Использование динамической маршрутизации при организации множественного доступа к сети Интернет

Бурдуковский Александр Николаевич,
начальник ОИТ ЦИТСиЗИ тыла МВД по Республике Бурятия,
подполковник внутренней службы

Успешная деятельность любой организации в современных условиях обуславливается многими факторами, среди которых следует отметить, пожалуй, общий для всех — доступ к информации, необходимой для выполнения возложенных на организацию обязанностей и функций. Не являются исключением из этого правила и органы правопорядка, для которых своевременный доступ к информационным ресурсам правоохранительной направленности, в том числе размещенным в сети Интернет, является неотъемлемой частью повседневной оперативно-служебной деятельности.

Несмотря на то, что в настоящее время большинство правоохранительных органов, в том числе органы внутренних дел, имеют доступ к ресурсам сети Интернет, организация указанного доступа в каждом конкретном случае имеет свои индивидуальные особенности, будь то количество или характеристики каналов связи, протоколы канального уровня, используемые при организации «последней мили», телекоммуникационное оборудование и т. д. Вместе с тем, большинство специалистов в области сетевых технологий используют один общий подход при организации доступа к сети Интернет — статическую маршрутизацию.

В данной статье рассматривается динамическая маршрутизация как альтернативный подход к организации доступа к информационным ресурсам сети Интернет, ее достоинства и недостатки.

Выбор типа маршрутизации при организации доступа к сети Интернет

В большинстве случаев у специалистов в области сетевых технологий не возникает вопрос о том, какой тип маршрутизации выбрать при создании внутренней сети организации. Ответ очевиден — динамическая маршрутизация, которая, в сравнении со статической маршрутизацией, позволяет значительно сократить «административные расходы», связанные с планированием, конфигурацией и обслуживанием вычислительной сети. Кроме того, протоколы «внутреннего шлюза» (IGP), используемые при динамической маршрутизации в рамках одной автономной системы, имеют множество встроенных функций, позволяющих автоматически (без участия администратора) анонсировать новые подсети, выбирать наилучший маршрут к сети назначения, балансировать нагрузку, проводить автоматическое суммирование, избегать «петель маршрутизации» и многое другое.

Вместе с тем, при подключении к сети Интернет ответ на вопрос о том, какой тип маршрутизации выбрать при организации указанного информационного взаимодействия, не столь очевиден. Ведь в данном случае и статическая, и динамическая маршрутизация имеют свои преимущества и недостатки.

Для принятия правильного решения о том, какой тип маршрутизации использовать при организации подключения к сети Интернет, необходимо проанализировать два основных фактора: тип и характеристики телекоммуникационного оборудования[1], используемого при организации доступа к сети Интернет; количество каналов доступа к сети Интернет.

Тип и характеристики телекоммуникационного оборудования

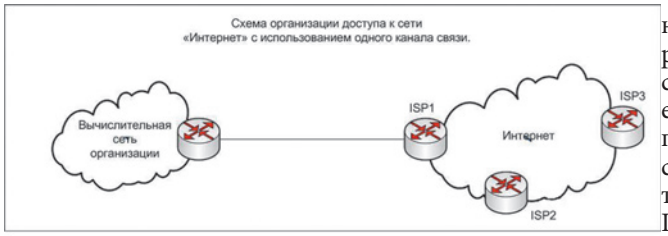
Для подключения к сети Интернет организации используют различные типы телекоммуникационного оборудования, выбор которого определяется технологией «канального уровня», используемой при создании «последней мили», а также финансовыми возможностями организации. Вместе с тем в большинстве случаев в состав телекоммуникационного оборудования входит маршрутизатор, выполняющий, среди прочего, функции по передаче трафика между рабочими станциями организации и устройствами, расположенными в сети Интернет.

Производительность любого маршрутизатора зависит от типа центрального процессора и объема оперативной памяти, входящих в его состав. При этом при использовании динамической маршрутизации потребление ресурсов центрального процессора и оперативной памяти носит, зачастую, экстенсивный характер, что обусловлено наличием большого числа различных структур данных, используемых протоколами динамической маршрутизации при реализации своих функций. В связи с чем применение для подключения к сети Интернет динамической маршрутизации на низкопроизводительных маршрутизаторах не будет являться оптимальным решением.

Количество каналов доступа к сети Интернет

В большинстве случаев организации используют один канал доступа к информационным ресурсам сети Интернет, что в первую очередь обусловлено минимизацией финансовых затрат, необходимых для организации и обслуживания канала связи, приобретения телекоммуникационного оборудования и т. д. Вместе с тем использование одного канала связи негативно сказывается на отказоустойчивости сети, и, в конечном итоге, может привести к отсутствию доступа к информационным ресурсам, размещенным в се-

1 Под телекоммуникационным оборудованием в данной статье подразумевается оборудование организации (не оператора связи), выполняющее функции по коммутации и маршрутизации трафика.



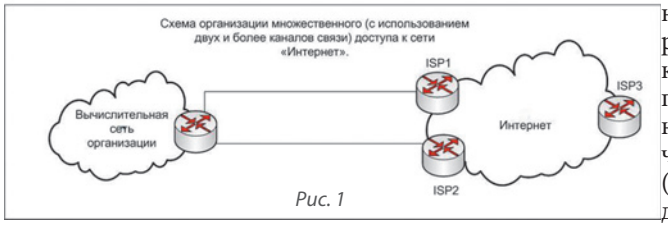


Рис. 1

ти Интернет и необходимым для осуществления повседневной деятельности организации.

При использовании единственного канала связи представляется наиболее оптимальным применять статическую маршрутизацию для передачи трафика между рабочими станциями организации и устройствами, расположенными в сети Интернет, так как в данном случае динамическая маршрутизация не имеет никаких преимуществ перед статической, скорее наоборот — оказывает негативное влияние, чрезмерно потребляя ресурсы маршрутизатора.

В случае наличия множественного (двух и более каналов) доступа к сети Интернет преимущества динамической маршрутизации становятся очевидными, будь то автоматический (без участия администратора) выбор наилучшего маршрута к устройствам, расположенным в сети Интернет, использование резервного канала связи в случае, если основной «выходит из строя», возможность балансировки нагрузки и многое другое. Кроме того, применение динамической маршрутизации при организации множественного доступа к сети Интернет позволяет сетевым устройствам (маршрутизаторам) своевременно реагировать на изменения, происходящие в сети Интернет, тем самым максимально сокращая время, в течение которого информационные ресурсы указанной сети могут быть недоступны для пользователя внутренней сети организации.

Использование протокола граничного шлюза[2] для динамического обмена информацией о маршрутах, существующих в сети Интернет

Основная задача протоколов динамической маршрутизации — наполнение таблицы маршрутизации устройства информацией о существующих подсетях и соответствующих маршрутах к ним. Разные IGP-протоколы динамической маршрутизации, такие как EIGRP, OSPF, RIP, прекрасно справляются с этой задачей, но не подходят (не применяются) для динамического обмена информацией о существующих в сети Интернет маршрутах.

В первую очередь это связано с тем, что перечисленные протоколы относятся к категории протоколов «внутреннего шлюза» и предназначены для осуществления динамической маршрутизации внутри автономных систем, т. е. сетей передачи данных, находящихся под единым управлением.

Сеть Интернет может быть представлена как совокупность множества автономных систем, каждая из которых находится под управлением определенного поставщика услуг доступа к сети Интернет (Internet Service Provider). Для динамического обмена информацией о подсетях, существующих в каждой автономной системе, используются протоколы «внешнего шлюза» (EGP), наиболее известным представителем которых на сегодняшний день является BGP.

Протокол BGP относится к протоколам «путь векторного типа» и предназначен для изучения, распространения и выбора наилучшего пути к подсети назначения, расположенной в сети Интернет. Как и протоколы динамической маршрутизации «дистанционно-векторного типа», BGP в своих обновлениях распространяет информацию о существующих внутри автономных систем префиксах (подсетях), а также метриках маршрутов для достижения указанных префиксов.

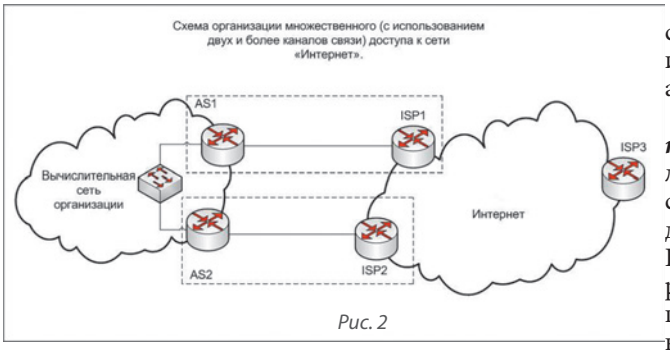


Рис. 2

Основное отличие BGP от протоколов «дистанционно-векторного типа» состоит в том, что помимо префиксов BGP также распространяет различные «атрибуты пути» (вес, номера автономных систем, идентификаторы маршрутизаторов, локальную преференцию и др.), которые предоставляют сетевому инженеру широкий спектр возможностей влияния на выбор наилучшего маршрута к сети назначения.

Использование BGP в качестве протокола динамической маршрутизации при организации доступа к информационным ресурсам сети Интернет предполагает конфигурацию данного протокола на телекоммуникационном оборудовании как организации, так и, в случае множественного подключения, на телекоммуникационном оборудовании поставщиков доступа к сети Интернет. При этом сетевой инженер организации должен согласовать с представителем ISP следующие обязательные атрибуты (параметры):

- Диапазон публичных IP-адресов, выделяемых организации поставщиком услуг доступа к сети Интернет.
- Номер автономной системы, к которой относится выделенный организации публичный диапазон IP- адресов.
- Дополнительные параметры (использование аутентификации, тип применяемого BGP, тип BGP обновлений, которыми должны обмениваться маршрутизаторы и т. д.), используемые при конфигурации и функционировании BGP.

Далее кратко рассмотрим каждый из указанных выше атрибутов.

Диапазон публичных IP-адресов (далее рассматривается протокол IPv4): диапазон частных IP-адресов, который использует организация для создания собственной сети передачи данных, не может быть использован для подключения к сети Интернет, так как частные IP-адреса не являются глобально маршрутизируемыми. В связи с этим организации необходимы IP-адреса из публичного диапазона, посредством которых представляется возможным взаимодействовать с устройствами, расположенными с сети Интернет.

2 Далее BGP.

Публичные IP-адреса могут быть заимствованы из диапазона IP-адресов поставщика услуг доступа к сети Интернет посредством выделения последним для организации подсети с определенным префиксом. При этом при определении префикса целесообразно исходить из минимального количества устройств организации, которые должны быть непосредственно подключены к сети Интернет (т. е. должны иметь публичный IP-адрес). В большинстве случаев для подключения организации к указанной сети необходимо выделение подсети с тридцатым (/30) префиксом.

Следует отметить, что при организации множественного подключения к сети Интернет каждый поставщик услуг доступа к информационным ресурсам указанной сети выделяет организации подсеть из собственного диапазона публичных IP-адресов. При этом выделение единственного публичного IP-адреса, в том числе с использованием протокола DHCP, нецелесообразно, что в первую очередь объясняется структурой и принципами работы протокола BGP.

Номер автономной системы: номер автономной системы является атрибутом пути, который распространяется в BGP-обновлениях и используется данным протоколом для выбора наилучшего маршрута к сети назначения, а также устранения петель маршрутизации.

Номер автономной системы возможно получить двумя способами: запросить у организации (IANA), курирующей вопросы распределения и осуществляющей контроль за использованием в сети Интернет номеров автономных систем (применим только для поставщиков доступа к сети Интернет); использовать публичный номер автономной системы, выделенный поставщику доступа к сети Интернет.

В большинстве случаев используется второй способ, при котором поставщик доступа к сети Интернет просто сообщает сетевому инженеру организации номер публичной автономной системы, используемый поставщиком.

Дополнительные параметры, используемые при конфигурации и функционировании BGP: BGP использует множество дополнительных параметров, влияющих на его работу. В свете рассматриваемой темы наиболее важным дополнительным параметром, по мнению автора, является тип обновлений, которыми обмениваются соседние BGP-маршрутизаторы.

На сегодняшний день существует три вида BGP-обновлений: обновления, содержащие только «маршрут по умолчанию»; полные обновления (содержат все известные BGP-префиксы); частичные обновления (содержат «маршрут по умолчанию», а также только те префиксы, которые являются частью публичного диапазона IP-адресов, выделенных поставщику доступа к сети Интернет).

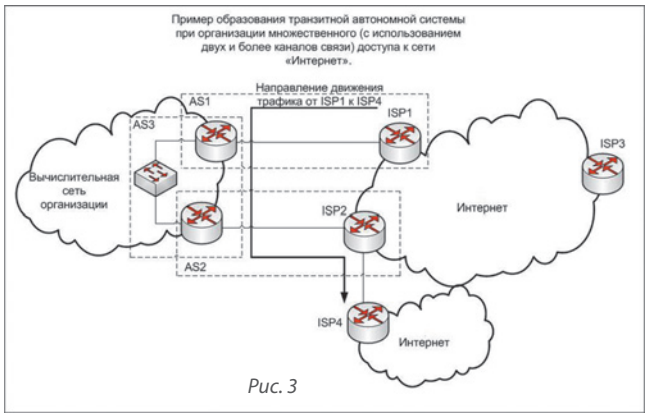


Рис. 3

В целях сокращения нагрузки на телекоммуникационное оборудование (чрезмерного потребления ресурсов центрального процессора и объемов свободной памяти маршрутизатора) целесообразно получать от поставщика услуг доступа к сети Интернет BGP-обновления, содержащие только «маршрут по умолчанию».

После того как между организацией и поставщиком доступа к сети Интернет согласованы все обязательные параметры, на телекоммуникационном оборудовании настроен протокол BGP, проведена отладка и проверка его работоспособности — организация получает доступ к информационным ресурсам указанной сети, а сетевой инженер широкий набор средств, позволяющих эффективно управлять указанным доступом.

Транзитная автономная система

Преимущества использования протокола BGP при организации множественного доступа к сети Интернет видны «невооруженным глазом», при этом при организации указанного вида доступа существуют и недостатки, которые не столь очевидны.

Основным недостатком использования протокола BGP при организации множественного доступа к сети Интернет является создание так называемых «транзитных» автономных систем, при которых трафик, предназначенный для узлов, находящихся в сети Интернет, передается через автономную систему (телекоммуникационное оборудование) организации. При этом пользователи организации, использующие информационные ресурсы указанной сети, наблюдают полное отсутствие доступа к сети Интернет либо значительное падение скорости доступа к указанным информационным ресурсам.

Созданию «транзитной» автономной системы способствуют следующие факторы: использование двух и более маршрутизаторов при организации доступа к сети Интернет; использование нескольких поставщиков доступа к сети Интернет; распространение поставщикам услуг доступа к сети Интернет маршрутов с наилучшей метрикой.

Совокупность перечисленных факторов приводит к тому, что поставщики доступа к сети Интернет используют автономную систему организации для передачи трафика, предназначенного устройствам, расположенным в указанной сети и находящимся в зоне ответственности других поставщиков доступа к сети Интернет.

Для избежания создания «транзитных» автономных систем применяется фильтрация префиксов, позволяющая направлять поставщику доступа к сети Интернет информацию только о тех префиксах, которые необходимы для организации доступа к информационным ресурсам указанной сети.

Наилучшим примером фильтрации префиксов в данном случае является информирование поставщика услуг доступа к сети Интернет о префиксе публичных IP-адресов, выделенных организации данным поставщиком. В этом случае предпосылки, способствующие созданию «транзитной» автономной системы, отсутствуют.

Список используемой литературы

1. В. Одом. CCNP Route 642–902. Официальный сертификационный гид.— СискоПресс, 2010,— 730 с.
2. Н. Кочарянс. CCIE Routing and Switching v5.0. Официальный сертификационный гид. Том 1.— СискоПресс, 2015,— 742 с.