

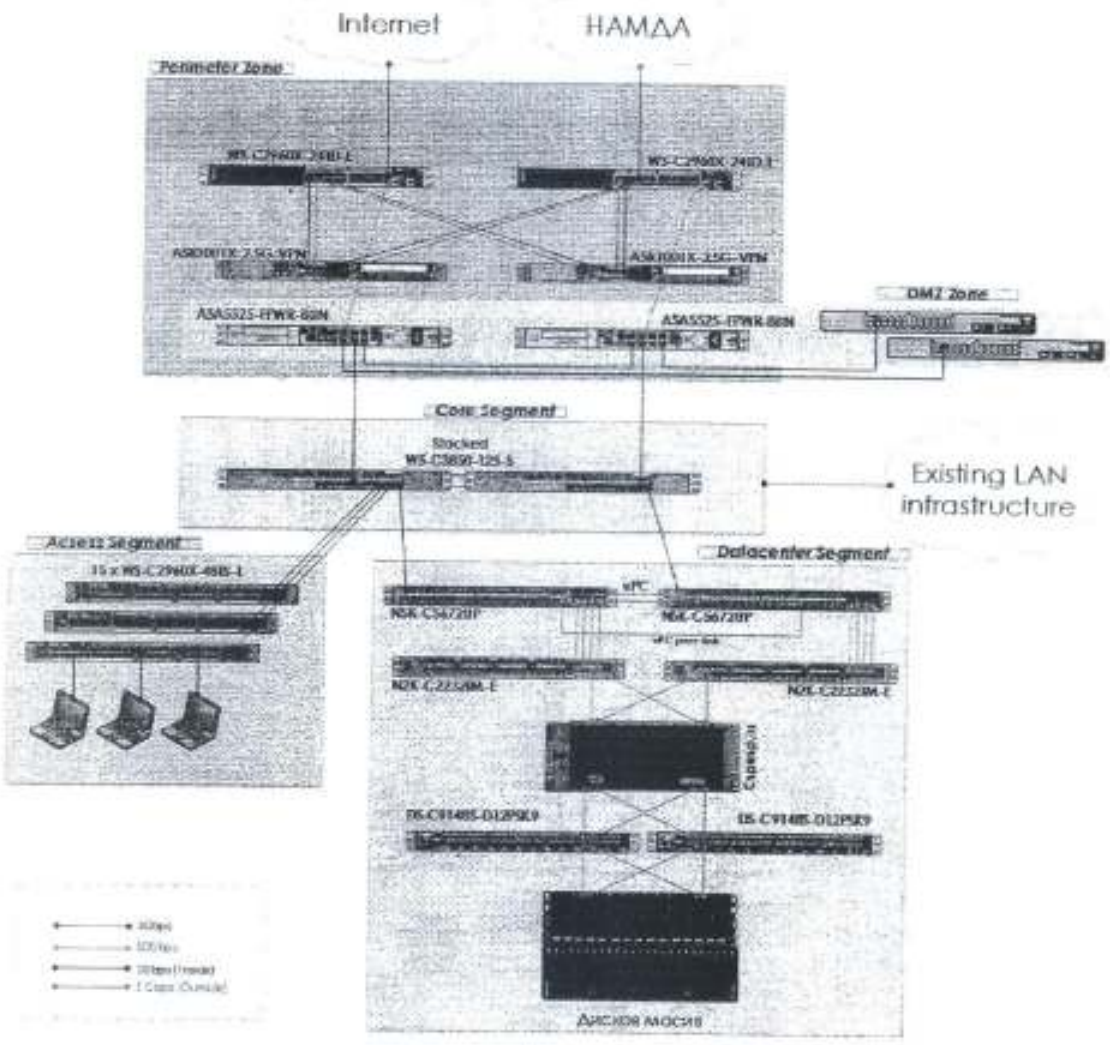
чл. 2 от ЗЗЛД

	профили	
5502105	Кабелен канал 36U за шкаф 2000мм височ. RAL9005	1
7240210	19" 1U разклонител, 7 гнезда тип „Шуко", 2м кабел без накрайник	2

2. Дизайн на техническото предложение

Целта на тази глава е да се опишат накратко дизайна, архитектурата, технологиите, решенията и способите които ще се използват при изграждането на комуникационната инфраструктура на територията на НСИ в град София.

В основата на дизайна на техническото решение е изборът на надеждно и многофункционално оборудване от доказан производител. Изборът в конкретния случай е Cisco Systems, компания с доказано високо качество и водещ пазарен дял. На фигурата по-долу е показана общата топология от гледна точка на комуникационната инфраструктура.



Фигура 1: Топология на мрежата

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

Комуникационната инфраструктура ще бъде разделена на отделни сегменти на база предназначението и функционалността, която ще изпълнява. Предвидено е

- Периметър зона(Perimeter zone) – това е зоната, чрез която се осъществява връзка към външни за НСИ комуникационни инфраструктури – Интернет, НАМДА и т.н. В нея са включени следните устройства – резервирана двойка периметър комутатори 2960X, резервирана двойка маршрутизатори ASR 1001X, както и резервирана двойка защитни стени ASA 5525X. Тези устройства ще осигурят високите нива на информационна сигурност, както и надеждността на връзките. Едновременно с това ще се гарантира висока отказоустойчивост на дизайна на периметър зоната и редица възможности за бъдещото развитие;
- Зони за сигурност(DMZ) – за да се гарантира сигурността на комуникационната инфраструктура, както и да се осигури прецизен контрол на приложенията, които са публично достъпни, ще бъдат обособени съответните зони за сигурност. Трафикът между тях и останалите сегменти от мрежата ще се контролира с помощта на защитните стени Cisco ASA 5525X;
- Гръбнак на мрежата(Core segment) – Т.нар. Core, или гръбнакът на мрежата, ще бъде изграден с помощта на едни от най-модерните и функционални комутатори към момента – Cisco 3850. Неговата задача ще бъде да осигури надеждна и високоскоростна Layer 3 връзка между всички мрежови сегменти – Perimeter, Datacenter, Access и съществуваща LAN инфраструктура. Използването изцяло на Layer 3 в този сегмент ще гарантира прецизния контрол на трафика, резервираността, както и възможността за бъдещото използване на маршрутизиращ протокол в мрежата;
- Сегмент за обработка на данни(Datacenter segment) – в този сегмент от информационната инфраструктура на НСИ ще се оформи т.нар. изчислителен център за данни. Тук ще се извършва обработката и съхранението на данни. За тази цел в него ще се използват най-модерните мрежови и SAN комутатори, предоставящи възможност за връзки със скорост до 40Gbps. Цялото оборудване в този сегмент ще е напълно резервирано. За да се постигне по-голяма гъвкавост и да се осигури функционалност, комутаторите Cisco Nexus 5672UP разполагат с унифицирани портове за осигуряване на Ethernet, FC и FCoE свързаност;
- Сегмент за достъп(Access segment) – в този сегмент ще са разположени потребителските работни станции, IP базирани телефони, принтери и т.н. Той ще бъде изграден с помощта на модерни комутатори 2960X, които ще бъдат свързани към Core комутаторите 3850. За осигуряване на резервираност в бъдеще следва да бъдат добавени нови връзки към Core сегмента от всеки от комутаторите за достъп.

Новата локална мрежова инфраструктура, която ще бъде изградена в НСИ, ще предоставя връзки с капацитет от 1 Gbps на всички портове за достъп, позволяваща високоскоростна свързаност на потребителите до информационната система. Всеки

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

един от комутаторите за достъп ще бъде свързан посредством 1 Gbps оптична (MMF) uplink връзка към опорното ниво(Core segment), където ще се извършва т.нар. Inter-VLAN маршрутизация. Трафикът в мрежовата инфраструктура ще бъде обособен в няколко логически подмрежи, съобразно най-добрите практики за изграждане на подобни архитектури. Всяка отделна IP мрежа ще използва уникален VLAN ID идентификатор. Предвидени са и два (2) броя гранични комутатори, които ще терминират връзките към външните за НСИ комуникационни структури. Тези устройства ще бъдат обединени в едно логическо такова посредством Cisco FlexStack+ технологията, позволяваща до 80 Gbps комуникация между членовете на стека.

Предвидените опорни комутатори са от серията Cisco 3850, предоставящи общо 24x1Gbps (12 на комутатор) порта и които ще бъдат обединени в логически стек посредством Cisco StackWise-480 технологията, позволяваща до 480 Gbps комуникация между членовете на логическия стек.

Към опорния слой ще бъдат свързани и двойка сървърни (Datacenter segment) комутатори Nexus 5672UP, които ще предоставят унифицирани (FC, FCoE и Ethernet) портове към изчислителната инфраструктура. Скоростта между опорния слой и сървърните комутатори ще бъде 2x1 Gbps или общ агрегиран капацитет от 2 Gbps.

Подобно на технологията Cisco StackWise при опорните комутатори, при сървърите комутаторите ще се използва технология vPC, която им позволява да се представят като едно логическо устройство на други устройства, към които са свързани. По този начин се постига по-добро уплътнение на линиите за пренос на данни, по-висока отказоустойчивост и по-добро и улеснено управление. За целта между двата дейтацентър комутатора се активират 2x10 Gbps връзки обособени за vPC функционалността.

За да се осигури високоскоростна и надеждна връзка към дейтацентър сегмента, в който са разположени сървърите ще се използват 1Gbps връзки, които са обединени в логически линии с помощта на двете основни технологии:

- От страна на комутаторите Cisco 3850 се използва Port Channel технологията;
- От страна на дейтацентър комутаторите ще се използва VPC технологията.

С тяхна помощ се изгражда единна логическа свързаност със скорост от 2 Gbps между LAN и Datacenter сегментите. Тези 2 линии със скорост 1Gbps се използват едновременно, като трафика се балансира по тях. Чрез реализиране на подобна схема на свързване, отпадане на коя да е от връзките, или някое от устройствата не води до прекъсване на услуги и така се гарантира работоспособността на комуникационната инфраструктура.

Предвидени са високопроизводителни защитни стени Cisco ASA 5525 с FirePower, които ще инспектират клиентския трафик, ще осигуряват защита от атаки срещу информационните системи. Защитните стени ще работят в Active/Standby failover режим. За осигуряване на комуникациите в интернет периметъра и нужните нива на информационна сигурност ще се използват двойка Cisco маршрутизатори от ново

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

поколение Cisco ASR1001, които освен достъп до интернет ще осигуряват сигурен отдалечен достъп за контрагенти, служители и тн. до инфраструктурата и приложенията в изчислителния център.

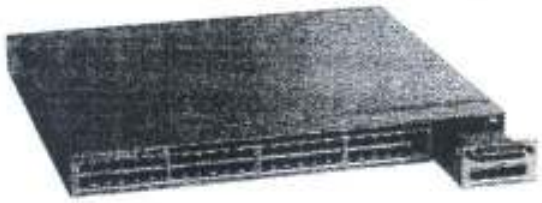
Интернет достъпа в локалната мрежова инфраструктура на НСИ ще се осигурява от маршрутизаторите Cisco ASR1001 след извършване на NAT (Network Address Translation). За целта ще се използват списъци за контрол на достъпа (ACL), конфигурирани на двата маршрутизатора, в които ще бъдат описани мрежите и хостовете, които ще имат достъп до интернет.

В текущия дизайн е предвиден и един (1) брой 42U сървърен шкаф с размери (800x2000x1000мм). Всички основни хардуерни компоненти в предложената инфраструктура ще бъдат монтирани в предложения 42U сървърен шкаф, който ще бъде оборудван с всички необходими за нормалната работа на активното оборудване пасивни компоненти – PDU, аранжиращи панели и др.

3. Взаимовръзки, капацитети и функционалности на техническата инфраструктура

3.1. Опорни комутатори Cisco 3850

Опорните комуникационни устройства ще бъдат комутаторите от най-ново поколение Cisco 3850. Те ще се използват за осигуряване на 1Gbps мрежова свързаност към сървърните комутатори и към комутаторите за достъп на територията на НСИ. Тези устройства са с изключително висока степен на отказоустойчивост и голяма производителност, с което се гарантира надеждността на изградената комуникационна инфраструктура. Опорните комутатори притежават следните технически параметри и фунционалност:



- Възможност за работа като едно логическо устройство с резервирани високоскоростни връзки между устройствата, с които се постига капацитет на преноса от 480 Gbps. Това практически означава, че двата опорни комутатора могат да бъдат разглеждани като едно устройство;
- 12 броя оптични SFP порта 10/100/1000 Mbps;
- Възможност за споделяне на захранването между комутатори, които са обединени в едно логическо устройство. При тази конфигурация двата основни комутатора могат да работят при проблем с един захранващ блок;
- Възможност за поддръжка wireless контролер с до 40Gbps капацитет и до 100 безжични точки за достъп и 2000 безжични клиенти (изисква лиценз);
- Поддръжка на Layer 3 функционалност и основни маршрутизиращи протоколи – статично маршрутизиране, RIPv1, RIPv2, RIPng
- Възможност за поддръжка на OSPFv3, BGPv4 и IS-ISv4 (изисква лиценз);
- Висока производителност при комутиране на пакети от 68 Gbps;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

- Производителност от 50,5 Mpps;
- Поддръжка на Ethernet Jumbo Frame от 9198 байта;
- Изчисленото средно време преди отказ (MTBF) 315,840 часа.

3.2. Комутатори за достъп Cisco 2960X

Надеждни 48-портови гигабитови комутатори, които осигуряват висока скорост на пренос на данни и голяма надеждност. С тяхна помощ ще бъде изграден сегмента за достъп в комуникационната инфраструктура на НСИ. Комутаторите за достъп Cisco 2960X притежават следните технически параметри и функционалност:

- 48 x10/100/1000 ethernet порта (медни);
- Разполага с 4 x 1 Gbps порта за uplink;
- Висока производителност при комутиране на пакети от 216 Gbps;
- Поддържа 107.1 Mpps forwarding производителност
- Поддръжка на 1023 активни VLAN мрежи при 4096 VLAN ID индекса;
- Поддръжка на Ethernet Jumbo Frame от 9216 байта;
- Изчисленото средно време преди отказ (MTBF) 442,690 часа;

3.3. Граничии комутатори Cisco 2960X

Надеждни 24-портови гигабитови комутатори, които осигуряват висока скорост на пренос на данни и голяма надеждност. Комутаторите за достъп Cisco 2960X притежават следните технически параметри и функционалност:

- 24 x10/100/1000 ethernet порта (медни);
- Възможност за 2 x 10 Gbps порта за uplink;
- Висока производителност при комутиране на пакети от 216 Gbps;
- Поддържа 95.2 Mpps forwarding производителност
- Поддръжка на 1023 активни VLAN мрежи при 4096 VLAN ID индекса;
- Поддръжка на Ethernet Jumbo Frame от 9216 байта;
- Изчисленото средно време преди отказ (MTBF) 569,520 часа;

3.4. Защитни стени Cisco ASA 5525X

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

Устройства от най-ново поколение, които предоставят висока производителност. Предназначението им в мрежата ще бъде да инспектират клиентския трафик, да осигуряват защита от интрузии (IPS). Част от основните характеристикина устройствата са:

- Производителност от 1 Gbps при инспектиране на трафика (SPI);
- 300 Mbps производителност за VPN с 3DES/AES криптиране;
- Поддържа 750 IPsec VPN тунела;
- Поддържа 300 000 едновременни връзки;
- Поддържа 20 000 нови връзки за секунда;
- Има вграден модул с 8 броя медни Gigabit Ethernet порта;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

3.5. Маршрутизаторите Cisco ASR 1001-X

Специализирани устройства от най-ново поколение, способни да се справят с трафик достигащ до 20Gbps. Тези маршрутизатори разполагат с най-модерната хардуерна архитектура, която им осигурява възможност за извършване на множество функции едновременно, без това да влияе на производителността. Част от основните характеристикина устройствата са:

- Производителност от 2.5Gbps;
- 6 броя вградени SFP-базирани 1Gbps интерфейси;
- Възможност за надграждане на производителността до 20Gbps;
- Възможност за обработка до 8Gbps криптиран трафик;
- 8GB оперативна памет;
- Възможност за резервиране на софтуера чрез едновременно изпълнение на две инстанции на операционната система.

3.6. Сървърните комутатори Cisco Nexus 5672UP

Устройства с най-модерна хардуерна архитектура, осигуряващи 10Gbps и 40Gbps свързаност, предоставящи възможност за едновременна връзка към Ethernet, Fibre Channel и FCoE устройства и позволяващи производителност от 1,44Tbps (терабита в секунда). Част от основните характеристикина устройствата са:

- Производителност от 1.44Tbps;
- Разполага с унифицирани портове за осигуряване на Ethernet, FC и FCoE свързаност;
- Разполага 48 броя фиксирани 1Gbps/10Gbps интерфейса;
- Всеки от фиксираните интерфейси на комутатора поддържа Ethernet и FCoE свързаност;
- 16 броя от интерфейсите на комутатора са универсални и да могат да работят с 2, 4 и 8 Gbps Fibre Channel интерфейси;
- Разполага с 6 броя 40Gbps Ethernet/FCoE интерфейси.

3.7. SAN комутатори Cisco MDS 9148S

Специализираните SAN комутатори Cisco MDS 9148S са устройства предназначени за осигуряване на връзка на системи за съхранение на

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

данни. Това са устройства от най-ново поколение, които гарантират 16Gbps Fibre Channel свързаност на всичките си 48 порта, като архитектурата им е неблокируема. Т.е. могат да бъдат натоварвани напълно, на всички портове, с максимална скорост, като това няма да доведе до загуба на данни. Част от основните характеристикина устройствата са:

- Всички портове поддържат автоматична настройка на скоростта си на 2/4/8/16 Gbps;
- Имат лиценз за работа с 36 броя интерфейси и те са окомплектовани със съответните 16 Gbps FC SFP+ модули;
- Разполагат с 256 буфер кредити на всяка група от по 4 порта;
- Поддържат виртуален SAN (VSAN) технология;
- Поддържат Access Control Lists (ACLs);
- Разполагат с по 2 броя захранващи блока за осигурявне на 1+1 резервираност;
- Захранващите блокове са сменяеми, без да се налага прекъсване на работата на устройството(hot-swappable).

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

4. Протоколи за комуникация и взаимодействие между тях.

Тази част от документа описва основните технологии и протоколи, които ще бъдат използвани при изграждането на мрежовата инфраструктура. Всяка технология е описана, като са изброени основните характеристики и приложение конкретния дизайн.

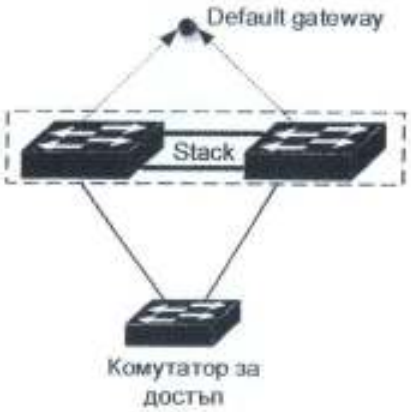
4.1. Резервиране на граничните комутатори с помощта на Cisco StackWise технологията

Тези комутатори ще бъдат обединени в една логическа система, използвайки Сиско технологията – StackWise. Чрез този метод, конфигурационната и рутиращата информация се споделя между всички комутатори в една стекираща система. Комутатори могат да бъдат добавяни или отстранявани от една система, без това да повлияе на работоспособността на останалите.

Комутаторите се обединяват в една логическа единица, чрез използването на специален за целта стекиращ кабел, както е показано на фигура 10. Всеки един комутатор в една стекираща система, има възможност да стане т.нар master или member в съответната йерархия. Master комутаторът се избира чрез определени критерии и служи като контролен център на цялата стак система. Всеки комутатор в системата има уникален номер, но цялата система разполага с един IP адрес и се управлява като един

4.1. Резервиране на опорните комутатори с помощта на Cisco StackWise технологията

Опорните комутатори Cisco 3850 също ще бъдат обединени в едно логическо устройство с помощта на Cisco StackWise технологията. При тях Layer 3 интерфейсите ще са логически SVI интерфейси, които ще бъдат прехвърляни на другото устройство при отпадане на т.нар. master в steck-а.



Фигура 4-1 - Default Gateway резервиране

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000031

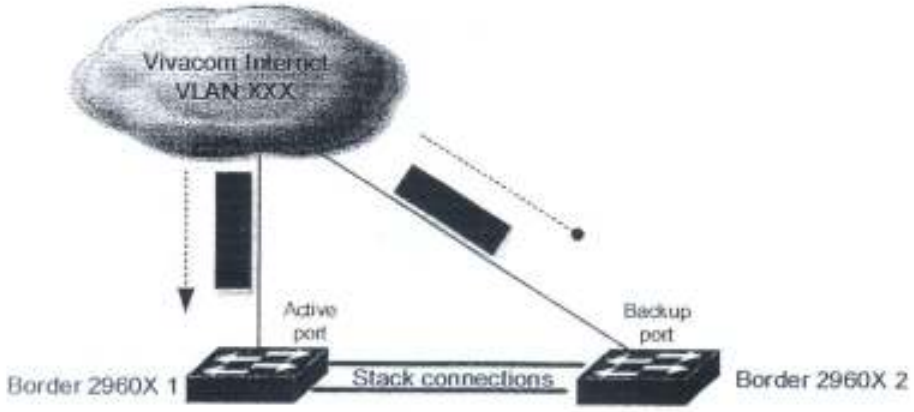
чл. 2 от ЗЗЛД

При тази конфигурация, чрез използването на SVI интерфейси във Stack конфигурация, при отпадане на един от двата опорни комутатора, Layer 3 интерфейса няма да отпадне, а ще продължи да работи на другия комутатор.

За целите на бъдещото развитие на мрежата се препоръчва изграждането на резервни връзки от всеки от комутаторите за достъп към Core сегмента. За да постигне прозрачност при добавянето на резервирана свързаност, всички физически линии ще бъдат конфигурирани в логически PortChannel интерфейси. Така при добавяне на нова връзка няма да има нужда от преконфигуриране на съществуващите и съответно няма да се наблюдава никакво прекъсване и загуба на трафик.

4.2. Резервиране на връзките с помощта на Cisco Flex Link технология

Периметър комутаторите разполагат с технология, която им позволява допълнително повишаване на отказоустойчивостта. Целта е услугите да се получават на Layer 2 през първия комутатор от т.нар. Stack и в случай на отпадане на оптичната линия да се прехвърлят през втория. За целта се използва Flex Link технологията на Cisco, при която единия порт е backup на другия.



Фигура 4-2 - Резервиране с помощта на Flex Link

Препоръчва се тази технология да се използва в бъдеще, като за целта се изгради втора оптична свързаност към Internet доставчика/доставчиците. Втората оптична свързаност следва да използва независими от първата трасета. През двете оптични връзки доставчиците следва да осигурят една и съща Layer 2 свързаност до техните маршрутизатори. По този начин с помощта на Flex Link технологията ще се осигури мигновено и прозрачно за потребителите и услугите прехвърляне на трафика в случай на проблем с оптично трасе или устройство.

4.3. Резервиране на свързаността към маррутизаторите 1001X

За постигане на висока степен на резервиране с голямо бързодействие, като с това не се блокират част от връзките в мрежата ще се използва EtherChannel протоколът (познат

чл. 2 от ЗЗЛД

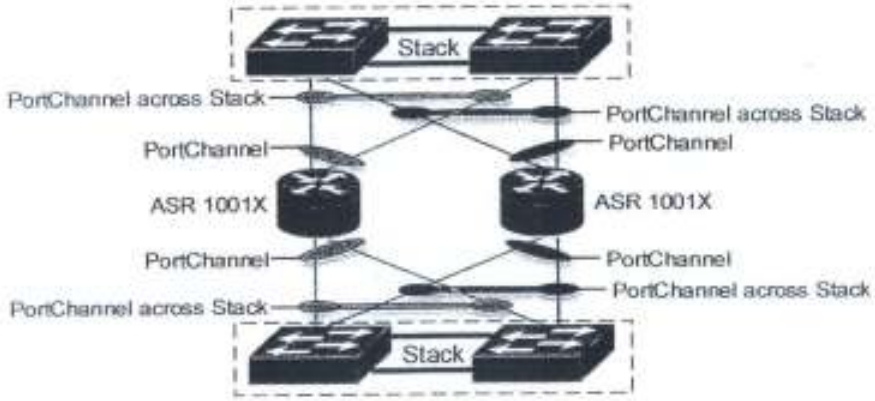
чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

също като Port Channel). Това е протокол, който е набор от две или повече физически връзки, които са обединени, с цел да формират една логическа връзка, като с това споделят своя bandwidth. Например, ако обединим два интерфейса, всеки с капацитет от по 1Gbps и използваме Port Channel протокола, двата интерфейса ще сформират един логически с общ капацитет от 2Gbps. При проблем с един от интерфейсите, работоспособността на втория не се нарушава, като единствено споделеният bandwidth отпада. Т.е. работещият интерфейс ще продължи работа с капацитет от 1Gbps. В допълнение обединените интерфейси, извършват т.нар. load balancing, т.е разпределят входящия и изходящия трафик равномерно през обединените интерфейси, предотвратявайки натоварването на единия или другия.

В конкретния дизайн ще се използва Port Channel за връзката между комутаторите за достъп и стакнатите опорни комутатори. За всяка връзка (комутатор-комутатор) ще се използват по два интерфейса в Port Channel. На следващата фигура е показана топологията на обединението на портовете:



Фигура 4-3 - EtherChannel и StackWise в Интернет периметъра

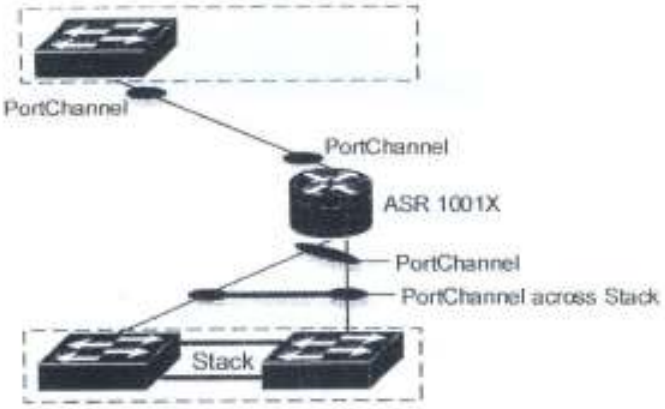
С помощта на така изградената схема ще се постигне пълно резервиране в периметъра на мрежата на НСИ. При отпадане на коя да е от връзките или устройствата, пътят на трафика ще остане незасегнат и комуникациите няма да бъдат прекъснати. На схемата по-долу е илюстрирано отпадане на две устройства от различен тип, което не засяга комуникациите. Например хардуерен проблем с граничен комутатор Cisco 2960X и BGP маршрутизатор Cisco 1001X:

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

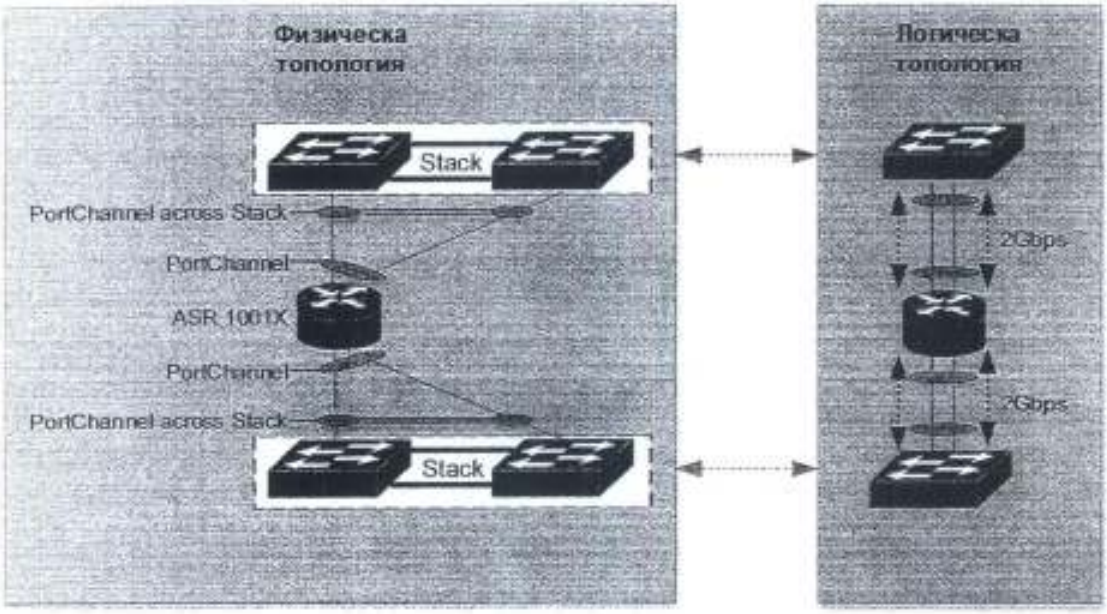
000033

чл. 2 от ЗЗЛД



Фигура 4-4 - Работа при едновременна авария на две устройства от различен тип

Освен резервиране ще се осигури и обединение на връзките, като логическата свързаност между комутаторите и маршрутизаторите ще е по 2Gbps, както за външните интерфейси, така и за вътрешните такива.



Фигура 4-5 - Обединява на интерфейсите към Интернет маршрутизаторите с цел резервиране

При използване на технологиите StackWise и EtherChannel, както е показано по-горе, се постига следното:

- Високоскоростни 2Gbps връзки между устройствата;
- Балансиране на натоварването на по линиите;
- Високоскоростно прехвърляне на трафика при отпадане на коя да е от връзките.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

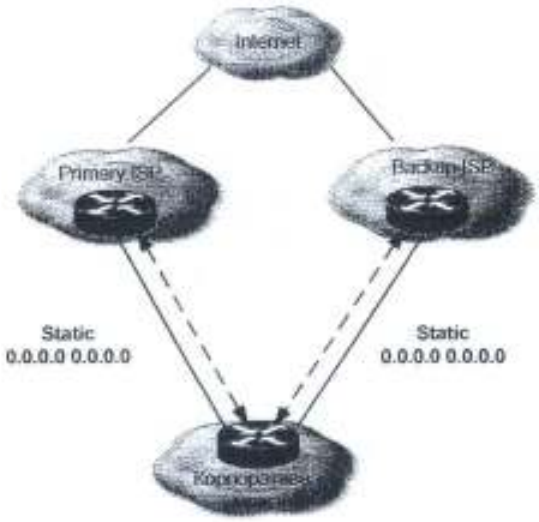
000087

чл. 2 от ЗЗЛД

4.4. Маршрутизиращ протокол BGP

Един от най-добрите начини за резервиране на Интернет свързаността на дадена организация е свързването към два независими Интернет доставчика и използването на маршрутизиращия протокол BGP (Border Gateway Protocol). По този начин се постига високо ниво на резервираност първо поради факта, че линиите, по които се предоставя свързаността са независими. Освен това, с помощта на BGP маршрутизиращия протокол се позволява голяма прецизност при управлението на входящия и изходящия трафик и се гарантира резервирането на трафика през различните доставчици.

При използването на два Интернет доставчика са възможни два начина на маршрутизиране на информацията. Първият е чрез използването на статични пътища по подразбиране към всеки от двата доставчика, както е показано на схемата по-долу.



Фигура 4-6 - Статична маршрутизация

Този начин не се препоръчва при големи мрежи и не може да се прилага при използването на собствено адресно пространство.

Вторият начин е чрез използването на динамично маршрутизиране. За целта се използва маршрутизиращия протокол BGP. Чрез него се обменя маршрутизиращата информация в Интернет. Използва се от всички Интернет доставчици в цял свят, като основен протокол за обмяна на адресна информация между Автономните Системи. Този метод е силно препоръчителен при наличието на повече от един Интернет доставчик и задължителен при използването на собствена Автономна Система и независимо адресно пространство.

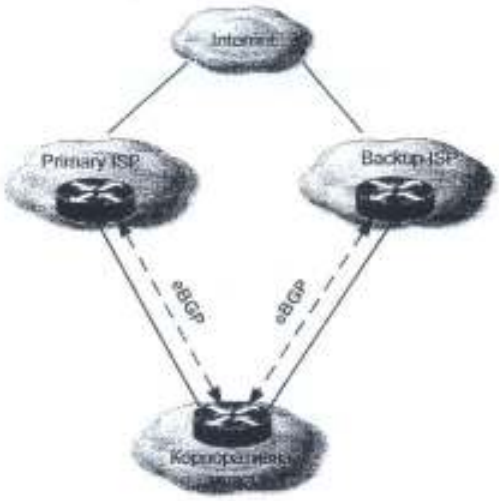
Методът за маршрутизиране чрез използване на BGP маршрутизиращия протокол при наличието на два Интернет доставчика е силно препоръчителен. По-долу е показа принципна схема на корпоративна мрежа с два Интернет доставчика и BGP сесии с тях:

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД



Фигура 4-7 - BGP маршрутизация

BGP маршрутизиращият протокол се използва винаги при необходимост от прецизен контрол при обмяната на информация с Интернет доставчика и при определяне на пътищата на изходящия и входящия трафик. Също така, той е необходим за анонсирането на независимото адресно пространство към Интернет. Предимство при използването му е, че при отпадане на едната от линиите към някой от доставчиците, другата поема целия трафик, като това става автоматично. Адресното пространство продължава да се анонсира през този, към който линията е активна.

Собствена Автономна система

Всяка Автономна Система притежава уникален Autonomous System Number (ASN) номер. С този номер се определят маршрутите на дадена организация при анонсирането им към Интернет. На база на него останалите мрежи по цял свят знаят, че даденитe мрежови префикси принадлежат на съответната организация.

Този номер трябва да бъде получен, като за него се попълва специална форма в съответния регистър. За Европа този регистър е RIPE (http://www.RIPE.net/). За да се получи номер на Автономна система трябва да се попълни RIPE NCC Autonomous System Number Request Form към съответния регистър, който в този случай е RIPE. Формата се подава през LIR (Local Internet Registry) – Локален Интернет Регистър. LIR статут имат по-големите Internet доставчици, на които е позволено да предоставят IP адресно пространство на своите клиенти.

Независимо Адресно Пространство

За постигането на максимална гъвкавост и независимост от Интернет доставчиците, всяка Автономна Система е нужно да притежава собствено адресно пространство, което е регистрирано на нейно име. По този начин смяната на доставчика няма да доведе до преадресиране в организацията.

Независимото адресно пространство, което се регистрира от RIPE е клас C IP мрежа (/24). За да се получи, отново е необходимо да се попълни набор от документи,

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

необходими на RIPE да определят нуждата от адресно пространство на дадената организация.

Асиметрично маршрутизиране

При използването на BGP протокола и повече от един Интернет доставчик е възможно да се получи асиметрично маршрутизиране. Това е нормално поведение в Интернет, като е възможно изпращането на трафик до дадена дестинация през единия доставчик е възможно връщането му през другия. Асиметричното маршрутизиране често води до случан, в които някои приложения може да не работят коректно или въобще не работят. Друг проблем при асиметричното маршрутизиране е това, че повечето съвременни защитни стени, които обикновено са в периметъра на корпоративните мрежи, не пропускат подобен тип трафик. Поради тази причина, както и следвайки най-добрите практики, маршрутизаторите за първото Layer 3 устройство, което ще посреща трафика към мрежата на НСИ.

4.5. Използване на HSRP протокол

HSRP е протокол, който позволява два или повече маршрутизатора да бъдат обединени в един логически, със собствен IP адрес и MAC адрес. Обединените маршрутизатори, работят в т.нар. active-standby режим, обменяйки си информационни HSRP съобщения на всеки 3 секунди по подразбиране. При отпадане на active маршутизатора, след определен интервал от време (по подразбиране 10 секунди), следващият по приоритет в HSRP сегмента, автоматично става active. По този начин всички хостове за които общия IP адрес е default gateway не нарушават своята работоспособност

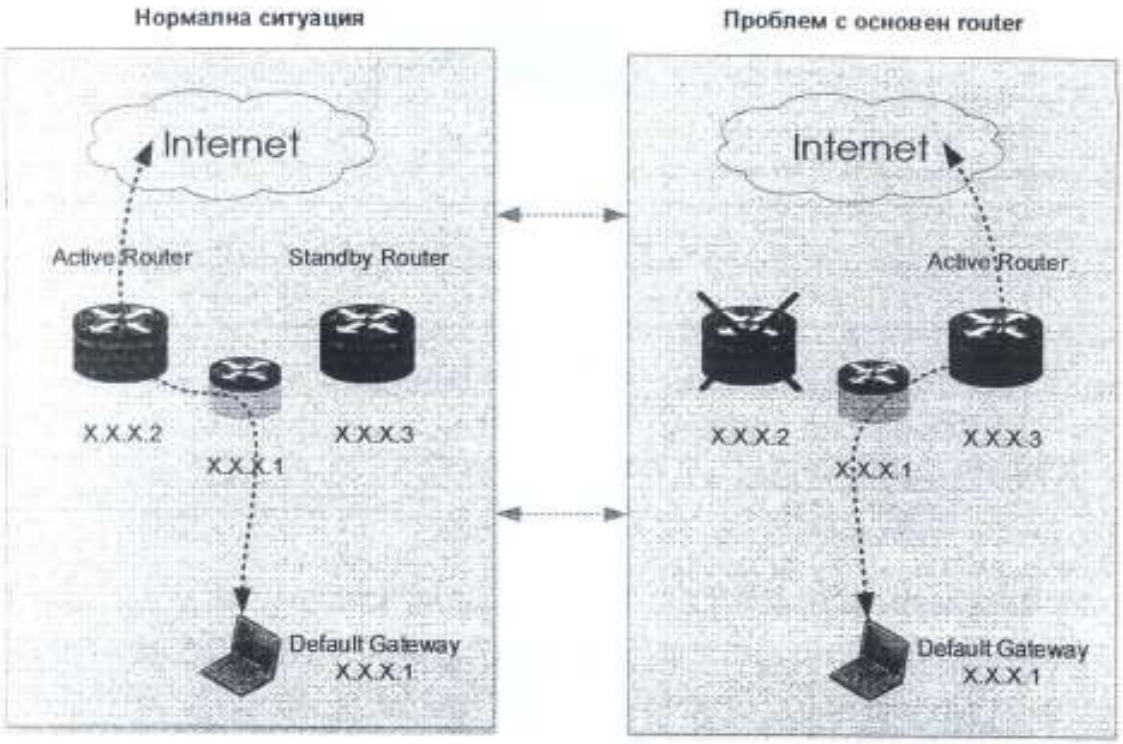
В мрежата на НСИ HSRP протокола ще се използва от маршрутизаторите ASR 1001X. По този начин те ще изглеждат като едно логическо устройство и проблем с кое да е от тях ще остане прозрачен за потребителите и услугите.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000000

чл. 2 от ЗЗЛД



Фигура 4-8 - Резервиране с помощта на HSRP протокол

4.6. IPsec VPN свързаност до отдалечени офиси

За да се осигури надеждна свързаност към отдалечените офиси на НСИ ще се използват ISsec VPN свързаност, защитена с помощта на най-модерните алгоритми за криптиране на информацията. Предложените параметри на VPN свързаността са следните:

Препоръчителни параметри на ISAKMP - Фаза 1:

Параметър	
Encryption Algorithm	256-битов AES
Hash Algorithm	Secure Hash Standard
Authentication method	Pre-Shared Key
Diffie-Hellman group	5 (1536 bit)
Lifetime	86400 seconds, no volume limit

* Ключът за всяка от VPN връзките се уточнява допълнително и се разменя между двете страни по защитен метод, за да се гарантира конфиденциалността му!

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000091

чл. 2 от ЗЗЛД

Препоръчителни параметри на IPsec - Фаза 2:

Параметър	Стойност
Encryption Algorithm	256-битов AES
Hash Algorithm	Secure Hash Standard
IPsec protocol	ESP
Authentication	HMAC-SHA
Lifetime	4608000 kilobytes/3600 seconds

4.7. Резервиране на IPSec сесиите

За резервиране на IPSec сесиите към мрежата на НСИ в бъдеще може да се използва IPSec High Availability функционалността поддържана от Cisco маршрутизаторите в периметъра на мрежата. Двойката маршрутизатори ASR 1001X, терминираща IPSec връзките използва HSRP протоколата като по този начин двете устройства изглеждат като едно физическо.

При така избраната схема Hot Standby Router Protocol (HSRP) протокола се използва за постигане на резервираност между маршрутизаторите като устройствата от отдалечените офиси виждат виртуалния IP address на HSRP групата. По този начин се позволява централните маршрутизатори да изглеждат като едно устройство за отдалечените и прехвърлянето на работата да става прозрачно и без прекъсване на връзката. Веднъж изградена IPSec връзката с активния маршрутизатор, цялата информация за нея като Internet Key Exchange (IKE) Security Association (SAs) и IPsec Security Associations се изпращат на резервния маршрутизатор с помощта на IPC (Inter-Process Communication) и така и двата поддържат информация за сесиите. При отпадане на основния прехвърлянето става прозрачно и сесиите не се разпадат.

IPSec Stateful Failover (VPN High Availability) е функционалност позволяваща при конфигурация с резервирани маршрутизатори резервният да продължи да обработва и пренасочва трафика при проблем. Резервният маршрутизатор поема работата на основния автоматично при отпадане на активния като процеса е прозрачен за потребителите. Времето за извършване на процеса зависи от таймерите на HSRP протокола.

Друга възможност за резервиране на VPN сесии е Active/Standby failover режима на работа на защитните стени ASA 5525X. С тяхна помощ може да се изграждат, както IPsec базирани, така и SSL базирани VPN връзки, които биват автоматично резервирани. Състоянието на VPN връзките бива репликирано от активната, на резервната ASA и при отпадане основното устройство, сесиите се прехвърлят автоматично и прозрачно за потребителите.

чл. 2 от ЗЗЛД

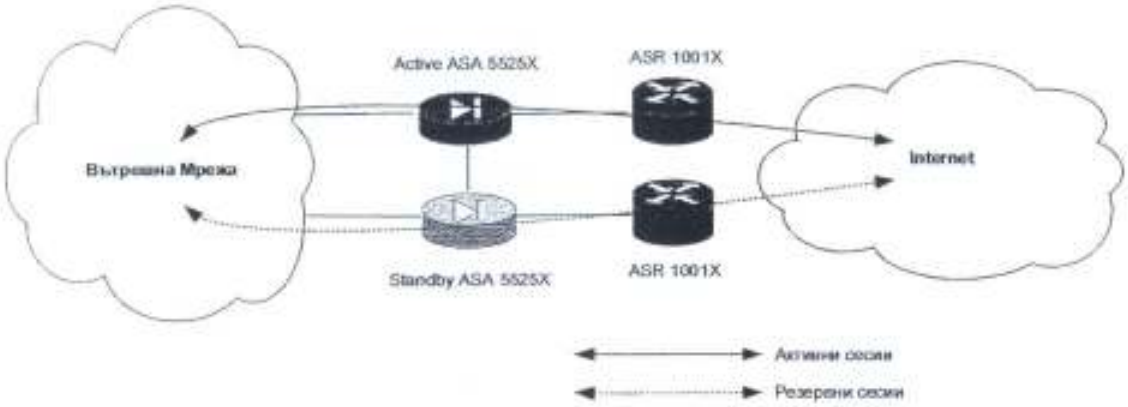
чл. 2 от ЗЗЛД

000032

чл. 2 от ЗЗЛД

4.8. Резервиране на защитните стени ASA 5525X

В мрежата на НСИ защитните стени Cisco ASA 5525X ще работят в режим на failover Active/Standby. Това води до увеличаване на надеждността в периметър зоната, където са предвидени две защитни стени, които ще работят в режим Active/Standby със Stateful Failover. При отпадане на едно от устройствата или на наблюдаван интерфейс, другото устройство може напълно да заеме функциите на първото до неговото възстановяване в работоспособно състояние. Всъщност устройствата ще бъдат напълно еднакви в конфигурацията си (чрез функцията failover) и ще обменят информация освен за състоянието на връзките си към свързаните мрежи, така и за състоянието на изградените сесии през основното. По този начин се осигурява високата отказоустойчивост на системата, понеже при отпадане на основното устройство, резервното може да поеме неговата работа дори като запази вече изградените сесии. Такова прехвърляне от активно към резервно устройство остава незабелязано за крайния потребител на системата.



Фигура 4-9 - Active/Standby Failover режим на работа

4.9. Изграждане на зани за сигурност и DMZ зони

За да се осигури прецизен контрол на трафика преминаващ през защитните стени ASA 5525X, всеки от интерфейсите им ще бъде конфигуриран с определено ниво на сигурност. По този начин ще се разграничат по-сигурните от по-несигурните интерфейси и връзки, като например т.нар. outside интерфейс към Internet и inside интерфейс към локалната мрежа. Основните функции на защитните стени включват:

- Запазват и анализират информация за състоянието на връзките, изградени през устройството;
- По подразбиране са разрешени само еднопосочните връзки от интерфейс с по-високо ниво на сигурност към интерфейс с по-ниско ниво (изходящи връзки);
- Наблюдават се пакетите в обратна посока за валидност (т.е. ако не принадлежат на вече изградена сесия или са били модифицирани по пътя, те се забраняват);

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

- Правят първоначалния sequence number случаен, за да не може да се повлияе на нерегламентирано изграждане на нови сесии, които не произхождат от сигурната мрежа или разпадане на вече изградени такива.

За осъществяване на посочените функции защитните стени използват концепцията за нива на сигурност на всеки интерфейс (security level), както е показано на фигурата по-долу:

Фигура 4-10 - Нива на сигурност при защитните стени ASA

Интерфейсите на защитните стени на Cisco трябва да бъдат обозначени със съответния security level, за да може операционната система да изгради съответствие на нивото на сигурност със съответните правила за обработване на трафика. Един интерфейс се смята за по-сигурен от друг, ако неговата стойност на нивото за сигурност е по-висока от стойността на втория. В такъв случай трафикът е разрешен по подразбиране (без специфициране на други правила) само от по-сигурния към по-малко сигурния. Ако сесиите произхождат от по-несигурен към по-сигурен интерфейс, то трафика трябва изрично да бъде разрешен с използването на листа за достъп, както е посочено на фигурата по-горе.

Стойността на нивото на сигурност може да варира в граници от 0 (най-малко сигурен - Internet) до 100 (най-сигурен - вътрешна мрежа). Препоръчително е за крайните устройства, намиращи се зад интерфейс с ниво на сигурност 100, да не се изграждат директни връзки от глобалното Интернет пространство. Тоест, ако дадено устройство трябва да има директна връзка от Интернет, то да бъде поставено в така наречената DMZ (De-Militarized Zone) зона. Това представлява буферна зона със

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

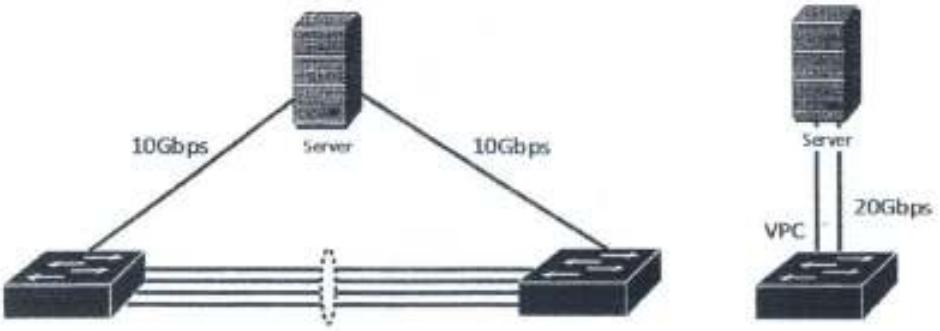
0000347

чл. 2 от ЗЗЛД

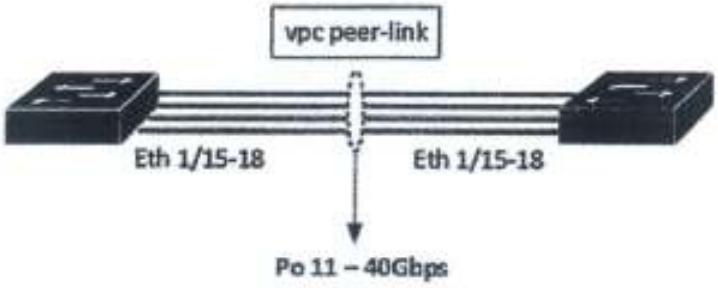
съответните правила за сигурност, в която се поставят устройства (сървъри), който трябва да бъдат достъпвани, както от вътрешната мрежа, така и от несигурната зона (Интернет).

4.10. VPC технология за резервиране на дейтацентър комутатори

За резервирена не дейтацентър комутаторите Cisco Nexus 5000 ще се използва технология, която им позволява да се представят като едно логическо устройство на други устройства, към които са свързани. По този начин се постига по-добро уплътнение на линиите за пренос на данни, по-висока отказоустойчивост и по-добро и улеснено управление.



За целта в мрежата на НСИ ще се изгради 40Gbps свързаност между двата дейтацентър комутатора Cisco Nexus 5000, използваща 4 броя 10Gbps интерфейси. Тя ще служи за т.нар. vpc peer link между двата комутатора и ще осигурява високоскоростна резервирана връзка.



чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000095

чл. 2 от ЗЗЛД

4.11. Маршрутизиращ протокол OSPF

За целите на бъдещото развитие, в гръбнака на мрежата може да се внедри и използва OSPF маршрутизиращия протокол, за който има възможност за поддръжка в избраните опорни и datacenter комутатори. С негова помощ ще се осигури данамично обновяване на маршрутизиращата информация в устройства и ще се гарантира коректността на пътищата на трафика.

4.12. Методи за гарантиране на качеството на услугите

Съществуват различни методи и механизми за осигуряване качество на услугите (Qualisty of Service). QoS е метод за осигуряване и гарантиране на качеството на услугите. Предимствата при прилагане на **QoS** методите са следните:

- Гарантиране на различни параметри на QoS в зависимост от типа трафик – малки закъснения за VoIP трафик, малки загуби за трафик от критични бизнес приложения и др.
- Управление и предотвратяване на претоварвания (congestion management, avoidance)
- Ограничаване на трафика (traffic shaping);

QoS налага качество на услугите, като работи с определени мрежови параметри:

- Загуби (**loss**);
- Забавяне (**delay**);
- Вариации на забавянето (**jitter**);

Механизмите за осигуряване на качеството на услугите са различни по своя характер и имплементиране. Като при различните мрежови архитектури се предлагат различни методи за QoS, като могат да се разграничат следните основни метода:

- **CBWFQ (Class Based Weighted Fair Queue)**

При CBWFQ могат да се определят различни класове трафик, като максималния брой на класовете е 64. Определянето може да стане чрез NBAR (автоматизирано разпознаване на типа на трафика) или ACL (Access-Contol Lists). CBWFQ гарантира минимална честотна лента за всеки клас. Когато линията е свободна, този клас може да взима от свободната честотна лента на другите класове.

- **LLQ (Low Latency Queuing).**

Това е метод, при който един или повече от класовете се дефинират чрез „**Priority queue**", т.е. този клас е с най-голям приоритет. Използва се при нужда от приоритизиране на VoIP трафик.

Основен момент в осигуряване на QoS е маркирането и класификацията на трафика. За целта се използват главно следните технологии:

- **IP DSCP (Differentiated Service Code Point)** – Позволява маркиране на трафика на мрежово ниво (в заглавната информация на IP пакета).
- **CoS (Class of Service)** – Позволява маркиране на трафика на канално ниво (във VLAN заглавната информация на Ethernet рамката). CoS ползва 802.1Q/802.1p.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

което задължава при необходимост от пренос на трафик, маркиран с CoS, задължително този трафик да има и 802.1Q заглавна информация.

Предложението съгласно добрите практики е да се използва QoS модел, чрез класифициране на трафика възможно най-близо до неговия източник, т.е. мрежовото ниво за достъп (класификация на постъпващият трафик от клиентите на мрежата). Класификацията на трафика постъпващ в слоя за достъп ще става с помощта на различни ACL (Access Control Lists) листи с който ще определим кой трафик е полезен, класифицираме и маркираме.

Фигура 4-11 – Класифициране на мрежовия трафик

Принципна шаблонна конфигурация за дефиниране на ACL листи на всеки един комутатор за достъп:

```
ip access-list extended [Име на ACL]
 permit udp any any [Име на протокола]
 permit tcp any any [Име на протокола]
 deny   ip any any
!
```

След като дефинираме ACL листи вече можем да дефинираме и самите трафик класове, в зависимост от посоката на трафика. Дефинирането на класове се извършва чрез следната шаблонна конфигурация

```
!
class-map match-all [Име на класа]
 match access-group name [Име на ACL]
!
```

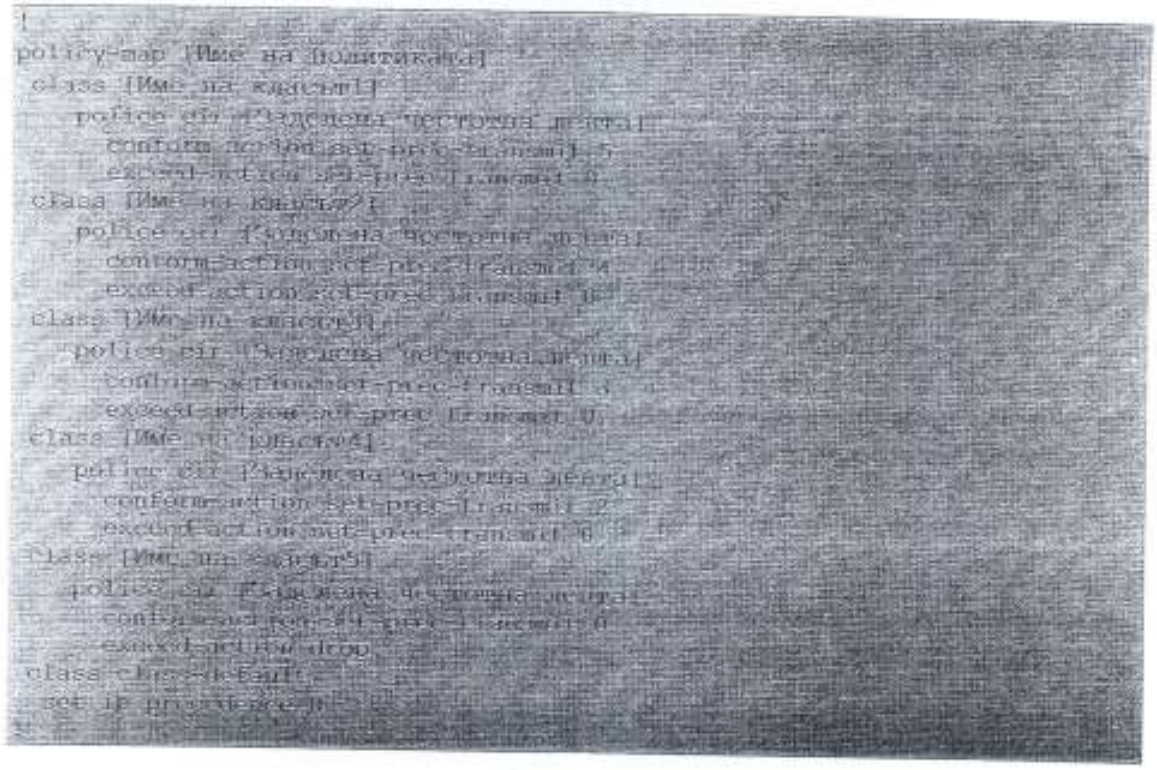

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000037

чл. 2 от ЗЗЛД

Следваща стъпка е конфигурирането на политика на всеки един клас който сме дефинирали:



Политиките трябва да съобразени със скоростта порта и с договорената между устройствата скорост. Най накрая се прилага политиката на даденият клиентския интерфейс:

4.13. Бъдещо разширение на системата в цялост

Предложеното хардуерно решение осигурява множество възможности за бъдещо развитие и разширение:

- Сървърни комутатори
  - Възможност за увеличение на портовете чрез свързване на отдалечени комутационни модули, които да се управляват от комутатора:
    - Максимум 24 броя комутационни модула;
  - Възможност за поддръжка на BGP, PBR, MSDP, uRPF чрез добавяне на допълнителен лиценз;
- Опорни комутатори
  - Възможност за добавяне на още седем (7) комутатора от същата серия към съществуващия логически стек;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000093

чл. 2 от ЗЗЛД

- Възможност за управление и контрол на безжична мрежа, чрез добавяне на допълнителен лиценз:
  - максимум 100 безжични точки
  - максимум 2000 клиента
- Възможност за поддръжка на OSPF, BGPv4 и IS-ISv4, след закупуване на допълнителен лиценз;

- Защитни стени
  - Възможност за увеличаване броя на логическите контексти в конфигурацията до максимум 20 броя след закупуване на допълнителен лиценз;
- Маршрутизатори
  - Възможност за разширение на производителността до 20 Gbps след закупуване на допълнителен лиценз;
  - Възможност за разширение на оперативната памет до 16 GB;
  - Възможност за разширение на паметта за съхранение на данни с 400-GB твърд SSD диск;
- Комутатори за достъп
  - Възможност за добавяне на още една uplink връзка към опорното ниво, с цел резервираност;
  - Възможност за добавяне на стекиращ модул към всеки комутатор и обединяването им в един логически, с цел резервираност;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000033

чл. 2 от ЗЗЛД

5. Приемни изпитания

5.1. Цел на приемните изпитания

Целта на приемните изпитания е извършването на набор от тестови процедури, които ще бъдат изпълнени за проверка на правилното функциониране на мрежата на НСИ. Тези тестове ще бъдат проведени с цел да се провери надеждността и правилното функциониране на системата, както и да се докаже работоспособността на средата изложените основни параметри от техническата спецификация.

5.2. Методология за провеждане на приемните изпитания

Тестването на системата ще бъде направено съобразно описаните тестови сценарии в този документ. Всеки един тестов сценарии включва конкретни стъпки за изпълнение, както и критерий за успешен тест. Резултатите и коментарите от тестовете ще бъдат отразени в констативен протокол – Приложение 1. Забелязаните отклонения (ако има такива) по време на тестовете следва да бъдат описани в детайли, също както и последователността от действия, които водят до отклонението, за да могат да бъдат повторени и отстранени в кратки срокове.

5.2.1. Отговорности и роли на технически лица

Техническите лица, отговорни за провеждане на функционалните тестове, са записани в следващата таблица.

Таблица 2 - Отговорници за тестовете

Име	Минимален брой участници	Компания	Условия за участие
Системен инженер	1	Телелинк ЕАД	След съгласуване
Отговорно лице	1	НСИ	След съгласуване

5.2.2. Времеви интервал за провеждане на тестовете

Времевия интервал, в който ще се провеждат функционалните тестове, ще бъде предварително съгласуван с експерти от НСИ, за да се осигури времеви прозорец за провеждането им:

Начална дата и час:.....

Крайна дата и час: .....

5.2.3. Оборудване участващо в тестовете

За успешното осъществяване на тестовете са необходими следното оборудване и софтуер:

- Минимум един преносим компютър (Notebook);
- Цялото комуникационно оборудване, съгласно изплълнената схема на свързаност и комуникация в настоящото техническото предлжоение;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000100

чл. 2 от ЗЗЛД

5.3. Процедури за тестване доказващи работоспособността на средата и заложените основни параметри и услуги от техническото предложение

Описаните тестови процедури в настоящата точка целят да докажат работоспособността на решението и средата, както и заложените основни параметри от техническото предложение.

5.3.1. [T1] Тест за проверка на достъпа до Интернет

Тест 1	Проверка на достъпа до Интернет
Цел на теста	Да се провери коректният достъп до Интернет от локалните мрежи в централата на НСИ
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Критерий за успешен тест	Успешно отваряне на български, както и чуждестранни сайтове от Интернет. Например: проверява се достъпа до www.abv.bg и www.reuters.com

Процедура за изпълнение:

- Стартираме cmd и пускаме ping до abv.bg, reuters.com, gmail.com;
- Проверяваме да ли имаме ping към адресите;
- Отваряме web browser, и се опитваме да отворим abv.bg, reuters.com, gmail.com.

5.3.2. [T2] Тест за проверка на Email услугата

Тест 2	Тест за проверка на Email услугата
Цел на теста	Да се провери дали Email услугата работи коректно през новата инфраструктура – дали се получават имейли между вътрешни потребители, както и да се провери изпращането и получаването на мейли от и към външни за фирмата email адреси
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Да има достъп до корпоративен мейл акаунт от НСИ

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000101

Критерий за успешен тест	Успешно изпращане и получаване на мейли между потребители на НСИ, както и изпращане и получаване на мейли от и към потребители, които не са част от директорията на дружеството

чл. 2 от ЗЗЛД

Процедура за изпълнение:

- Отваря се мейл акаунт, който да е част от корпоративната директория на НСИ;
- Създава се тестови мейл с прикачен тестови файл, който се изпраща към друг акаунт от НСИ;
- Проверява се коректното изпращане и получаване на мейла;
- Създава се тестови мейл с прикачен тестови файл, който се изпраща към мейл акаунт, който не е част от НСИ (например email в www.gmail.com);
- Проверява се коректното изпращане и получаване на мейла;
- След като мейла е получен в пощенската кутия на получателя се отговаря на писмото и се проверява дали имейла е получен в пощенската кутия от корпоративната директория на НСИ.

5.3.3. [Т3] Тест за проверка на достъпа до публичните услуги

Тест 3	Тест за проверка на достъпа до публичните услуги
Цел на теста	Да се провери дали има нормален достъп до web ресурсите от вътрешни и външни мрежи за НСИ
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Компютър с инсталиран web browser
Критерий за успешен тест	Успешен достъп до web услугите на НСИ

Процедура за изпълнение:

1. Осигурява се достъп до компютър, намиращ се извън мрежата на НСИ;
2. Отваря се web browser и се прави опит за отваряне на ……., както и на други web портали, свързани с НСИ – например ……..

5.3.4. [Т4] Тест за проверка на достъпът на отдалечените офиси до централата

Цел на теста	Да се провери функционалният достъп на отдалечените офиси до нужните ресурси, минаващи през централата на

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

	НСИ
Уреди/оборудване	- Персонален компютър(лаптоп) - Достъп до компютър в отдалечен офис на НСИ
Необходима предварителна подготовка	Трябва да има осигурен достъп до компютър в отдалечен офис (напр. с Remote Desktop)
Критерии за успешен тест	Успешен достъп до ресурсите на НСИ, нужни за нормалната работа на отдалеченият офис

Процедура за изпълнение:

- Осигурява се достъп до компютър, намиращ се в мрежата на НСИ
- Проверява се връзката между компютър в отдалечения офис и DNS сървъра – ping X.X.X.X

5.4. Допълнителни процедури за тестови изпитания за доказване на пълната работоспособност на комуникационната среда

Описаните тестови процедури в настоящата точка целят да докажат пълната работоспособност на решението и средата, които надхвърлят минималните основни параметри от техническото предложение, а именно резервираност и отказоустойчивост на услугите при отпадане на ключови мрежови компоненти.

5.4.1. [T5] Тест за резервираност на периметър маршрутизаторите

Тест 5	Проверка за резервираността на периметър маршрутизаторите
Цел на теста	Да се провери дали при отпадане на един от периметър маршрутизаторите, услугите продължават да функционират нормално през другия периметър маршрутизатор
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Компютърът да е включен във вътрешната мрежа на НСИ
Критерии за успешен тест	Нормално функциониране на услугите след изключване на основния периметър маршрутизатор

Процедура за изпълнение:

- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес в Интернет (например ping www.abv.bg -t)

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

00010

чл. 2 от ЗЗЛД

- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес на рутер в отдалечен офис
- Изключва се захранването на основния периметър маршрутизатор
- Проверява се дали ICMP reply съобщенията продължават да пристигат
- За по-пълна проверка на услугите, може да се изпълнят последователно предишните тестове T1 – T4
- След приключване на теста се включва захранването на основния периметър маршрутизатор и се проверяват отново услугите

5.4.2. [T6] Тест за резервираност на защитните стени

Тест 6	Проверка за резервираност на защитните стени
Цел на теста	Да се провери дали при отпадане на една от защитните стени, услугите продължават да функционират нормално през другата защитна стена
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Компютърът да е включен във вътрешната мрежа на НСИ
Критерий за успешен тест	Нормално функциониране на услугите след изключване на активната от двете защитни стени

Процедура за изпълнение:

- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес в Интернет (например ping www.abv.bg -t)
- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес на маршрутизатор в отдалечен офис
- Изключва се захранването на основната защитна стена
- Проверява се дали ICMP reply съобщенията продължават да пристигат
- За по-пълна проверка на услугите, може да се изпълнят последователно предишните тестове T1 – T4
- След приключване на теста се включва захранването на основната защитна стена и се проверяват отново услугите

5.4.3. [T7] Тест за резервираност на периметър комутаторите

Тест 7	Проверка за резервираност на периметър комутаторите
Цел на теста	Да се провери дали при отпадане на периметър комутаторите, услугите продължават да функционират нормално през резервното устройство

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000194

чл. 2 от ЗЗЛД

Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Компютърът да е включен във вътрешната мрежа на НСИ
Критерий за успешен тест	Нормално функциониране на услугите след изключване на един от двата периметър комутатори

Процедура за изпълнение:

- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес в Интернет (например ping www.abv.bg -t);
- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес на маршрутизатор в отдалечен офис;
- Изключва се захранването на първия периметър комутатор;
- Проверява се дали ICMP reply съобщенията продължават да пристигат;
- За по-пълна проверка на услугите, може да се изпълнят последователно предишните тестове T1 – T4;
- Включва се захранването на първия периметър комутатор;
- Изключва се захранването на втория периметър комутатор ;
- Проверява се дали ICMP reply съобщенията продължават да пристигат;
- За по-пълна проверка на услугите, може да се изпълнят последователно предишните тестове T1 – T4;
- След приключване на теста се включва захранването на втория периметър комутатор и се проверяват отново услугите.

5.4.4. [T8] Тест за резервираност на опорните комутатори

Тест 8	**Проверка за резервираността на опорните комутатори**
Цел на теста	Да се провери дали при отпадане на един от опорните комутатори, услугите продължават да функционират нормално през второто устройство и то става master, поемайки всички SVI интерфейси
Уреди/оборудване	- Персонален компютър(лаптоп) - Прав мрежови Ethernet кабел
Необходима предварителна подготовка	Компютърът да е включен във вътрешната мрежа на НСИ
Критерий за успешен тест	Нормално функциониране на услугите след изключване на един от двата опорни комутатора

Процедура за изпълнение:

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000105

чл. 2 от ЗЗЛД

- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес в Интернет (например ping www.abv.bg -t);
- Пуска се перманентен ping от компютъра във вътрешната мрежа до адрес на маршрутизатор в отдалечен офис;
- Пуска се ping до SVI интерфейса, който е default gateway в дадения VLAN;
- Изключва се захранването опорния комутатор, който е master;
- Проверява се дали ICMP reply съобщенията продължават да пристигат;
- За по-пълна проверка на услугите, може да се изпълнят последователно предишните тестове T1 – T4;
- След приключване на теста се включва захранването на първия опорен комутатор и се проверяват отново услугите.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000106

Приложение 1

чл. 2 от ЗЗЛД

Констативен Протокол

към

Приемните изпитания

Дата:.....

На база извършените приемни изпитания се констатира следното:

№	Наименование	Резултат		Забележки
		Да	Не	
1.	Проверка на достъпа до Интернет	☐	☐	
2.	Тест за проверка на Email услугата	☐	☐	
3.	Тест за проверка на достъпа до публичните услуги	☐	☐	
4.	Проверка на достъпът на отдалечените офиси до ресурсите на централата	☐	☐	
5.	Проверка на резервираност на периметър маршрутизаторите	☐	☐	
6.	Проверка на резервираност на защитните стени	☐	☐	
7.	Проверка на резервираност на периметър комутаторите	☐	☐	
8.	Проверка на резервираност на опорните комутатори	☐	☐	

На база критериите за успешност и съгласно процедурата за приемни изпитания за правилното функциониране на комуникационна инфраструктура на НСИ, всички изпитания се проведоха .....

(успешно/неуспешно)

Забележки/Коментари:.....

.....

.....

.....

Комисия в състав:

За НСИ:

1. .....
2. .....
3. .....

За Телелинк:

1. .....
2. .....
3. .....

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000107

чл. 2 от ЗЗЛД

6. Процедури за експлоатация

По-долу са описани всички основни процедури за експлоатация на предложеното оборудване и съпътстващия го софтуер. Те включват:

- принципни процедури за експлоатацията на предложеното техническото решение, които съдържат конфигурационни шаблони за типове оборудване и услуги;
- принципни процедури за поддръжка на комуникационната среда съгласно техническите параметри.

Настоящото ръководство е предназначено за техническия персонал, отговорен за администрирането на комуникационната инфраструктура на НСИ. Ръководството съдържа процедури, указания и шаблони на конфигурации за най-често използваните функционалности на системите и типовете устройства, които могат да послужат в изпълнението на ежедневните задачи на техническите лица .

Ръководството може да се използва като допълнение към официалната продуктова документация на системите.

6.1. Принципни процедури за поддръжка на комуникационната среда съгласно техническите параметри

6.1.1. Обновяване на софтуера на опорните комутатори

Стъпките, описани по-долу, са необходими за извършването на процедурата за обновяване на софтуера на опорните комутатори:

- Сваля се необходимия софтуер за комутаторите от сайта на производителя – http://www.cisco.com . Софтуера може да бъде намерен на следния линк - http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi
- Копира се системния софтуер на работна станция/сървър, на който е инсталиран TFTP сървър софтуер, в определената за целта TFTP директория. Необходимо е пътя до нея да е конфигуриран правилно в TFTP сървъра и той да е стартиран. Възможно е да се наложи изключване на firewall софтуера на дадената работна станция/сървър, за да не се блокират входящите TFTP заявки от мрежовите устройства, чийто софтуер трябва да бъде обновен;
- Изгражда се защитена SSH сесия до мрежовото устройство, за да се получи достъп до командния интерфейс(CLI);
- Използва се следната команда за да се извърши копиране на новия софтуер - **copy tftp flash**;
- Инсталира се системния софтуер с помощта на командата - **software install file flash:cat3k_caa-universalk9.SPA.03.03.xx.xx.xx.xx.xx.bin switch 1-2**

6.1.2. Обновяване на софтуера на комутаторите за достъп

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

Стъпките, описани по-долу, са необходими за извършването на процедурата за обновяване на софтуера на комутаторите за достъп:

- Сваля се необходимия софтуер за комутаторите от сайта на производителя – http://www.cisco.com . Софтуера може да бъде намерен на следния линк - http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi
- Копира се системния софтуер на работна станция/сървър, на който е инсталиран TFTP сървър софтуер, в определената за целта TFTP директория. Необходимо е пътя до нея да е конфигуриран правилно в TFTP сървъра и той да е стартиран. Възможно е да се наложи изключване на firewall софтуера на дадената работна станция/сървър, за да не се блокират входящите TFTP заявки от мрежовите устройства, чийто софтуер трябва да бъде обновен;
- Изгражда се защитена SSH сесия до мрежовото устройство, за да се получи достъп до командния интерфейс(CLI);
- Използва се следната команда за да се извърши копиране на новия софтуер - **copy tftp flash**;
- Настройва се комутатора да зарежда новия системен софтуер с помощта на командата – **boot system flash:/<името-на-файла.bin>**
- Рестартира се устройството, за да може да зареди новия системен софтуер;

Обновяването на софтуера на граничните комутатори се извършва по същите стъпки.

6.1.3. Обновяване на софтуера на защитните стени

Стъпките, описани по-долу, са необходими за извършването на процедурата за обновяване на софтуера на защитните стени:

- Сваля се необходимия софтуер за защитните стени от сайта на производителя – http://www.cisco.com . Софтуера може да бъде намерен на следния линк - http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi
- Копира се системния софтуер на работна станция/сървър, на който е инсталиран TFTP сървър софтуер, в определената за целта TFTP директория. Необходимо е пътя до нея да е конфигуриран правилно в TFTP сървъра и той да е стартиран. Възможно е да се наложи изключване на firewall софтуера на дадената работна станция/сървър, за да не се блокират входящите TFTP заявки от мрежовите устройства, чийто софтуер трябва да бъде обновен;
- Изгражда се защитена SSH сесия до мрежовото устройство, за да се получи достъп до командния интерфейс(CLI);
- Използва се следната команда за да се извърши копиране на новия софтуер - **copy tftp flash**;
- Настройва се комутатора да зарежда новия системен софтуер с помощта на командата – **boot system flash:/<името-на-файла.bin>**
- Рестартира се устройството, за да може да зареди новия системен софтуер;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000110

чл. 2 от ЗЗЛД

6.1.4. Обновяване на софтуера на маршрутизаторите ASR 1001X

Стъпките, описани по-долу, са необходими за извършването на процедурата за обновяване на софтуера на маршрутизаторите ASR 1001X:

- Сваля се необходимия софтуер за комутаторите от сайта на производителя – http://www.cisco.com . Софтуера може да бъде намерен на следния линк - http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi
- Копира се системния софтуер на работна станция/сървър, на който е инсталиран TFTP сървър софтуер, в определената за целта TFTP директория. Необходимо е пътя до нея да е конфигуриран правилно в TFTP сървъра и той да е стартиран. Възможно е да се наложи изключване на firewall софтуера на дадената работна станция/сървър, за да не се блокират входящите TFTP заявки от мрежовите устройства, чийто софтуер трябва да бъде обновен;
- Изгражда се защитена SSH сесия до мрежовото устройство, за да се получи достъп до командния интерфейс(CLI);
- Използва се следната команда за да се извърши копиране на новия софтуер - **copy tftp flash**;
- Настройва се комутатора да зарежда новия системен софтуер с помощта на командата – **boot system flash:/<името-на-файла.bin>**
- Рестартира се устройството, за да може да зареди новия системен софтуер;

6.1.5. Конфигурационни шаблони

6.1.5.1. Конфигуриране на VLAN

За конфигурирането на VLAN се използват следните основни команди:

```
!
vlan vlan-id
 name vlan-name
 mtu mtu-size
!
```

- **#vlan** *vlan-id* – посредством тази команда се създава VLAN със съответния му идентификационен номер. Ако този VLAN не съществува при въвеждането, то той бива създаден. Стандартно той може да бъде от 1 до 4094.
- **#name** *vlan-name* – чрез тази команда се задава име на съответния VLAN, като ако то не бъде конфигурирано, се създава автоматично по следния модел: VLANxxxx (като xxxx е номера на VLAN-а с водещи нули до запълване на четирите знака).
- **#mtu** *mtu-size* – променя размера на Maximum Transmission Unit (MTU) за съответния VLAN .

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000112

чл. 2 от ЗЗЛД

След като се създадат съответните VLAN-и, необходимо е да се конфигурира ръчно всеки интерфейс на комутатора, който ще участва в някой от създадените VLAN-и, тъй като в Cisco IOS софтуера по подразбиране всички интерфейси са във VLAN 1. За да се промени съответния интерфейс, той се поставя в режим access и чрез допълнителна команда се указва към кой VLAN ще принадлежи. Тъй като тази процедура се извършва ръчно, при необходимост от преместване на даден потребител от един физически интерфейс към друг, то тази процедура трябва да се повтори, за да може новият интерфейс, към който ще бъде свързан потребителя да е в същия VLAN, както и преди.

Тъй като в мрежата на НСИ фКще се имплементира и IP телефония, ще бъде необходимо да се създаде един допълнителен VLAN за тази цел. На всеки интерфейс към крайните устройства, на които има свързан IP телефон, трябва да се добави и VLAN за Voice, освен за access. Access VLAN-а ще се определя за конкретен потребител от табл. 4.2, в зависимост от това към кой отдел принадлежи потребителя. За изпълнението на гореописаната конфигурация се използват следните команди:

```
!
interface <interface number>
 description <interface description>
 switchport mode access
 switchport access vlan <vlan-id>
 switchport voice vlan <vlan-id>
!
```

6.1.5.2. Конфигуриране на SVI и InterVLAN Routing

За да е възможно комуникирането между различните VLAN-и се използва InterVLAN маршрутизиране, което ще бъде описано по-долу.

За мрежата на НСИ то ще се осъществява чрез Cisco 3850 комутаторите. Използват се Cisco 3850 за маршрутизиране, тъй като тази серия комутатори са високоскоростни и високопроизводителни устройства с възможност за Layer 3 функционалност. Осъществявайки маршрутизирането на комутаторите трафикът, който не е предназначен за външни мрежи се затваря във вътрешната мрежа и няма да натоварва допълнително защитните стени, които иначе биха обработвали целия трафик. Преди да бъде изпълнено каквото и да е конфигуриране за InterVLAN маршрутизиране, трябва да се осигури самото маршрутизиране. Това става със следната команда:

```
!
ip routing
!
```

След като се определи кои VLAN-и ще трябва да участват в маршрутизирането, те трябва да се добавят към VLAN database т.е. да се създадат, ако все още не са. За да може комутаторът да осъществи маршрутизирането между VLAN-ите, се създават VLAN интерфейси, назначават им се IP адреси и се активират. Ето защо се определят предварително IP адресите, които ще се използват на VLAN интерфейсите на

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000112

чл. 2 от ЗЗЛД

комутатора. Така когато комутаторът получи пакет предназначен за друга подмрежа/VLAN, той проверява в маршрутната таблица, за да определи накъде трябва да препрати пакета. След като се определи, пакетът се изпраща към VLAN интерфейса на съответната дестинация. На свой ред, след това се изпраща към порта, към който е свързано крайното устройство, за което е предназначен.

Следната конфигурация трябва да бъде въведена, за да се изпълни InterVLAN маршрутизирането, за всеки VLAN участващ в процеса:

```
!
interface vlan <vlan-id>
 ip address <a.b.c.d> <a.b.c.d>
 no shutdown
!
```

6.1.5.3. Конфигуриране на SSH(Secure Shell) достъп

За отдалечен достъп до комуникационното оборудване ще се използва Secure Shell(SSH) протоколът. SSH е сигурен протокол за комуникация, тъй като предаваните данни се криптират, за разлика от Telnet протокола, при който данните се предават в чист текст. SSH ще бъде имплементиран на всяко едно комуникационно устройство в мрежата.

Конкретно за комутаторите, SSH достъп се конфигурира по следния начин:

```
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
line vty 0 15
 transport input ssh
 login authentication default
!
```

Описание на параметрите на командите:

- **aaa new-model** – специфицира използването на aaa модела(authentication, authorization and accounting);
- **aaa authentication login default local** – специфицира автентикацията по подразбиране да се извършва локално срещу потребителите, дефинирани в съответното устройство;
- **aaa authorization exec default local** – специфицира да бъдат използвани правата, които има потребителя, дефинирани в системата;
- **line vty 0 15** – влиза в конфигурационен режим на терминалите на устройството;
- **transport input ssh** – специфицира използвания протокол за автентикация и ауторизация да бъде SSH;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000

чл. 2 от ЗЗЛД

- **login authentication default** – специфицира, че автентикацията ще е локална, тъй като това е стойността по подразбиране, зададена с командата *aaa* authentication login default local.

Потребителите се дефинират в устройствата по следния начин:

```
!
username <username> privilege <level> secret <password>
!
```

6.1.5.4. Сигурност при достъпа от конзолен порт

Конзолният достъп изисква по-ниско ниво на сигурност от отдалечения. Злонамерен потребител, който придобие физически достъп до конзолния порт, придобива възможност и за CLI достъп до устройството. По този начин той си осигурява възможност за игнориране на системните пароли и всички други логически нива на сигурност при зареждане на устройството и достъпване до привилегирован режим с пълни администраторски права върху него. Следователно, от съществено значение е физическата сигурност на всички маршрутизатори и access / core комутатори в мрежата на НСИ.

За да се гарантира някакво ниво на сигурност за достъпа до конзолната линия на комутаторите, е имплементирана следната конфигурация:

```
!
username <username> secret <password>
!
line con 0
 exec-timeout 60 0
 logging synchronous
 login authentication default
 history size 256
!
```

В горепосочената конфигурация се използва локален метод на автентикация на конзолния порт, посредством дефинираните в конфигурационния файл потребителски имена и пароли.

6.1.5.5. Конфигурация на logging

За успешно проследяване на събитията в защитната стена ще бъде имплементирана функцията за записване на журнални съобщения. Препоръчително е тези съобщения да бъдат записвани, както локално на устройствата (в буферната памет), така и на logging server. Това може да се имплементира със следните команди:

```
!
logging enable
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000

чл. 2 от ЗЗЛД

```
logging buffer-size 512000
logging buffered debugging
logging host inside  syslogd_server_ip
logging trap debugging
!
```

Описание на действието на командите:

- **logging enable** – пуска функцията за записване на журналните съобщения;
- **logging buffer-size** <*buffer_size*>– указва големината на локалната буферна памет за записване на журналните съобщения;
- **logging buffered** <*logging_level*> - указва нивото на важност на журналните съобщения, записвани в буферната памет;
- **logging host inside** <*syslogd_server_ip*> - указва IP адреса на отдалечения Syslog сървър за изпращане на журналните съобщения;
- **logging trap** <*logging_level*> - указва нивото на важност на журналните съобщения, изпращани към отдалечения Syslog сървър.

За указване на правилната часова зона и лятно часово време ще се конфигурират следните команди:

```
clock timezone EUST 2

clock summer-time EUST recurring last Sun Mar 4:00 last Sun Oct 4:00
```

6.2. Шаблони на конфигурации по типове устройства

Всяко ново устройство, което ще бъде добавяно в мрежата на НСИ към един от следните основни типове:

- Граничен комутатор

```
version 12.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname  NAME
!
logging buffered 64000 informational
aaa new-model
aaa authentication login default local
aaa authentication login VTY local
aaa authentication login CONSOLE local
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000

чл. 2 от ЗЗЛД

```
aaa authorization exec default local
enable secret 5 $1$A1.6s$ETQYh13d/TH0/jcmFcrpO1
!
username <NAME> privilege 15 secret 5 $1$4OQC$Zis4x/3M1EWPFiRfiBrAo.
clock timezone EET 2
clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
ip subnet-zero
no ip source-route
no ip gratuitous-arps
!
ip tcp synwait-time 10
no ip domain-lookup
ip domain-name <NAME>
ip ssh time-out 120
ip ssh authentication-retries 3
vtp mode transparent
!
no file verify auto
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan <ID>
 name <NAME>
!

interface FastEthernet X/Y
 description <NAME>
 switchport trunk allowed vlan <ID>
 switchport mode trunk
 no cdp enable
 spanning-tree bpdufilter enable
!
interface FastEthernet X/Y
 description <NAME>
 switchport trunk allowed vlan <ID>
 switchport mode trunk
!
interface Vlan X
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan Y
 ip address <IP> <MASK>
 no ip route-cache
!
no ip http server
!
ip access-list extended Permit_VTY_Access
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

0001

чл. 2 от ЗЗЛД

```
 permit ip <IP> <MASK> any
 deny   ip any any
logging <IP>
no cdp run
snmp-server community <NAME> RO 17
snmp-server host <IP> version 2c <NAME>
!
line con 0
 login authentication CONSOLE
line vty 0 4
 access-class Permit_VTY_Access in
 exec-timeout 3 0
 privilege level 15
 login authentication VTY
 transport input telnet ssh
line vty 5 15
 access-class Permit_VTY_Access in
 exec-timeout 3 0
 privilege level 15
 login authentication VTY
 transport input telnet ssh
!
end
```

- Маршрутизатор

```
config-register 0x2102
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname <NAME>
!
boot-start-marker
boot system flash bootflash:<NAME>
boot-end-marker
!
vrf definition <NAME>
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 512000 informational
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

0001

чл. 2 от ЗЗЛД

```
enable secret 4 Ug3jA0c5wwS3EcwZY.ka596eZn1AanLz.IH8V1oUzM
!
aaa new-model
aaa local authentication attempts max-fail 10
!
aaa authentication login default local
aaa authentication login VTY local
aaa authentication login CONSOLE local
aaa authentication login HTTPS local
aaa authorization exec default local
aaa authorization exec HTTPS local
!
aaa session-id common
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00
no ip source-route
no ip gratuitous-arps
!
no ip bootp server
no ip domain lookup
ip domain name NAME
!
login block-for 120 attempts 15 within 120
login quiet-mode access-class SSH-ONLY-MODE
login on-failure log every 10
!
multilink bundle-name authenticated
!
key chain cpg-key-chain
 key 1
  key-string 7 <removed>
!
archive
 log config
  logging enable
  logging size 1000
  hidekeys
 path flash:auto-cfg
 write-memory
 time-period 1440
!
username NAME privilege 15 secret 4
<redacted>
!
redundancy
 mode none
!
ip ftp source-interface NAME
ip tftp source-interface NAME
ip ssh port 22 rotary 10
ip ssh source-interface NAME
ip ssh version 2
ip ssh dscp 48
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

00011

чл. 2 от ЗЗЛД

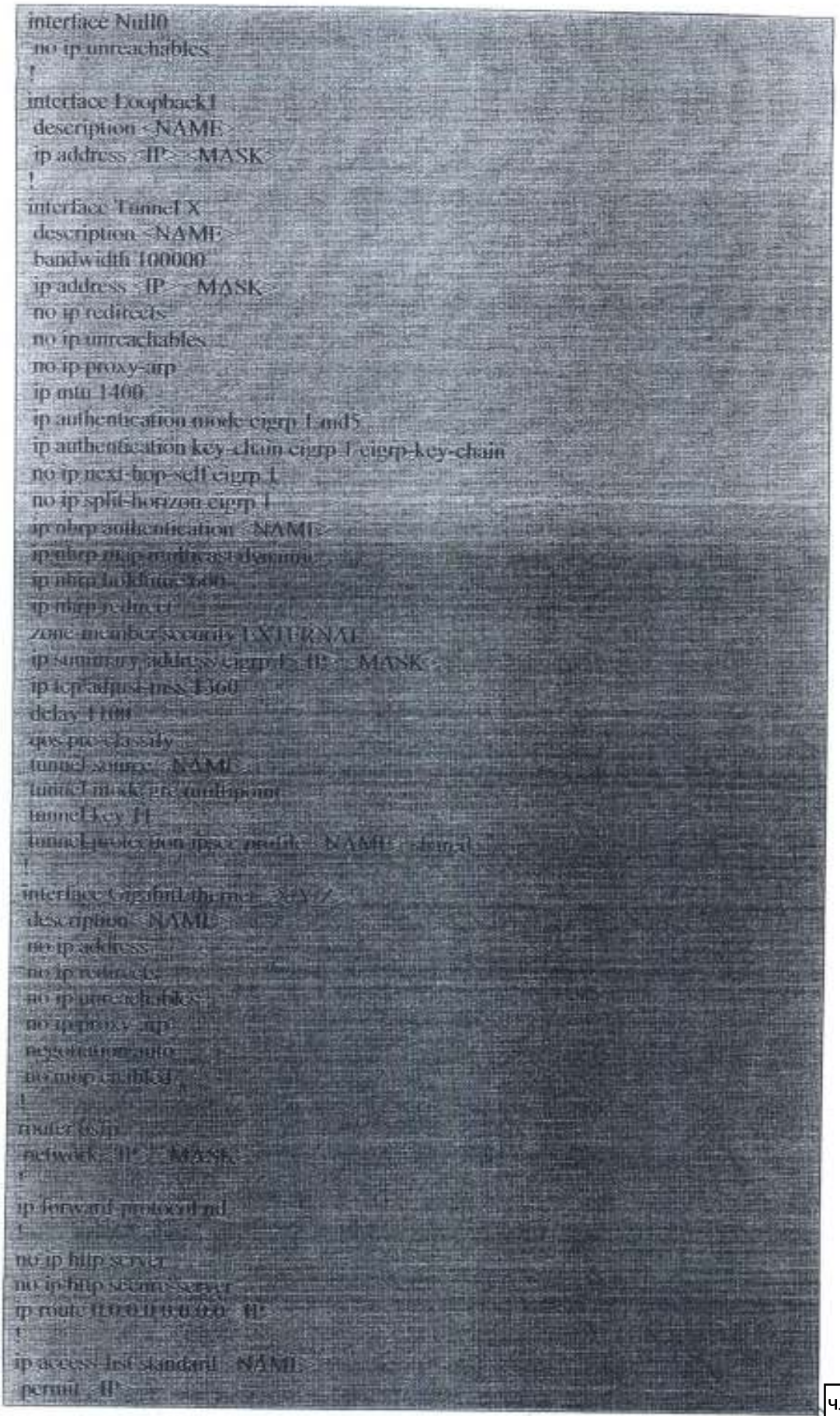
```
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name MANAGEMENT
class-map match-any CALL-SIGNALING
 match ip dscp cs3
 match ip dscp af31
class-map type inspect match-any INT-EXT-class
 match protocol icmp
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
 match protocol snmp
 match protocol snmp
 match protocol syslog
 match protocol pop3
 match protocol dns
 match protocol skinny
 match protocol h323
 match protocol sip
 match protocol telnet
 match protocol ssh
 match access-group name ftpcmd-9990
!
policy-map NAME
 class VOICE
  priority percent 33
 class CALL-SIGNALING
  bandwidth percent 5
 class INTERNETWORK-CONTROL
  bandwidth percent 10
!
zone security INTERNAL
zone security EXTERNAL
zone-pair security EXT-INT source EXTERNAL destination INTERNAL
 service-policy type inspect INT-EXT-policy
zone-pair security INT-EXT source INTERNAL destination EXTERNAL
 service-policy type inspect INT-EXT-policy
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 28800
crypto isakmp key reserved address IP MASK no-xauth
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set SOME_NAME esp-aes esp-sha-hmac
 mode transport
!
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000119

чл. 2 от ЗЗЛД



```
interface Null0
 no ip unreachables
!
interface Loopback1
 description <NAME>
 ip address <IP> <MASK>
!
interface Tunnel X
 description <NAME>
 bandwidth 100000
 ip address <IP> <MASK>
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip mtu 1400
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 eigrp-key-chain
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp authentication <NAME>
 ip nhrp map multicast dynamic
 ip nhrp holdtime 3600
 ip nhrp redirect
 zone-member security EXTERNAL
 ip summary-address eigrp 1 <IP> <MASK>
 ip tcp adjust-mss 1360
 delay 1100
 qos pre-classify
 tunnel source <NAME>
 tunnel mode gre multipoint
 tunnel key 11
 tunnel protection ipsec profile <NAME> shared
!
interface GigabitEthernet X/Y/Z
 description <NAME>
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 negotiation auto
 no mop enabled
!
router eigrp
 network <IP> <MASK>
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 <IP>
!
ip access-list standard <NAME>
 permit <IP>
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000120

чл. 2 от ЗЗЛД

```
!
ip prefix-list <NAME> permit <NET>
logging source-interface <interface>
logging <IP>
!
access-list <ID> permit ip any any
!
route-map DEFAULT_ROUTE permit 10
 match ip address prefix-list DEFAULT_ROUTE
!
snmp-server community <STRING> RW SNMP-RW-ACL
snmp-server community <STRING> RO SNMP-RO-ACL
snmp ifmib ifindex persist
!
control-plane
!
banner login ^C

THIS IS A PRIVATE NETWORK. It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.

^C
!
line con 0
 login authentication CONSOLE
 stopbits 1
line aux 0
 access-class 50 in
 login authentication VTY
 transport input all
 stopbits 1
line vty 0 4
 access-class <NAME> in vrf-also
 exec-timeout 0 0
 privilege level 15
 login authentication VTY
 rotary 10
 transport input ssh
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000121

чл. 2 от ЗЗЛД

```
line vty 5 15
 access-class <NAME> in vrf-also
 exec-timeout 0 0
 privilege level 15
 login authentication VTY
 rotary 10
 transport input ssh
!
ntp logging
!ntp authentication-key 10 md5 <removed>
ntp authenticate
ntp source Loopback1
ntp master 5
end
```

- Защитна стена

```
config-register 0x1
!
ASA Version 9.2(3)
!
hostname <NAME>
!enable password <removed>
!passwd <removed>
names
!
interface GigabitEthernet X/Y
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet X/Y
 description <to name>
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
 security-level 100
 no ip address
!
boot system disk0:/asa923-smp-k8.bin
boot system disk0:/asa912-smp-k8.bin
boot system disk0:/asa861-2-smp-k8.bin
ftp mode passive
clock timezone eet 2
clock summer-time eet recurring last Sun Mar 3:00 last Sun Oct 4:00
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network <NAME>
object service <NAME>
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000122

чл. 2 от ЗЗЛД

```
object-group network <NAME>
 network-object object <NAME>
object-group service <NAME>
 service-object tcp source eq <PROTOCOL / PORT>
 service-object udp source eq <PROTOCOL / PORT>
access-list <NAME> extended permit ip <NAME> <NAME>
logging enable
logging timestamp
logging buffer-size 100000
logging console critical
logging buffered informational
logging asdm errors
logging host localLan <IP ADDRESS>
logging class auth console debugging
logging class vpn buffered debugging console debugging
logging class webvpn console debugging
logging class svc buffered debugging
logging class ssl console debugging
mtu DMZ 1500
mtu lan 1500
mtu edge 1500
mtu outside 1500
mtu localLan 1500
failover
monitor-interface edge
monitor-interface outside
monitor-interface localLan
no monitor-interface management
icmp unreachable rate-limit 1 burst-size 1
icmp permit any lan-transport
asdm image disk0:/asdm-66114.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (NAME) source static <RANGE> destination static <NET> no-proxy-arp
!
object network <HOST>
 nat (localLan,outside) dynamic pat-pool <ADDRESS>
!
access-group outside-in in interface outside
!
route-map redistr-static-2-ospf permit 10
match ip address 56
!
route-map redistr-static-2-ospf deny 100
!
router ospf <ID>
 router-id <ID>
 network <NETWORK MASK> area <MASK>
 log-adj-changes
 redistribute connected subnets
 redistribute static subnets route-map redistr-static-2-ospf
!
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000123

чл. 2 от ЗЗЛД

```
route outside 0.0.0.0 0.0.0.0 <ADDRESS>
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-message "MESSAGE"
aaa-server RSARADIUS protocol radius
! key  <removed>
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
snmp-server host localfan <ADDRESS> community *****
no snmp-server location
no snmp-server contact
sysopt connection tcpmss 1400
crypto ipsec ikev1 transform-set ESP-AES128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
!
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 30
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics host number-of-rate 3
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate
200
ntp server <ADDRESS>
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 2
 anyconnect image disk0:/anyconnect-linux-2.5.2014-k9.pkg 3
 anyconnect enable
 tunnel-group-list enable
!
class-map global-class
 match any
class-map inspection_default
 match default-inspection-traffic
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000124

чл. 2 от ЗЗЛД

```
class-map vipsecurity
 match access-list vipsecurity-qos
!
policy-map localLan-qos
 class vipsecurity
  police input 512000
  police output 512000
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect pptp
 class class-default
  user-statistics accounting
policy-map outside_policy
 class global-class
  ips inline fail-open sensor vs0
!
service-policy global_policy global
service-policy localLan-qos interface localLan
prompt hostname priority state
no call-home reporting anonymous
: end
```

- Комутатор за център за данни

```
version 7.0(7)N1(1)
hostname <NAME>

feature telnet
cfs eth distribute
feature udld
feature lacp
feature vpc
feature lldp
feature fex

username <NAME> password 5 $1$KPKf2FU1$3zHRceMQVCZ1cHY6q8GR2/
role network-admin

banner motd
#
```

54

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000125

чл. 2 от ЗЗЛД

```
THIS IS A PRIVATE NETWORK. It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.
#

ip domain-lookup
ip domain-name <NAME>
ip name-server <IP> use-vrf management
fex 100
  pinning max-links 1
  description <NAME>
fex 101
  pinning max-links 1
  description <NAME>
snmp-server user admin network-admin auth md5
0xeb3697afbd033ed86fe053aa7862addd priv
0xeb3697afbd033ed86fe053aa7862addd localizedkey

ntp server <IP> use-vrf management

vlan <IDs>
udld aggressive
vrf context management
  ip route 0.0.0.0/0 <IP>
vpc domain 10
  role priority 100
  peer-keepalive destination <IP> source <IP>
  delay restore 150
  peer-gateway


interface port-channel10
  description <NAME>
  switchport mode trunk
  speed 10000
  vpc 10

interface port-channel99
  switchport mode trunk
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000133

чл. 2 от ЗЗЛД

```
  spanning-tree port type network
  speed 10000
  vpc peer-link

interface Ethernet X/Y
  description <NAME>
  switchport mode trunk
  channel-group 10 mode active

interface mgmt0
  vrf member management
  ip address <IP/MASK>

interface Ethernet X/Y/Z
  description <NAME>
  switchport access vlan <ID>

clock timezone EEST 2 0
clock summer-time EEST 5 sun mar 03:00 5 sun oct 04:00 60
cli alias name wr copy running-config startup-config
line console
line vty
boot kickstart bootflash:/n6000-uk9-kickstart.7.0.7.N1.1.bin
boot system bootflash:/n6000-uk9.7.0.7.N1.1.bin
poap transit
logging server <IP> 5 use-vrf management facility local2
```

- SAN комутатор

```
version 7.0(7)N1(1)
hostname <NAME>

feature telnet
cfs eth distribute
feature udld
feature lacp
feature vpc
feature lldp
feature fex

username <NAME> password 5 $1$KPKf2FU1$3zIIReeMQVCZ1cHY6q8GR2/
role network-admin

banner motd
#
THIS IS A PRIVATE NETWORK. It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000127

чл. 2 от ЗЗЛД

```
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.
#

ip domain-lookup
ip domain-name <NAME>
ip name-server <IP> use-vrf management
fex 100
 pinning max-links 1
 description <NAME>
fex 101
 pinning max-links 1
 description <NAME>
snmp-server user admin network-admin auth md5
0xeb3697afbd033ed86fe053aa7862addd priv
0xeb3697afbd033ed86fe053aa7862addd localizedkey
ntp server <IP> use-vrf management

vlan <IDs>
udld aggressive
vrf context management
 ip route 0.0.0.0/0 <IP>
vpc domain 10
 role priority 100
 peer-keepalive destination <IP> source <IP>
 delay restore 150
 peer-gateway


interface port-channel10
 description <NAME>
 switchport mode trunk
 speed 10000
 vpc 10

interface port-channel99
 switchport mode trunk
 spanning-tree port type network
 speed 10000
 vpc peer-link

interface Ethernet X/Y
 description <NAME>
 switchport mode trunk
 channel-group 10 mode active

interface mgmt0
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000123

чл. 2 от ЗЗЛД

```
  vrf member management
  ip address <IP/MASK>

interface Ethernet X/Y/Z
  description <NAME>
  switchport access vlan <ID>

clock timezone EEST 2 0
clock summer-time EEST 5 sun mar 03:00 5 sun oct 04:00 60
cli alias name wr copy running-config startup-config
line console
line vty
boot kickstart bootflash:/n6000-uk9-kickstart.7.0.7.N1.1.bin
boot system bootflash:/n6000-uk9.7.0.7.N1.1.bin
poap transit
logging server 192.168.20.38 5 use-vrf management facility local2
```

- Комутатор за достъп

```
config-register 0xF
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname <NAME>
!
boot-start-marker
boot-end-marker
!
logging buffered 512000 informational
enable secret 5 $1$8nfG$hWd7qdgFQA/oF2Vjrh.B31
!
username <username> privilege 15 secret 5 $1$V4H2$9QI28g5AbEvaAky7zW6B.1
!
macro name FREE-PORT
description ### FREE-PORT ###
 switchport access vlan 99
 switchport trunk native vlan 99
 switchport trunk allowed vlan 99
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 shutdown
@
macro name PC-PHONE
 description <NAME>
switchport access vlan $DATA_VLAN
switchport mode access
switchport nonegotiate
```


чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000123

чл. 2 от ЗЗЛД

```
 switchport voice vlan $VOIP_VLAN
 switchport port-security maximum 3
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 load-interval 30
 mls qos trust cos
 storm-control broadcast level 2.00
 storm-control multicast level 10.00
 storm-control action shutdown
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 10
!
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY local
aaa authentication login CONSOLE local
aaa authorization exec default local
!
aaa session-id common
clock timezone EET 2
clock summer-time TEST recurring last Sun Mar 3:00 last Sun Oct 4:00
system mtu routing 1500
vtp domain <DOMAIN>
vtp mode transparent
no ip source-route
no ip gratuitous-arps
!
ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name <DOMAIN>
login block-for 120 attempts 15 within 120
login quiet-mode access-class SSH_QUIET_MODE
login on-failure log every 10
!
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig (STP)
errdisable recovery cause pagp-flap
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000130

чл. 2 от ЗЗЛД

```
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause loopback
errdisable recovery cause small-frame
errdisable recovery interval 120
archive
 log config
  logging enable
  logging size 1000
  hidekeys
 path flash:auto-cfg
 maximum 5
 write-memory
 time-period 1440
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan <ID>
 name <NAME>
!
ip ssh dscp 48
ip ssh version 2
!
interface FastEthernet <slot / port>
 description <DESCRIPTION>
 switchport access vlan <ID>
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 storm-control broadcast level 2.00
 storm-control multicast level 10.00
 storm-control action shutdown
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/1
 description <NAME>
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000131

чл. 2 от ЗЗЛД

```
 switchport trunk allowed vlan <IDs>
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface <VLAN ID>
 description <NAME>
 ip address <IP> <MASK>
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
!
ip default-gateway <IP>
no ip http server
no ip http secure-server
!
ip access-list standard <NAME>
 permit <IP>
!
logging source-interface <interface>
logging <SERVER>
logging <SERVER>
snmp-server community <STRING> RW SNMP-RW-ACL
snmp-server community <STRING> RO SNMP-RO-ACL
snmp ifmib ifindex persist
banner login ^C
THIS IS A PRIVATE NETWORK. It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.

^C
!
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000132

чл. 2 от ЗЗЛД

```
line con 0
 login authentication CONSOLE
line vty 0 4
 access-class <NAME> in
 login authentication VTY
 transport input ssh
line vty 5 15
 access-class <NAME> in
 privilege level 15
 login authentication VTY
 transport input ssh
!
ntp logging
!ntp authentication-key 10 md5 <removed>
ntp authenticate
ntp source <interface>
ntp server <server> prefer
end
```

- Опорен комутатор

```
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname <NAME>
!
boot-start-marker
boot-end-marker
!
enable secret 4 qux5eyZdQEnpHOdI.qSq.98RQlrFUMGiCUL7QO4gTq2w
!
username <NAME> privilege 15 secret 4
m1LMCctNdAAdv0zRzWHe10hQXi9vTF22OHNzz0pz3Bo
aaa new-model
!
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
!
aaa session-id common
clock timezone EEST 2 0
clock summer-time EEST recurring last Sun Mar 4:00 last Sun Oct 4:00
system mtu routing 1500
no ip source-route
ip routing
no ip gratuitous-arps
!
!
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000133

чл. 2 от ЗЗЛД

```
no ip domain-lookup
ip domain-name <NAME>
login block-for 300 attempts 3 within 10
!
spanning-tree mode <MODE>
!
!
vlan internal allocation policy ascending
!
ip ftp source-interface <interface>
ip ssh version 2
!
interface GigabitEthernet <X/Y/Z>
 description <NAME>
 switchport access vlan <ID>
 switchport mode access
 spanning-tree portfast
!
interface Vlan X
 description ### DISABLED ###
 no ip address
 shutdown
!
interface <interface>
 description <NAME>
 ip address <IP> <MASK>
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 <IP>
!
ip access-list extended <NAME>
 remark <NAME>
 permit ip <IP> <MASK> any
 permit ip host <IP> any
 remark <NAME>
 permit ip <IP> <MASK> any
!
line con 0
 exec-timeout 60 0
 logging synchronous
 history size 256
line vty 0 4
 access-class <NAME> in
 logging synchronous
 history size 256
 transport preferred ssh
 transport input ssh
 transport output ssh
line vty 5 15
 access-class <NAME> in
 logging synchronous
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000134

```
 history size 256
 transport preferred ssh
 transport input ssh
 transport output ssh
!
ntp server <IP> prefer
end
```

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000135

чл. 2 от ЗЗЛД

7. Обучение на персонала

По-долу е описан подробен план за обучение на персонала, който включва описание на обхвата, методологията, стратегията, учебната база, учебна програмата(тематика) и графика на обучението. Основно са засегнати:

- методи за обучение, които ще включват теоретични лекции и практически упражнения, с което ще се осигури получаването на необходимите теоретични и практически знания по поддръжката и експлоатацията на изградената мрежа;
- предложеният подход за обучение, който позволява гъвкавост при формирането на групите за обучение;
- графикът на обучението е реалистичен и изпълним;
- учебната база и технически средства за провеждане на обучението ще бъдат осигурени от Изпълнителя;
- учебната програма обхваща тематиките на обучението, съгласно предложеното оборудване по техническата спецификация, дизайна на мрежата, процедури за конфигурации и др. Програмата може да бъде допълнена след изрично изискване от страна на Възложителя.

7.1. Обхват на обучението

Документът описва начина за провеждане на обучение на екип от специалисти на Възложителя, като целта на провежданите занятия е аудиторията да бъде запозната със съвременните технологии, оборудване и системи, използвани при изграждането на новата комуникационна инфраструктура на територията на НСИ.

Обучението ще бъде фокусирано върху технологиите, оборудването и системите, които ще изграждат комуникационната инфраструктура и нейните специфични функционалности. След завършване на обучението, екипът, който ще бъде обучаван, ще има познания за дизайна, конфигурацията, функционалността и услугите на мрежата, както и за процедурите по експлоатация и начина на работа с различните компоненти и системи.

Предвиденото обучение е с техническа насоченост, ще се проведе в рамките на 5 работни дни, съгласно предварително подготвени и съгласувани с Възложителя графици.

7.2. Документация за обучение

Изпълнителят се ангажира с осигуряването и разпространението на всички материали, които са необходими за провеждане на обучението. Материалите за обучението ще бъдат осигурени от Изпълнителя, като те ще включват материали и ръководства от

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000193

производителя на оборудването, както и специфично изготвени за обучението презентации, примерни сценарии и упражнения, където е възможно.

чл. 2 от ЗЗЛД

Занятията на обучението ще се проведат в помещения на Изпълнителя, който разполага с модерна и напълно оборудвана лаборатория. Обучението ще бъде проведено на български език.

В настоящия документ е включен примерен график обучението, който ще бъде съгласуван допълнително с Възложителя.

7.3. Методология на обучението

Занятията на обучението ще се провеждат под формата на семинари, които ще съдържат последователност от лекции и упражнения при използване на следните техники:

- Презентации – концептуално представяне на възможностите и функциите на комуникационното оборудването, което ще се използва в проекта, като също така ще се наблегне на конкретните конфигурационни шаблони за различните типове услуги и функционалността на отделните компоненти в мрежата;
- Демонстрации – ще се проиграят типични сценарии, като се демонстрират стъпки от процеса на експлоатация на комуникационното оборудване;
- Самостоятелни упражнения – курсистите ще имат възможност самостоятелно да се запознаят с възможностите на отделните компоненти на оборудването и начина на работа с мрежата;
- Обобщения – в края на всеки учебен ден се прави обобщение на ключовите знания, необходими за работа с мрежата;
- Въпроси и отговори – лекциите и упражненията протичат интерактивно, като основна задача на всеки лектор е да придобие увереност, че преподавания материал е усвоен от курсистите. Стремежът е максимално пълно да се отговори на всички възникнали въпроси по време на обучението.

Използвайки комбинацията от всички горни описание методи се гарантира осигуряването и получаването на необходимите теоретични и практически знание по поддръжката и експлоатацията на изградената мрежа.

7.4. Стратегия на обучението

Техническото обучение на екипа на Възложителя е ключов момент при експлоатацията на мрежата, като основната цел е провеждането на качествени и ефективни занятия, които да запознаят специалистите с работата с мрежовите устройства и дизайна на мрежата.

Основната задача на Изпълнителя е провеждането на качествено обучение, чрез лектори, които са специалисти с опит и познания в дадената област и предварително подготвени учебни материали и упражнения.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000137

чл. 2 от ЗЗЛД

Задача на Възложителя е изборът на точния екип от специалисти, които са пряко свързани с процеса по експлоатация и поддръжка на комуникационната инфраструктура.

7.5. Учебна база

Занятията ще бъдат проведени в лабораторна среда на Изпълнителя. Учебната зала, в която ще се провежда обучението ще бъде оборудвана с мултимедиен проектор, LAN мрежа, интернет достъп, както и сдостъп до оборудването на изградената комуникационна инфраструктура. За всеки инженер участващ в обучението ще има работно място, както и отделен комплект с учебни материали. За целите на обучението ще бъдат демонстрирани възможностите на оборудването в комуникационната система на Възложителя и/или свободно оборудване от лабораторията на Изпълнителя.

7.6. Учебна програма и предмет на обучението

За инсталираното комуникационно оборудване и дизайна на мрежата и ще бъде проведено необходимото техническо обучение на членове на екипа по експлоатация на системата от страна на Възложителя. След успешното приключване на курса, те ще имат придобити знания за изградената система, структурата, компонентите и работните й възможности. След края на курса ще бъде подписан протокол и ще бъдат издадени персонални удостоверения за преминат курс на обучение.

Обучението ще бъде съобразено с доставеното оборудване, техните конфигурации и функционалност.

№	Обучение	Съставни Модули	Продължителност
1.	Мрежова инфраструктура	Въведение в дизайна на мрежата	2 дни
		Използвани технологии	2 дни
		Специфика и поддръжка на мрежата	1 ден

В следващата част от документа са описани по-подробно темите в отделните модули на обучението, което ще бъде проведено.

Обучението ще запознае аудиторията с изградената комуникационна инфраструктура, като ще бъдат обяснение хардуерните архитектури на оборудването и използваните технологии. Обучаващият се екип ще бъде запознат с комуникационните протоколи и техните конфигурации, които са използвани така изградената мрежа. Крайната цел е персоналът, който ще експлоатира инфраструктурата, да добие пълна представа за спецификите и използваните технологични похвати в нея, за да може да я поддържа и оперира свободно.

Програма за обучението

Въведение в дизайна на мрежата

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000133

чл. 2 от ЗЗЛД

Запознаване с мрежовите устройства, използвани за изграждане на мрежата:

- Комутатори за център за данни – Cisco Nexus 5600 и Cisco Nexus 2000;
- Гранични комутатори – Cisco Catalyst 2960-X;
- Маршрутизатори – Cisco ASR 1001-X;
- Защитни стени – Cisco ASA 5525-X Adaptive Security Appliance;
- SAN комутатори – Cisco MDS 9148S Multilayer Fabric Switch;
- Комутатор за достъп – Cisco Catalyst 2960-X;
- Опорен комутатор – Cisco Catalyst 3850;

Логическа и физическа топология на мрежата

- Сегменти на мрежата:
  - Периметър зона (Perimeter zone)
  - Зони за сигурност (DMZ)
  - Гръбнак на мрежата (Core segment)
  - Сегмент за обработка на данни (Datacenter segment)
  - Сегмент за достъп (Access segment)
- Физическа свързаност;
- Интерфейси за връзка към доставчиците на услуги;
- Интерфейси за връзка към съществуващата комуникационна среда;
- IP/Ethernet;

Конвенция за именуване

- Конвенция за именуване на интерфейсите;
- Конвенция за именуване на устройствата;
- Конвенция за именуване при VPN услугите;

Схема на адресация в мрежата

- Адресация между директно свързаните устройства;
- Регионална адресация;
- Адресация при VPN услугите;

Използвани технологии

Layer 2 (Data Link)

- Ethernet базирани мрежи;

Layer 3 (Network)

- Основи на маршрутизиращите протоколи:
  - Статично маршрутизиране;
  - Динамично маршрутизиране с OSPF;
  - Динамично маршрутизиране с BGP;
  - Редистрибуция на информация за маршрутите между динамичните протоколи;
- Основи и работа на IPSec протокола;

Резервиране на услугите

- Cisco StackWise технологията
- Cisco Flex Link технология
- Port-Channel технология

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000139

чл. 2 от ЗЗЛД

- Работа на HSRP протокола
- Резервиране на IPSec сесиите

Зони за сигурност и списъци за контрол на достъпа

- Принцип на работа на защитните стени ASA
- Failover режими на работа
- Обособяване на зони за сигурност
- Списъци за контрол на достъпа
- Средства за анализ и управление на ASA

Механизми за осигуряване качество на услугите - QoS

- QoS модели – DiffServ и IntServ;
- Механизми за осигуряване на качество на услугите на второ ниво;
- Механизми за осигуряване на качество на услугите на трето ниво

Поддръжка и работа с мрежовата инфраструктура

- Запознаване с конфигурационни шаблони използвани в мрежата;
- Типове конфигурации на портове;
- Конфигурации по типове устройства;
- Управление и промени на конфигурациите в мрежата.

7.7. Списък от курсисти

Преди началото на курса Възложителя трябва да предостави списък с предвидените участниците в курса, както и да гарантира за тяхното присъствие, което ще бъде удостоверявано по време на обученията чрез попълване на присъствен лист.

Изпълнителят има възможност да осигури обучаване на максимум 10 служители на Възложителя.

Предлагаме възможност да се сформират различни групи курсисти в зависимост от тематиката на обучението и специфичните задължения на конкретния служител на Възложителя, с което ще се предостави и постигне гъвкавост на ръководството на Възложителя да подбере точните кадри за обучение. По този начин също така ще се повиши квалификацията на служителите в тяхната област на ежедневна работа.

7.8. График на обучението

Заложените програма и график на учебните занятия е реалистичен и изпълним, тъй като е съобразен с коректните тематики и необходимото време за практически упражнения за лесно възприемане и осъзнаване на новия материал от курсисти.

Описание		
Мрежова инфраструктура		
Запознаване с мрежовите устройства	2 часа	1

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

Описание	Време на продължителността	[illegible]
Логическа и физическа топология на мрежата	4 часа	1
Конвенция за именуване	1 час	1
Схема на адресация в мрежата	1 час	1
Използвани технологии		
Ethernet базирани мрежи	2 часа	2
Статично маршрутизиране	2 часа	2
Динамично маршрутизиране – OSPF, BGP	2 часа	2
Редистрибуция	2 часа	2
Основи и работа на IPSec протокола	2 часа	3
Cisco StackWise технологията	1 час	3
Cisco Flex Link технология	0.5 часа	3
Port-Channel технология	0.5 часа	3
Работа на HSRP протокола	1 час	3
Резервиране на IPSec сесиите	1 час	3
Зони за сигурност и списъци за контрол на достъпа		
Принцип на работа на защитните стени ASA	1 час	3
Failover режими на работа	1 час	3
Обособяване на зони за сигурност	1 час	4
Списъци за контрол на достъпа	1 час	4
Средства за анализ и управление на ASA	2 часа	4
Механизми за осигуряване качество на услугите – QoS		
QoS модели – DiffServ и IntServ	2 часа	4
Механизми за осигуряване на качество на услугите на второ ниво	1 час	4
Механизми за осигуряване на качество на услугите на трето ниво	1 час	4
Поддръжка и работа с мрежовата инфраструктура		
Конфигурационни шаблони	2 часа	5
Типове конфигурации на портове	2 часа	5
Конфигурации по типове устройства	2 часа	5
Управление и промени на конфигурациите в мрежата	2 часа	5
	Общо:	**5 работни дни**

***Един учебен ден включва 8 учебни часа. Учебната програма е отворена и може да претърпи промени след изрично изискване от страна на Възложителя!**

7.9. Организация на обучението

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

За провеждане на ефективно и качествено обучение трябва да се създаде организация, която да включва специалисти със следните роли:

- Лектори от страна на Изпълнителя, които ще водят учебните занятия;
- Координатор на учебните занятия от страна на Изпълнителя;
- Координатор на учебните занятия от страна на Възложителя;
- Курсисти;

7.10. Учебни материали

Учебните материали ще бъдат осигурени от Изпълнителя. Всички учебни материали ще бъдат предоставени в електронен и печатен вариант на всеки курсист, като електронната им версия ще бъде осигурена на курсистите преди започването на самия учебен процес, за да се осигури възможност за запознаване с нея. Допълнително ще бъдат предоставени подробни ръководства за потребителя, съгласно официалната документация на производителя в електронен формат.

7.11. Оценка на преподавателя

В края на провежданото обучение всички курсистите попълват Анкетна карта, в която изразяват своето мнение за качеството и ефективността на проведеното обучение и на получените учебни и помощни материали.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000142

чл. 2 от ЗЗЛД

8. Техническа спецификация

8.1. Комуникационен шкаф – 1 брой

Компоненти	Изисквания	Предлагаме
Физически характеристики	Височина минимум 42RU	**[Отговаря]** Комуникационния шкаф е с височина 42RU
	Размери минимум 800x2000x1000мм / ШхВхД	**[Отговаря]** Комуникационния шкаф е с размери 800x2000x1000мм / ШхВхД
	Предни и задни монтажни профили с маркировка на всеки RU и възможност за регулиране по дълбочина	**[Отговаря]** Предните и задни монтажни профили са с маркировка на всеки RU и възможност за регулиране по дълбочина
	Обща товароносимост на предни и задни профили не по-малко от 1400кг.	**[Надвишава]** Общата товароносимост на предни и задни профили на комуникационния шкаф е до 1500кг.
	Предна и задна вентилирани врати на 85%	**[Отговаря]** Предната и задна врата на комуникационния шкаф са вентилирани на 85%
	Покривна плоча с кабелни входове с четки	**[Отговаря]** Покривна плоча на комуникационния шкаф е с кабелни входове с четки
	Вентилаторен покрив с термостат	**[Отговаря]** Комуникационния шкаф е окомплектован с вентилаторен покрив с 2 вентилатора и термостат
	Да предоставя възможност за нивелиране	**[Отговаря]** Комуникационния шкаф е окомплектован с пълен комплект (4бр.) крака за нивелиране

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000143

чл. 2 от ЗЗЛД

Окомплектовка	Да бъде окомплектован със заземителен комплект	**[Отговаря]** Комуникационния шкаф е окомплектован със заземителен комплект
	Да бъде окомплектован със 8 броя аранжиращи панели с височина не по-голяма от 1RU	**[Отговаря]** Комуникационния шкаф е окомплектован с 8 броя аранжиращи панели с височина 1RU
	Да бъде окомплектован с 2 броя полици с височина 2RU	**[Отговаря]** Комуникационния шкаф е окомплектован с 2 броя полици с височина 2RU
	Да бъде окомплектован с 2 броя 19-инчови разклонители със 7 гнезда тип „шуко“ с височина не по-голяма от 1RU	**[Отговаря]** Комуникационния шкаф е окомплектован с 2 броя 19-инчови разклонители със 7 гнезда тип „шуко“ с височина от 1RU

8.2. Граничен комутатор – 2 броя

Компоненти	**Изисквания**	**Предлагаме**
Хардуер	Минимум 512MB DRAM	**[Отговаря]** Комутаторът разполага с 512MB DRAM
	Минимум 128 MB Flash памет	**[Отговаря]** Комутаторът разполага с 128 MB Flash памет
Производителност и функционалности	Минимум 216Gbps комутираща матрица	**[Отговаря]** Комутаторът поддържа 216 Gbps комутираща матрица
	Минимум 95 Mpps ниво на предаване на данни	**[Надвишава]** Комутаторът поддържа 95.2 Mpps ниво на предаване на данни
	Минимум 16000 MAC адреса	**[Отговаря]** Комутаторът поддържа 16000 MAC адреса
	Минимум 9198 байта MTU за L3 пакет за гигабит етернет портовете	**[Отговаря]** Комутаторът поддържа 9198 байта MTU за L3 пакет за гигабит етернет портовете
	Минимум 9200 байта MTU за L2 рамка за гигабит етернет портовете	**[Надвишава]** Комутаторът поддържа 9216 байта MTU за L2 рамка за гигабит

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

00014

чл. 2 от ЗЗЛД

		етернет портовете
	Да поддържа конфигурация в клъстерен режим със скорост на връзката между комутаторите в клъстера от минимум 78Gbps	**[Надвишава]** Комутаторът поддържа конфигурация в клъстерен режим със скорост на връзката между комутаторите в клъстера от 80Gbps
	Автоматично активиране на порт, който е бил деактивиран поради грешка в мрежата	**[Отговаря]** Комутаторът поддържа автоматично активиране на порт, който е бил деактивиран поради грешка в мрежата
	Да поддържа TFTP и NTP протоколи	**[Отговаря]** Комутаторът поддържа TFTP и NTP протоколи
	Да поддържа следните механизми за превенция на цикли в мрежата: 802.1s, 802.1d или еквивалентни	**[Отговаря]** Комутаторът поддържа 802.1s и 802.1d механизми за превенция на цикли в мрежата
	Проследяване на Layer 2 маршрут	**[Отговаря]** Комутаторът поддържа проследяване на Layer 2 маршрут
	Да поддържа LACP Link Aggregation Control Protocol	**[Отговаря]** Комутаторът поддържа LACP Link Aggregation Control Protocol
	Да поддържа минимум 4096 VLAN идентификационни номера	**[Отговаря]** Комутаторът поддържа 4096 VLAN идентификационни номера
	Да поддържа 1023 активни VLAN	**[Отговаря]** Комутаторът поддържа 1023 активни VLAN
	Да поддържа технология за отдалечено наблюдение, анализиране и управление на трафика.	**[Отговаря]** Комутаторът поддържа технология за отдалечено наблюдение, анализиране и управление на трафика.
Физически характеристики	Да бъде окомплектован с необходимите монтажни елементи за монтаж в 19" комуникационен шкаф, максимална височина 1 RU	**[Отговаря]** Комутаторът е окомплектован с необходимите монтажни елементи за монтаж в 19"

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

0001:3

чл. 2 от ЗЗЛД

		комуникационен шка и е с максимал височина от 1 RU
	Максимално тегло на устройството 4.0kg	**[Отговаря]** Комутаторът е с тегло от 4.0 kg
	MTBF не по-малко от 560 000 часа	**[Надвишава]** MTBF - 569,520 часа
	Трябва да поддържа индикатори минимум за следните характеристики: интегритет на линията, активиран, деактивиран порт, скорост и дуплекс на порта	**[Отговаря]** Комутаторът поддържа индикатори за следните характеристики: интегритет на линията, активиран, деактивиран порт, скорост и дуплекс на порта
	Работна температура: от -5 до 45°C	**[Отговаря]** Работна температура: от -5 до 45°C
Захранване	Устройството трябва да поддържа входно захранващо напрежение от 100 до 240V AC	**[Отговаря]** Комутаторът поддържа входно захранващо напрежение от 100 до 240V AC

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

0001-13

чл. 2 от ЗЗЛД

	Максимална консумация 0,035 kVA	**[Отговаря]** Максимална консумация 0,034 kVA
Интерфейси и модули	Минимум 24 x 10/100/1000 RJ45 ethernet порта (медни)	**[Отговаря]** Комутаторът разполага с 24 x 10/100/1000 RJ45 Ethernet порта (медни)
	Минимум 2 x 10GE SFP+ слота за uplink	**[Отговаря]** Комутаторът разполага с 2 x 10GE SFP+ слота за uplink
	Да бъде окомплектован с необходимите модули и материали за конфигурация в клъстерен (stack) режим	**[Отговаря]** Комутаторът с окомплектован с всички необходимитмодули и материали за конфигурация в клъстерен (stack) режим
Стандарти и сертификати	UL 60950-1, второ издание	**[Отговаря]** UL 60950-1, второ издание
	CAN/CSA 22.2 No. 60950-1, второ издание	**[Отговаря]** CAN/CSA 22.2 No. 60950-1, второ издание
	EN 60950-1, второ издание	**[Отговаря]** EN 60950-1, второ издание
	IEC 60950-1, второ издание	**[Отговаря]** IEC 60950-1, второ издание
	AS/NZS 60950-1	**[Отговаря]** AS/NZS 60950-1
	47CFR част 15 клас A	**[Отговаря]** 47CFR част 15 клас A
	EN 55022 клас A	**[Отговаря]** EN 55022 клас A
	CISPR22 клас A	**[Отговаря]** CISPR22 клас A
	ICES003 клас A	**[Отговаря]** ICES003 клас A
	AS/NZS CISPR22 клас A	**[Отговаря]** AS/NZS CISPR22 клас A
	VCCI клас A	**[Отговаря]** VCCI клас A
	CNS13438 клас A	**[Отговаря]** CNS13438 клас A
	EN61000-3-2	**[Отговаря]**

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000147

чл. 2 от ЗЗЛД

		EN61000-3-2
	EN61000-3-3	**[Отговаря]** EN61000-3-3
	KN22 клас A	**[Отговаря]** KN22 клас A
	EN55024	**[Отговаря]** EN55024
	CISPR24	**[Отговаря]** CISPR24
	EN300386	**[Отговаря]** EN300386
	KN24	**[Отговаря]** KN24
	Reduction of Hazardous Substances (ROHS) включващ директива 2011/65/EU	**[Отговаря]** Reduction of Hazardous Substances (ROHS) включващ директива 2011/65/EU
Качество на услугите	Да поддържа 802.1p class of service (CoS)	**[Отговаря]** Комутаторът поддържа 802.1p class of service (CoS)
	Да поддържа класификация на базата на source и destination IP адреси, MAC адреси или Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) номера на портове	**[Отговаря]** Комутаторът поддържа класификация на базата на source и destination IP адреси, MAC адреси или Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) номера на портове
	Минимум 8 изходящи опашки за порт	**[Отговаря]** Комутаторът поддържа 8 изходящи опашки за порт
	Да поддържа DSCP класифициране	**[Отговаря]** Комутаторът поддържа DSCP класифициране
	Да поддържа автоматично осигуряване на качество на услугите включващо класифициране на трафика и конфигурация на изходящите опашки на всеки порт	**[Отговаря]** Комутаторът поддържа автоматично осигуряване на качество на услугите включващо класифициране на трафика и конфигурация на изходящите опашки на всеки порт
Сигурност	Да поддържа динамично, порт-базирана сигурност и потребителска автентикация	**[Отговаря]** Комутаторът поддържа динамично, порт-

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000125

чл. 2 от ЗЗЛД

		базирана сигурност потребителска автентикация
	Да поддържа динамично присъединяване на VLAN към потребител независимо от това къде е свързан потребителя	**[Отговаря]** Комутаторът поддържа динамично присъединяване на VLAN към потребител независимо от това къде е свързан потребителя
	Да позволява прилагането на политики за сигурност за всеки отделен порт на комутатора	**[Отговаря]** Комутаторът позволява прилагането на политики за сигурност за всеки отделен порт на комутатора
	ДА поддържа технология за отдалечен достъп посредством SSH протокол	**[Отговаря]** Комутаторът поддържа технология за отдалечен достъп посредством SSH протокол
	Да поддържа SNMP v1, v2, v3	**[Отговаря]** Комутаторът поддържа SNMP v1, v2, v3
	ДА поддържа тегнология предоставяща AAA- RADIUS, TACACS+ или еквивалентни	**[Отговаря]** Комутаторът поддържа тегнология предоставяща AAA-RADIUS, TACACS+
	MAC адрес нотификация за добавяне или премахване на потребители в мрежата	**[Отговаря]** Комутаторът поддържа MAC адрес нотификация за добавяне или премахване на потребители в мрежата
	ДА поддържа DHCP snooping	**[Отговаря]** Комутаторът поддържа DHCP snooping
	Да предотвратява възможността крайни устройства, които не са част от администрираната мрежа да приемат ролята на Spanning-Tree root комутатори.	**[Отговаря]** Комутаторът предотвратява възможността крайни устройства, които не са част от администрираната мрежа да приемат ролята на Spanning-Tree root комутатори.
	IGMP филтриране осигуряващо мултикаст автентикация и лимитиране на конкурентните мултикаст стриймове	**[Отговаря]** Комутаторът поддържа IGMP филтриране

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000119

чл. 2 от ЗЗЛД

		осигуряващо мултикаст автентикация и лимитиране на конкурентните мултикаст стриймове
	Да поддържа поне 625 IPv4 Security ACE записа и 500 IPv4 QoS ACE записа	**[Отговаря]** Комутаторът поддържа 625 IPv4 Security ACE записа и 500 IPv4 QoS ACE записа
Управление	Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh	**[Отговаря]** Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000150

чл. 2 от ЗЗЛД

8.3. Маршрутизатор – 2 броя

Компоненти	Изисквания	Предлагаме
Хардуер	Да има възможност за включване на минимум 1GB външна USB памет	**[Отговаря]** Маршрутизаторът има възможност за включване на 1GB външна USB памет
	Да има минимум 1 вграден специализиран процесор за обработка на мрежовия трафик	**[Отговаря]** Маршрутизаторът има 1 вграден специализиран процесор за обработка на мрежовия трафик
	Да има минимум 2.0 GHz Quad-Core CPU	**[Отговаря]** Маршрутизаторът има 2.0 GHz Quad-Core CPU
	Да има минимум 8GB DRAM памет	**[Отговаря]** Маршрутизаторът има 8GB DRAM памет
	Да има възможност за надграждане до минимум 16GB DRAM	**[Отговаря]** Маршрутизаторът има възможност за надграждане до минимум 16GB DRAM
	Да има минимум 8GB flash памет	**[Отговаря]** Маршрутизаторът има минимум 8GB flash памет
	Да има възможност за надграждане с минимум 400-GB твърд SSD диск	**[Отговаря]** Маршрутизаторът има възможност за надграждане с 400-GB твърд SSD диск
	Да разполага минимум с 10 Mb TCAM памет	**[Отговаря]** Маршрутизаторът разполага с 10 Mb TCAM памет
Софтуер	Да има възможност за софтуерна резервираност	**[Отговаря]** Маршрутизаторът има възможност за софтуерна резервираност
	Да има 64 битова (64 bit) операционна система	**[Отговаря]** Маршрутизаторът има 64 битова (64 bit) операционна система
Производителност и функционалности	Да има производителност минимум 2,4 Gbps	**[Надвишава]** Маршрутизаторът има производителност 2,5 Gbps

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000131

чл. 2 от ЗЗЛД

	Да има възможност за увеличаване на производителността чрез отключване с допълнителен софтуерен лиценз до поне 20 Gbps	**[Отговаря]** Маршрутизаторът им възможност з увеличаване н производителността чрез отключване с допълнителен софтуерен лиценз до 20 Gbps
	Да има вграден хардуерен модул за криптиране на трафик	**[Отговаря]** Маршрутизаторът има вграден хардуерен модул за криптиране на трафик
	Да има възможност да обработва минимум 8 Gbps криптиран трафик	**[Отговаря]** Маршрутизаторът има възможност да обработва 8 Gbps криптиран трафик
	Да поддържа минимум 960 000 IPv4/IPv6 маршрута	**[Надвишава]** Маршрутизаторът поддържа 1,000,000 IPv4/IPv6 маршрута
	Да има минимум 18Mpps производителност при обработка на пакети	**[Надвишава]** Маршрутизаторът има 19Mpps производителност при обработка на пакети
	Да има минимум 6Mpps производителност при комбинирана работа със следните услуги IPv4 forwarding, ACL, QoS	**[Надвишава]** Маршритизаторът има 6.7Mpps производителност при комбинирана работа със следните услуги IPv4 forwarding, ACL, QoS
	Да поддържа минимум 3800 списъка за контрол на достъпа (ACL) и минимум 48 000 ACE (записа) за система	**[Надвишава]** Маршрутизаторът поддържа 4000 списъка за контрол на достъпа (ACL) и минимум 50 000 ACE (записа) за система
	Да има възможност да поддържа минимум 3800 L2TP тунела	**[Надвишава]** Маршрутизаторът поддържа 4000 L2TP тунела
	Да поддържа минимум 96 000 multicast маршрута	**[Надвишава]** Маршрутизаторът поддържа 100 000 multicast маршрута

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000152

чл. 2 от ЗЗЛД

	Да поддържа минимум 3 500 multicast групи	**[Надвишава]** Маршрутизаторът поддържа 400 мултикаст групи
	Да има възможност да поддържа минимум 15 000 QoS опашки	**[Надвишава]** Маршрутизаторът поддържа 16 000 QoS опашки
	Да поддържа минимум 3 нива на QoS йерархия	**[Отговаря]** Маршрутизаторът поддържа 3 нива на QoS йерархия
	Да поддържа минимум 2 low-latency queuing (LLQ) QoS опашки на политика	**[Отговаря]** Маршрутизаторът поддържа 2 low-latency queuing (LLQ) QoS опашки на политика
	Да има възможност за минимум 1800 real time CRTP сесии	**[Надвишава]** Маршрутизаторът има възможност за 2000 real time CRTP сесии
	Да поддържа минимум 7 800 IPsec тунела	**[Надвишава]** Маршрутизаторът поддържа 8000 IPsec тунела
	Да има възможност за функционалност на защитна стена която може да обработва минимум 1700000 сесии	**[Надвишава]** Маршрутизаторът има възможност за функционалност на защитна стена която може да обработва 2,000,000 сесии
	Да може да обработва минимум 1700000 NAT сесии	**[Надвишава]** Може да обработва 2,000,000 NAT сесии
	Да поддържа минимум 7800 Layer 3 VPN	**[Надвишава]** Поддържа 8000 Layer 3 VPN
	Да поддържа минимум 3900 GRE тунела	**[Надвишава]** Поддържа 4000 GRE тунела
	Да поддържа route-reflector BGP функционалност при скалируемост от минимум 4800000 IPv4 или 2800000 IPv6 маршрута	**[Надвишава]** Поддържа route-reflector BGP функционалност при скалируемост от минимум 5,250,000 IPv4 или 4,250,000 IPv6 маршрута
	Да поддържа Ethernet over Multiple Protocol Label Switching (EoMPLS)	**[Отговаря]** Поддържа Ethernet over Multiple Protocol Label Switching (EoMPLS)

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000153

чл. 2 от ЗЗЛД

	Да поддържа Virtual Private Lan Service (VPLS) услуги	**[Отговаря]** Поддържа Virtual Priva Lan Service (VPL услуги
	Да поддържа Layer 3 VPN услуги	**[Отговаря]** Маршрутизаторът поддържа Layer 3 VPN услуги
	Да поддържа Multiprotocol Label Switching (MPLS)	**[Отговаря]** Поддържа Multiprotocol Label Switching (MPLS)
	Да поддържа RIP, OSPF и BGP маршрутизиращи протоколи	**[Отговаря]** Поддържа RIP, OSPF и BGP маршрутизиращи протоколи
	Да поддържа Protocol Independent Multicast	**[Отговаря]**
Физически характеристики	Да се монтира в стандартен 19'' комуникационен шкаф, като заема не повече от 1RU (Rack unit)	**[Отговаря]** Възможност за монтаж в стандартен 19'' комуникационен шкаф, като заема 1RU (Rack unit)
	Работна температура от 0 до 40°C	**[Отговаря]** Работна температура от 0 до 40°C
	Работна влажност от 10 до 85%	**[Отговаря]** Работна влажност от 10 до 85%
Захранване	Да има резервирано модулно AC захранване	**[Отговаря]** Има резервирано модулно AC захранване
	Да поддържа входно напрежение в интервала от 85 до 264 VAC	**[Отговаря]** Маршрутизаторът поддържа входно напрежение в интервала от 85 до 264 VAC
	Да има максимална консумация при AC захранване, не по голяма от 250W	**[Отговаря]** Маршрутизаторът има максимална консумация при AC захранване от 250W
Интерфейси и модули	Да има минимум 6 оптични SFP 1 Gigabit Ethernet слота	**[Отговаря]** Маршрутизаторът има 6 оптични SFP 1 Gigabit Ethernet слота
	Да бъде окомплектован с 6 оптични SFP преобразувателя поддържащи стандарт 1000BASE-T	**[Отговаря]** Маршрутизаторът е окомплектован с 6 оптични SFP преобразувателя поддържащи стандарт 1000BASE-T

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000154

чл. 2 от ЗЗЛД

	Да има минимум 2 оптични SFP+ 10 Gigabit Ethernet слота	**[Отговаря]** Маршрутизаторът има 2 оптични SFP+ 10 Gigabit Ethernet слота
	Да има минимум 1 слот за бъдещо надграждане с мрежови интерфейси	**[Отговаря]** Маршрутизаторът има 1 слот за бъдещо надграждане с мрежови интерфейси
	Да има минимум 1 брой Aux и 1 брой Console портове	**[Отговаря]** Маршрутизаторът има 1 брой Aux и 1 брой Console портове
	Да има минимум 1 брой RJ-45 10/100/1000 Ethernet порт за управление	**[Отговаря]** Маршрутизаторът има 1 брой RJ-45 10/100/1000 Ethernet порт за управление
	Да има възможност за бъдещо разширение с минимум 1 порт 10GE LAN/WAN-PHY	**[Отговаря]** Маршрутизаторът има възможност за бъдещо разширение с 1 порт 10GE LAN/WAN-PHY
Стандарти и сертификати	EN 60950-1	**[Отговаря]** EN 60950-1
	UL60950-1	**[Отговаря]** UL60950-1
	No. 60950-1-03	**[Отговаря]** No. 60950-1-03
	EN55022/CISPR 22 Information Technology Equipment	**[Отговаря]** EN55022/CISPR 22 Information Technology Equipment
	EN55024/CISPR 24 Information Technology Equipmen	**[Отговаря]** EN55024/CISPR 24 Information Technology Equipmen
	EN300 386 Telecommunications Network Equipment	**[Отговаря]** EN300 386 Telecommunications Network Equipment
	EN50082-1/EN61000-6-1 Generic Immunity Standard	**[Отговаря]** EN50082-1/EN61000-6-1 Generic Immunity Standard
	Да отговаря минимум на GR-1089 стандарта	**[Отговаря]** Отговаря на GR-1089 стандарта
	Да е съвместим със стандарта RFC 2737	**[Отговаря]** Съвместим е със стандарта RFC 2737

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000155

чл. 2 от ЗЗЛД

Управление	Да поддържа минимум telnet, ssh, console, RFC 2665, SNMP	**[Отговаря]** Поддържа telnet, SSH, console, RFC 2665, SNMP
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000153

чл. 2 от ЗЗЛД

8.4. Защитна стена – 2 броя

Компоненти	Изисквания	Предлагаме
Хардуер	Да разполага със твърд диск тип SSD, минимум 120 GB	**[Отговаря]** Разполага с твърд диск тип SSD, минимум 120 GB
	Да разполага с RAM памет, минимум 8GB	**[Отговаря]** Разполага с RAM памет - 8GB
	Да разполага с flash памет за операционната система на защитната стена - минимум 8GB	**[Отговаря]** Разполага с flash памет за операционната система на защитната стена - 8GB
	Архитектура на системната шина: Multibus	**[Отговаря]** Архитектура на системната шина: Multibus
Софтуер	Да бъде доставено със софтуер за управление и мониторинг на нивото на защитеност на мрежата	**[Отговаря]** Разполага със софтуер за управление и мониторинг на нивото на защитеност на мрежата
	Софтуера за управление и мониторинг на нивото на защитеност на мрежата да поддържа управление на минимум 2бр. защитни стени едновременно	**[Отговаря]** Софтуера за управление и мониторинг на нивото на защитеност на мрежата поддържа управление на 2бр. защитни стени едновременно
	Да бъде окомплектовано с необходимия софтуер и/или лицензи за обновяване на информацията за IPS записите в рамките на минимум 3 години	**[Отговаря]** Окомплектовано е с необходимия софтуер и лицензи за обновяване на информацията за IPS записите в рамките на 3 години
	Устройството да бъде окомплектовано с приложение за отдалечен достъп за потребители	**[Отговаря]** Окомплектовано е с приложение за отдалечен достъп за потребители
Производителност и функционалности	Да има възможност на минимум 1000 Mbps пропусквателна способност на защитната стена при включен контрол на приложенията	**[Надвишава]** Има възможност за 1100 Mbps пропусквателна способност на защитната стена при включен контрол на приложенията

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000157

чл. 2 от ЗЗЛД

	Да има възможност на минимум 500Mbps пропусквателна способност с включен контрол на приложенията и система за откриване и предотвратяване на атаки (Intrusion prevention system)	**[Надвишава]** Им възможност за 600Mb пропусквателна способност с включе контрол приложенията и система за откриване и предотвратяване на атаки (Intrusion prevention system)
	Да поддържа минимум 500 000 едновременни сесии	**[Отговаря]** Поддържа 500 000 едновременни сесии
	Да има възможност да поддържа минимум 3000 приложения за контрол	**[Отговаря]** Поддържа контрол на над 3000 приложения
	Да има възможност на минимум 280 000 000 уеб страници (URL адреси) за контрол	**[Отговаря]** Поддържа контрол на над 280 000 000 уеб страници (URL адреси)
	Да поддържа минимум 2Gbps инспекция на пакети	**[Отговаря]** Поддържа 2Gbps инспекция на пакети
	Да поддържа минимум 1Gbps инспекция при множество протоколи (HTTP, SMTP, FTP, IMAP4, DNS и др.)	**[Отговаря]** Поддържа 1Gbps инспекция при множество протоколи (HTTP, SMTP, FTP, IMAP4, DNS и др.)
	Да има възможност на минимум 700 крипто IPsec тунели	**[Надвишава]** Има възможност за 750 крипто IPsec тунели
	Да поддържа криптиране на VPN трафика - пропусквателна способност не по-малко от 300 Mbps	**[Отговаря]** Поддържа криптиране на VPN трафика - пропусквателна способност от 300 Mbps
	Да има възможност на минимум 700 потребители за отдалечен достъп	**[Надвишава]** Има възможност за 750 потребители за отдалечен достъп
	Да има възможност на минимум 200 виртуални VLANs интерфейса	**[Отговаря]** Има възможност за 200 виртуални VLANs интерфейса
	Да поддържа режим за резервиране на защитната стена за по голяма надежност	**[Отговаря]** Поддържа режим за резервиране на защитната стена за по голяма надежност
Физически характеристики	Работна температура от -5 до 40 градуса по Целзий	**[Отговаря]** Работна температура от -5 до 40 градуса по Целзий

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000153

чл. 2 от ЗЗЛД

	Работна влажност до 90%	**[Отговаря]** Работ влажност до 90%
	Максимално топлоотделяне - 380 Btu/hr	**[Надвишава]** Максимално топлоотделяне - 369 Btu/hr
	Да бъде окомплектовано с необходимите материали за монтаж в стандартен комуникационен шкаф, 19 инча	**[Отговаря]** окомплектовано е с необходимите материали за монтаж в стандартен комуникационен шкаф, 19 инча
	Максимална височина – 1 Rack Unit	**[Отговаря]** Има височина – 1 Rack Unit
	Тегло не по-голямо от 12кг	**[Отговаря]** Има тегло от 10кг.
	Да бъде окомплектовано със захранващ модул за AC захранващо напрежение	**[Отговаря]** Окомплектовано е със захранващ модул за AC захранващо напрежение
	Честота на променливото захранващо напрежение - 50/60 Hz	**[Отговаря]** Честота на променливото захранващо напрежение - 50/60 Hz
	Захранващ ток – максимум 5A при входно AC напрежение	**[Отговаря]** Захранващ ток – максимум 4.85A при входно AC напрежение
Интерфейси и модули	Да разполага с допълнителен разширителен слот за интерфейсни карти - минимум 1 брой	**[Отговаря]** Разполага с 1 брой допълнителен разширителен слот за интерфейсни карти
	Да разполага с минимум 8 медни интерфейса по 1 Гигабит	**[Отговаря]** Разполага с 8 медни интерфейса по 1 Гигабит
	Да разполага с минимум 1 GE отделен интерфейс за управление	**[Отговаря]** Разполага с 1 GE отделен интерфейс за управление
	Да разполага с минимум 1 брой RJ45 сериен порт	**[Отговаря]** Разполага с минимум 1 брой RJ45 сериен порт
Стандарти и сертификати	EN 60950-1:2006+A11:2009	**[Отговаря]** EN 60950-1:2006+A11:2009
	UL 60950-1:2007	**[Отговаря]** UL 60950-1:2007
	CSA C22.2 No. 60950-1-07	**[Отговаря]** CSA C22.2 No. 60950-1-07
	CE: EN55022 2006+A1: 2007 Class A;	**[Отговаря]** CE: EN55022 2006+A1: 2007 Class A;

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000159

чл. 2 от ЗЗЛД

	EN55024 1998+A1:2001+A2:2003;	**[Отговаря]** EN55024 1998+A1:2001+A2:2003;
	EN61000-3-2 2009;	**[Отговаря]** EN61000-3-2 2009;
	EN61000-3-3 2008	**[Отговаря]** EN61000-3-3 2008
	FCC: CFR 47, Part 15 Subpart B Class A 2010,ANSI C63.4 2009	**[Отговаря]** FCC: CFR 47, Part 15 Subpart B Class A 2010,ANSI C63.4 2009
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

8.5. Комутатор за център за данни – 2 броя

Компоненти	Изисквания	Предлагаме
Производителност и функционалности	Комутатор за осигуряване на високоскоростна 10Gbps и 40Gbps Ethernet свързаност	**[Отговаря]** Комутатор за осигуряване на високоскоростна 10Gbps и 40Gbps Ethernet свързаност
	Комутаторът да разполага с неблокируема архитектура	**[Отговаря]** Комутаторът разполага с неблокируема архитектура
	Да притежава производителност от минимум 1,4 Tbps (терабита в секунда)	**[Надвишава]** Комутаторът притежава производителност от 1,44 Tbps (терабита в секунда)
	Да притежава производителност от минимум 1000 Mpps при 64-байтови пакети	**[Надвишава]** Комутаторът притежава производителност от 1071 Mpps при 64-байтови пакети
	Да притежава архитектура за неблокируема обработка на трафика на всички интерфейси при работа в Layer 2 и Layer 3 режим	**[Отговаря]** Комутаторът притежава архитектура за неблокируема обработка на трафика на всички интерфейси при работа в Layer 2 и Layer 3 режим
	Хардуерната архитектура на комутатора да осигурява комутиране/маршрутизиране на трафика в рамките на 1 микросекунда независимо от големината на пакетите	**[Отговаря]** Комутаторът има хардуерната архитектура за осигуряване на комутиране/маршрутизиране на трафика в рамките на 1 микросекунда независимо от големината на пакетите
	Да поддържа комбинирано минимум 250000 MAC адреси и ARP записи	**[Надвишава]** Комутаторът поддържа комбинирано минимум 256000 MAC адреси и ARP записи
	Да поддържа обновяване на софтуера без прекъсване на Layer 2 услугите	**[Отговаря]** Комутаторът поддържа обновяване на софтуера без прекъсване на Layer 2 услугите
	Поддръжка на стандартна IEEE 802.1Q VLAN енкапсулация	**[Отговаря]** Комутаторът поддържа стандартна IEEE 802.1Q VLAN енкапсулация
	Поддръжка на минимум 4000 VLAN мрежи	**[Отговаря]** Комутаторът поддържа 4000 VLAN мрежи
	Поддръжка на Rapid Per-VLAN Spanning Tree Plus (PVRST+) или еквивалент	**[Отговаря]** Комутаторът поддържа Rapid Per-VLAN Spanning Tree Plus (PVRST+)

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000161

	Поддръжка на IEEE 802.1s Multiple Spanning Tree Protocol с минимум 60 инстанции	**[Надвишава]** Комутаторът поддържа IEEE 802.1s Multiple Spanning Tree Protocol с минимум 64 инстанции
	Поддръжка на технология за обединяване на минимум 15 физически порта в един логически и балансиране на трафика по тях	**[Надвишава]** Комутаторът поддържа технология за обединяване на 16 физически порта в един логически и балансиране на трафика по тях
	Поддръжка на технология позволяваща на две устройства свързани към трето, да изглеждат като едно логическо и връзките да бъдат обединени	**[Отговаря]** Комутаторът поддържа технология позволяваща на две устройства свързани към трето, да изглеждат като едно логическо и връзките да бъдат обединени
	Поддръжка на IEEE 802.3ad Link Aggregation Control Protocol (LACP)	**[Отговаря]** Комутаторът поддържа IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	Поддръжка на Jumbo frames на всички портове до 9216 байта	**[Отговаря]** Комутаторът поддържа Jumbo frames на всички портове до 9216 байта
	Поддръжка на IEEE 802.3x Pause frames	**[Отговаря]** Комутаторът поддържа IEEE 802.3x Pause frames
	Поддръжка на следните механизми за Storm control - unicast, multicast и broadcast	**[Отговаря]** Комутаторът поддържа следните механизми за Storm control - unicast, multicast и broadcast
	Поддръжка на Private VLANs	**[Отговаря]** Комутаторът поддържа Private VLANs
	Поддръжка наVLAN remapping	**[Отговаря]** Комутаторът поддържа VLAN remapping
	Да предоставя възможност за бъдещо увеличение на портовете чрез свързването на отдалечени комутационни модули, които да се управляват от комутатора	**[Отговаря]** Комутаторът предоставя възможност за бъдещо увеличение на портовете чрез свързването на отдалечени комутационни модули, които да се управляват от комутатора
	Да поддържа управление на минимум 20 отдалечени комутационни модули, които да се управляват от комутатора	**[Надвишава]** Комутаторът поддържа управление на 24 отдалечени комутационни модули, които да се управляват от комутатора

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000102

чл. 2 от ЗЗЛД

	Да поддържа технология за създаване на независими виртуални портове на комутатора, които да бъдат присъединявани на всяка виртуална машина, като по този начин тя изглежда директно свързана към самия него	**[Отговаря]** Комутаторът поддръжа технология за създаване на независими виртуални портове на комутатора, които да бъдат присъединявани на всяка виртуална машина, като по този начин тя изглежда директно свързана към самия него
	Поддръжка на минимум 30,000 IPv4 и 7000 IPv6 host префикси	**[Надвишава]** Комутаторът поддръжа 32,000 IPv4 и 8000 IPv6 host префикси
	Поддръжка на минимум 7500 мултикаст (IPv4)	**[Надвишава]** Комутаторът поддръжа 8000 мултикаст (IPv4)
	Поддръжка на минимум 7500 IGMP snooping групи	**[Надвишава]** Комутаторът поддръжа
	Поддръжка на минимум 4000 Virtual Routing and Forwarding (VRF) инстанции	**[Отговаря]** Комутаторът поддръжа 4000 Virtual Routing and Forwarding (VRF) инстанции
	Поддръжка на механизъм за Equal-Cost Multipathing (ECMP) по минимум 60 равностойни пътища	**[Надвишава]** Комутаторът поддръжа механизъм за Equal-Cost Multipathing (ECMP) по минимум 64 равностойни пътища
	Поддръжка на минимум 3500 Layer 3 ACL записа	**[Надвишава]** Комутаторът поддръжа 4000 Layer 3 ACL записа
	Поддръжка на Routing Information Protocol Version 2	**[Отговаря]** Комутаторът поддръжа Routing Information Protocol Version 2
	Поддръжка на Open Shortest Path First Version 2 (OSPFv2)	**[Отговаря]** Комутаторът поддръжа Open Shortest Path First Version 2 (OSPFv2)
	Да има възможност за Border Gateway Protocol (BGP)	**[Отговаря]** Комутаторът има възможност за Border Gateway Protocol (BGP)
	Да има възможност за Intermediate System-to-Intermediate System (IS-IS)	**[Отговаря]** Комутаторът има възможност за Intermediate System-to-Intermediate System (IS-IS)
	Поддръжка на статично IPv6 маршрутизиране	**[Отговаря]** Комутаторът поддръжа статично IPv6 маршрутизиране
	Поддръжка на IPv6 маршрутизиране с помощта на OSPFv3	**[Отговаря]** Комутаторът поддръжа IPv6 маршрутизиране с помощта на OSPFv3

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000103

чл. 2 от ЗЗЛД

	Поддръжка на IPv6 маршрутизиране с помощта на BGPv6	**[Отговаря]** Комутаторът поддръжа IPv6 маршрутизиране с помощта на BGPv6
	Поддръжка на IPv6 VRF-lite	**[Отговаря]** Комутаторът поддръжа IPv6 VRF-lite
	Поддръжка на Virtual Router Redundancy Protocol (VRRP)	**[Отговаря]** Комутаторът поддръжа Virtual Router Redundancy Protocol (VRRP)
	Поддръжка на Protocol Independent Multicast Version 2 (PIMv2) sparse mode	**[Отговаря]** Комутаторът поддръжа Protocol Independent Multicast Version 2 (PIMv2) sparse mode
	Маханизми за осигуряване на качество на услугите	**[Отговаря]** Комутаторът поддръжа изискваните маханизми за осигуряване на качество на услугите
	Поддръжка на Layer 2 IEEE 802.1p CoS	**[Отговаря]** Комутаторът поддръжа Layer 2 IEEE 802.1p CoS
	Работа с минимум 8 броя unicast и 8 броя multicast опашки на порт	**[Отговаря]** Комутаторът поддръжа 8 броя unicast и 8 броя multicast опашки на порт
	Да поддържа конфигуриране на QoS политики на база порт	**[Отговаря]** Комутаторът поддръжа конфигуриране на QoS политики на база порт
	QoS класификация, базирана на списъци за контрол на достъпа (Layer 2, 3 и 4)	**[Отговаря]** Комутаторът поддръжа QoS класификация, базирана на списъци за контрол на достъпа (Layer 2, 3 и 4)
	Всеки от 10 или 40 Gigabit Ethernet интерфейсите да има възможност да бъде конфигуриран като FCoE интерфейс	**[Отговаря]** Всеки от 10 или 40 Gigabit Ethernet интерфейсите има възможност да бъде конфигуриран като FCoE интерфейс
	Разделение на SAN от LAN администрацията	**[Отговаря]** Комутаторът поддръжа разделение на SAN от LAN администрацията
	Протоколи за автентикация и контрол на достъпа - RADIUS и TACACS+ или еквивалентен	**[Отговаря]** Комутаторът поддръжа протоколи за автентикация и контрол на достъпа - RADIUS и TACACS+ или еквивалентен
	Да поддържка Syslog	**[Отговаря]** Комутаторът поддръжа Syslog
	Да поддържа SNMPv1, v2, и v3 (за IPv4 и IPv6)	**[Отговаря]** Комутаторът поддръжа SNMPv1, v2, и v3 (за IPv4 и IPv6)

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

	Да поддържа Remote monitoring (RMON)	**[Отговаря]** Комутаторът поддръжа Remote monitoring (RMON)
	Да поддържа Advanced Encryption Standard (AES) криптиране на управляващия трафик	**[Отговаря]** Комутаторът поддръжа Advanced Encryption Standard (AES) криптиране на управляващия трафик
	Да поддържа Network Time Protocol (NTP)	**[Отговаря]** Комутаторът поддръжа Network Time Protocol (NTP)
	Да поддържа механизъм за rollback на конфигурацията	**[Отговаря]** Комутаторът поддръжа механизъм за rollback на конфигурацията
	Да поддържа Secure Shell Version 2 (SSHv2)	**[Отговаря]** Комутаторът поддръжа Secure Shell Version 2 (SSHv2)
	Да поддържа XML интерфейс, базиран на NETCONF	**[Отговаря]** Комутаторът поддръжа XML интерфейс, базиран на NETCONF
	Да поддържа контрол на достъпа базиран на роли (Role-based Access Control)	**[Отговаря]** Комутаторът поддръжа контрол на достъпа базиран на роли (Role-based Access Control)
	Да разполага с вграден анализатор на трафика(пакети)	**[Отговаря]** Комутаторът разполага с вграден анализатор на трафика(пакети)
Интерфейси и модули	Комутаторът да разполага с унифицирани портове за осигуряване на Ethernet, FC и FCoE свързаност	**[Отговаря]** Комутаторът разполага с унифицирани портове за осигуряване на Ethernet, FC и FCoE свързаност
	Комутаторът да разполага с минимум 48 броя фиксирани 1Gbps/10Gbps интерфейса	**[Отговаря]** Комутаторът разполага 48 броя фиксирани 1Gbps/10Gbps интерфейса
	Всеки от фиксираните интерфейси на комутатора да поддържа Ethernet и FCoE свързаност	**[Отговаря]** Всеки от фиксираните интерфейси на комутатора поддържа Ethernet и FCoE свързаност
	Минимум 15 броя от интерфейсите на комутатора да са универсални и да могат да работят с 2, 4 и 8 Gbps Fibre Channel интерфейси	**[Надвишава]** 16 броя от интерфейсите на комутатора са универсални и да могат да работят с 2, 4 и 8 Gbps Fibre Channel интерфейси
	Комутаторът да разполага с минимум 6 броя 40Gbps Ethernet/FCoE интерфейси	**[Отговаря]** Комутаторът разполага с 6 броя 40Gbps Ethernet/FCoE интерфейси

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000103

чл. 2 от ЗЗЛД

	Всеки комутатор да е окомплектован с минимум 8 броя кабели с по 2 броя 10GBASE SFP+ интерфейси с дължина 5 метра	**[Отговаря]** Комутаторът е окомплектован с 8 броя кабели с по 2 броя 10GBASE SFP+ интерфейси с дължина 5 метра
	Всеки комутатор да бъде окомплектован с допълнителен разширителен модул с минимум 32 броя 1/10 Gbps Ethernet Base-T и минимум 8 броя 10 Gigabit Ethernet SFP+ интерфейси. Всички интерфейси да поддържат FCoE	**[Отговаря]** Всеки комутатор е окомплектован с допълнителен разширителен модул с 32 броя 1/10 Gbps Ethernet Base-T и 8 броя 10 Gigabit Ethernet SFP+ интерфейси. Всички интерфейси поддържат FCoE
	Да има конзолен порт и специално предназначен за управление 10/100/1000 Mbps Ethernet порт извън мрежата за данни	**[Отговаря]** Комутаторът има конзолен порт и специално предназначен за управление 10/100/1000 Mbps Ethernet порт извън мрежата за данни
Физически характеристики	Да разполага с минимум 3 броя вентилаторни блока за осигурявне на 2+1 резервираност	**[Отговаря]** Комутаторът разполага с 3 броя вентилаторни блока за осигурявне на 2+1 резервираност
	Вентилаторните блокове да бъдат сменяеми, без да се налага прекъсване на работата на устройството(hot-swappable)	**[Отговаря]** Вентилаторните блокове са сменяеми, без да се налага прекъсване на работата на устройството (hot-swappable)
Захранване	Да разполага с минимум 2 броя захранващи блока за осигурявне на 1+1 резервираност	**[Отговаря]** Комутаторът разполага с 2 броя захранващи блока за осигурявне на 1+1 резервираност
	Захранващите блокове да бъдат сменяеми, без да се налага прекъсване на работата на устройството(hot-swappable)	**[Отговаря]** Захранващите блокове са сменяеми, без да се налага прекъсване на работата на устройството (hot-swappable)
	Захранващите блокове да осигуряват минимум 90% ефективност при натоварване от 30%	**[Надвишава]** Захранващите блокове осигуряват минимум 90% ефективност при натоварване от 25%
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** Устройствата са с гаранционен срок 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000103

чл. 2 от ЗЗЛД

8.6. SAN комутатор – 2 броя

Компоненти	Изисквания	Предлагаме
Интерфейси и модули	Да предоставя 16 Gbps Fibre Channel свързаност	**[Отговаря]** SAN комутаторът предоставя 16 Gbps Fibre Channel свързаност
	Да предоставя минимум 48 броя фиксирани 16 Gbps порта	**[Отговаря]** SAN комутаторът разполага с 48 броя фиксирани 16 Gbps порта
	Всички портова да поддържат автоматична настройка на скоростта си на 2/4/8/16 Gbps.	**[Отговаря]** Всички портове на SAN комутаторът поддържат автоматична настройка на скоростта си на 2/4/8/16 Gbps.
	Да бъде лицензиран за работа на минимум 36 броя интерфейси, които да са окумплектовани със съответните 16 Gbps SFP+ модули.	**[Отговаря]** SAN комутаторът е лицензиран за работа на 36 броя интерфейси, които са окомплектовани със съответните 16 Gbps SFP+ модули
Производителност и фупкционалности	Буфер кредити: минимум 256 на всяка група от по 4 порта.	**[Отговаря]** SAN комутаторът има следните буфер кредити: минимум 256 на всяка група от по 4 порта.
	Да поддържа виртуален SAN (VSAN) технология	**[Отговаря]** SAN комутаторът поддържа виртуален SAN (VSAN) технология
	Да поддържа Access Control Lists (ACLs)	**[Отговаря]** SAN комутаторът поддържа Access Control Lists (ACLs)
	Да поддържа VSAN RBAC чрез RADIUS и TACACS+, SFTP, SSHv2, SNMPv3	**[Отговаря]** SAN комутаторът поддържа VSAN RBAC чрез RADIUS и TACACS+, SFTP, SSHv2, SNMPv3
	Всички описани по-горе функционалност и протоколи да бъдат включени в предложението	**[Отговаря]** Всички описани по-горе функционалност и протоколи са включени в предложението
Захранване	Да разполага с минимум 2 броя захранващи блока за осигурявне на 1+1 резервираност	**[Отговаря]** SAN комутаторът разполага с 2 броя захранващи блока за осигурявне на 1+1 резервираност
	Захранващите блокове да бъдат сменяеми, без да се налага прекъсване на работата на устройството(hot-swappable)	**[Отговаря]** Захранващите блокове са сменяеми, без да се налага прекъсване на работата на устройството(hot-swappable)

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000107

чл. 2 от ЗЗЛД

Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** Устройствата са с гаранционен срок 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

8.7. Комутатор за достъп – 15 броя

Компоненти	Изисквания	Предлагаме
Хардуер	Минимум 512MB DRAM	**[Отговаря]** Комутаторът разполага с 512MB DRAM
	Минимум 128 MB Flash памет	**[Отговаря]** Комутаторът разполага с 128 MB Flash памет
Производителност и функционалности	Минимум 216 Gbps комутираща матрица	**[Отговаря]** Комутаторът поддържа 216 Gbps комутираща матрица
	Минимум 107 Mpps ниво на предаване на данни	**[Надвишава]** Комутаторът поддържа 107.1 Mpps ниво на предаване на данни
	Минимум 16000 MAC адреса	**[Отговаря]** Комутаторът поддържа 16000 MAC адреса
	Минимум 9198 байта MTU за L3 пакет за гигабит етернет портовете	**[Отговаря]** Комутаторът поддържа 9198 байта MTU за L3 пакет за гигабит етернет портовете
	Да има възможност за конфигурация в клъстерен режим със скорост на връзката между комутаторите в клъстера от минимум 78Gbps	**[Надвишава]** Комутаторът поддържа конфигурация в клъстерен режим със скорост на връзката между комутаторите в клъстера от 80Gbps
	Автоматично активиране на порт, който е бил деактивиран поради грешка в мрежата	**[Отговаря]** Комутаторът поддържа автоматично активиране на порт, който е бил деактивиран поради грешка в мрежата
	Да поддържа TFTP и NTP протоколи	**[Отговаря]** Комутаторът поддържа TFTP и NTP протоколи
	Да поддържа следните механизми за превенция на цикли в мрежата: 802.1s, 802.1d или еквивалентни	**[Отговаря]** Комутаторът поддържа 802.1s и 802.1d механизми за превенция на цикли в мрежата
	Проследяване на Layer 2 маршрут	**[Отговаря]** Комутаторът поддържа проследяване на Layer 2 маршрут

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000

	Да поддържа LACP Link Aggregation Control Protocol	**[Отговаря]** Комутаторът поддържа LACP Link Aggregation Control Protocol
	Да поддържа минимум 4096 VLAN идентификационни номера	**[Отговаря]** Комутаторът поддържа 4096 VLAN идентификационни номера
	Да поддържа 1023 активни VLAN	**[Отговаря]** Комутаторът поддържа 1023 активни VLAN
	Да поддържа технология за отдалечено наблюдение, анализиране и управление на трафика.	**[Отговаря]** Комутаторът поддържа технология за отдалечено наблюдение, анализиране и управление на трафика.
Физически характеристики	Да бъде окомплектован с необходимите монтажни елементи за монтаж в 19" комуникационен шкаф, максимална височина 1 RU	**[Отговаря]** Комутаторът е окомплектован с необходимите монтажни елементи за монтаж в 19" комуникационен шкаф и е с максимална височина от 1 RU
	Максимално тегло на устройството 4.4kg	**[Отговаря]** Комутаторът е с тегло от 4.2 kg
	MTBF не по-малко от 442 000 часа	**[Надвишава]** MTBF - 442,690
	Трябва да поддържа индикатори минимум за следните характеристики: интегритет на линията, активиран, деактивиран порт, скорост и дуплекс на порта	**[Отговаря]** Комутаторът поддържа индикатори за следните характеристики: интегритет на линията, активиран, деактивиран порт, скорост и дуплекс на порта
	Работна температура: от -5 до 45°C	**[Отговаря]** Работна температура: от -5 до 45°C
Захранване	Устройството трябва да поддържа входно захранващо напрежение от 100 до 240V AC	**[Отговаря]** Комутаторът поддържа входно захранващо напрежение от 100 до 240V AC
	Максимална консумация 0,052 kVA	**[Отговаря]** Максимална консумация 0,051 kVA
Интерфейси и модули	Минимум 48 x 10/100/1000 RJ45 ethernet порта (медни)	**[Отговаря]** Комутаторът разполага с 48 x 10/100/1000 RJ45 Ethernet порта (медни)
	Минимум 2 x 1GE SFP слота за uplink	**[Надвишава]** Комутаторът разполага с 4 x 1GE SFP слота за uplink
	Да бъде окомплектован с минимум 1бр. 1000BASE-SX оптичен преобразувател за	**[Отговаря]** Комутаторът е окомплектован с 1бр. 1000BASE-SX оптичен

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

	multi-mode оптичен кабел	преобразувател за multi-mode оптичен кабел
	Да има възможност за допълнителна окомплектовка с необходимите модули и материали за конфигурация в клъстерен (stack) режим	**[Отговаря]** Комутаторът има възможност за допълнителна окомплектовка с необходимите модули и материали за конфигурация в клъстерен (stack) режим
Стандарти и сертификати	UL 60950-1, второ издание	**[Отговаря]** UL 60950-1, второ издание
	CAN/CSA-C22.2 No. 60950-1, второ издание	**[Отговаря]** CAN/CSA-C22.2 No. 60950-1, второ издание
	EN 60950-1, второ издание	**[Отговаря]** EN 60950-1, второ издание
	IEC 60950-1, второ издание	**[Отговаря]** IEC 60950-1, второ издание
	AS/NZS 60950-1	**[Отговаря]** AS/NZS 60950-1
	47CFR част 15 клас A	**[Отговаря]** 47CFR част 15 клас A
	EN55022 клас A	**[Отговаря]** EN55022 клас A
	ICES003 клас A	**[Отговаря]** ICES003 клас A
	VCCI клас A	**[Отговаря]** VCCI клас A
	CNS13438 клас A	**[Отговаря]** CNS13438 клас A
	EN61000-3-2	**[Отговаря]** EN61000-3-2
	EN61000-3-3	**[Отговаря]** EN61000-3-3
	KN22 клас A	**[Отговаря]** KN22 клас A
	EN55024	**[Отговаря]** EN55024
	CISPR24	**[Отговаря]** CISPR24
	EN300386	**[Отговаря]** EN300386
	KN24	**[Отговаря]** KN24
	Reduction of Hazardous Substances (ROHS) включващ директива 2011/65/EU	**[Отговаря]** Reduction of Hazardous Substances (ROHS) включващ директива 2011/65/EU
Качество на услугите	Да поддържа 802.1p class of service (CoS)	**[Отговаря]** Комутаторът поддържа 802.1p class of service (CoS)
	Да поддържа класификация на базата на source и destination IP	**[Отговаря]** Комутаторът поддържа

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

	адреси, MAC адреси или Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) номера на портове	класификация на базата на source и destination IP адреси, MAC адреси или Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) номера на портове
	Минимум 8 изходящи опашки за порт	**[Отговаря]** Комутаторът поддържа 8 изходящи опашки за порт
	Да поддържа DSCP класифициране	**[Отговаря]** Комутаторът поддържа DSCP класифициране
	Да поддържа автоматично осигуряване на качество на услугите включващо класифициране на трафика и конфигурация на изходящите опашки на всеки порт	**[Отговаря]** Комутаторът поддържа автоматично осигуряване на качество на услугите включващо класифициране на трафика и конфигурация на изходящите опашки на всеки порт
	Да поддържа динамично присъединяване на VLAN към потребител независимо от това къде е свързан потребителя	**[Отговаря]** Комутаторът поддържа динамично присъединяване на VLAN към потребител независимо от това къде е свързан потребителя
	Да позволява прилагането на политики за сигурност за всеки отделен порт на комутатора	**[Отговаря]** Комутаторът позволява прилагането на политики за сигурност за всеки отделен порт на комутатора
	Да поддържа технология за отдалечен достъп посредством SSH протокол	**[Отговаря]** Комутаторът поддържа технология за отдалечен достъп посредством SSH протокол
	Да поддържа SNMP v1, v2, v3	**[Отговаря]** Комутаторът поддържа SNMP v1, v2, v3
	Да поддържа технология предоставяща AAA- RADIUS, TACACS+ или еквивалентни	**[Отговаря]** Комутаторът поддържа тегнология предоставяща AAA-RADIUS, TACACS+
	ДА поддържа DHCP snooping	**[Отговаря]** Комутаторът поддържа DHCP snooping
	Да предотвратява възможността крайни устройства, които не са част от администрираната мрежа да приемат ролята на Spanning-Tree root комутатори.	**[Отговаря]** Комутаторът предотвратява възможността крайни устройства, които не са част от администрираната мрежа да приемат ролята на Spanning-Tree root комутатори.
	Да поддържа поне 625 IPv4	**[Отговаря]**

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

	Security ACE записа и 500 IPv4 QoS ACE записа	Комутаторът поддържа 625 IPv4 Security ACE записа и 500 IPv4 QoS ACE записа
Управление	Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh	**[Отговаря]** Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

8.8. Опорен комутатор – 2 броя

Компоненти	Изисквания	Предлагаме
Производителност и функционалности	Да бъде оборудван с не по-малко от 12 броя 10/100/1000 SFP слота	**[Отговаря]** Комутаторът е оборудван с 12 броя 10/100/1000 SFP слота
	Устройството трябва да е окомплектовано със следните интерфейсни модули: • 10 броя 1000BASE-SX оптичен преобразувател за multi-mode оптичен кабел	**[Отговаря]** Комутаторът е окомплектовано със следните интерфейсни модули: 10 броя 1000BASE-SX оптичен преобразувател за multi-mode оптичен кабел
	Да поддържа комутационна матрица с капацитет от минимум 68 Gbps	**[Отговаря]** Комутаторът поддържа комутационна матрица с капацитет от 68 Gbps
	Да има възможност за свързване на комутаторите в стак, със скорост на връзката минимум 480 Gbps	**[Отговаря]** Комутаторът има възможност за свързване на комутаторите в стак, със скорост на връзката 480 Gbps
	Да има производителност не по-малка от 50 Mpps	**[Надвишава]** Комутаторът има производителност от 50.5 Mpps
	Брой поддържани MAC адреси – минимум 32,000	**[Отговаря]** Брой поддържани MAC адреси –32,000
	Да има модулно AC токозахранване	**[Отговаря]** Има модулно AC токозахранване
	Общ брой IPv4 маршрута – минимум 24,000	**[Отговаря]** Общ брой IPv4 маршрута

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000172

чл. 2 от ЗЗЛД

		– 24,000
	Минимум оперативна памет – DRAM 4GB	**[Отговаря]** Оперативна памет – DRAM 4GB
	Минимум flash памет за съхранение на конфигурационни файлове – 2Gb	**[Отговаря]** Комутаторът има flash памет за съхранение на конфигурационни файлове – 2Gb
	Да поддържа минимум 4000 VLAN ID идентификатори на виртуални мрежи	**[Отговаря]** Комутаторът поддържа 4000 VLAN ID идентификатори на виртуални мрежи
	Да поддържа минимум 1000 комутируеми виртуални интерфейси (SVI)	**[Отговаря]** Комутаторът поддържа 1000 комутируеми виртуални интерфейси (SVI)
	Да поддържа обработка на рамки с големина над 9000 байта	**[Отговаря]** Комутаторът поддържа обработка на рамки с големина над 9000 байта
	При пълен стек да има възможност за минимум 200 L3 порта	**[Надвишава]** При пълен стек, комутаторът има възможност за 208 L3 порта
	Да поддържа RIPv1,v2, RIPng и статични маршрути	**[Отговаря]** Комутаторът поддържа RIPv1,v2, RIPng и статични маршрути
	Да има възможност за поддръжка на OSPF, BGPv4 и IS-ISv4, с цел бъдещо разширение	**[Отговаря]** Комутаторът има има възможност за поддръжка на OSPF, BGPv4 и IS-ISv4, след закупуване на допълнителен лиценз
	Да поддържа IGMP v1/2/3 snooping функционалност за IPv4	**[Отговаря]** Комутаторът поддържа IGMP v1/2/3 snooping функционалност за IPv4
	Всеки комутатор/стек да може да балансира трафика по пътища с различна метрика	**[Отговаря]** Всеки комутатор/стек може да балансира трафика по пътища с различна метрика
	Да поддържа споделяне на захранване между комутаторите в един stack	**[Отговаря]** Комутаторът поддържа споделяне на захранване между комутаторите в един stack

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000173

чл. 2 от ЗЗЛД

	Да поддържа листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси и Layer 4 TCP/UDP номера на портове	**[Отговаря]** Комутаторът поддържа листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси и Layer 4 TCP/UDP номера на портове
	Да поддържа изолиране на потребителите от един и същ VLAN	**[Отговаря]** Комутаторът поддържа изолиране на потребителите от един и същ VLAN
Стандарти и сертификати	Да поддържа следните стандарти: IEEE 802.1s, IEEE 802.1w, IEEE 802.11, IEEE 802.1x, IEEE 802.1x-Rev, IEEE 802.3ad, IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports	**[Отговаря]** Комутаторът поддържа следните стандарти: IEEE 802.1s, IEEE 802.1w, IEEE 802.11, IEEE 802.1x, IEEE 802.1x-Rev, IEEE 802.3ad, IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports
	IEEE 802.1D Spanning Tree Protocol	**[Отговаря]** IEEE 802.1D Spanning Tree Protocol
	IEEE 802.1p CoS prioritization	**[Отговаря]** IEEE 802.1p CoS prioritization
	IEEE 802.1Q VLAN	**[Отговаря]** IEEE 802.1Q VLAN
	IEEE 802.3 10BASE-T specification	**[Отговаря]** IEEE 802.3 10BASE-T specification
	IEEE 802.3u 100BASE-TX specification	**[Отговаря]** IEEE 802.3u 100BASE-TX specification
	IEEE 802.3ab 1000BASE-T specification	**[Отговаря]** IEEE 802.3ab 1000BASE-T specification
	IEEE 802.3z 1000BASE-X specification	**[Отговаря]** IEEE 802.3z 1000BASE-X specification
	RMON I и II standards	**[Отговаря]** RMON I и II standards
	SNMPv1, SNMPv2c и SNMPv3	**[Отговаря]** Комутаторът поддържа SNMPv1, SNMPv2c и SNMPv3
	Работен температурен диапазон от -5° до +45 °C (1500m)	**[Отговаря]** Работен температурен

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000

чл. 2 от ЗЗЛД

		диапазон от -5° до +45 °C (1500m)
	Работна относителна влажност от 10 до 90% (без кондензация)	**[Отговаря]** Работна относителна влажност от 10 до 95% (без кондензация)
	Сертификати за безопасност: UL 60950-1, CAN/CSA-C22.2 No. 60950-1, EN 60950-1, IEC 60950-1, CCC, CE Marking	**[Отговаря]** Комутаторът има следните сертификати за безопасност: UL 60950-1, CAN/CSA-C22.2 No. 60950-1, EN 60950-1, IEC 60950-1, CCC, CE Marking
	Да бъде окомплектован с всички необходими елементи за монтаж в 19'' комуникационен шкаф	**[Отговаря]** Комутаторът е окомплектован с необходимите монтажни елементи за монтаж в 19" комуникационен шкаф, максимална височина 1 RU
Управление	Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh	**[Отговаря]** Възможност за достъп до команден интерфейс за управление чрез конзола/telnet/ssh
Гаранционен срок	36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни	**[Отговаря]** 36 месеца с време за подмяна на дефектирал хардуер и възстановяване на услугите до 3 работни дни

Забележка: *В колона „Предлагаме" по позиции трябва да бъде посочена техническа характеристика (спецификация) на всеки предложен компонент.* ***Трябва да са попълнени точните технически характеристики (спецификации) на всеки предложен компонент или конкретния предлаган модел.***

Декларираме, че хардуерните компоненти, които ще доставим, ще са оригинални, нови, неупотребявани, в момента са в производство и има поддръжка за тях.

Предложените от нас технически характеристики на продуктите се потвърждават от приложените техническа брошура и разпечатка на посочената по-долу интернет страницата на производителя (дава се адресът на интернет страницата на производителя, където е публикуван предлаганият модел (същата да не е home-страницата на производителя).

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000173

чл. 2 от ЗЗЛД

Наименование на продукта	Производител	Държава на произход	Интернет страница на производителя[1]
Комуникационен шкаф	Rittal	China	http://www.rittal.com/com-en/product/show/variantdetail.action?c=/Enclosures/IT%20network%20and%20server%20enclosures/TS%20IT&categoryPath=/PG0001/PG0002SCHRANK1/PG0039SCHRANK1/PGR10466SCHRANK1&productID=5509110 http://www.rittal.com/imf/none/3_2841/Rittal_5509110_Technical_details_3_2841 http://www.rittal.com/com-en/product/list/variations.action?c=/Enclosures/IT network and server enclosures/TS IT&categoryPath=/PG0001/PG0002SCHRANK1/PG0039SCHRANK1/PGR10466SCHRANK1/PRO29845SCHRANK&productID=PRO29845
Граничен комутатор	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html
Маршрутизатор	Cisco Systems	China	http://www.cisco.com/c/en/us/products/routers/asr-1001-x-router/index.html http://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-441072.html http://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/datasheet-c78-731640.html

[1] Посочва се интернет страница на производителя (на български или английски език), от която да с виждат техническите характеристики на предлаганите продукти. Тези характеристики трябва д съответстват на предложените от участника.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000173

чл. 2 от ЗЗЛД

Наименование на продукта	Производител	Държава на произход	Интернет страница на производителя[1]
Защитна стена	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html http://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-732251.html
Комутатор за център за данни	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/datasheet-c78-730760.html http://www.cisco.com/c/en/us/products/switches/nexus-2000-series-fabric-extenders/index.html
SAN комутатор	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9148s-16g-multilayer-fabric-switch/datasheet-c78-731523.html
Комутатор за достъп	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html
Опорен комутатор	Cisco Systems	China	http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/data_sheet_c78-720918.html

Декларираме, че захранването на предлаганото оборудване е 220 V AC, 50 Hz, БДС стандарт на кабели и конектори.

Декларираме, че предлаганото оборудване е сертифицирано и покрива изискванията в съответствие с международните и европейски стандарти за електромагнитно излъчване и безопасност.

Декларираме, че времето за реакция е максимум 4 часа и времето за отстраняване на проблем е до 5 работни дни в срока на гаранционната поддръжка на оборудването.

Декларираме, че ще предоставяме оборотна техника в случай на необходим ремонт за повече от 5 работни дни.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000177

чл. 2 от ЗЗЛД

Тази оферта е със срок на валидност 90 (деветдесет) дни от крайния срок за приемане на офертите в процедурата и ще остане обвързваща за нас до изтичане на този срок. До подготвяне на официален договор, тази оферта, наред с известието от Ваша страна за възлагане на обществена поръчка ще формират обвързващо споразумение между двете страни.

Към техническото предложение прилагаме:

- Техническа брошура от производителя, която потвърждава предложените от нас характеристики.
- Разпечатка от сайта на производителя на български или английски език с технически характеристики на техниката, която предлагаме.
- Описание на функциониращата ни сис[illegible] обслужване на сервизни заявки и организация на гара[illegible]нс.

чл. 2 от ЗЗЛД

11.03.2016 г.

ПОДПИС

ПЕЧАТ

Дете[illegible]андров
Мен
„Тел

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000173

ОБРАЗЕЦ № 11

ДО
ПРЕДСЕДАТЕЛЯ
НА НСИ
ул. "П. Волов" № 2,
гр. София

ЦЕНОВО ПРЕДЛОЖЕНИЕ [1]

за участие в открита процедура за възлагане на обществена поръчка с предмет:

„Доставка, монтаж, конфигурация и интеграция на комуникационно оборудване към съществуващата ИТ инфраструктура на НСИ"

„Телелинк" ЕАД,

с БУЛСТАТ/ЕИК/Номер на регистрация в съответната държава 130545438, регистрирано в Софийски Градски Съд с данни по регистрацията: регистриран по ф.д. № 5699/2001 г., регистрация по ДДС: BG130545438, със седалище гр. София 1756, община Столична, район Изгрев, Бизнес център Литекс Тауър, ул. Лъчезар Станчев № 3, ет. 4 и адрес на управление гр. София 1756, община Столична, район Изгрев, Бизнес център Литекс Тауър, ул. Лъчезар Станчев № 3, ет. 4, адрес за кореспонденция: гр. София 1756, община Столична, район Изгрев, Бизнес център Литекс Тауър, ул. Лъчезар Станчев № 3, ет. 4, телефон за контакт 02/970 40 40, факс 02/970 40 42, електронна поща office@telelink.com

банкова сметка: IBAN: BG16 UNCR 7630 1022 5953 89, BIC: UNCRBGSF

представлявано от Детелин Цветанов Александров в качеството на Мениджър продажби и пълномощник на Цветан Димитров Мутафчиев – Изпълнителен директор на „Телелинк" ЕАД

УВАЖАЕМИ ГОСПОДИН ПРЕДСЕДАТЕЛ,

С настоящото Ви представяме нашето ценово предложение за участие в откритата от Вас процедура за възлагане на обществена поръчка и съгласно техническото ни предложение.

No	Наименование	Единична цена лева, без ДДС	Брой	Обща цена, лева, без ДДС
1	Комуникационен шкаф	7 030,62 лв.	1	7 030,62 лв.

[1] *Попълнената от участника оферта съгласно този образец се поставя в плик № 3 с надпис "Предлагана цена".*

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

2	Граничен комутатор	5 413,84 лв.	2	10 827,68 лв.
3	Маршрутизатор	44 003,05 лв.	2	88 006,10 лв.
4	Защитна стена	17 732,18 лв.	2	35 464,36 лв.
5	Комутатор за център за данни	46 804,41 лв.	2	93 608,82 лв.
6	SAN комутатор	33 399,94 лв.	2	66 799,88 лв.
7	Комутатор за достъп	5 166,42 лв.	15	77 496,30 лв.
8	Опорен комутатор	16 058,76 лв.	2	32 117,52 лв.
9	Инсталация, конфигурация, интеграция	32 821,17 лв.	1	32 821,17 лв.
10	Обучение	5 791,97 лв.	1	5 791,97 лв.
			Обща стойност без ДДС:	**449 964,42 лв.**
			ДДС 20%	**89 992,88 лв.**
			Обща стойност с ДДС:	**539 957,30 лв.**

2. Обща стойност за доставка на техниката и гаранционно обслужване **449 964,42лв. без ДДС** /словом/ **четиристотин четиридесет и девет хиляди, деветстотин шестдесет и четири лева и четиридесет и две стотинки без ДДС.**

Декларираме, че сме съгласни с условията поставени от Възложителя и начина на плащане, /посочен в документацията за участие в обществената поръчка/.

Приемаме, че единствено и само ние ще бъдем отговорни за евентуално допуснати грешки или пропуски в изчисленията на предложената от нас цена.

Декларираме, че всички еднократни разходи, които биха могли да възникнат при доставката са изцяло за сметка на Изпълнителя и в полза на Възложителя.

Цените се посочват в български лева със закръгляване до втория знак след десетичната запетая.

Евентуални грешки и/или неточности могат да доведат до отстраняването на участника от процедурата.

Предложените цени в настоящата ценова оферта за целия срок на изпълнение на поръчката.

чл. 2 от ЗЗЛД

11.03.2016 г.

ПОДПИС

ПЕЧАТ

Дете[illegible]ександров
Мен[illegible]и
„Тел[illegible]

Този документ задължително се поставя от участника в отделен запечатан непрозрачен плик с надпис ПЛИК № 3.

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

чл. 2 от ЗЗЛД

000653