1. Цели: получить инфраструктуру ЦО, способную обеспечить работу в случае отказа каких-либо элементов:

- Одного из ISP, с кратковременной деградацией и последующем автоматическом восстановлении доступа к сети интернет

- Одного из узлов оборудования соответствующего уровня (при наличии дублирующего узла Access, Distribution, Core, EDGE)

- Отказа ряда линков, соединяющих Access, Distribution, Core, EDGE с возможной частичной деградацией пропускной способности, но сохранением доступности сервисов

- Отказа адресного пространства IPv4/IPv6, с сохранением доступ к ресурсам интернет при наличии соответствующих A-записей DNS

1. Что планировалось: получить опыт в проектировании инфраструктуры ЦОД и ЦО, способную обеспечить работу в случае отказа каких-либо элементов инфраструктуры:

* Рассмотреть способы дублирования физического оборудование уровня Access, Distribution, Core, EDGE (Stack, Модульность, избыточные линки, резервные ноды)
* Рассмотреть способы создания отказоустойчивого подключение к двум ISP (PBR или AS, то есть провайдеро-независимые адреса)
* Разработать логическую адресацию в режиме Dual Stack IPv4/IPv6 с применением методов динамического выделения клиентам IP-адресов (DHCP Cisco, DNS Windows Server 2016)
* Построение отказоустойчивых VPN-туннелей (GRE без шифрования с редистрибуцией маршрутов)

1. Используемые технологии:

- Виртуализация GNS3 L2/L3 имиджи оборудование/образы IOS с поддержкой протоколов динамической маршрутизации

- LACP - физическое резервирования линков

- Протоколы

- OSPFv2/OSPFv3 – один из сегментов полностью OSPFv3,

с редистрибуцией маршрутов IPv6 перфиксов

- BGP

- DUAL Stack IPv4/IPv6

- Windows Server 2016 - роль DHCP, DNS

1. Что получилось:

- Разработано адресное пространство ЦО и регионов в DUAL Stack IPv4/IPv6 с учетом выделения сетевых сегментов под сервисы/области использования

- В системе виртуализации GNS3 построена типовая инфраструктура ЦО и дочернего общества с выделением ACCESS/Distribution/CORE

- Настроены L3-связность всех линков ACCESS/Distribution/CORE оборудования ЦО

- Настроен протокол динамической маршрутизации OSPF на оборудовании ACCESS/Distribution/CORE ЦО Москва, один сегмент целиком на новом OSPFv3

- Настроено BGP- подключение к ISP 1,2 с учетом выбранных номеров AS и провайдеро-независимые адреса для двух регионов. BGP на EDGE-оборудовании ЦО и СПб настроено с учетом DUAL Stack IPv4/IPv6.

- Настроен VPN-туннели между офисами ЦО, СПб

- Настроен сервис DHCP/DNS сервера в ЦО на DUAL Stack IPv4/IPv6 под Windows Server 2016

1. Схемы/архитектура

* Реализованная L2 архитектура DataCenter-CORE-ACCESS ЦО/СПб

1. Выводы

В результате грамотного планирования и выполнения работ по настройке оборудования удалось добиться следующего:

- Адресное пространство спроектировано с учетом суммаризации маршрутов до определенных зон/сервисов и уменьшению размеров таблиц работающих в сети протоколов динамической маршрутизации, и как следствие уменьшению нагрузки на ресурсы оборудования.

- Отказ одного из ISP, приводит к кратковременной деградации сервиса доступа к услуге Интернет и последующему автоматическому восстановлению доступа к сервису, за счет работы протокола BGP. Требуется настройка таймеров, чтобы снизить стандартную 180-секундную задержку срабатывания протокола BGP

- Отказ одного из зарезервированных узлов оборудования уровня Distribution, Core, EDGE не приводит значительным проблемам в системе, поскольку протокол динамической маршрутизации OSPF автоматически перестраивает маршруты оборудования

- Отказа ряда линков, соединяющих Access, Distribution, Core, EDGE приводит к частичной деградации пропускной способности, но при этом сохраняется доступности сервисов

- Сбой в работе какого-либо протокола IPv4, или IPv6 сказывается только на доступности хостов в данном адресном пространстве. Резервное адресное пространство сохраняет работоспособность, и, как следствие, при наличии соответствующих A-записей DNS сохраняется доступность сервиса размещенного в Internet