УДК 004

ПРОЕКТИРОВАНИЕ СЕТЕВОЙ ИНФРАСТРУКТУРЫ И РЕАЛИЗАЦИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СТАНДАРТА GIGABIT ETHERNET ОДНОГО ИЗ ИЗДАТЕЛЬСТВ Г. КАЛУГА

Раевский В.А.

канд. техн. наук,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Тимашов Д.С.

инженер отдела эксплуатации телекоммуникаций,

«Калугаэнерго», филиал ПАО «Россети Центр и Приволжье»

Калуга, Россия

Говорова Е.С.

студент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация

В настоящей статье изложены особенности проектирования локальной вычислительной сети одного из издательств г. Калуга; приводится схема спроектированной сети. Рассматривается назначение IP-адресации по технологии Variable Length Subnet Mask. Анализируются достоинства и недостатки протоколов маршрутизации внутреннего шлюза, обосновывается выбор протокола Routing Information Protocol (RIP). Приводятся некоторые выполненные мероприятия по конфигурированию сетевых устройств.

Ключевые слова: локальная вычислительная сеть, проектирование, IP-адрес, протокол маршрутизации, конфигурирование.

NETWORK INFRASTRUCTURE DESIGN AND IMPLEMENTATION OF A LOCAL COMPUTING NETWORK GIGABIT ETHERNET STANDARD OF ONE OF THE PUBLISHERS KALUGA CITY

Raevsky V.A.
Candidate of Technical Sciences,
Kaluga State University named after K.E. Tsiolkovski,
Kaluga, Russia

Timashov D.S.
telecommunications operation departmental engineer,
PJSC Rosseti Center and Privolzhsky District, Kalugaenergo branch,
Kaluga, Russia

Govorova E.S.
Undergraduate Student,
Kaluga State University named after K.E. Tsiolkovski,
Kaluga, Russia

Abstract

This article describes the features of designing a local computer network for one of the publishing houses in Kaluga, Russia. It provides a diagram of the designed network and discusses the use of Variable Length Subnet Mask technology for IP addressing. The article analyzes the advantages and disadvantages of internal

gateway routing protocols and justifies the choice of Routing Information Protocol (RIP). It also describes some of the configuration steps taken for network devices.

Keywords: local area network, design, IP address, routing protocol, configuration.

Обоснование актуальности. Представленная статья является продолжением работы [5], в которой обосновывается актуальность реализации локальной вычислительной сети стандарта Gigabit Ethernet одного из издательств г. Калуга.

Проектирование сетевой инфраструктуры. Проектирование сетевой инфраструктуры включает в себя разработку проекта сети и реализованных в ней решений, связанных с функционированием сети, ее внутренней адресацией, способами взаимодействий сетевых устройств, а также определением мер по ее безопасности [2; 7].

Локальная вычислительная сеть организации включает в себя 28 рабочих станций и сервер. Исходя из Технического задания Заказчика [5], сеть следует разделить (сетевой уровень) на семь сегментов: три сегмента для журналистского отдела, редакционный отдела, отдела бухгалтерии соответственно; один сегмент для сервера организации; три сегмента между маршрутизаторами. Каждый сегмент должен быть подключен к маршрутизатору; узлы в сегменте (за исключением сегментов между маршрутизаторами и сегмента сервера) объединяются с помощью коммутатора. Спроектированная структура сети представлена на рис. 1 (под межсетевым экраном понимается набор настроек безопасности маршрутизатора, обеспечивающего доступ к сети Интернет). Выбор сетевого оборудования для локальной вычислительной сети организации представлен в [5].

Диапазоны назначаемых IP-адресов определены по технологии Variable Length Subnet Mask (VLSM, маски подсетей переменной длины) [8], исходя из требуемого по Техническому заданию числа узлов в сегменте (см. Таблицу 1).

Далее необходимо определить протокол, используемый для межсетевого взаимодействия внутри ЛВС и обеспечивающий нахождение и фиксацию оптимальных маршрутов продвижения данных через составную сеть TCP/IP [1].

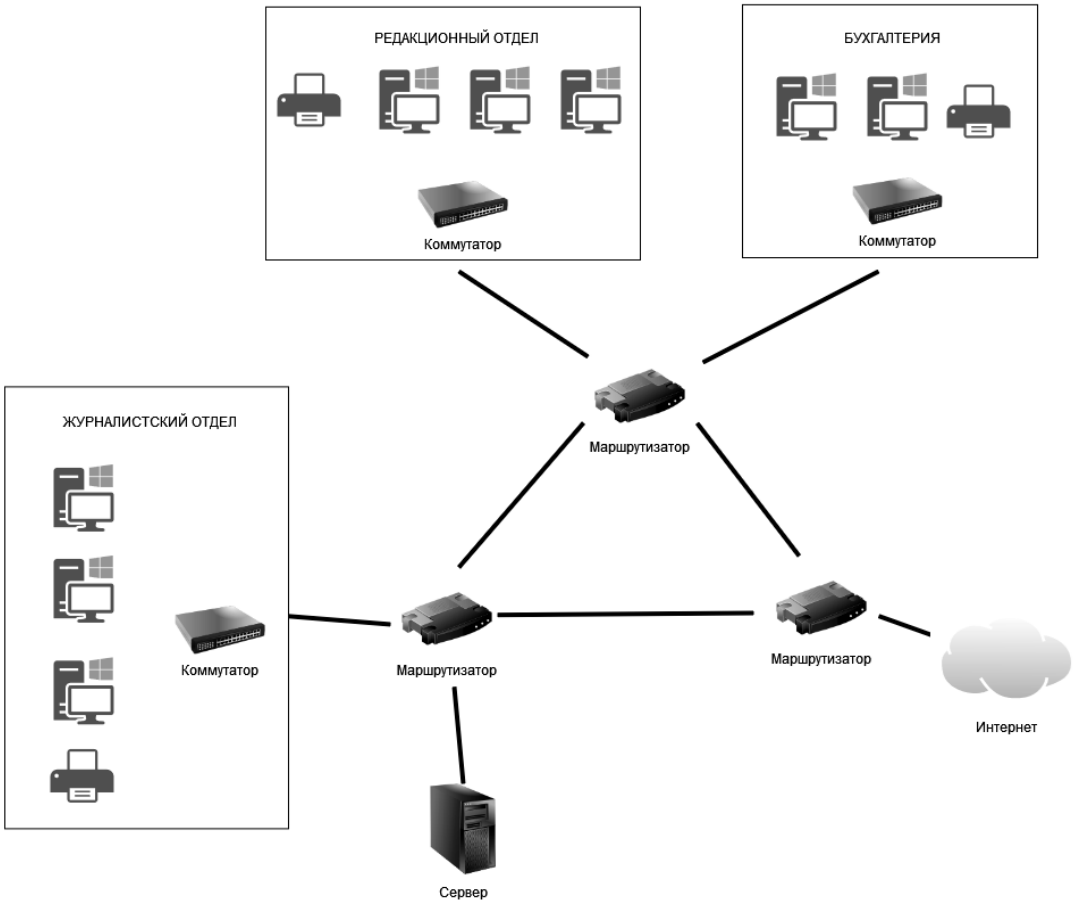

Рис. 1 – Структура локальной вычислительной сети организации

Таблица 1 – Диапазоны адресов в сети

Номер подсети	Выделено адресов	Остаток свободных адресов	IP адрес подсети	Маска подсети	Префикс маски	Диапазон адресов	IP адрес широко-вещания

1	64	27	192.168.1.0	255.255.255.192	/26	192.168.1.1 - 192.168.1.62	192.168.1.63
2	32	0	192.168.1.64	255.255.255.224	/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	16	4	192.168.1.96	255.255.255.240	/28	192.168.1.97 - 92.168.1.110	192.168.1.111
4	8	1	192.168.1.112	255.255.255.248	/29	192.168.1.113 - 192.168.1.118	192.168.1.119
5	4	0	192.168.1.120	255.255.255.252	/30	192.168.1.121 - 192.168.1.122	192.168.1.123
6	4	0	192.168.1.124	255.255.255.252	/30	192.168.1.125 - 192.168.1.126	192.168.1.127
7	4	0	192.168.1.128	255.255.255.252	/30	192.168.1.129 - 192.168.1.130	192.168.1.131

Различают статическую и динамическую маршрутизацию. В сети, основанной на статической маршрутизации, таблицы маршрутизации заполняются вручную администратором сети и остаются неизменяемыми. Такой подход наиболее распространен в небольших сетях.

Динамическая маршрутизация основана на использовании протоколов маршрутизации, которые позволяют маршрутизаторам обмениваться информацией о состоянии сети и автоматически обновлять таблицы маршрутизации. Динамическая маршрутизация является более гибкой и масштабируемой, поскольку обеспечивает быструю адаптацию к изменениям топологии сети, качеству линий связи и т.п. Рассмотрим достоинства и недостатки дистанционно-векторных протоколов маршрутизации и протоколов по состоянию канала связи [6; 10; 11; 13].

Преимущества дистанционно-векторных протоколов:

1) простота реализации;

2) низкое использование ресурсов сети;

3) быстрая сходимость в малых сетях.

Недостатки дистанционно-векторных протоколов:

1) медленная реакция на изменения в сети;

2) низкая сходимость в больших сетях;

3) подвержены проблемам существования петель маршрутизации.

Преимущества протоколов по состоянию канала связи:

1) быстрая сходимость в любых сетях;

2) поддержка сложных топологий сетей;

3) возможность использования различных метрик для выбора оптимальных маршрутов.

Недостатки протоколов по состоянию канала связи:

1) сложность в реализации;

2) потенциальная сложность в диагностировании проблем и отладке.

Исходя из анализа достоинств и недостатков, учитывая особенности вычислительной сети Заказчика и возможность дальнейшего администрирования сети на аутсорсинге, по согласованию с Заказчиком выбран дистанционно-векторный протокол Routing Information Protocol (RIP) как наиболее простой в реализации.

Кроме того, для сетевых устройств необходимо реализовать процессы аутентификации, авторизации и учета (Authentication, Authorization, Accounting, AAA) [4; 14] в дополнение к реализованным мерам безопасности [2]. При аутентификации пользователь подтверждает свою личность, используя логин и пароль, сертификаты, биометрические данные и другие методы. Протоколы RADIUS [12] и TACACS+ [9] позволяют централизованно управлять процессами AAA для всех устройств в сети. Сравнение данных протоколов представлено в таблице 2.

Таблица 2 – Характеристики протоколов RADIUS и TACACS+

	RADIUS	TACACS+
Используемые протоколы и порты	UDP: 1812 & 1813 или UDP: 1645 & 1646	TCP: 49
Сервисы	Объединяет аутентификацию и авторизацию	Разные процессы для аутентификации, авторизации и учета
Шифрование	Шифруется только пароль	Шифруется пакет
Поддерживаемые типы аутентификации	Clear text (ASCII, PAP), CHAP	Clear text (ASCII, PAP), CHAP, ARAP
Возможность перенаправления запроса	Есть	Нет
Основное назначение	Доступ к сети	Администрирование устройств

Так как в Техническом задании Заказчика установлено требование на разграничение процессов аутентификации, авторизации, учитывая, что в сети будут использоваться устройства Cisco [5], в качестве протокола AAA следует использовать протокол TACACS+ фирмы Cisco.

Описание некоторых мероприятий по конфигурированию сетевых устройств. Рассматривается конфигурирование маршрутизатора-шлюза для сегмента сети журналистского отдела. Изменение имени маршрутизатора (см. Рис. 2).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#ip domain-name router1.domain
```

Рис. 2 – Конфигурирование имени маршрутизатора

Генерация ключа для протокола SSH (см. Рис. 3).

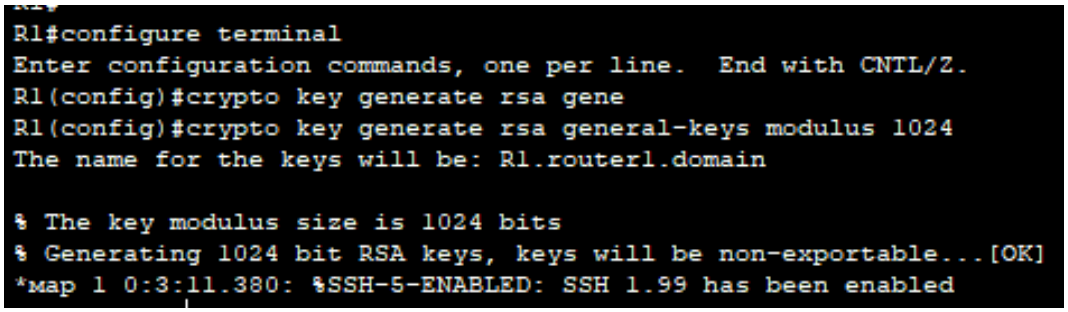

Рис. 3 – Конфигурирование (генерация) ключа для SSH

Конфигурирование SSH на маршрутизаторе и разрешение подключения удаленной консоли по линиям VTY (см. Рис. 4).

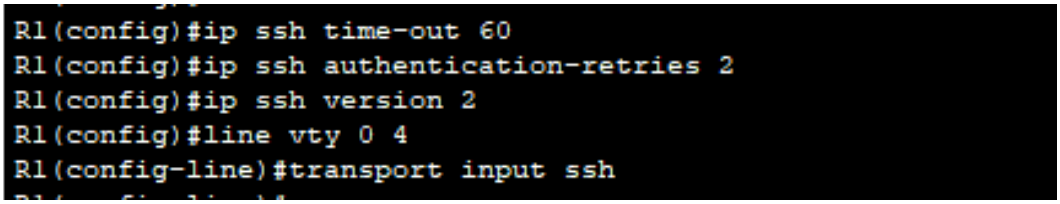

Рис. 4 – Конфигурирование SSH на маршрутизаторе

Назначение IP-адресов для интерфейсов (портов) маршрутизатора (см. Рис. 5), исходя из таблицы 1.

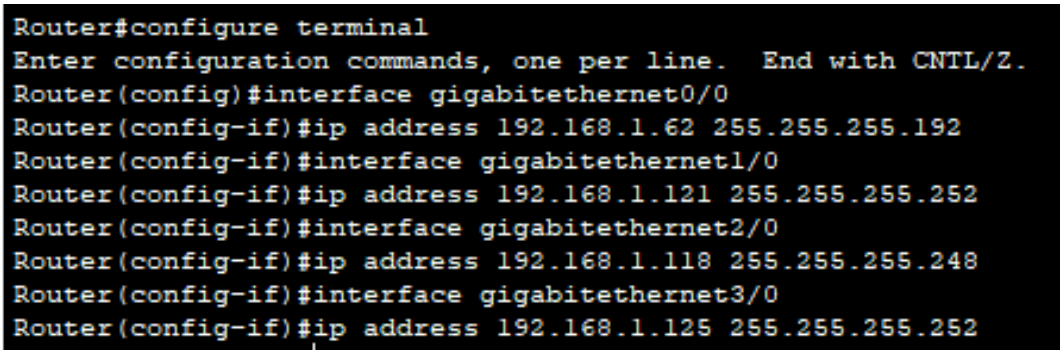

Рис. 5 – Конфигурирование IP-адресов на портах маршрутизатора

Для обеспечения передачи данных между устройствами из разных сегментов сети проведено конфигурирование протокола RIP (см. Рис. 6).

Необходимо использовать RIP v2 (см. Рис. 7), поскольку RIP v1 не работает с масками переменной длины.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.1.112
Router(config-router)#network 192.168.1.124
Router(config-router)#network 192.168.1.128
```

Рис. 6 – Конфигурирование протокола RIP на маршрутизаторе

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
```

Рис. 7 – Включение RIP v2

Узлы сети будут получать IP-адреса с помощью протокола DHCP (Dynamic Host Configuration Protocol) с сервера организации, но поскольку сегменты сети разделены маршрутизаторами, широковещательные запросы, с помощью которых работает протокол, не смогут пройти маршрутизаторы. Для обеспечения функционирования DHCP в межсетевой среде необходимо использовать технологию DHCP Relay (Option 82) на маршрутизаторах. Осуществляется путем указания IP-адреса DHCP-сервера на интерфейсе шлюза для подсети (см. Рис. 8).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip helper-address 192.168.1.113
```

Рис. 8 – Конфигурирование DHCP Relay (Option 82)

Для включения службы AAA были выполнены следующие действия (см. Рис. 9).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#aaa authentication login default group tacacs+
Router(config)#tacacs-server host 192.168.1.113
Router(config)#tacacs-server key 123
Router(config)#line vty 0 4
Router(config-line)#login authentication default
Router(config-line)#exit
Router(config)#line con 0
Router(config-line)#login authentication default
Router(config-line)#exit
```

Рис. 9 – Конфигурирование службы AAA

Для сетевых устройств необходимо ограничить доступ на управление по Telnet и SSH. Для этого использовались списки доступа ACL (Access Control List). Реализация мер приведена на рис. 10.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 permit 192.168.1.56 0.0.0.7
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
```

Рис. 10 – Конфигурирование ограничения доступа по линиям Telnet и SSH

С целью отслеживания состояния сети, а также контроля инцидентов, необходимо включить логирование на устройствах, для этого на каждом устройстве должно быть настроено время. Следует использовать протокол NTP (Network Time Protocol), позволяющий устройствам получать время с удаленного сервера. После включения протокола NTP следует активировать логирование; логи хранятся непосредственно на устройстве (см. Рис. 11).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ntp server 192.168.1.101
Router(config)#logging buffered 16384
```

Рисунок 11 – Конфигурирование NTP и логирования

Для подключения к сети Интернет использована технология NAT (Network Address Translation), которая позволяет преобразовывать IP-адреса и/или порты для пакетов данных, проходящих через сетевое устройство [3].

Существует несколько видов NAT:

1) static NAT (статический NAT) – позволяет назначить постоянное соответствие между внешним и внутренним IP-адресом;

2) dynamic NAT (динамический NAT) – назначает внешний IP-адрес из пула доступных адресов, когда внутреннее устройство запрашивает доступ к внешней сети;

3) NAT overload (PAT – Port Address Translation) – это расширение динамического NAT, при котором на одном публичном IP-адресе могут быть отображены порты разных внутренних устройств, порт PAT позволяет маршрутизатору использовать один внешний IP-адрес для нескольких устройств в локальной сети.

Выполнено конфигурирование NAT с перегрузкой (PAT). Создан access-list, содержащий внутренние адреса сети; пул адресов, в который транслируется трафик; соответствующие интерфейсы промаркированы как внутренние и внешние; выполнено конфигурирование непосредственно трансляции (см. Рис. 12).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.63 any
Router(config)#access-list 100 permit ip 192.168.1.64 0.0.0.31 any
Router(config)#access-list 100 permit ip 192.168.1.96 0.0.0.15 any
Router(config)#access-list 100 permit ip 192.168.1.112 0.0.0.7 any
Router(config)#ip nat pool NAT_pool 91.113.0.0 91.113.0.10 netmask 255.255.0.0
Router(config)#interface gig0/0
Router(config-if)#ip nat inside
Router(config-if)#interface gig1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source list 100 pool NAT_pool overload
```

Рис. 12 – Конфигурирование NAT на одном из маршрутизаторов

Заключение. Исходя из материалов, представленных в [5] и настоящей статье, выбрана сетевая топология и архитектура вычислительной сети, активное сетевое и серверное оборудование, проводная среда передачи данных. Спроектирована локальная вычислительная сети стандарта Gigabit Ethernet, осуществлено назначение IP-адресации. В качестве протокола внутреннего шлюза выбран протокол RIP. Осуществлено конфигурирование сетевых устройств. Вышесказанное позволяет утверждать, что цель работы по переходу вычислительной сети организации на стандарт Gigabit Ethernet достигнута.

Библиографический список:

1. Болотов, Д.А. Протоколы маршрутизации в корпоративных сетях / Д.А. Болотов // Экономические и информационные аспекты развития региона: теория и практика : международная научно-практическая конференция,18–19 марта 2015 г. – Ставрополь : «АГРУС», 2015. – С. 59-61.

2. Иванец, М.Э., Ткаченко, А.Л. Анализ угроз информационной безопасности для коммерческой организации / М.Э. Иванец, А.Л. Ткаченко // Цифровая трансформация промышленности: тенденции и перспективы : сборник научных трудов по материалам 2-й Всероссийской научно-практической конференции,

11 ноября 2021 г. – Москва : Общество с ограниченной ответственностью «Русайнс», 2021. – С. 364-370.

3. Иванова, А.А. Применение технологии NAT для повышения информационной безопасности компьютерных сетей / А.А. Иванова // Инжиниринг предприятий и управление знаниями (ИП&УЗ-2023) : сборник научных трудов XXVI Российской научной конференции (молодежная секция), 29–30 ноября 2023 г. В 2-х томах. Том 2. – Москва : Российский экономический университет имени Г. В. Плеханова, 2023. – С. 84-88. – URL: https://elibrary.ru/download/elibrary_68016858_34565102.pdf (дата обращения 18.06.2025).

4. Исхаков, А. Ю. Обеспечение безопасности оборудования Cisco Systems с помощью списков контроля доступа / А. Ю. Исхаков, С. Ю. Исхаков, О. А. Кондратова, Н. Т. Югов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1-2(25). – С. 97-99.

5. Раевский, В.А., Тимашов, Д.С., Говорова, Е.С. Выбор сетевой топологии, архитектуры и оборудования для реализации локальной вычислительной сети стандарта Gigabit Ethernet одного из издательств г. Калуга / В.А. Раевский, Д.С. Тимашов, Е.С. Говорова // Научный журнал «Дневник науки» : [сайт]. – 2025. – №6. – С. [--? - --?]. – URL: https://dnevniknauki.ru/images/publications/2025/6/technics/Raevsky_Timashov_Govorova.pdf. – Дата публикации: [--?.06.2025].

6. Семенов, Ю. А. Протоколы и алгоритмы маршрутизации в Интернет / Ю. А. Семенов. – Москва : Интернет-университет информационных технологий (ИНТУИТ), 2016. – 998 с. – ISBN 978-5-94774-707-2.

7. Ткаченко, А.Л., Донецков, А.М., Раевский, В.А., Сорочан, В.В. Выявление DOS атаки на WI-FI сеть / А.Л. Ткаченко, А.М. Донецков, В.А. Раевский, В.В. Сорочан // Вестник Калужского университета. – 2024. – №2(63). – С. 61-65. –

URL: https://elibrary.ru/download/elibrary_67857303_87398354.pdf (дата обращения: 02.06.2025)
8. Федорова, В.А., Мурашов, М.В. Адресация и маршрутизация в компьютерных сетях : учебно-методическое пособие / В.А. Федорова, Мурашов М.В.. – Москва : Московский государственный технический университет имени Н.Э. Баумана, 2019. – 44 с. – ISBN 978-5-7038-5240-8 // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/110605.html (дата обращения: 07.06.2025).
9. Configuring TACACS+ // Cisco: Software, Network, and Cybersecurity Solutions : [сайт]. – URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3e/consolidated_guide/configuration_guide/b_consolidated_3650_3se_cg/b_consolidated_3650_3se_cg_chapter_01000001.pdf (дата обращения 18.06.2025).
10. RFC 1058. Routing Information Protocol : Historic/ C. Hendrick // // Rfc-editor : [сайт]. – URL: https://www.rfc-editor.org/rfc/rfc1058.txt (дата обращения 12.06.2025).
11. RFC 1131. OSPF Version 2 : Draft Standard / J. Moy ; Proteon, Inc. // Rfc-editor : [сайт]. – URL: https://www.rfc-editor.org/rfc/rfc1247.txt (дата обращения 13.06.2025).
12. RFC 2138. Remote Authentication Dial In User Service (RADIUS) : Internet standard / C. Rigney, A. Rubens, W. Simpson, S. Willens // Rfc-editor : [сайт]. – URL: https://www.rfc-editor.org/rfc/rfc2138.txt (дата обращения 17.06.2025).
13. RFC 2453. Rip Version 2 : Internet standard / G. Malkin // Rfc-editor : [сайт]. – URL: https://www.rfc-editor.org/rfc/rfc2453.txt (дата обращения 13.06.2025).
14. RFC 2903. Generic AAA Architecture : Experimental / C. de Laat, G. Gross, L. Gommans [и др.] ; Utrecht University [и др.] // Rfc-editor : [сайт]. – URL: https://www.rfc-editor.org/rfc/rfc2903.txt (дата обращения 17.06.2025).

Оригинальность 76%