**BC/NW 2021№ 1 (37):4.2**

**ИССЛЕДОВАНИЕ СПОСОБОВ СОКРАЩЕНИЯ ВРЕМЕНИ РАЗВЕРТЫВАНИЯ И ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЯ ВИРТУАЛЬНЫХ СТЕНДОВ В ОБЛАКЕ БАНКА**

**Данилин Д.Г. Коняева В.В.**

Введение

В данной статье исследуется время переходного процесса при появлении

отказов на уровне доступа, распределения и ядра корпоративной сети

для протоколов OSPF и EIGRP.

Переходной процесс – процесс соглашения между маршрутизаторами сети относительно оптимальных маршрутов для передачи данных.

Время переходного процесса – время между выходом из строя одного узла или линии связи и моментом, когда таблицы маршрутизации всех маршрутизаторов будут перестроены в соответствии с новой топологией, если отказ в сети привел к изменению таковой.

Переходной процесс в сетях передачи данных непосредственно связан с возникновением сетевого отказа.

Несмотря на то, что выпускаемое в настоящее время сетевое активное оборудование считается высоконадежным элементом, отказы в сетях не являются редкими случаями и могут быть обусловлены разнообразными факторами, в частности:

* естественным старением аппаратной части маршрутизаторов;
* сбоями в программном обеспечении;
* сбоями в электропитании;
* некорректным обслуживанием технического персонала;
* сбоями оптического оборудования;
* обрывом кабеля.

Прекращение информационного обмена на несколько секунд, возникающее в результате сетевого отказа, критично, так как приводит к потере большого количества данных.

Одним из важнейших понятий при анализе переходного процесса сети является понятие отказа.

Отказ объекта или его элемента в общем случае можно определить как событие, заключающееся в нарушении работоспособного состояния объекта или его элемента.

Термин «отказ» можно разделить на относящиеся к нему характеристики, например, постепенный или внезапный отказ. Причинами постепенного отказа могут быть систематические нарушения условий эксплуатации (нарушение температурного режима или уровня влажности в помещении). Внезапные отказы обусловлены резкими, непредсказуемыми изменениями параметров устройства. Причиной такого отказа может служить резкий «скачок» напряжения или нарушения, связанные с электропитанием объекта.

Так же отказы можно классифицировать, как случайные или систематические, зависимые или независимые. Раскроем детально вышеобозначенные определения.

Систематические отказы обусловлены разными причинами, в числе которых можно выделить некорректные действия обслуживающего персонала. Случайные отказы связаны с непредусмотренными перегрузками объекта, сбоями системы управления или программного обеспечения.

В случае, когда отказ одного элемента ведет к выходу из строя других объектов, отказ можно классифицировать, как зависимый. Напротив, если выход из строя одного устройства или его элемента не влияет на работоспособность других устройств сети, то отказ такого типа можно назвать независимым.

Кроме того, отказы можно классифицировать по характеру проявления на скрытые и явные.

Скрытым отказом называется такой, который возможно определить при проведении различных видов профилактических работ или во время проведения тестового контроля работоспособности сети и ее элементов.

Явный отказ возможно обнаружить во время непрерывного мониторинга состояния сети и ее компонентов средствами систем мониторинга.

Классификацию возможно продолжить понятийными фиксациями полного и частичного отказа объекта связи и его элементов, находящихся под контролем.

При возникновении частичного отказа работоспособность объекта может быть сохранена с возможной потерей нескольких параметров надежности, что может привести к снижению уровня производительности сети.

Если речь идет о полном отказе объекта, то его применение невозможно до проведения работ по восстановлению полной работоспособности.

Процесс восстановления объекта после выхода из строя сводится к обнаружению неисправного элемента и его блокировки. Очевидно, что объекты можно разделить на восстанавливаемые, в случае когда объекту возможно вернуть рабочее состояние, и невосстанавливаемые, если проведение работ по восстановлению невозможно.

В статье предполагается, что в сети могут возникать только отказы, которые порождают одновременно не более одного переходного процесса.

**Модель корпоративной сети**

После анализа ряда существующих и эксплуатируемых сетей для исследования была выбрана корпоративная сеть передачи данных, изображенная на рис.1

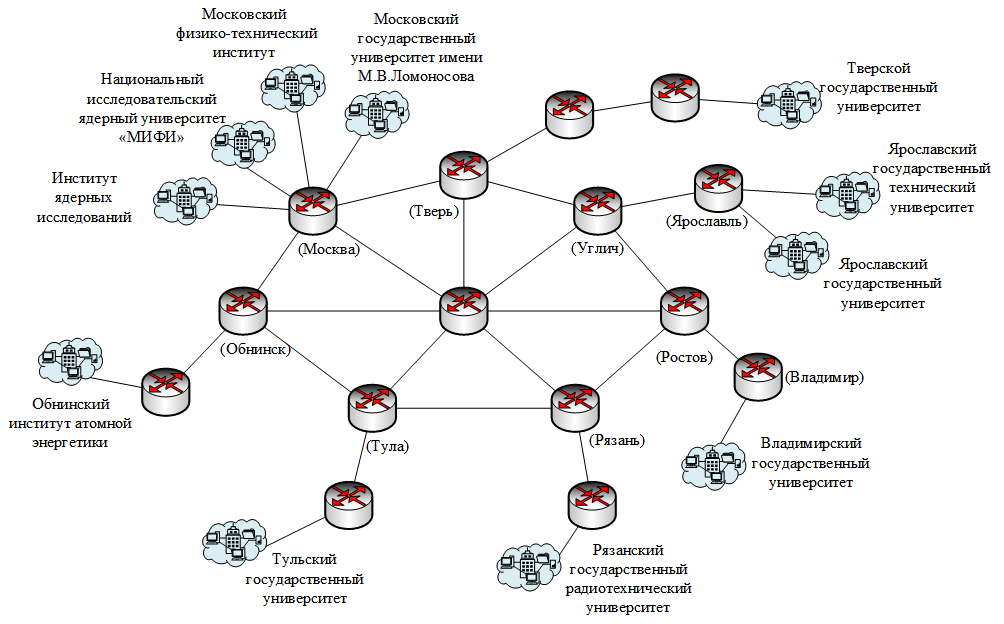


Рис.1 Структура территориально-распределенной сети

Технология STM-4 будет использоваться для построения магистрального кольца. В качестве среды передачи данных для связующей магистрали выбрано одномодовое оптоволокно с возможностью дальности передачи до 120 км. Технология Gigabit Ethernet, реализованная на витой паре категории 6, будет применяться для связи уровня распределения и доступа. Технология Fast Ethernet будет использоваться для подключения конечных устройств. Таким образом, географическое расположение объектов полностью оправдано, и построенная модель сети может быть масштабирована на сети корпоративного предприятия.

Взяв за основу предложенную структуру, построим математическую модель сети в виде графа. Граф является взвешенным, то есть каждое ребро имеет характеристику – вес, определяемую пропускной способностью. Вершинами построенного графа являются узлы сети и тупиковые сети, а ребра – это каналы связи.

В табл.1 приведено соответствие между используемыми технологиями передачи и соответствующими значениями для ребер графа сети.

Таблица 1

Соответствие пропускных способностей, используемых технологий и метрик ребер графа

|  |  |  |
| --- | --- | --- |
| Технология передачи данных | Пропускная способность, Мбит/с | Метрика ребра графа |
| Fast Ethernet | 1000 | 1 |
| STM-4 | 622 | 15 |
| Gigabit Ethernet | 100 | 100 |

Полученный граф сети приведен на рис.2

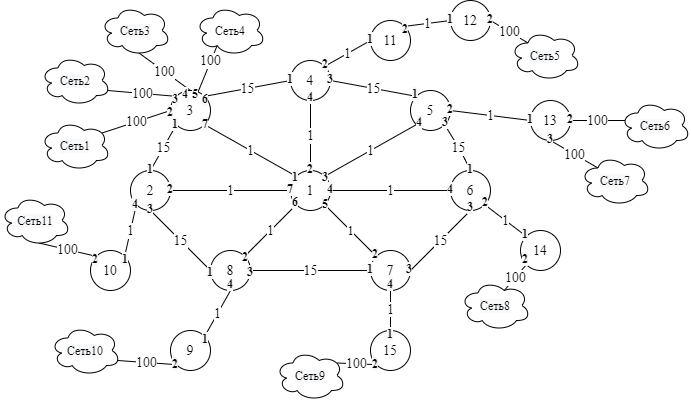


Рис.2 Математическая модель исследуемой сети

Также необходимо описать адресное пространство, так как для моделирования возникновения переходного процесса понадобится проводить анализ построенных таблиц маршрутизации. В табл. 2 приведено распределение адресного пространства для модели корпоративной сети, изображенной на рис.2.

Таблица 2

Распределение адресного пространства в корпоративной сети

|  |  |  |
| --- | --- | --- |
| **Соединение** | **IP-адрес** | **Маска сети** |
| Сеть1 - маршрутизатор №3 | 172.16.2.0 | 255.255.255.240 |
| Сеть2 - маршрутизатор №3 | 172.16.3.0 | 255.255.255.240 |
| Сеть3 - маршрутизатор №3 | 172.16.4.0 | 255.255.255.240 |
| Сеть4 - маршрутизатор №3 | 172.16.5.0 | 255.255.255.240 |
| Сеть5 - маршрутизатор №12 | 172.16.6.0 | 255.255.255.240 |
| Сеть6 - маршрутизатор №13 | 172.16.7.0 | 255.255.255.240 |
| Сеть7 - маршрутизатор №13 | 172.16.8.0 | 255.255.255.240 |
| Сеть8 - маршрутизатор №14 | 172.16.9.0 | 255.255.255.240 |
| Сеть9 - маршрутизатор №15 | 172.16.10.0 | 255.255.255.240 |
| Сеть10 - маршрутизатор №9 | 172.16.0.0 | 255.255.255.240 |
| Сеть11 - маршрутизатор №10 | 172.16.1.0 | 255.255.255.240 |
| Маршрутизатор №10 – маршрутизатор №2 | 10.0.0.8 | 255.255.255.252 |
| Маршрутизатор №9 – маршрутизатор №8 | 10.0.0.0 | 255.255.255.252 |
| Маршрутизатор №15 – маршрутизатор №7 | 10.0.0.64 | 255.255.255.252 |
| Маршрутизатор №14 – маршрутизатор №6 | 10.0.0.68 | 255.255.255.252 |
| Маршрутизатор №13 – маршрутизатор №5 | 10.0.0.72 | 255.255.255.252 |
| Маршрутизатор №12 – маршрутизатор №11 | 10.0.0.80 | 255.255.255.252 |
| Маршрутизатор №11 – маршрутизатор №4 | 10.0.0.76 | 255.255.255.252 |
| Маршрутизатор №8 – маршрутизатор №7 | 10.0.0.60 | 255.255.255.252 |
| Маршрутизатор №8 – маршрутизатор №2 | 10.0.0.4 | 255.255.255.252 |
| Маршрутизатор №8 – маршрутизатор №1 | 10.0.0.40 | 255.255.255.252 |
| Маршрутизатор №7 – маршрутизатор №6 | 10.0.0.48 | 255.255.255.252 |
| Маршрутизатор №7 – маршрутизатор №1 | 10.0.0.44 | 255.255.255.252 |
| Маршрутизатор №6 – маршрутизатор №5 | 10.0.0.56 | 255.255.255.252 |
| Маршрутизатор №6 – маршрутизатор №1 | 10.0.0.36 | 255.255.255.252 |
| Маршрутизатор №5 – маршрутизатор №4 | 10.0.0.52 | 255.255.255.252 |
| Маршрутизатор №5 – маршрутизатор №1 | 10.0.0.32 | 255.255.255.252 |
| Маршрутизатор №4 – маршрутизатор №3 | 10.0.0.24 | 255.255.255.252 |
| Маршрутизатор №4 – маршрутизатор №1 | 10.0.0.28 | 255.255.255.252 |
| Маршрутизатор №3 – маршрутизатор №2 | 10.0.0.12 | 255.255.255.252 |
| Маршрутизатор №3 – маршрутизатор №1 | 10.0.0.20 | 255.255.255.252 |
| Маршрутизатор №2 – маршрутизатор №1 | 10.0.0.16 | 255.255.255.252 |

Составленная карта адресного пространства оптимальна, так как обеспечивает эксплуатацию всего диапазона адресов.

**Эксперимент**

Общепринятой моделью создания сетей является иерархическая модель межсетевого взаимодействия компании Cisco. Разделение сложной задачи проектирования корпоративной сети на подзадачи упрощает обслуживание внедренной сети, так как подобный подход повышает управляемость сети, в случае отказа позволяя оперативно обслужить устройство, вышедшее из строя. Кроме преимущества в виде более удобного мониторинга сети, подобная концепция позволяет просто наращивать новое оборудование, напротив, убирать узлы, а также внедрять новые услуги.

В соответствии с данной концепцией выделяют три уровня иерархии:

• ядро сети;

• уровень распределения;

• уровень доступа.

Разработанная модель корпоративной сети, изображенная на рис.3, соответствует вышеописанному принципу построения. Для более детального анализа влияния переходного процесса на эффективность сети, эксперименты будут проведены на всех уровнях иерархии сети.

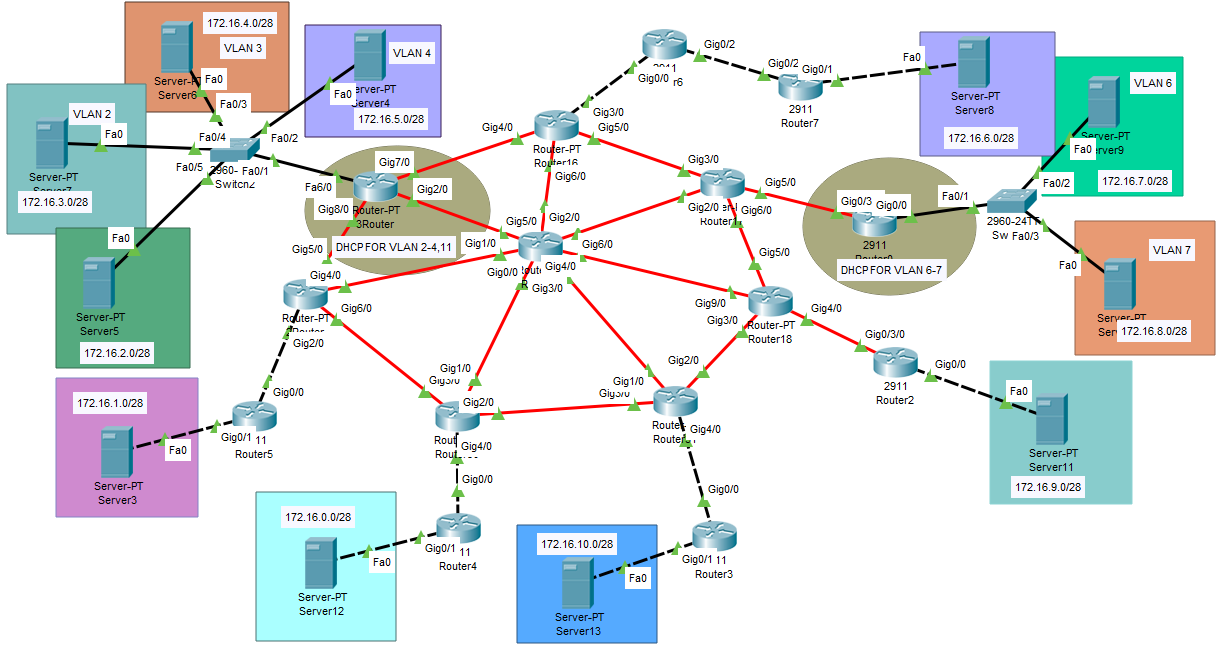


Рис.3 Исследуемая корпоративная сеть

Данный уровень предназначен для подключения конечных хостов и периферии к ЛВС.

Для анализа времени переходного процесса внесем неисправность с отсутствием доступа к подсети 172.16.9.0/28, возникшую в результате отказа канала связи. Получившаяся топология представлена на рис 4.

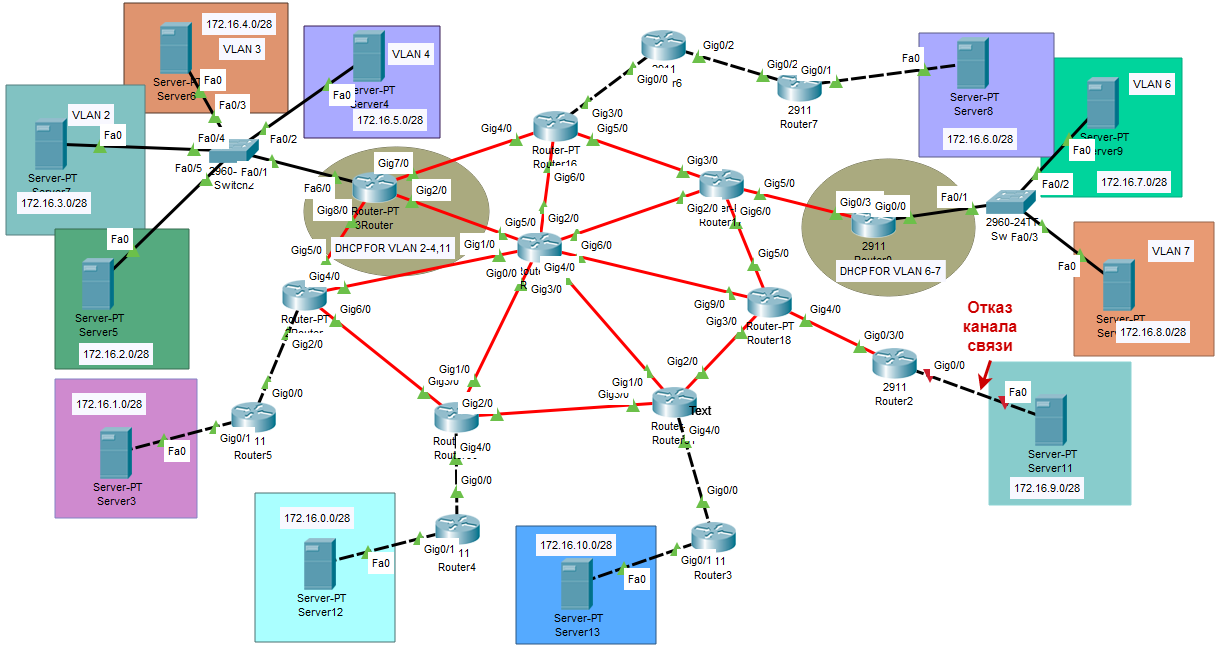


Рис.4 Топология сети с неисправностью на уровне доступа

Результат исследования времени переходного процесса в сети с использованием протокола OSPF представлен на рис.5

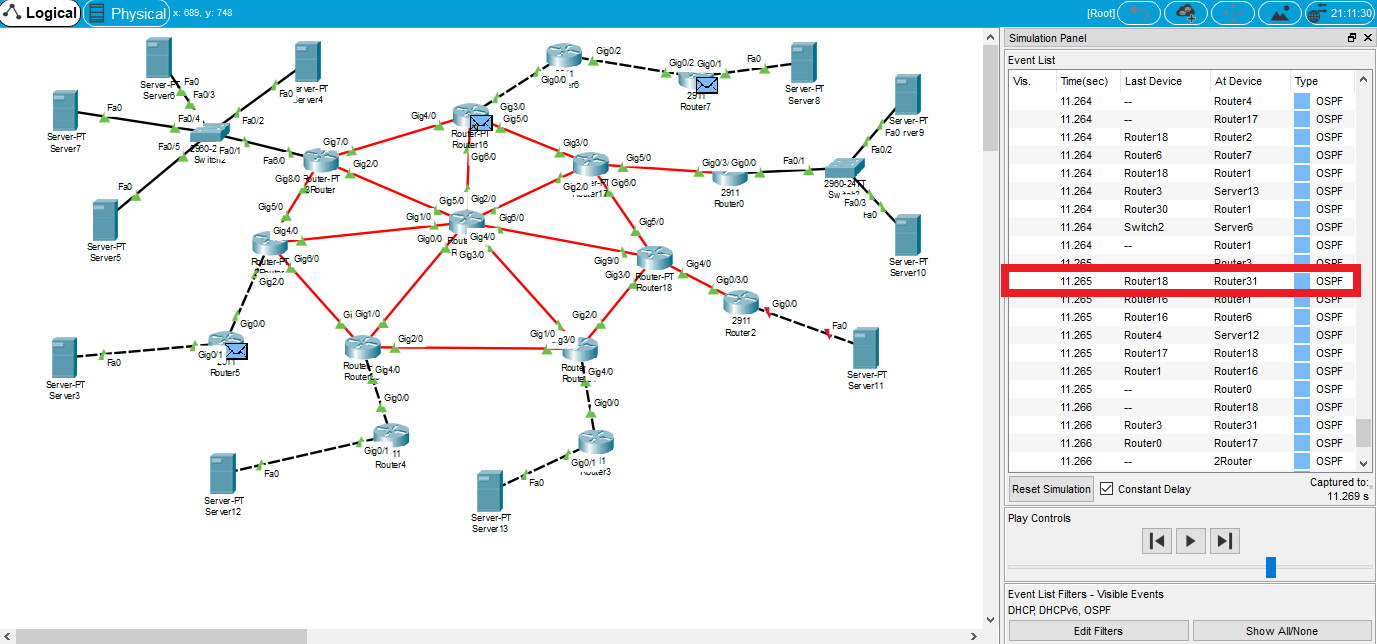


Рис.5 Время переходного процесса на уровне доступа в сети OSPF

Продемонстрируем таблицу маршрутизации узла №7 до возникновения переходного процесса и после на рис.6.

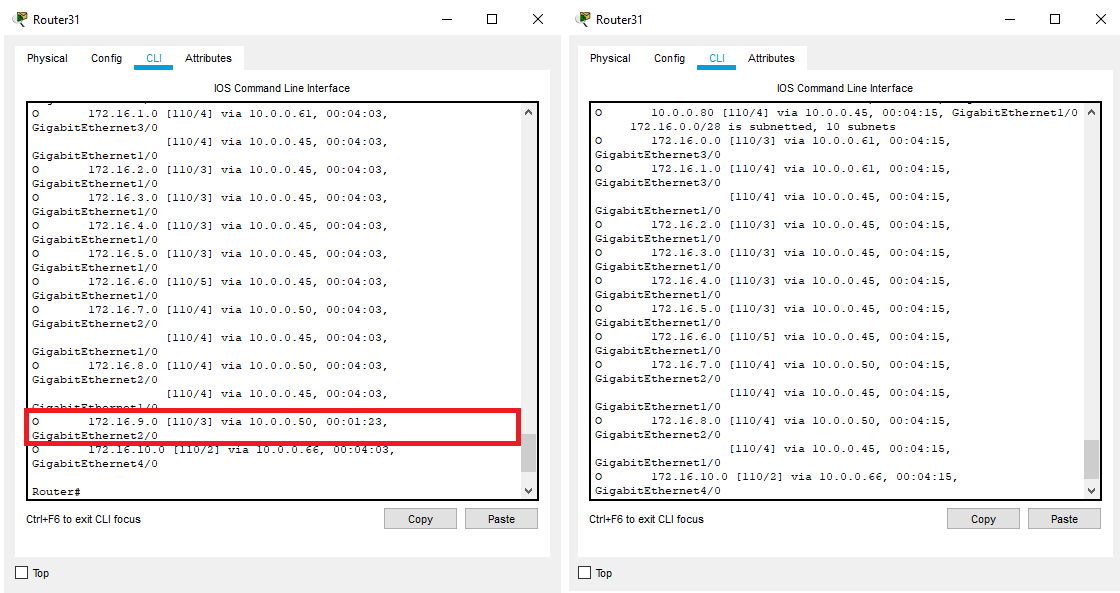


Рис.6Таблица маршрутизации OSPF

Маршрутизатор №7 (рис.2), получив пакет обновлений от маршрутизатора №6 (рис.2), исключил из таблицы маршрутизации недоступную подсеть 172.16.9.0/28, а остальные маршруты были подтверждены с интервалом в 12с. Аналогичное действие было произведено остальными узлами сети. Таким образом, можно сделать вывод, что обработка переходного процесса в сети OSPF составила 11.265 с.

Результат исследования времени переходного процесса в сети с использованием протокола динамической маршрутизации EIGRP представлен на рис.7

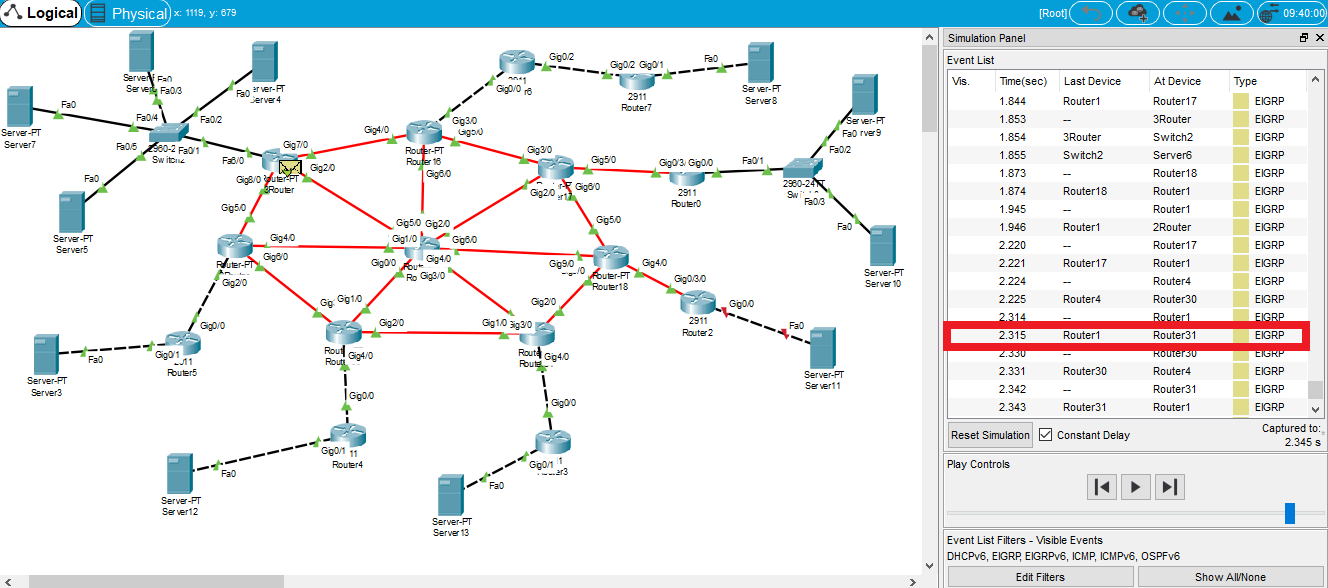


Рис.7 Время переходного процесса на уровне доступа в сети EIGRP

Маршрутизатор №7 (рис.2), получив пакет обновлений от маршрутизатора №1, исключил из таблицы маршрутизации сеть 172.16.9.0/28. Продемонстрируем таблицу маршрутизации узла №7 до возникновения переходного процесса и после на рис.8.

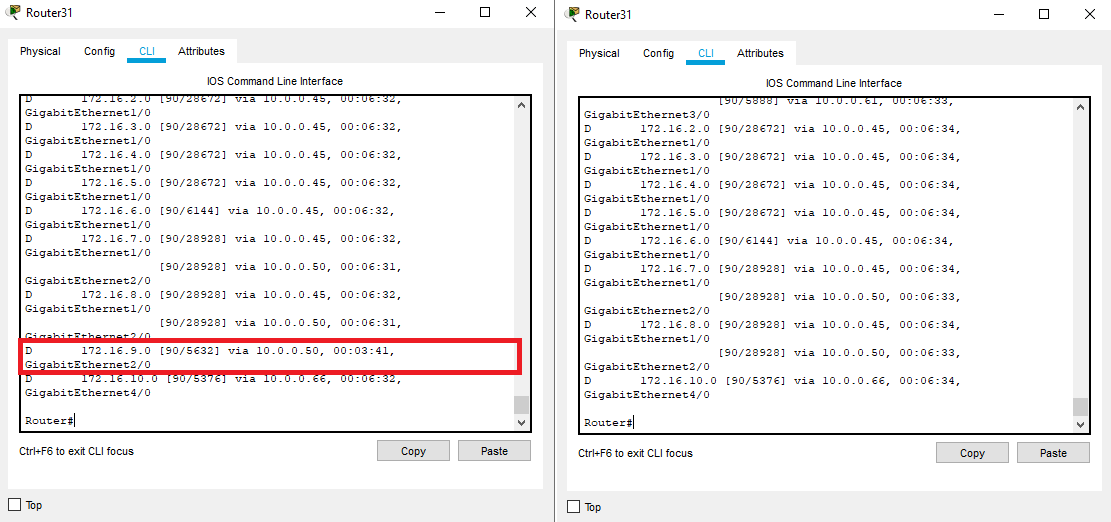


Рис.8 Таблица маршрутизации

В результате моделирования недоступная подсеть была удалена из таблицы маршрутизации, а остальные маршруты были подтверждены с интервалом в 2с. Таким образом, можно сделать вывод, что обработка переходного процесса в сети EIGRP составила 2.315 с.

**Неисправность на уровне распределения.**

Данный уровень предназначен для решения задачи объединения широковещательных доменов, поддержки технологии предоставления различным классам трафика различных приоритетов в обслуживании, обеспечения высокого уровня доступности центральных устройств сетевой топологии для пользователей.

Для анализа времени переходного процесса внесем неисправность, связанную с отказом узла сети №7(рис.2), в результате недоступными являются подсети 10.0.0.44/30, 10.0.0.48/30, 10.0.0.60/30, 10.0.0.64/30.

Получившаяся топология представлена на рис.9.

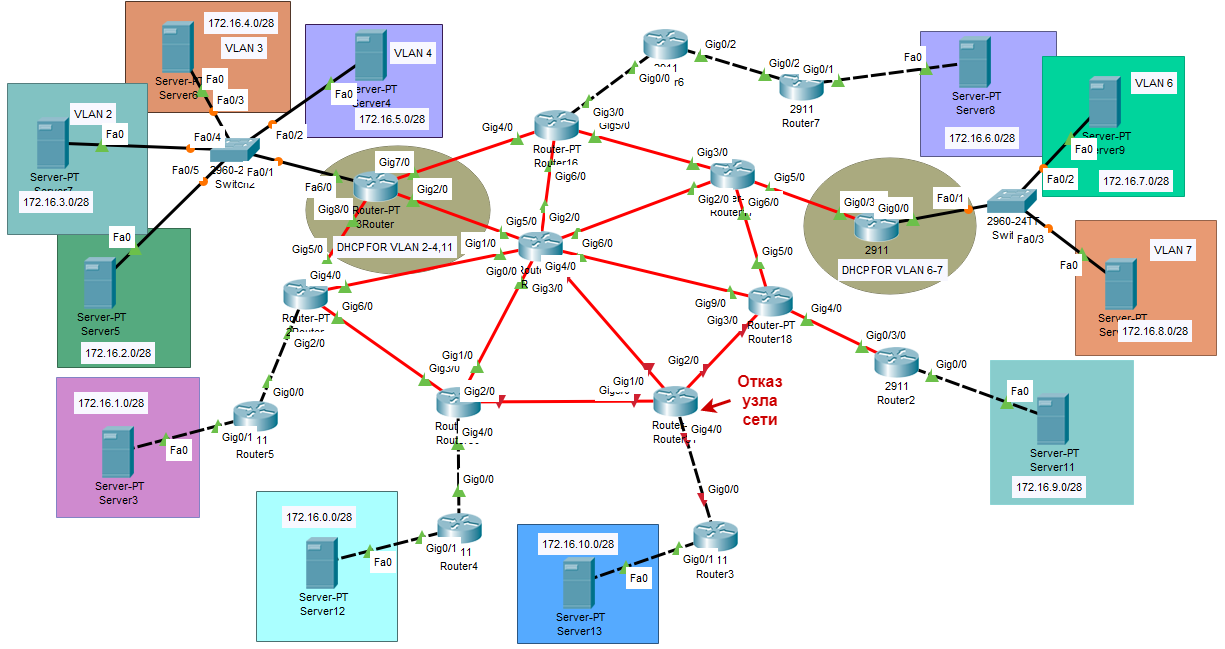


Рис.9 Топология сети с неисправностью на уровне распределения

Результат исследования времени переходного процесса в сети с использованием протокола динамической маршрутизации OSPF представлен на рис.10.

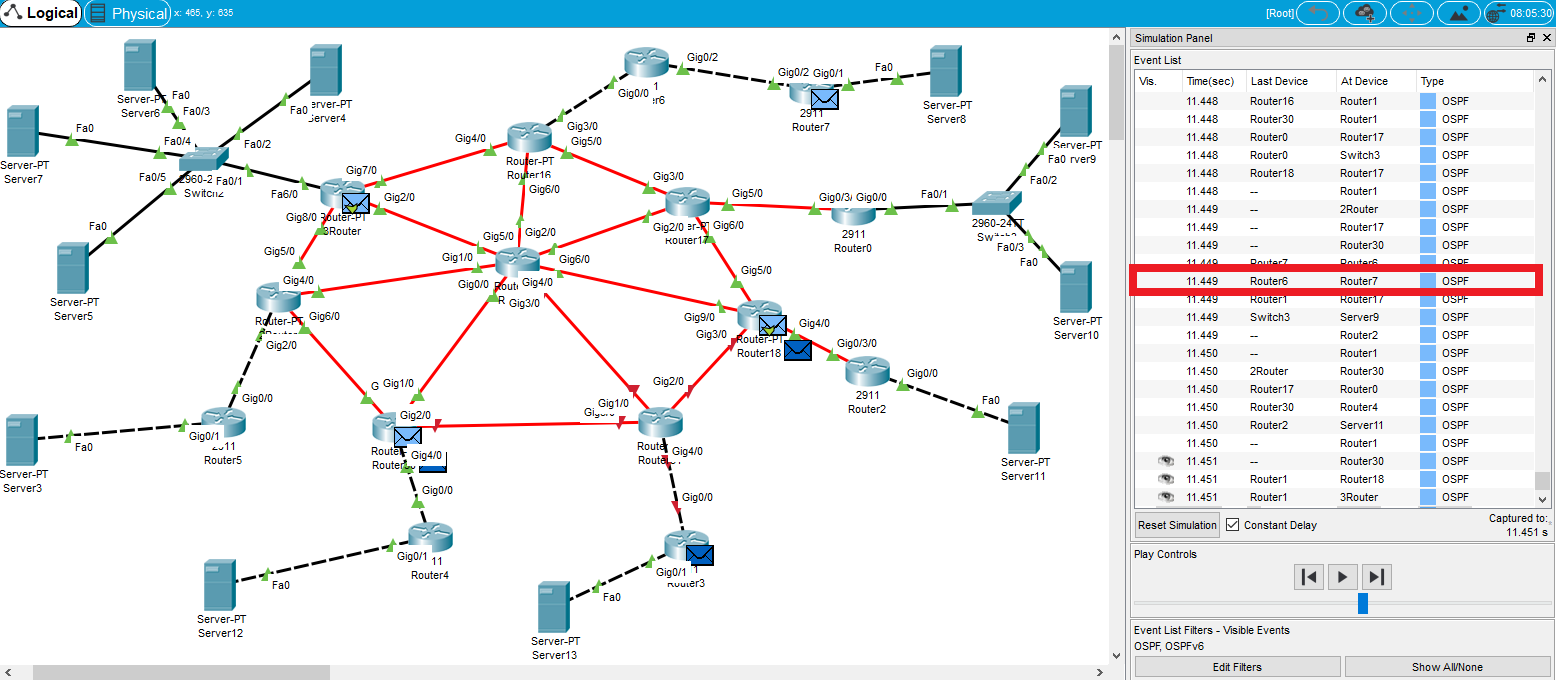


Рис.10 Время переходного процесса на уровне распределения в сети OSPF

Маршрутизатор №12 (рис.2), получив пакет обновлений от маршрутизатора №11, исключил из таблицы маршрутизации недоступные подсети, а остальные маршруты были подтверждены с интервалом в 12с. Аналогичное действие было произведено остальными узлами сети. Продемонстрируем таблицу маршрутизации узла №12 до возникновения переходного процесса и после на рис.11.

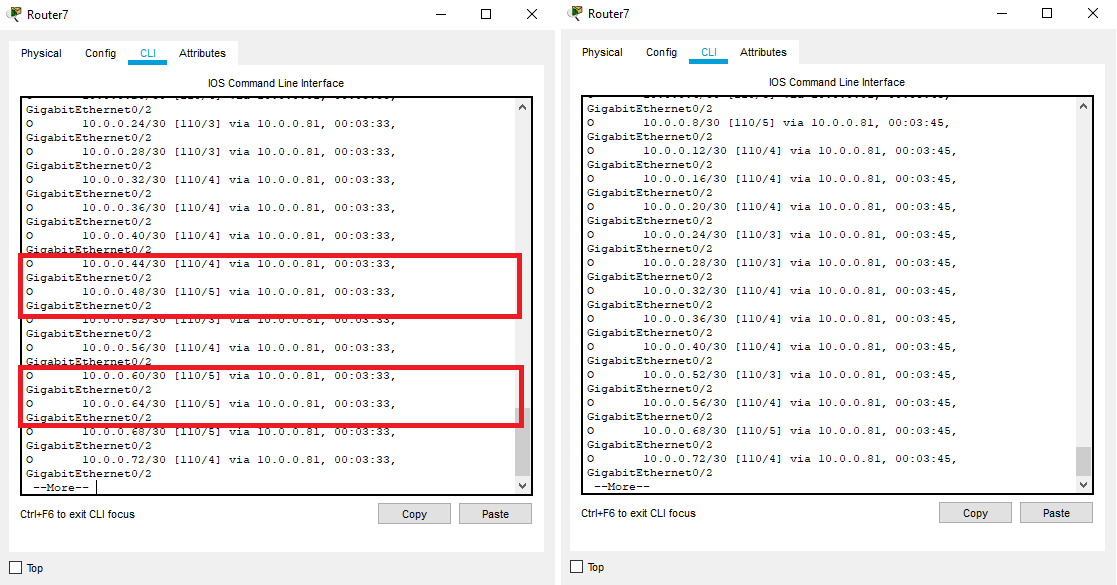


Рис.11 Таблица маршрутизации OSPF

Таким образом, можно сделать вывод, что обработка переходного процесса, возникшего в результате отказа узла на уровне распределения в сети с использованием протокола OSPF, составила 11.449с.

Результат исследования времени переходного процесса в сети с использованием протокола динамической маршрутизации EIGRP представлен на рис.12.

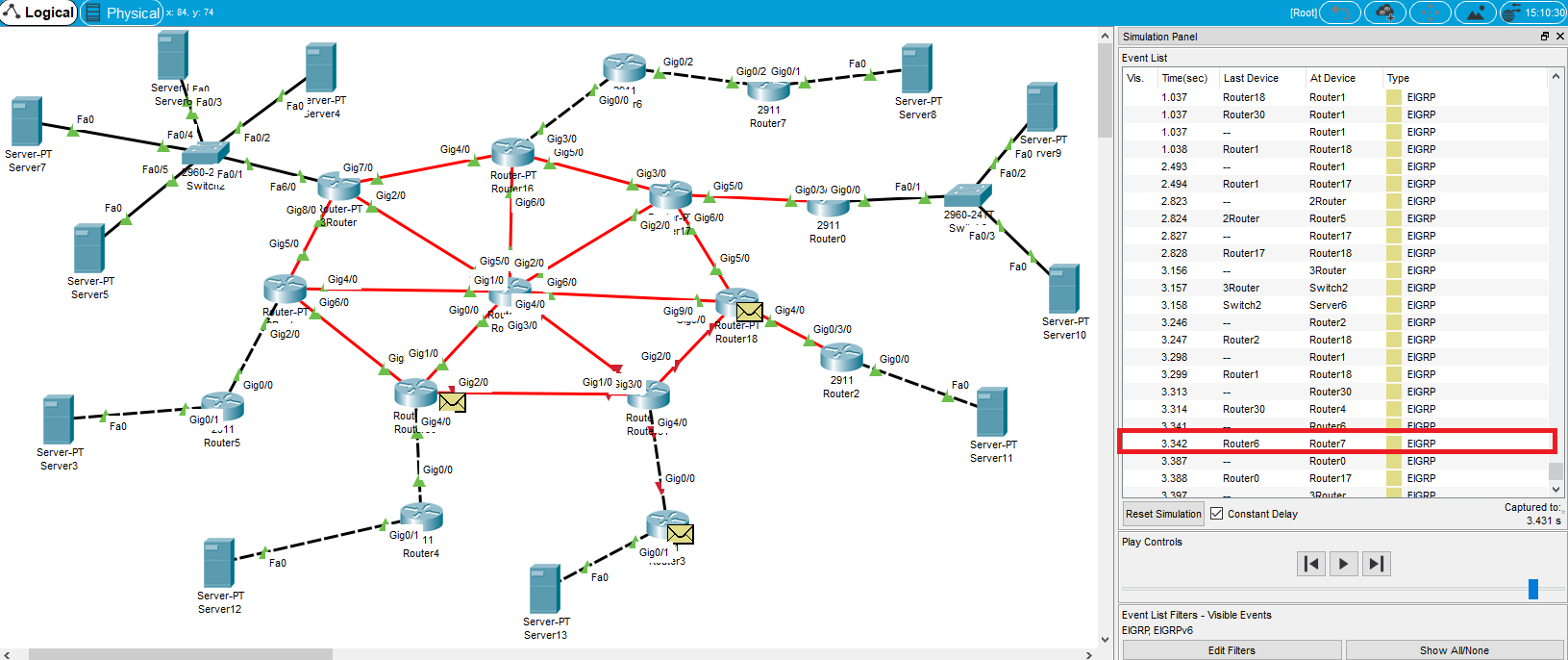


Рис.12 Время переходного процесса на уровне распределения в сети EIGRP

Маршрутизатор №12, получив пакет обновлений от маршрутизатора №11, исключил из таблицы маршрутизации недоступные подсети, а остальные маршруты были подтверждены с интервалом в 4с. Аналогичное действие было произведено остальными узлами сети. Продемонстрируем таблицу маршрутизации узла №12 до возникновения переходного процесса и после на рис.13.

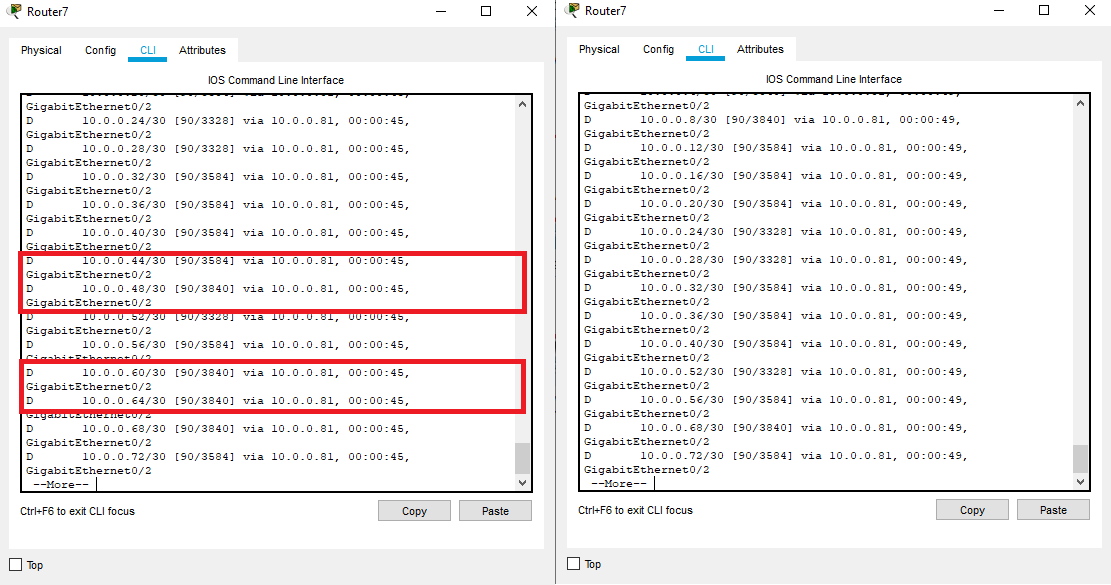


Рис.13 Таблица маршрутизации EIGRP

Таким образом, можно сделать вывод, что обработка переходного процесса, возникшего в результате отказа узла на уровне распределения в сети с использованием протокола OSPF составила 3.342 с.

**Неисправность в ядре сети**

Данный уровень модели сети представляет набор сетевых устройств, обеспечивающих отказоустойчивость путем резервирования каналов связи, которые обладают высокой пропускной способностью, что обеспечивает высокоскоростную передачу данных между подсетями.

Для анализа времени переходного процесса внесем неисправность, связанную с отказом канала связи между маршрутизатором ядра и маршрутизатором №5 (рис.2), в результате недоступной является подсеть 10.0.0.32/30.

Получившаяся топология представлена на рис.14.

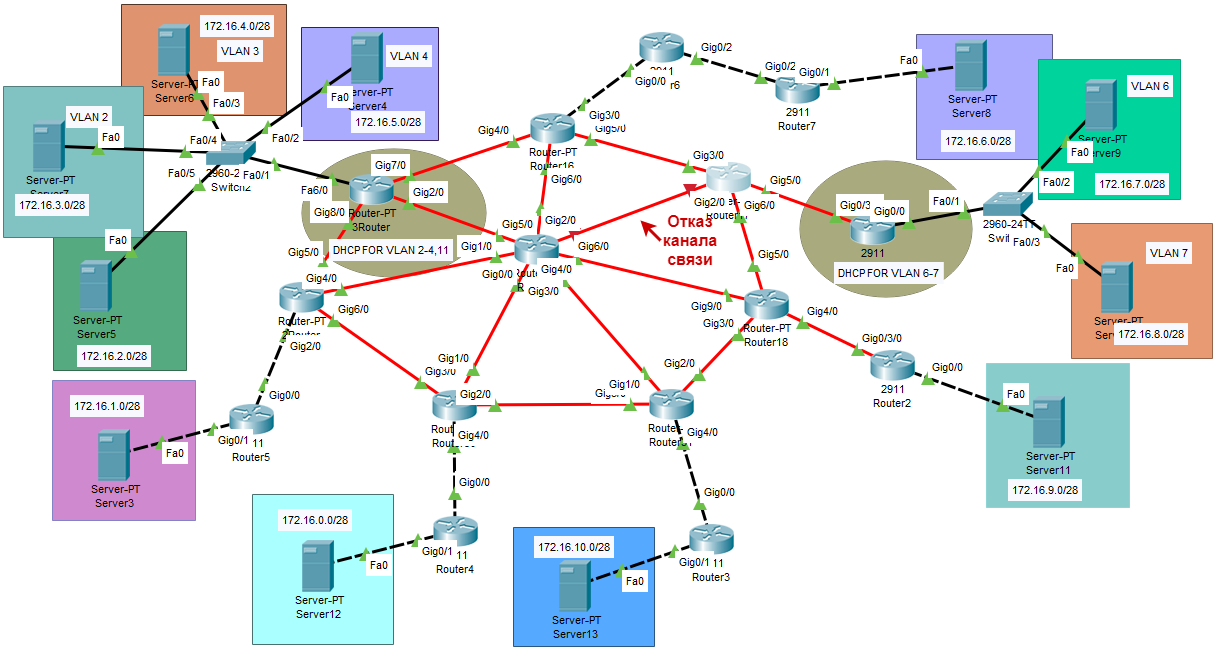


Рис.14 Топология сети с неисправностью на уровне ядра

Результат исследования времени переходного процесса в сети с использованием протокола динамической маршрутизации OSPF представлен на рис.15.

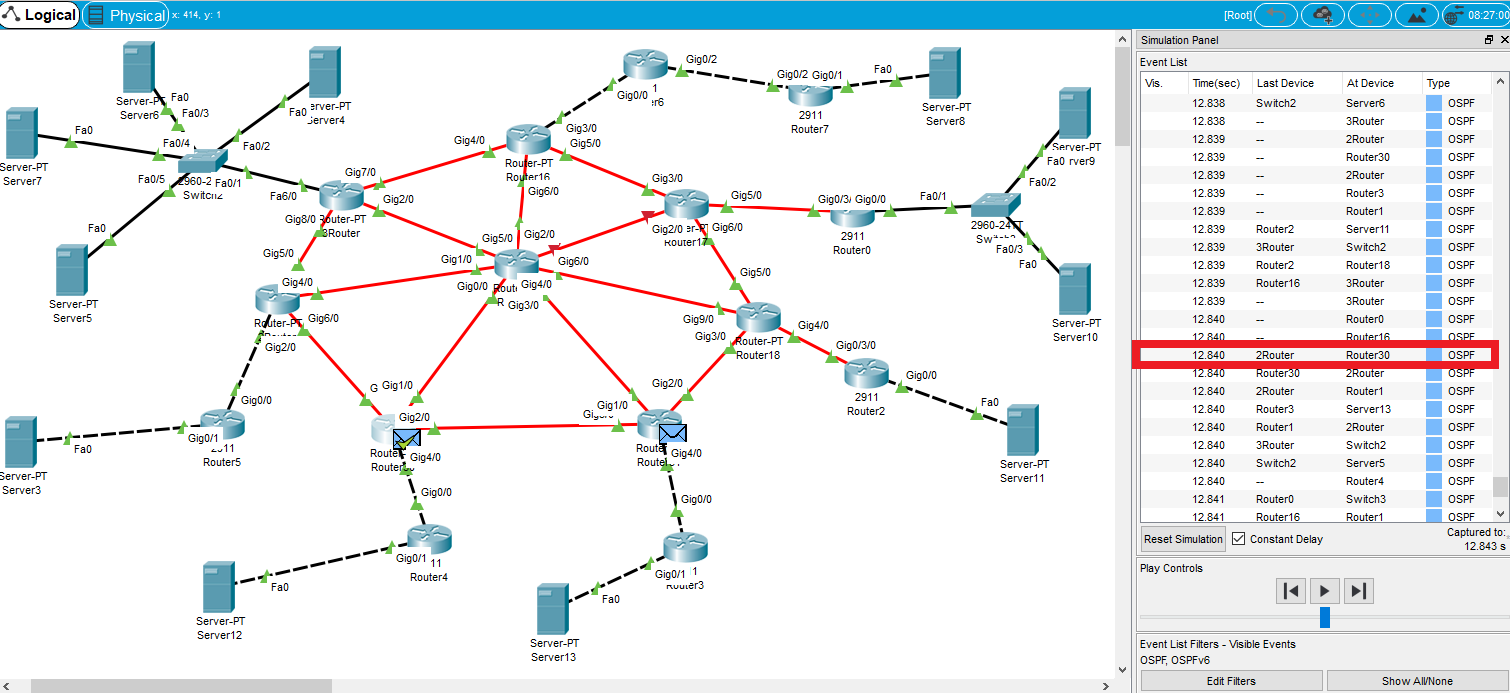


Рис.15 Время переходного процесса на уровне ядра в сети OSPF

Маршрутизатор №8 (рис.2), получив пакет обновлений от маршрутизатора, №2, исключил из таблицы маршрутизации недоступные подсети, а остальные маршруты были подтверждены с интервалом в 13с. Аналогичное действие было произведено остальными узлами сети. Продемонстрируем таблицу маршрутизации узла №8 до возникновения переходного процесса и после на рис.16.

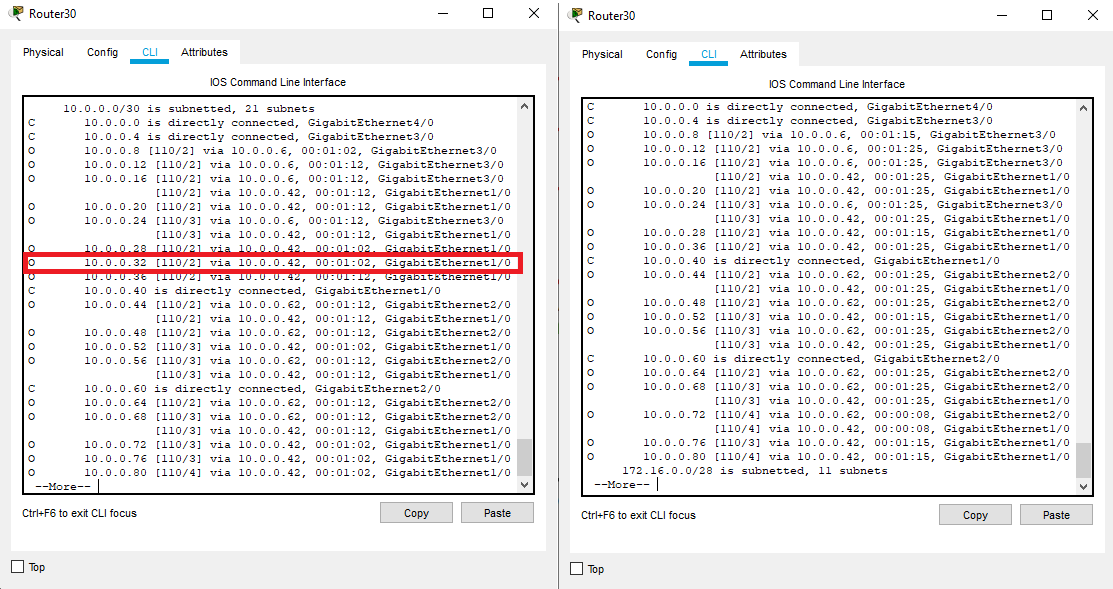


Рис.16 Таблица маршрутизации OSPF

Таким образом, можно сделать вывод, что обработка переходного процесса, возникшего в результате выхода из строя канала связи на уровне ядра с использованием протокола OSPF, составила 12.840 с.

Результат исследования времени переходного процесса в сети с использованием протокола динамической маршрутизации EIGRP представлен на рис.17.

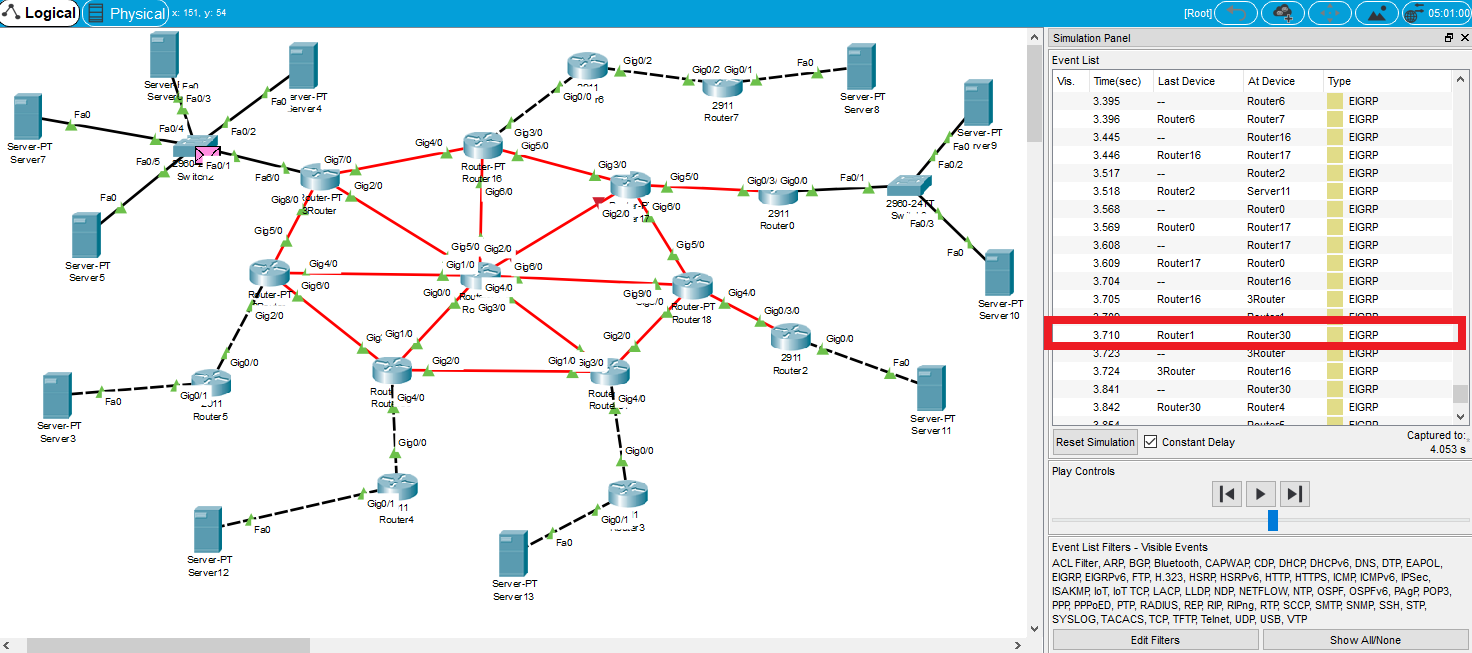


Рис.17 Время переходного процесса на уровне ядра в сети EIGRP

Маршрутизатор №8 (рис.2), получив пакет обновлений от маршрутизатора, №1, исключил из таблицы маршрутизации недоступные подсети, а остальные маршруты были подтверждены с интервалом в 4с. Аналогичное действие было произведено остальными узлами сети. Продемонстрируем таблицу маршрутизации узла №8 до возникновения переходного процесса и после на рис18.

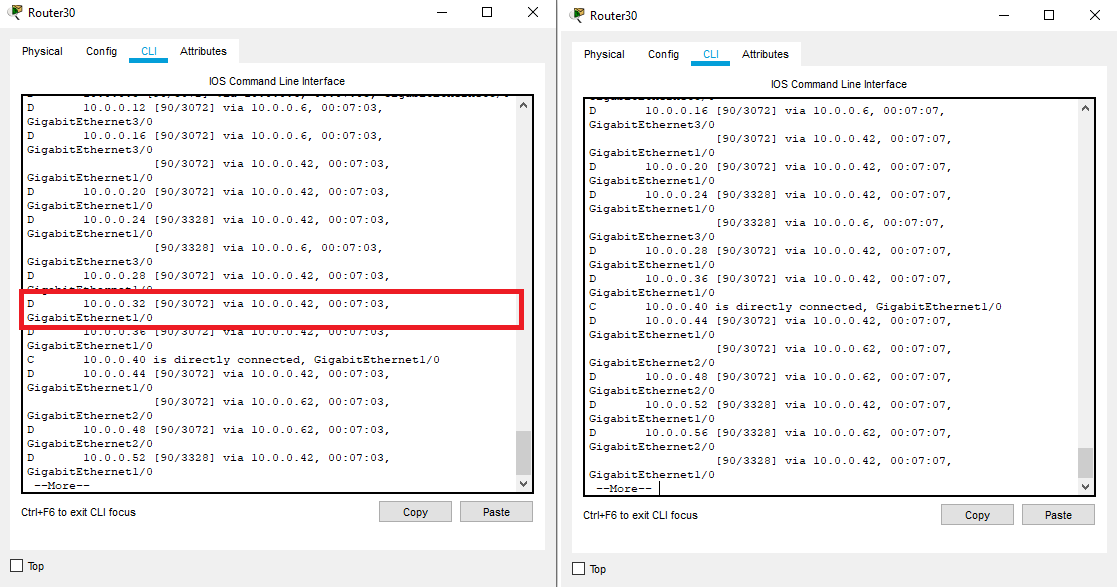


Рис.18 Таблица маршрутизации EIGRP

В результате моделирования недоступная подсеть была удалена из таблицы маршрутизации, а остальные маршруты были подтверждены с интервалом в 4с.

Таким образом, можно сделать вывод, что обработка переходного процесса, возникшего в результате выхода из строя канала связи на уровне ядра с использованием протокола EIGRP, составила 3.710 с.

**5.3 Анализ полученных результатов моделирования**

Полученные результаты приведены в табл.9.

**Результаты моделирования**

Таблица 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ эксперимента** | **Неисправность** | **Время переходного процесса, с** | | |
|  |  |  | OSPF | EIGRP |
| 1 | Неисправность на уровне доступа | 11.265 | 2.315 |
| 2 | Неисправность на уровне распределения | 11.449 | 3.342 |
| 3 | Неисправность в ядре сети | 12.840 | 3.710 |



Из полученных при моделировании результатов можно сделать вывод, что время сходимости сети в протоколе EIGRP меньше, так как он достаточно просто выбирает оптимальный маршрут, что присуще дистанционно-векторным протоколам, и экономит пропускную способность каналов связи за счет рассылки служебных сообщений только о состоянии связей и об их изменениях, что присуще протоколам состояния каналов.

Однако данный протокол является закрытым и поддерживается только на оборудовании Cisco, поэтому в сетях крупного масштаба, на оборудовании другого производителя рекомендуется использовать протокол OSPF.

**Литература**

|  |
| --- |
| 1. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, |
| технологии, протоколы. Учебник для вузов. 5-е изд. -СПб.: Питер, |
| 2016г. -960 с. |
| 1. У. Одом, Официальное руководство Cisco по подготовке к |
| экзаменам CCENT/CCNA ICND2. 3-е изд. -Cisco Press, 2012г. -736 с. |
| 1. Лимончелли Т., Страта Чейлап, Хоган К. Системное и сетевое |
| администрирование. Практическое руководство. 2-е изд. -СПб.: |
| Символ-Плюс, 2009г. -944с. |