Годишник Телекомуникации 2024, том 11, с. 91-106

Yearbook Telecommunications 2024, vol. 11, p. 91-106

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.10

МЕТОДОЛОГИЯ ЗА ПРОЕКТИРАНЕ, ИЗГРАЖДАНЕ И ОСТОЙНОСТЯВАНЕ И НА ФИРМЕНА МРЕЖА

Яна Иванова Дончева, Георги Костадинов Петров

Резюме: Настоящата публикация предлага опростена методология за проектиране, изграждане и конфигуриране и остойностяване на мрежи за малки и средни предприятия (INTRANET) отчитайки съвременните тенденции за извънофисна работа (EXTRANET). Обсъдени са основни ключови моменти, както и последващият мониторинг и поддръжка на мрежата. Накрая е разгледан практически пример прилагащ опростената методология за остойностяване на мрежовите компоненти.

Ключови думи: компютърни мрежи.

Abstract: This publication presents a simplified methodology for designing, building, configuring, and costing networks for small and medium-sized enterprises (INTRANET), taking into account current trends in remote work (EXTRANET). It discusses key aspects, as well as the subsequent monitoring and maintenance of the network. Finally, a practical example is provided, applying the simplified methodology for the costing of network components.

Keywords: computer nwtworks

1. ВЪВЕДЕНИЕ

Изграждането на мрежови архитектури за малки и средни преприятия отчитайки съвременните тенденции за разпределени офиси и изнесена работа за служителите отново придобива важност. Това е процес който включва внимателно планиране на мрежовата топология и архитектура на услугите отчитайки всички съвременни изисквания към мрежовите услугии, остойностяване и избор на подходящо оборудване, както и конфигуриране на мрежовите устройства, свързване на подсистеми, като разплащателни терминали, онлайн магазини, баркод четци и RFID идентификация за управление на складови наличности и малки производства, проследяване на фирмени автомобили чрез GPS и т.н. За да се гарантира стабилност, сигурност и ефективност на инфраструктурата, както и да се оценят бъдещите изисквания на потребителите от свързване на нови услуги, системи за достъп, видеомониторинг, изнесени роботизирани работни места и др. В днешно време, когато технологиите се развиват с бързи темпове, важно е мрежата да бъде съвместима с новите стандарти, като например безжични интернет връзки (Wi-Fi с поддръжка на голям брой активни устройства, VLAN), пето поколение мобилни мрежи (5G чрез фемтоклетки [1, 2]) и различни методи за защита като виртуални частни мрежи (VPN) и защитни стени (Firewall), интегрирана антивирусна защита на терминалите и клиентските устройства, както и систумите за контрол на достъпа, периметрова защита, следене на складовите наличности и автоматизацията на спедицията. Поддръжката и мониторингът на мрежата играят критична роля за осигуряване на нейната производителност и сигурност, както и следва

да се отчита и нуждата от редъндантност чрез 5G или друг достъп. Предложената методология претендира за изчерпаемост и приложимост и е резултат от многогодишния опит в планирането, проектирането и изграждането на фирмени мрежи. В края на публикацията е представен конкретен пример за проектиране и изграждане на подобна мрежа отчитайки методиката на оценяване на рентабилността съгласно законът на Меткалф [3], може да се развият и сценарии за внедряването на IoT устройства ползващи различни от IP протоколите, като тук важно е да се отчете предвижда ли се икономия от мащаба [4] при позване на медийни конвертори като ZigBee-WiFi или ще се взимат отделни WiFi, 5G, LoRa базирани устройства.

2. ОБЗОР НА ИЗПОЛЗВАНИТЕ В ПРАКТИКАТА МЕТОДОЛОГИИ

При изграждането на мрежови мрежови инфраструктури съществуват различни признати методологии, които предоставят конкретни насоки и практики в различни етапи на проекта. Изборът на подходяща методология зависи от специфичните нужди на проекта и организацията Табл. 1.

- **ITIL (Information Technology Infrastructure Library)** е най-разпространената методология за управление на IT услуги и предлага подробни насоки за изграждане и поддръжка на мрежови инфраструктури. Тя акцентира на жизнения цикъл на услугите и включва етапи като стратегия за услуги, проектиране, преход, експлоатация и подобрение и е подходящ за големи проекти.
- **TOGAF (The Open Group Architecture Framework)** предлага методология за проектиране на корпоративни архитектури, включително мрежови инфраструктури. TOGAF е полезен за дългосрочни проекти с голям мащаб.
- **PMI (Project Management Institute)** и стандартът **PMBOK (Project Management Body of Knowledge)** предоставят насоки за управление на проекти и може да се приложат в изграждането на мрежови инфраструктури.
- **Cisco CCNA (Cisco Certified Network Associate)** предлага специфични насоки за работа с Cisco оборудване и технологии. Подходяща е за по-малки или по-специализирани проекти, изискващи конкретни технически решения.
- **Scrum/Agile** методологиите предлагат гъвкав подход за проекти с непрекъснато променящи се изисквания. Те се основават на краткосрочни итерации (спринтове), като проектът се разработва постепенно и се адаптира по време на изпълнението.

Таблица 1. Сравнение между основни методологии за проектиране

Методология	Основен фокус	Подходящи за	Ключови етапи	Подходяща за
ITIL	Управление на IT услуги и инфраструктура	Големи, структурирани проекти с дългосрочна поддръжка	Стратегия, Проектиране, Преход, Експлоатация, Подобрение	Проекти с дългосрочни нужди за оптимизация и поддръжка
TOGAF	Корпоративна	Големи компании,	Планиране,	Стратегическо

Годишник Телекомуникации 2024, том 11, с. 91-106

Yearbook Telecommunications 2024, vol. 11, p. 91-106

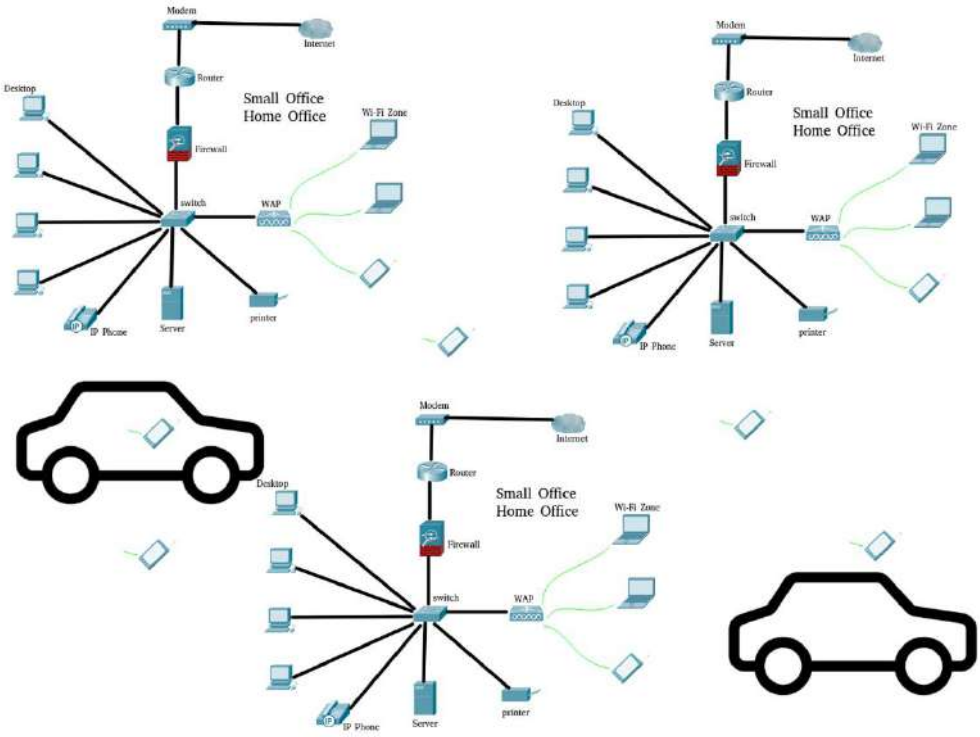
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.10

Методология	Основен фокус	Подходящи за	Ключови етапи	Подходяща за
	архитектура	комплексни решения	Проектиране, Изпълнение, Управление на промените	планиране и интегриране на архитектура
PMI/PMBOK	Управление на проекти	Проекти с ясни цели и ограничения	Иницииране, Планиране, Изпълнение, Контрол, Завършване	Структурирано управление на времето, бюджета и ресурсите
CCNA	Мрежови решения с Cisco оборудване	Специализирани проекти с Cisco технологии	Планиране, Избор на оборудване, Конфигуриране, Поддръжка	Проекти с конкретни Cisco технологии и решения
Scrum/Agile	Гъвкав подход за итеративни проекти	Проекти с променящи се изисквания	Планиране, Изпълнение в спринтове, Адаптиране	Проекти с динамични изисквания и нужда от бързо изпълнение

Изборът на методология за изграждане на мрежови инфраструктури трябва да бъде направен в зависимост от конкретните изисквания на проекта. Ако проектът е голям и има нужда от структурирано управление и дългосрочна поддръжка, ITIL и TOGAF могат да бъдат най-подходящи. За малки или специализирани проекти, които изискват специфично Cisco оборудване, CCNA е най-подходящото решение. За проекти с динамични изисквания и бързо внедряване, Scrum/Agile методологиите ще предоставят нужната гъвкавост и адаптивност. При проектирането на мрежови архитектури за нови малки и средни предприятия, от сферата на търговията, производството и спедицията обаче не може директно да бъдат приложени всички пунктове в по-горните методолгии, тъй като спазването им оскъпява неимоверно както самото проектиране, така и внедряване. Нововъзникващите бизнеси и стартъпи [5] изискват ценово ефективно гъвкаво и разтегливо решение, с възможност за виртуализация на регионален, континентален и междуконтинентален мащаб. Използването на отворени системи, като google и т.н. не е препоръчително, поради невъзможността от защита на интелектуалната собственост и търговската тайна, което в епохата на изкуствения интелект създава сериозни предизвикателства към новонавлизащите компании. Ето защо нашият екип препоръчва разгръщане на самостоятелна инфраструктура, която е редъндънтна и достатъчно ценово ефективна. Единствено и само внедряването на частна инфраструктура е в състояние да защити, както физическите процеси в тези предприятия, така и виртуалните трансфери на технологии и фирмена тайна. На фиг. 1 е дадена схема на класическа фирмена офис мрежа, при малки офиси е почти без значение опцията за по-нататъшно развитие на мрежата, но при компании имащи амбиции за развитие, скоро след стартирането броят

на малките офис и магазинни мрежи бързо нараства и те се изцправят пред типичните за това проблеми по свързване с VPN и организация на EXTRANET за своите служители и търговци. Компаниите често пренебрегват тези етапи на проектиране, като например не свързват възможностите за разкриване на офис в отдалечен град или регион, което често води до колосални трудности по осъществяване на мрежова свързаност и т.н. Тези трудности биха могли да бъдат частично заобиколени, ако на етапите на проектиране бъдат обхванати и бъдат подготвени конкретни алтернативи за това обезпечаване (5/4G, SAT, релейки и т.н.).



Фиг. 1 Блокова схема на несистематично проектирана разпределена корпоративна мрежа в малък мащаб

3. ПЛАНИРАНЕ И АНАЛИЗ НА НУЖДИТЕ

Използвайки основните общи концепции в по-горните методики ще изберем съкратена процедура подходяща при малки и средни фирми. Преди да започне изграждането на мрежата, е важно да се направи задълбочен анализ на нуждите на компанията, за да се осигури, че проектът ще отговори на конкретните изисквания и ще бъде мащабируем за бъдещи нужди. Този етап включва няколко ключови стъпки:

Годишник Телекомуникации 2024, том 11, с. 91-106
Yearbook Telecommunications 2024, vol. 11, p. 91-106
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.24.11.10

3.1. Оценка на броя и вида на устройствата, които ще бъдат свързани към мрежата

Първоначално трябва да се изготви списък на устройствата (типове), които ще се свързват към мрежата. Това включва както настолни компютри, лаптопи, принтери и скенери, така и сървъри, мрежови устройства (комутатори, рутери, точки за достъп) и IoT устройства (сензори, камери за видеонаблюдение, входни термоментри, интелигентни устройства), баркод, RFID, NFC четци, GPS проследяване на автомобили и пратки и много други. Оценката трябва да обхваща както наличните устройства, така и потенциалните нови устройства, които ще се добавят в бъдеще [6]. Като част от анализа е важно да се вземе предвид видът на устройствата – например, дали те ще се свързват чрез кабели (Ethernet, USB, RS232 – тъй като са налични редица устройства със стари интерфейси, като плотери, CNC машини, печатещи хелиографи, чиято подмяна е нецелесъобразна). Особено внимание следва да се отдели и на Wi-Fi, ZigBee, Bluethoot мрежата (2.4GHz или 5GHz, редица безжични устройства поддържат само 2.4GHz и само IPv4), което ще влияе на проектирането на топологията и изискванията към сигурността на мрежата.

3.2. Прогноза за бъдещото разширяване на мрежата

Технологиите и изискванията на бизнеса постоянно се променят, така че мрежата трябва да бъде проектирана с перспектива за бъдещо разширяване, както и свиване, тоест следва да се създаде с технологии позволяващи „разтегливост“. Това включва предвиждане на увеличение на броя на потребителите и устройствата, които ще бъдат свързани към мрежата, оценка на потенциалните начини на свързване на новите нодове (5G). Планирането за бъдещи разширения на мрежата трябва да обхваща капацитета на мрежовата инфраструктура и мащабируемостта.

3.3. Идентифициране на нуждата от интернет достъп и вътрешна комуникация

При анализа на нуждите трябва да се определи дали организацията ще разчита на централизирана интернет връзка, например оптика, или ще има нужда от множество независими интернет връзки по отделни локации, което често не може да се осигури от един и същи провайдер, за да осигури по-голяма надеждност следва да се обмисли и ползването на VPN с локален доставчик или изграждане на собствен с възможност за рутиране на VoIP трафик. Трябва да се оцени и какви скорости на интернет ще бъдат необходими за различните дейности в организацията – например, дали ще има нужда от високи скорости за видео конференции и видеонаблюдение, големи файлове или облачни услуги [7]. Вътрешната комуникация също трябва да бъде разгледана – какви протоколи и платформи ще се използват (ZigBee, Bluetooth 5, NFC, LoRa са системи изискващи мостова свързаност, за да предоставят услуги през корпоративния INTRANET) и как ще бъде осигурена сигурността и стабилността на тези комуникации. Проблемите с поддръжката също не са за пренебрегване, често тези системи са

непознати на повечето мрежови администратори, което налага изготвяне на надлеждна документация и инструкции за работа с тях.

3.4. Събиране на информация от различни отдели, за да се определят ресурсите, които ще са необходими

Мрежовият анализ трябва да обхваща всички отдели в компанията, за да се разберат специфичните им нужди. В стартъп компаниите тази структура е плоска, като повечето ползват изнесени логистични и счетоводни услуги. Всеки отдел може да има различни изисквания и нужди от мрежови ресурси, като: ИТ отдел, финансови и счетоводни отдели, маркетинг и продажби, обслужване на клиенти, производствени или складови екипи, доставки, специфична машинна свързаност [8]. Всеки обект трябва да подготви карта на ползваните услуги, въз основа на което ще се извърши преценка за обема на данни, който обработва, както и очакваните нива на трафик, съхранение и бекъп на данните. Това ще помогне за по-доброто планиране на необходимата мрежова и компютърна инфраструктура.

4. ПРОЕКТИРАНЕ НА МРЕЖОВАТА АРХИТЕКТУРА

Проектирането на мрежовата архитектура е критичен етап в изграждането на локална мрежа (LAN), който определя основната структура и ефективност на мрежата. За да се осигури максимална производителност, сигурност и мащабируемост и разтегливост на услугите, е необходимо внимателно планиране на различни аспекти на мрежата:

4.1. Разработка на мрежова топология

Топологията определя как устройствата ще бъдат свързани помежду си и как трафикът ще преминава през мрежата, IP мрежите имат йерархична логическа топология, но свързването на редица подсистеми чрез тях може да е предизвикателство [9, 10, 11]. В зависимост от нуждите на компанията и нейната инфраструктура, могат да бъдат избрани различни типове топологии:

- **Тип „Звезда“** (Star Topology)
- **Тип „Кръг“** (Ring Topology)
- **Тип „Шина“** (Bus Topology)
- **С комбинирани елементи**

4.2. Физическо и логическо разположение на мрежовите компоненти

След като е избрана топологията, следва да се проектира физическото и логическото разположение на мрежовите компоненти, т.нар. комуникационен шкаф. Това включва планиране на местоположението на рутери, комутатори, точки за достъп и други устройства, които ще формират основната инфраструктура на мрежата, наред с NVR, мрежови удължители и протоколни конвертори. Основните елементи, които трябва да се вземат предвид, са централизирано или дистрибутирано разположение, позициониране на рутери и комутатори, точки за достъп (Access Points) при по-големи обекти, като складова база и производствени халета.

Годишник Телекомуникации 2024, том 11, с. 91-106
Yearbook Telecommunications 2024, vol. 11, p. 91-106
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.24.11.10

4.3. Сегментиране на мрежата чрез VLAN (Virtual Local Area Networks)

Сегментирането на мрежата е важна стъпка за оптимизиране на трафика и повишаване на сигурността. VLAN (Virtual Local Area Network) позволява разделянето на мрежата на различни логически сегменти, въпреки че физическото разположение на устройствата може да остане непроменено. Това дава възможност за ефективно управление на мрежовия трафик, подобряване на производителността и повишаване на сигурността, разумно е разделяне на подсистемите като минимум в отделни виртуални канали. VLAN сегментацията има следните предимства, като: оптимизиране на трафика, повишена сигурност, подобрена поддръжка и управление, възможност за приоритизиране.

5. ИЗБОР НА ОБОРУДВАНЕ

След като мрежовата архитектура е проектирана, следва изборът на подходящо оборудване, което да отговори на изискванията на организацията и да осигури ефективността, сигурността и мащабируемостта на мрежата. Правилният избор на мрежови устройства е от съществено значение за стабилността и производителността на мрежата. Процесът на избор включва оценка на различни мрежови компоненти като маршрутизатори, комутатори, медийни конвертори и точки за достъп, които са основните елементи за изграждането на функционална и надеждна локална мрежа. Това включва следните основни стъпки:

5.1. Маршрутизатори (Рутери)

Маршрутизаторите са централни устройства в мрежата, които осигуряват комуникация между различните сегменти на мрежата, както и връзка с външния свят чрез интернет. Изборът на подходящ рутер е важен, за да се осигури стабилна, бърза и сигурна връзка между различните компоненти на мрежата. При избора на рутери трябва да се вземат под внимание следните фактори: пропускателна способност и производителност, сигурност, поддръжка на IPv6, мащабируемост.

5.2. Комутатори (Switches)

Комутаторите управляват трафика в мрежата, като осигуряват свързаност между устройствата в локалната мрежа (LAN). Те са отговорни за маршрутизирането на данни на второ ниво (Data Link Layer) и играят важна роля за оптимизиране на трафика и осигуряване на висока производителност. При избора на комутатори трябва да се разгледат следните аспекти:

- **Тип на комутаторите**: н**еуправляеми комутатори (Unmanaged Switches), управляеми комутатори (Managed Switches), слой 3 комутатори (Layer 3 Switches)**
- **Брой на портовете**
- **Поддръжка на PoE (Power over Ethernet)**

- **Скорост на портовете**: 100Mbps/1Gbps/10Gbps

5.3. Точки за достъп (Access Points)

Точките за достъп осигуряват безжична свързаност в мрежата, като позволяват на устройствата да се свързват към LAN чрез Wi-Fi. Те играят също така важна роля за разширяване на обхвата на мрежата и осигуряване на връзка в зони, където кабелната инфраструктура не е възможна или не е ефективна. При избора на точки за достъп трябва да се имат предвид следните фактори: стандарт на Wi-Fi (802.11ac) или (802.11ax), обхват на сигнала, поддръжка на Mesh мрежи, сигурност.

6. ИНСТАЛАЦИЯ НА МРЕЖОВОТО ОБОРУДВАНЕ

След като мрежовата архитектура е проектирана и необходимото оборудване е избрано, следва да се премине към фазата на инсталация на мрежовите компоненти. Тази стъпка е критична за създаването на физическата инфраструктура на мрежата и включва набор от дейности, които да осигурят стабилни и надеждни връзки между различните мрежови устройства. Инсталацията на мрежовото оборудване обикновено преминава през следните основни етапи:

6.1. Монтаж и свързване на устройствата според проекта за топология

Първоначално трябва да се извърши физическото разположение на устройствата в съответствие с предварително планираната мрежова топология. Това включва избор на място за рутери, комутатори, точки за достъп и други мрежови компоненти, като трябва да се вземе предвид защитен, но удобен за работа достъп, защита от физическа повреда, наводняване и т.н., добро охлаждане. След като устройството е монтирано, следва свързването му с други компоненти на мрежата чрез физически кабели, за да се гарантира, че всички устройства могат да комуникират помежду си, създавайки необходимата инфраструктура за пренос на данни.

6.2. Прокарване на кабели и осигуряване на стабилни физически връзки между мрежовите компоненти

Прокарването на кабелите е основна част от инсталацията на мрежовото оборудване и трябва да се извърши внимателно, за да се осигури стабилност, сигурност и бързина на връзките. Процесът включва: **подходящи кабели**: (като Cat5e, Cat6 или Cat6a), подреждане и организиране на кабелите – добре подреденият шкаф е гаранция за надеждна работа и дългосрочна експлоатация, стабилност на връзките, проверка на дължината на кабелите и аванс при оптики.

6.3. Свързване на устройствата към мрежата и тестване на първоначалната конфигурация

След като всички устройства са инсталирани и свързани физически чрез кабели, следва да се извърши тяхното свързване към мрежата. Това включва настройка на IP адреси, конфигуриране на маршрутизатори и комутатори, както и проверка на основната свързаност между устройствата.

Годишник Телекомуникации 2024, том 11, с. 91-106
Yearbook Telecommunications 2024, vol. 11, p. 91-106
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.24.11.10

- **Конфигуриране на IP адреси**: DHCP (Dynamic Host Configuration Protocol)
- **Настройка на маршрутизатори и комутатори**: VLAN, QoS (Quality of Service), защита чрез firewall и други политики за сигурност.
- **Тестване на свързаността**: Тестването на свързаността може да се извърши с помощта на различни мрежови инструменти като **ping**, **traceroute** и **speed test**.

7. КОНФИГУРИРАНЕ НА МРЕЖОВИТЕ УСТРОЙСТВА

След инсталацията на мрежовото оборудване следва ключовата фаза на конфигуриране на мрежовите устройства. Това включва настройка на мрежови параметри, мрежова сигурност и активиране на услуги, които ще осигурят гладкото функциониране на мрежата. Конфигурирането на мрежовите устройства е критичен етап, тъй като позволява на мрежата да започне да работи според нуждите на организацията и да осигури стабилност и сигурност в комуникациите между различните компоненти.

7.1. Настройка на IP адреси и конфигуриране на маршрутизиране между различни сегменти на мрежата

Настройката на IP адресите е първата стъпка в конфигурирането на мрежовите устройства. Всеки мрежови компонент трябва да има уникален IP адрес, за да може да комуникира с другите устройства в мрежата. След това се извършва конфигурирането на маршрутизаторите и свързването им с различни мрежови сегменти.

- **Ръчно задаване на IP адреси или DHCP**
- **Маршрутизиране между мрежови сегменти**: Ако мрежата е сегментирана с VLAN (Virtual Local Area Networks), рутерите трябва да бъдат конфигурирани.

7.2. Конфигуриране на VLAN за разделяне на различни мрежови ресурси и оптимизиране на трафика

Сегментирането на мрежата с VLAN е важен процес за управление на трафика и повишаване на сигурността. VLAN позволява логическо разделяне на мрежата, дори ако устройствата физически са свързани към една и съща мрежова инфраструктура.

- **Създаване на VLAN**
- **Маршрутизиране между VLAN (Inter-VLAN Routing)**
- **Управление на трафика**

7.3. Настройка на защитни механизми като защитни стени (firewall) и политики за достъп

Защитата на мрежата е една от най-важните стъпки при конфигурирането на мрежовите устройства. Конфигурирането на защитни стени (firewalls) и политики за достъп гарантира, че само упълномощените устройства и потребители могат да имат достъп до мрежовите ресурси, като същевременно се предотвратяват неоторизирани достъпи и външни атаки.

- **Конфигуриране на защитни стени**:
  - Ограничаване на достъпа до специфични външни ресурси.
  - Разрешаване само на конкретни протоколи и портове за комуникация.
  - Изграждане на правила за управление на трафика между вътрешните и външни мрежи.
- **Политики за достъп (Access Control Policies)**:
  - Автентикация и авторизация на потребители.
  - Определяне на нива на достъп за различни мрежови сегменти и устройства.
  - Прилагане на правила за сигурност, които ограничават достъпа до чувствителни данни и приложения.

7.4. Активиране на мрежови услуги като DNS, DHCP и други, необходими за функционирането на мрежата

За да функционира правилно мрежата, е необходимо да се активират и конфигурират различни мрежови услуги. Те осигуряват основни функционалности като разпознаване на имена на хостове и автоматично разпределение на IP адреси.

- **DNS (Domain Name System)**
- **DHCP (Dynamic Host Configuration Protocol)**
- **Допълнителни мрежови услуги**: мрежови услуги като VPN (Virtual Private Network) за сигурен достъп от отдалечени локации, NTP (Network Time Protocol) за синхронизация на времето, и други приложения, като бази данни, складови наличности, продажби, доставени стоки, места на автомобили и служители.

8. ТЕСТВАНЕ НА МРЕЖАТА

Тестването на мрежата е критична стъпка след конфигурирането на всички мрежови компоненти и преди пускането на мрежата в експлоатация. Това е процес, при който се валидира дали мрежата изпълнява заложените изисквания за производителност, свързаност и сигурност. Тестовете осигуряват, че мрежата функционира ефективно и безпроблемно, като същевременно отговаря на нуждите на организацията и предлага защита срещу външни и вътрешни заплахи.

8.1. Проверка на свързаността и бързината на трафика в мрежата

Една от първите стъпки в процеса на тестване е да се проверят основните мрежови параметри като свързаност и производителност. Тестването на свързаността включва проверка дали устройствата в мрежата могат да комуникират помежду си. Това обикновено включва изпълнението на базови мрежови тестове като:

- **Ping тестове**
- **Traceroute тестове**
- **Тестове на мрежова скорост (speed tests)**

Годишник Телекомуникации 2024, том 11, с. 91-106

Yearbook Telecommunications 2024, vol. 11, p. 91-106

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.10

8.2. Тестове за натоварване

Натоварването на мрежата е важен аспект, който трябва да бъде тестван, за да се уверите, че мрежата може да издържи на очакваните натоварвания и трафик. Това включва:

- **Тестове за максимален трафик**
- **Тестове за производителност при високо натоварване**
- **Тестове за мрежово претоварване** „ботълнекинг“ (bottlenecking).

8.3. Оценка на сигурността

Тестването на сигурността на мрежата е от решаващо значение, за да се гарантира, че мрежовите компоненти са защитени от потенциални атаки или пробиви. Основните стъпки при тестването на сигурността включват:

- **Проверка на защитни стени (firewalls)**
- **Тестове за уязвимости** използвайки специализирани инструменти като Nessus или OpenVAS.
- **Пенетрейшън тестове (Pen-testing)**
- **Проверка на политики за достъп**
- **Мониторинг за сигурност**: Използване на системи за мониторинг като IDS/IPS (Intrusion Detection and Prevention Systems)

9. ОБУЧЕНИЕ НА ПЕРСОНАЛА И ДОКУМЕНТИРАНЕ НА МРЕЖАТА

Обучението на персонала и документирането на мрежовата инфраструктура са не само важни за правилното функциониране на мрежата, но и ключови за осигуряване на дългосрочната ѝ стабилност и сигурност. Добре обучените служители и ясно документираната мрежова среда ще допринесат за ефективното управление, поддръжка и защита на мрежата.

9.1. Обучение на администратори

Една от основните стъпки е обучение на мрежовите администратори, които ще управляват и поддържат мрежата. Това обучение трябва да обхваща различни аспекти на управлението на мрежовата инфраструктура:

- **Управление на мрежовото оборудване**
- **Управление на сигурността**
- **Поддръжка и отстраняване на проблеми**

9.2. Обучение на крайни потребители

Обучението на крайни потребители е също толкова важно, за да се гарантира, че те ще използват мрежата по безопасен и ефективен начин. Това обучение трябва да включва:

- **Основи на мрежовата сигурност**
- **Управление на мрежови ресурси**
- **Политики за достъп**

9.3. Документиране на мрежовото оборудване и конфигурации

Документирането на мрежовата инфраструктура е от съществено значение за дългосрочната поддръжка и бързо отстраняване на проблеми. Това документиране трябва да включва:

- **Мрежово оборудване**
- **Мрежови конфигурации**
- **Процедури за отстраняване на проблеми и аварийни ситуации**
- **Резервни копия на конфигурации**

10. ПОДДРЪЖКА И МОНИТОРИНГ НА МРЕЖАТА

След като мрежата е изградена и тествана, е от съществено значение тя да бъде редовно наблюдавана и поддържана, за да се гарантира нейната стабилност, производителност и сигурност. Това включва непрекъснато наблюдение на състоянието на мрежата, управление на инциденти и извършване на редовни актуализации на софтуера и конфигурациите. Добре организираният мониторинг и поддръжка са важни за избягване на проблеми, които могат да повлияят на производителността и сигурността на мрежата.

10.1. Мониторинг на мрежовото състояние

Мониторингът на мрежата е ключов за откриването на проблеми още в началото, което позволява своевременно предприемане на действия. За целта могат да се използват различни софтуерни решения:

- **Nagios**: Това е мощен инструмент за мониторинг, който позволява наблюдение на мрежови устройства, сървъри и приложения.
- **Wireshark**: Wireshark е инструмент за анализ на мрежовия трафик, който позволява да се проследяват всички пакети, преминаващи през мрежата.
- **Периодичен мониторинг на производителността**: Използването на инструменти за мониторинг като **Prometheus** и **Grafana** осигурява визуализация на данните.

10.2. Управление на инциденти

Независимо от предварителните мерки за сигурност и мониторинг, могат да възникнат инциденти, които да застрашат стабилността и сигурността на мрежата. Процесът на управление на инциденти трябва да включва:

- **Детекция на инциденти**

Годишник Телекомуникации 2024, том 11, с. 91-106

Yearbook Telecommunications 2024, vol. 11, p. 91-106

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.10

- **Реакция на инциденти**
- **Анализ на инциденти**
- **Документиране на инциденти**

10.3. Редовни актуализации и управление на уязвимости

Редовното обновяване на мрежовото оборудване и софтуер е важен аспект за поддържането на мрежата в безопасно състояние. Необходими са редовни актуализации на операционните системи на сървърите, рутерите, комутаторите и защитните стени, за да се избегнат уязвимости, които могат да бъдат експлоатирани от злонамерени потребители.

- **Актуализации на софтуера**
- **Управление на уязвимости**
- **Прогноза и планиране на капацитет**

11. ЗАДАНИЕ ЗА ИЗГРАЖДАНЕ НА МРЕЖОВА ИНФРАСТРУКТУРА

Мрежова инфраструктура за три офиса (два в един град, един в друг)

Проектът ще обхваща изграждането на корпоративна мрежова инфраструктура за три офиса, два от които ще бъдат в същия град, а третият – в различен. Ще бъде проектирана мрежа за 50-100 устройства във всеки офис, като всяко работно място ще е оборудвано с баркодчетци, NFC RFID устройства, видеонаблюдение и други елементи, свързани със счетоводство, складова наличност, картови четци за разплащания и контрол на стоките. Офис 1 и Офис 2 (в същия град). Тези два офиса ще споделят основни мрежови ресурси и ще комуникират помежду си през централния офис в града.

- **Оборудване**: Всеки офис ще бъде оборудван със сървър, рутер, комутатор, безжични точки за достъп и устройства за управление на трафика.
- **Сигурност**: Всеки офис ще има защитни стени, като ще се използват най-съвременни технологии за предотвратяване на външни атаки, включително DDoS защита.
- **Точки за достъп**: В офиса ще има около 50 устройства.
- **Видеонаблюдение, контрол на стоките**: Складови наличности и системи за контрол ще бъдат интегрирани с мрежовата инфраструктура.
- **Принтери и други устройства**: Ще бъдат свързани периферни устройства, като принтери, скенери и други.

Точки за достъп и устройства:

- Във всеки офис ще бъдат разположени 10-15 безжични точки за достъп.
- Периферни устройства: Принтери, скенери, баркодчетци и NFC/RFID устройства.

Офис 3 (в друг град)

- Третият офис, разположен в различен град, ще бъде свързан към основната мрежова инфраструктура чрез VPN тунели. Оборудване: В този офис ще се инсталира същото оборудване като в офисите в същия град, с добавен рутер за връзка през интернет.

Точки за достъп и устройства:

- Около 15 устройства, включително баркодчетци, NFC/RFID устройства, принтери, и видеонаблюдение. Допълнителни мобилни устройства за служители.

Табилца 1. Общ бюджет за проекта (за трите офиса):

Оборудване	**Вариант 1** (Бюджетен)	**Вариант 2** (Среден клас)	**Вариант 3** (Премиум)
Рутер	TP-LINK Archer AX20	TP-LINK Archer AX73 / AX5400	Cisco RV340W
Цена	159 лв.	249.99 лв.	699 лв.
Wi-Fi стандарт	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Скорост	1.8 Gbps	4.8 Gbps	1.7 Gbps (с допълнителни функции за VPN)
Безжични точки за достъп	TP-LINK EAP245	Huawei AirEngine 5762-12	Ubiquiti UniFi 6 Long-Range
Цена	189 лв.	287.46 лв.	459 лв.
Wi-Fi стандарт	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Скорост	1.7 Gbps	4.8 Gbps	3.5 Gbps (обхват до 183 метра)
Комутатор	TRENDnet 5 портов (Gbit/s)	TRENDnet 8 портов (Gbit/s, 802.1p)	Cisco Catalyst 2960X
Цена	159 лв.	317 лв.	1,200 лв.
Порти	5 порта (Gigabit Ethernet)	8 порта (Gigabit Ethernet)	24 порта (Gigabit Ethernet + PoE)
Сигурност	Защитна стена (между устройства)	Защитна стена (между устройства и външния свят)	Интегрирана защита от атаки и VPN
Съхранение на данни	Не поддържа външни дискове	Поддръжка за USB портове и NAS	Поддръжка за външни дискове и RAID конфигурации
Модем	Не е включен	Cisco FPR1010E NGFW-K9 (защитна стена)	Cisco Meraki MX67

Годишник Телекомуникации 2024, том 11, с. 91-106

Yearbook Telecommunications 2024, vol. 11, p. 91-106

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.10

Оборудване	**Вариант 1** (Бюджетен)	**Вариант 2** (Среден клас)	**Вариант 3** (Премиум)
Цена	-	1,349.75 лв.	1,600 лв.

ЗАКЛЮЧЕНИЕ

Процесът на изграждане и поддръжка на локална мрежа е многостранен и изисква внимание към всички технически детайли. Добре проектираната мрежова архитектура, използването на нови технологии като Wi-Fi и 5G, както и правилната конфигурация на мрежовите устройства и сигурността чрез VPN и защитни стени, създават стабилна и сигурна основа за работа. Редовният мониторинг и поддръжка, както и обучението на персонала относно сигурността и правилното използване на мрежата, са важни за нейното безпроблемно функциониране. Чрез ефективното документиране и внедряване на съвременни технологии за управление на мрежовия трафик, организацията може да гарантира бърз, надежден и сигурен достъп до данни и ресурси. Систематизацията на задачите и дейностите при изграждането на локална мрежа е ключова за успешното реализиране на проекта и гарантиране на дългосрочна ефективност. Всеки етап от процеса трябва да бъде изпълняван с внимание към детайлите и последователност, за да се осигури оптимална производителност, сигурност и мащабируемост на мрежата. Правилният избор на компоненти, внимателното планиране на мрежовата архитектура и съответната конфигурация на устройствата осигуряват не само стабилност и надеждност, но и лесно разширяване и поддръжка на мрежата в бъдеще. Осигурената защита срещу външни и вътрешни заплахи, както и внедряването на технологии с висока производителност, ще позволи на организацията да се адаптира към динамичните изисквания на съвременната работна среда. Завършването на този проект ще предостави на компанията не само стабилна и сигурна мрежова инфраструктура, но и гъвкава основа за бъдещото й развитие и интеграция с нови технологии. Това ще гарантира, че мрежата ще бъде в състояние да отговори на нарастващите нужди на бизнеса и да поддържа безпроблемната му работа в дългосрочен план. Включените разходи за поддръжка осигуряват дългосрочната надеждност и функционалност на мрежата. Изборът на компоненти и специалисти гарантира не само качествено изграждане на мрежата, но и безпроблемно й функциониране през цялата година.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ (REFERENCES)

[1] ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Изследване на фемтоклетъчни технологии за мобилни клетъчни мрежи. *Годишник Телекомуникации* [онлайн]. 2022, (9), с. 53-59 [прегледан 26.03.2025]. eISSN 2534-854X. Достъпен на: https://doi.org/10.33919/YTelecomm.22.9.5 [PASARELSKI, Rosen i Teodora PASARELSKA. Izsledvane na femtokletachni tehnologii za mobilni kletachni mrezhi. *Godishnik Telekomunikatsii* [onlayn]. 2022, (9), s. 53-59 [pregledan 26.03.2025]. eISSN 2534-854X. Dostapen na: https://doi.org/10.33919/YTelecomm.22.9.5]

[2] ПАСАРЕЛСКИ, Росен. *Нови 5G мобилни клетъчни системи: Изследване на взаимодействието между 4G-LTE и 5G системите: архитектура, мрежови функции, интерфейс и протоколи*. София: Нов български университет, 2024. ISBN 978-619-233-282-2. [PASARELSKI, Rosen Ivanov. *Novi 5G mobilni kletachni sistemi: Izsledvane na vzaimodeystvieto mezhdu 4G-LTE i 5G sistemite: arhitektura, mrezhovi funktsii, interfeys i protokoli*. Sofia: Nov balgarski universitet, 2024. ISBN 978-619-233-282-2.]

[3] NOSOVICKI, Dmitri. Metcalfe's Law Revisited. *arXiv* [online]. [viewed 26.03.2025]. Available from: 10.48550/arXiv.1604.05341

[4] Network Diagram Examples. *ConceptDraft* [online]. [viewed 26.03.2025]. Available from: https://www.conceptdraw.com/examples/topology-of-intranet
[5] АВРАМОВ, Йосиф. *Финансов инженеринг в телекомуникациите*. София: Нов български университет, 2021. ISBN 978-619-233-191-7. [AVRAMOV, Yosif. *Finansov inzhenering v telekomunikatsiite*. Sofia: Nov balgarski universitet, 2021. ISBN 978-619-233-191-7.]
[6] СТЕФАНОВА, Тереза. *Новите технологии: приложения, професии, умения: монография*. София: Аскони-издат, 2024. ISBN 978-954-383-151-7. [STEFANOVA, Tereza. *Novite tehnologii: prilozhenia, profesii, umenia: monografia*. Sofia: Askoni-izdat, 2024. ISBN 978-954-383-151-7.]
[7] ПАСАРЕЛСКИ, Росен. *Услуги в центровете за данни* [онлайн]. София: Нов български университет, 2024 [прегледан 26.03.2025]. ISBN 978-619-233-300-3. Достъпен на: https://publishing-house.nbu.bg/bg/elektronni-izdaniq/knigi/uslugi-v-centrovete-za-danni [PASARELSKI, Rosen. *Uslugi v tsentrovete za danni* [onlayn]. Sofia: Nov balgarski universitet, 2024 [pregledan 26.03.2025]. ISBN 978-619-233-300-3. Dostapen na: https://publishing-house.nbu.bg/bg/elektronni-izdaniq/knigi/uslugi-v-centrovete-za-danni]
[8] Small Office Home Office SOHO. *Network Fundamentals CCNA 200-301* [online]. [viewed 26.03.2025]. Available from: https://ccnatutorials.in/network-fundamentals-ccna-200-301/small-office-home-office-soho/
[9] CHEN, Min, Jiafu WAN, and Fang LI. Machine-to-Machine Communications: Architectures, Standards and Applications. *KSII Transactions on Internet and Information Systems* [online]. 2012, vol. 6(2), pp. 480-497 [viewed 26.03.2025]. eISSN 1976-7277. Available from: 10.3837/tiis.2012.02.002.
[10] LAN Topologies. *NetConsultantsch2* [online]. [viewed 26.03.2025]. Available from: https://cdn.ttgtmedia.com/searchNetworking/Downloads/NetConsultantsch2.pdf
[11] Exploring the Modern Computer Network: Types, Functions, and Hardware. *Cisco Press* [online]. [viewed 26.03.2025]. Available from: https://www.ciscopress.com/articles/article.asp?p=2158215&seqNum=6
[12] СТОИЛОВ, Емил. *Проектиране на корпоративни мрежи. Архитектура*. Част I [онлайн]. София: Нов български университет, 2014 [прегледан 26.03.2025]. Научен електронен архив на НБУ. Достъпен на: https://eprints.nbu.bg/id/eprint/2219/ [STOILOV, Emil. Proektirane na korporativni mrezhi. Arhitektura. Chast I [onlayn]. Sofia: Nov balgarski universitet, 2014 [pregledan 26.03.2025]. Nauchen elektronen arhiv na NBU. Dostapen na: https://eprints.nbu.bg/id/eprint/2219/]

Contacts:
Yana Ivanova Doncheva, New Bulgarian University, department “Telecommunications”, yanadonch@gmail.com
Assoss.Prof. Georgi Petrov, New Bulgarian University, department “Telecommunications”, gpetrov@nbu.bg

Date of receipt of the manuscript: 09.09,2024
Date of adoption for publication: 30.09.2024