УДК 004.72

А.И. Ролик, В.А. Иосифов

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ В КОРПОРАТИВНОЙ IP-СЕТИ

Введение

Успешность и конкурентоспособность современных предприятий существенно зависит от эффективности использования информационных технологий (ИТ), призванных обеспечить поддержку бизнес-процессов и процессов деятельности предприятия. Для поддержания работоспособности ИТ-системы предприятия, оптимального распределения и перераспределения ограниченных информационных и телекоммуникационных ресурсов создаются различные системы управления ИТ-инфраструктурой (СУИ) [1]. Один из основных комплексов задач, решаемых СУИ, связан с управлением сетевыми ресурсами, поскольку от работоспособности корпоративной сети существенно зависит эффективность функционирования всей ИТ-системы. Большинство систем управления сетями ориентированы на управление только оборудованием с целью поддержания эксплуатационных характеристик и показателей работы сети на заданном уровне. При этом управление, как правило, осуществляется без учета типов информационных потоков, транспортируемых сетью, и их значимости для поддержания бизнес-процессов. Это приводит к тому, что при перегрузке сети ухудшаются параметры передачи всех потоков, независимо от их важности. Совершенно естественным является стремление разработать и использовать в СУИ механизмы управления сетью, учитывающие важность передаваемых потоков и, в случае перегрузки сети, ограничивающие передачу низкоприоритетных потоков с целью сохранения качества передачи высокоприоритетных.

Настоящая работа посвящена разработке системы адаптивного управления информационными потоками в корпоративной IP сети, учитывающей значимость передаваемой информации для поддержания бизнес-процессов и осуществляющей распределение и перераспределение потоков в сети с учетом условий их передачи, изменяющихся приоритетов бизнес-процессов и текущего состояния сети.

Анализ работ по управлению информационными потоками

Управление информационными потоками чаще всего используется для борьбы с сетевыми перегрузками, возникающими при превышении входящей нагрузкой пропускной способности сети. В [2] рассматриваются вопросы управления потоками информации с целью предотвращения потери работоспособности сети, вызванной запредельными входящей и транзитной нагрузками. Однако управление потоками в сетях рассматривается без учета их приоритетов.

Множество работ, например [3—5], по агрегации трафика, оптимизации сетевых потоков, достижению максимальной загруженности сети и пр. посвящены решению различных задач сетевого управления, но при этом не учитываются требования к транспортировке информационных потоков, предъявляемые со стороны бизнес-процессов.

Решение всего комплекса задач адаптивного автоматического управления потоками при изменении значимости бизнес-процессов сложно реализовать на основе управления с помощью правил (Policy-Based Management, PBM) [6], поскольку изменение критериев оптимальности управляющих решений требует постоянного экспертного вмешательства. Кроме того, основным недостатком таких систем является их привязанность к нижним уровням модели OSI, не связанным напрямую с поддержкой бизнес-процессов. Системы управления по заранее определенным политикам позволяют увеличить показатели качества работы сети, например, сократить время неработоспособности, увеличить загрузку сети до предельных значений и пр. [7,8], но при этом не учитывают приоритеты информационных потоков, задаваемые прикладным уровнем.

Существует большое количество работ и обзоров по адаптивному управлению сетями, учитывающих требования к качеству передачи данных, предъявляемых отдельными приложениями [9]. В отличие от систем поддержки работы приложений, которые предоставляют средства для автоматизации их работы, но не дают возможности контроля и управления перегрузками в сети, системы управления приложениями и потоками позволяют реализовать приоритетную передачу информации отдельных приложений. Работы [10,11] рассматривают применение механизмов QoS, позволяющих предоставить каждому приложению требуемую полосу пропускания, однако не учитывают важность работающих приложений. За счет централизованного управления получение требуемого качества достигается для каждого из предопределенных потоков, но при этом низкоприоритетные потоки без учета передаваемой в них информации могут требовать такого же качества обслуживания, что и высокоприоритетные. Это не позволяет строить системы управления сетями, оптимизирующие загруженность каналов связи с учетом известных приоритетов информационных потоков и требований к качеству передачи, выдвигаемых со стороны бизнес-процессов.

Постановка задачи

Необходимо разработать систему автоматического управления информационными потоками (СУИП) в корпоративной IP сети, учитывающую приоритеты потоков данных, генерируемых приложениями, поддерживающими бизнес-процессы, и обладающую способностью адаптации к изменению приоритетов потоков, загруженности каналов связи и отказам сетевого оборудования.

 ISSN 1562-9945

Управление информационными потоками в сетях с коммутацией пакетов

В настоящее время для мониторинга работы и управления сетевым оборудованием применяется большое количество разнообразных систем управления как дорогостоящих фирменных, так и условно бесплатных универсальных [1,2]. При этом превалирует подход обособленного решения отдельных задач сетевого управления без рассмотрения в тесной взаимосвязи проблем управления распределением общих информационных и телекоммуникационных ресурсов корпоративных ИТ-систем с учетом значимости распределенных приложений, поддерживающих бизнес-процессы или процессы деятельности. Более перспективным является подход к распределению ИТ-ресурсов с учетом стоимости передаваемой информации, определяемой на основании ее значимости для бизнес-процессов [12—15]. В этом случае выделение сетевых ресурсов бизнес-процессам, операциям, распределенным приложениям и пользователям производится с учетом их значимости для бизнеса, задаваемой соответствующей системой приоритетов, а перераспределение ресурсов происходит при изменении значимости бизнес-процессов или возникновении нештатных ситуаций в сети, создающих перегрузки. Перегрузки сетевого оборудования или каналов связи приводят к функциональным отказам и делают невозможным эффективное функционирование ИТ-системы. Для борьбы с перегрузками используются методы маршрутизации и управления потоками информации.

За счет использования протоколов маршрутизации, адаптивных к перегрузкам и отказам, можно решить проблему сетевых перегрузок, однако, если причиной перегрузок является существенное увеличение входящей нагрузки, то методами адаптивной маршрутизации можно лишь частично сгладить эту проблему. Более эффективным для борьбы с сетевыми перегрузками является управление входящими потоками информации. При этом, естественно, управление должно строиться таким образом, чтобы в случае угрозы возникновения сетевых перегрузок ограничивать или запрещать передачу низкоприоритетных потоков без ухудшения качества передачи потоков, генерируемых высокоприоритетными распределенными приложениями.

Для реализации такого управления необходимо постоянно иметь данные о значимости бизнес-процессов и изменении этой значимости, регулярно получать информацию о загруженности сети, состоянии узлов и каналов связи, выявлять, оценивать и ограничивать или блокировать низкоприоритетные потоки информации, вырабатывая оптимальные управляющие воздействия и оперативно их реализовывая.

В этом случае СУИП должна управлять сетевым оборудованием и потоками информации, получая информацию о функционировании прикладных процессов и их важности. Для этого СУИП необходимо работать практически на всех уровнях модели OSI от канального до прикладного уровня, используя возможности и функциональность каждого из

уровней для того, чтобы эффективно реализовывать на одних уровнях то, что нельзя сделать на других. Например, максимальная пропускная способность и загруженность сетевых ресурсов достигается при коммутации кадров на канальном уровне модели OSI, в то время, как для реализации возможности ограничения разных типов трафика в зависимости от сервиса или адресатов потоков, требуется обработка пакетов на сетевом уровне, что вызывает дополнительные задержки при обработке каждого отдельного пакета. При обработке пакетов на уровнях выше сетевого задержки, вызванные этой обработкой, необходимой для управления трафиком, суммарно превышают требования по каждому из потоков и не могут применяться в современных сетях с существующими требованиями к передаче потоков.

Каждый k-й бизнес-процесс b_k из множества бизнес-процессов $B = \{b_k\}$, $k = \overline{1, K}$, где K— количество бизнес-процессов, пользующихся поддержкой ИТ-системы, порождает множество информационных потоков $\lambda_k^P = \{\lambda_{kl}^P\}$, $k = \overline{1, K}$, $l = \overline{1, L_k}$, где L_k — количество потоков, генерируемых процессом b_k. Все потоки, непосредственно связанные с бизнес-процессами, создают суммарный трафик Λ^P, равный $\Lambda^P = \sum\limits_{k=1}^{K} \sum\limits_{l=1}^{L_k} \lambda_{kl}^P$.

Для каждого потока данных λ_{kl} из множества λ_k задается приоритет Pr_{kl}, $k = \overline{1, K}$, $l = \overline{1, L_k}$, причем Pr_{kl} принимает значения из упорядоченного множества целых чисел значений приоритетов $\Pi = \{1, \ldots, Pr_{\max}\}$, где $Pr_{\max}$ — максимальное значение, принятое для данной ИТ-системы.

Присвоение процессам или приложениям и, соответственно, потокам значений приоритетов осуществляется, исходя из значимости процессов или приложений, определяемых на основании анализа производственного или жизненного цикла предприятия, а также сложившейся ситуации на рынке или в отрасли. Значимость бизнес-процессов может быть определена экспертным путем, в результате работы системы автоматизации управления выполнением бизнеса, директивными указаниями руководства и другими способами. В ходе работы предприятия приоритеты бизнес-процессов, приложений и пр. могут меняться и СУИП должна оперативно реагировать на такое изменение.

Кроме потоков, порождаемых бизнес-процессами, в сетях передаются потоки, не имеющие непосредственного отношения к поддержанию бизнес-процессов. К таким потокам можно отнести потоки, создаваемые пользователями при использовании сетевых сервисов, и выполнении действий, не связанных с процессами деятельности. Например, запуск сетевых игр, обмен мультимедийными файлами, просмотр потокового видео и пр. При этом создается трафик $\Lambda^U = \sum\limits_{m=1}^{M} \sum\limits_{g=1}^{G_m} \lambda_{mg}^U$, где λ_{mg}^U один из g-ых потоков, $g = \overline{1, G_m}$, создаваемый m-м пользователем, $m = \overline{1, M}$, M — количество пользователей корпоративной ИТ-системы, G_m — количество потоков, связанных с рабочей станцией m-го пользователя. Потоки λ_{mg}^U, $m = \overline{1, M}$, $g = \overline{1, G_m}$, можно легко контролировать. Трафик Λ^U ограни-

чивается или блокируется СУИП в первую очередь, если он изначально не ограничен или не запрещен корпоративной политикой использования сетевых ресурсов. Каждому потоку λ_{mg}^{U} или типу трафика могут быть присвоены приоритеты со значениями из множества Π.

Весь остальной трафик Λ^{T} сети является технологическим и связан с необходимостью поддержания работоспособности ИТ-системы. Потоки трафика Λ^{T} связаны с работой СУИ, резервным копированием данных, обновлением программного обеспечения ИТ-системы и пр. и они также контролируются и управляются СУПИ, являющейся составной частью СУИ. Всем потокам этого трафика или генерирующим их приложениям присваивается приоритет из множества Π.

Суммарный трафик Λ^{Σ} ИТ-системы определяется как

$$\Lambda^{\Sigma} = \Lambda^{P} + \Lambda^{U} + \Lambda^{T}$$

и он не должен превышать суммарной пропускной способности сети C^{Σ}, т.е. должно выполняться условие:

$$\Lambda^{\Sigma} \leqslant C^{\Sigma}. \tag{1}$$

Учитывая тот факт, что выполнение условия (1) не исключает перегрузок отдельных каналов, целесообразно управлять входящими потоками таким образом, чтобы выполнялось условие

$$\Lambda_{i}^{\Sigma} \leqslant C_{i}. \tag{2}$$

для всех $i = \overline{1, I}$, где I — максимальное количество каналов связи, Λ_{i}^{Σ} — суммарный трафик в i-м канале, C_i — пропускная способность i-го канала, причем $C^{\Sigma} = \sum\limits_{i=1}^{I} C_i$.

Реализация в СУИП алгоритмов работы, обеспечивающих выполнение условия (2), требует сбора и обработки гораздо большего объема информации, чем при работе по условию (1), однако это позволяет избежать локальных перегрузок в сети и существенно повысить качество работы распределенных приложений.

Входными данными для СУИП являются сведения о загруженности отдельных каналов связи, выходными — команды управления сетевым оборудованием, ограничивающие или запрещающие прохождение отдельных потоков. Управление потоком осуществляется в каждом из узлов сети на входе в узел. При этом СУИП стремится пропустить через каждый узел сети максимальное количество потоков с требуемыми параметрами качества обслуживания.

Значения приоритетов информационных потоков Λ^{P} и Λ^{T}, а также требования к качеству обслуживания этих потоков задаются соответствующей таблицей. Пример фрагмента таблицы выглядит следующим образом.

Приоритеты потоков и требования к качеству передачи

Таблица 1

Приложение	Порт	Приоритет	Требуемая полоса пропускания, кб/с	Максимальная задержка, мс
СУИП	22, 23, 80	1	1024	1024
SAP	3201-3299	2	1024	1024
Система биллинга	3306, 1527	3	512	1024
1С Бухгалтерия	512	4	128	512
Электронная почта	25, 110, 143	5	64	256
Сервис обмена файлами	139, 445	6	512	256

Ограничение потоков возможно как для конкретного пользователя сети, так и для отдельного сетевого сервиса, включая или запрещая его для всех пользователей сети. Ограничения потоков информации производится только после полной утилизации сетевых ресурсов.

Оптимизация маршрутизации и агрегации трафика с использованием MPLS — коммутации пакетов по меткам позволяет достичь максимального использования ресурсов сети и применять QoS механизмы для достижения требуемых показателей качества по каждому из потоков. Однако при этом возможны случаи перегрузки сети и отсутствуют механизмы, позволяющие исправлять проблемы такого рода. В связи с невозможностью ограничения потоков информации на канальном уровне СУИП вынуждена управлять потоками информации на сетевом уровне.

Система управления потоками информации в IP-сети

Для эффективного управления использованием сетевых ресурсов, предотвращения негативных последствий перегрузок и неисправностей сетевых элементов в СУИП реализуются следующие группы функций:

— управление маршрутизацией в сети, агрегирование трафика и эффективное использование всей полосы пропускания каналов связи, реализуемые на сетевом уровне;

— управление входящими потоками при возникновении угроз перегрузки сети или каналов связи, включающее ограничение низкоприоритетных потоков трафика Λ^P, существенное ограничение или блокирование потоков трафика Λ^U,

— локализация и управление устранением неисправностей в сети.

Среднее время задержки D при передаче пакета по сети можно оценить по формуле:

$$D = H \times S \times (R + P/C),$$

 ISSN 1562-9945

где H — количество шагов ретрансляции, S — средняя длина очереди маршрутизатора, R— среднее время на решение задач маршрутизации в отдельном узле, P — средняя длина пакетов, а C — скорость передачи по линии связи, которая при проведении оценки считается одинаковой для всех каналов.

Управление параметром H осуществляется в СУИП протоколами динамической маршрутизации и оптимизацией сетевых потоков.

Критерий оптимального управления потоками заключается в поддержке максимально возможной скорости следования пакетов при отсутствии потерь из-за переполнения входных буферов, т. е.:

$S_q - S_q(t) \geqslant 0$, при $\tau(t) + u(t) \to \min$,

где S_q — размер входного буфера, $S_q(t)$ — текущее значение очереди, $\tau(t)$ — межкадровый интервал, $u(t)$ — переменная управления.

Структура предлагаемой СУИП представлена на рис. 11.

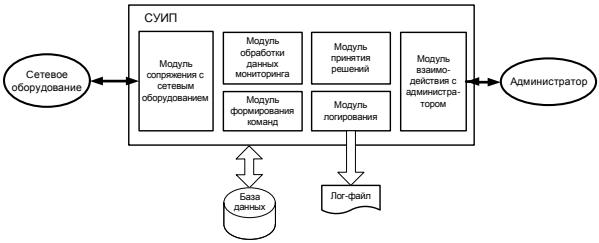

Рис. 1 – Структура СУИП

СУИП состоит из модуля принятия решений, модуля формирования команд, модуля обработки данных мониторинга, модуля сопряжения с сетевым оборудованием, модуля взаимодействия с администратором и модуля логирования.

Основные функции по управлению информационными потоками реализует модуль принятия решений, осуществляющий анализ состояния сети и отдельных трактов передачи данных, принимающий решения о необходимости управления сетевым оборудованием для улучшения состояния сети и выполнения действий на оборудовании для устранения последствий неисправностей. Кроме того, модуль изменяет частоту получения данных мониторинга и задает степень детализации этих данных, необходимую для локализации неисправностей или получения более точных сведений о состоянии сетевых элементов. Для ускорения работы СУИП модуль освобожден от формирования текстов команд и первичной обработки результатов мониторинга. Эти функции делегированы модулю формирования команд и модулю обработки данных мониторинга соответственно.

Структура таблиц базы данных (БД) СУИП приведена на рис. 2.

Из рис. 2 видно, что все команды, доступные для выполнения, находятся в отдельной таблице, что позволяет использовать только идентификаторы команд в пределах СУИП.

Рис. 2 – Структура базы данных СУИП

Система работает следующим образом.

С задаваемой администратором периодичностью, а по умолчанию один раз в минуту, собираются данные с сетевых устройств, анализируется состояние загруженности и работоспособности отдельных каналов связи и сети в целом. При этом определяется, какие потоки информации проходят через каждый интерфейс узлов сети и какую полосу пропускания при этом занимают.

Если канал связи загружен более чем на 80%, оператору выводится предупреждение о возможной перегрузке сети или отдельных трактов. Когда загрузка отдельного канала превышает 90% (значения порогов 80% и 90% — значения, устанавливаемые по умолчанию, в процессе работы администратор может их корректировать), СУИП автоматически предпринимает действия по ограничению входящей нагрузки и снижению загруженности канала. Для этого на сетевом уровне осуществляется перебор списка потоков информации, проходящих через интерфейс, и выдается управляющее воздействие на сетевой узел для абсолютного запрета прохождения или ограничения полосы пропускания некоторых из потоков. Причем потоки, попавшие в таблицу приоритетности, будут ограничены по полосе пропускания до требований, указанных в таблице. Потоки, не числящиеся в таблице приоритетов, будут автоматически последовательно запрещаться для прохождения по каналу связи, близкому к перегруженному состоянию. Данная процедура будет выполняться до тех пор, пока загрузка канала не опустится ниже заданного порогового значения. При дальнейшем снижении загруженности каналов, запрещенные потоки будут постепенно разрешаться.

Для получения от сетевого оборудования списков активных информационных потоков, используются программные средства удаленного доступа и выполнения удаленных команд. Управление включением и отключением потоков информации на сетевом устройстве автоматически выполняется разработанным программным обеспечением СУИП и реализуется модулем формирования команд и программным модулем сопряжения с сетевым оборудованием, использующим Expect::Perl.

На вход программного модуля сопряжения подается запрос, содержа-

щий IP-адрес или имя устройства при наличии DNS сервера, а также команда для выполнения или пакет команд. После этого ожидается ответ от оборудования. Полученные ответы записываются в БД для ведения операционной и аналитической деятельности. В результате анализа загрузки каналов связи определяется необходимость выполнения дополнительных действий на каждом из каналов связи ИТ-системы.

Пример команд, используемых для ограничения потока информации:

```
------------ Настройка ----------------
access-list 1 permit tcp any eq 80
access-list 1000 deny ip any
!
interface ethernet 1
  ip policy route-map PBR
!
route-map PBR permit 10
  match ip address 1
  set ip precedence priority
  set ip next-hop 1.1.1.2
  route-map PBR deny 1000
match ip address 1000
------------ Настройка ----------------
```

Для эффективной работы СУИП важно знать величину и нагрузку каждого потока на сеть. В зависимости от того, что необходимо видеть — текущую загрузку или общее количество пакетов, которые проходят через сетевое устройство, могут быть использованы различные способы получения необходимой информации. Первый способ предполагает выполнение удаленных команд и анализ полученных от оборудования ответов. Такой способ позволяет получить значение общего числа пакетов, переданных по каналу связи и относящихся к отдельному потоку, но не позволяет получить информацию о текущей нагрузке, создаваемой данным потоком для сети. Этот способ можно использовать только для сбора аналитической информации, кроме того, он не требует дополнительных настроек оборудования под каждый из потоков. Второй способ заключается в активации на каждом порту средств расчета объема трафика по каждому из сервисов, разработанных производителем сетевого оборудования и использующих фирменные алгоритмы. Несмотря на то, что такие расчеты требуют от оборудования дополнительной процессорной мощности, они позволяют получать точную информацию по каждому из сервисов в текущий момент времени. Именно такой способ используется в СУИП. Активация программных средств подсчета трафика производится командой ip nbar protocol discovery на нужном интерфейсе. Вывод команды просмотра имеет следующий вид (данные будут содержаться в таблице “Активные сервисы”):

```
Device{\#} show ip nbar protocol-discovery
FastEthernet0/0
```

```
Input Output
----- ------
Protocol Packet Count Packet Count
Byte Count Byte Count
30sec Bit Rate (bps) 30sec Bit Rate (bps)
30sec Max Bit Rate (bps) 30sec Max Bit Rate (bps)
--------------- ---------------------- ----------
ssh 27524274 699300
4420992684 145872150
4000 3000
3037000 271000
```

Ограничение потоков выполняется по заданной таблице приоритетов и требований показателей качества каждого из потоков. Система имеет возможность ограничить пропускную способность для каждого пользователя сети, по всему потоку сразу или по группе потоков и пользователей. Выполнение процедуры ограничения сводится к выполнению команд на сетевом оборудовании.

После выполнения действий по ограничению IP потока, СУИП оповещает пользователя о запрете данного потока и возможных причинах такого ограничения. Для оповещения приложения достаточно использование протоколов транспортного и сетевого уровня, которые доведут до приложения информацию о запрете потока и, в ряде случаев, причинах такого запрета потока. Для оповещения пользователей могут быть использованы, например, стандартные средства ОС Windows (Messenger Service и netsend), которые позволяют вывести на экран пользователя сообщение с необходимым текстом или агентские технологии СУИП [16].

Одна из задач, решаемых СУИП, заключается в минимизации времени неработоспособности наиболее приоритетных потоков. СУИП, в случае отказа канала связи или сетевого оборудования, сначала попытается перераспределить потоки, используя динамический протокол маршрутизации OSPF. Протокол автоматически перестраивает таблицы маршрутизации всех маршрутизаторов в сети, обходя отказавший канал передачи данных или оборудование.

Если этого будет недостаточно и в сети будут наблюдаться перегруженные участки, СУИП ограничивает наименее приоритетные потоки Λ^P и запрещает потоки Λ^U. Для этого СУИП постоянно собирает данные об активности потоков на каждом из интерфейсов работающего сетевого оборудования и, при возникновении нештатной ситуации, определяет потоки, которые должны быть запрещены для ликвидации перегрузки каналов связи.

Схема работы СУИП приведена на рис. 3.

СУИП ведет анализ активности сервисов на каждом из интерфейсов и находит закономерности в перегрузке каналов одними и теми же сервисами в сети. Система может вырабатывать управляющие воздействия и ограничить полосу пропускания для сервисов и исключать возможные всплески сетевой активности.

 ISSN 1562-9945

На рис. 3 поток 1 ограничивается, последующая передача потока 2 запрещается, а поток 3 передается без изменений.

Основным достоинством разрабатываемой СУИП является способность ограничения или блокирования только конкретных потоков отдельных пользователей. Реализация этой способности требует дорогостоящего оборудования и приводит к дополнительным задержкам в сети.

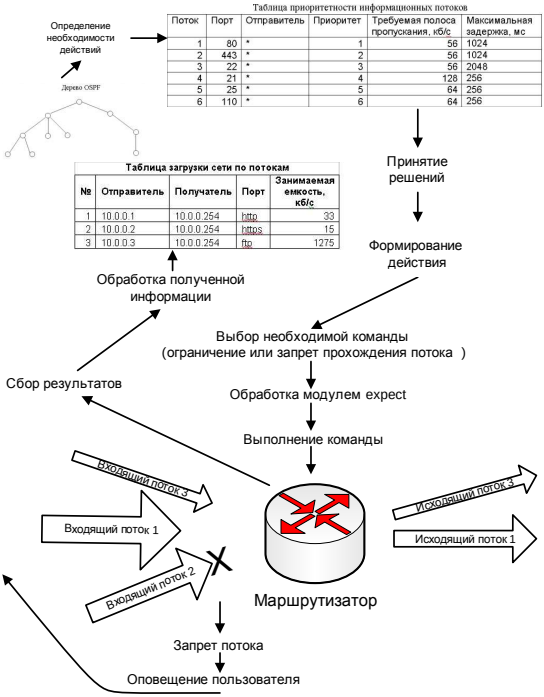

Рис. 3 – Схема работы СУИП

Разработанная СУИП предназначена для использования в корпоративных IP-сетях, построенных на основе маршрутизаторов Cisco (серии не ниже 72xx). Система устанавливается на ОС Unix. Для работы системы требуется поддержка языков C, PHP, Perl. Производительность протокола каждого порта маршрутизатора должна быть не меньше средней интенсивности суммарного трафика, проходящего через порт. Производительность внутренней шины маршрутизатора должна быть не меньше средней интенсивности суммарного трафика, передаваемого между портами, принадлежащими разным модулям маршрутизатора.

Выводы

В статье предложены методы адаптивного управления информационными потоками в корпоративной IP-сети с учетом загруженности каналов связи и приоритетов потоков данных.

Разработана адаптивная система управления информационными потоками в IP сети. Система распределяет и перераспределяет сетевые ресурсы в зависимости от требований бизнес-процессов и состояния корпоративной сети.

Нерешенным остается обоснование и выбор критериев для оценки качества работы сети.

Перспективным является создание обучаемой системы адаптивного управления с применением минимального количества экспертных данных и получения оптимального управления по различным критериям для масштабируемых сетей.

Литература

1. Система управління інформаційно-телекомунікаційною системою корпоративної АСУ/ С.Ф.Теленик, О.І.Ролік, М.М.Букасов, Р.Л.Соколовський // Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка. — 2006. — 45. — С. 112—126.
2. Дымарский Я.С., Крутякова Н.П., Яновский Г.Г. Управление сетями связи: принципы, протоколы, прикладные задачи. М.: ИТЦ “Мобильные коммуникации”.— 2003. — 384 с.
3. An overview of routing optimization for internet traffic engineering/ N. Wang, K. Hon Ho, G. Pavlou, M Howarth// IEEE Communications Surveys & Tutorials.—2008.Vol.10,No.1.—pp.36—56.
4. Towards Robust Multi-layer Traffic Engineering: Optimization of Congestion Control and Routing/ J. He, M. Bresler, M. Chiang, J. Rexford// IEEE Journal on Selected Areas in Communications. — 2007.— Vol. 25, Issue 5.— pp. 868—880.
5. Awduche D. O. MPLS and traffic engineering in IP networks// IEEE Communications Magazine. — 1999, December.— pp. 42—47.
6. Boros S. Policy-based network management with SNMP// Proceedings of the 6th Eunice Summer School, 2000. pp. 65—172.
7. Release Notes for QoS Policy Manager 1.1. Cisco Systems, Inc.—1999. — 8 p.
8. Verma D., Calo S., Amiri K. Policy based management of content distribution networks// IEEE Network.— 2002. — Vol. 16. No 2.— pp. 34–39.
9. Ролик А.И., Ружанская О.В. Сетевая модель обеспечения качества сервиса при передаче мультимедийной информации в глобальных сетях// Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка. — 2007. — 46.— С. 187—205.

 ISSN 1562-9945

10. Yau D. K. Y., Lam S. S. Migrating sockets — End system support for networking with quality of service guarantees// IEEE/ACM Transactions on Networking.— 1998.— vol. 6. No. 6.— pp. 700—716.

11. Xie G. G., Lam S. S. An efficient network architecture motivated by application-level QoS// High Speed Networking. — 1998.— Vol. 6.— No. 3.— pp. 165—179.

12. Ролик А.И. Модель управления перераспределением ресурсов информационно-телекоммуникационной системы при изменении значимости бизнес-процессов// Автоматика. Автоматизация. Электротехнические комплексы и системы. ХГТУ. — 2007. — 2 (20). — С. 73—82.

13. Теленик С.Ф., Ролік О.І., Букасов М.М. Моделі управління розподілом обмежених ресурсів в інформаційно-телекомунікаційній мережі АСУ// Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка. — 2006. — 44. — С. 234—239.

14. Управління доступом до обмежених ресурсів інформаційно-телекомунікаційної мережі АСУ військового призначення/ С.Ф.Теленик, О.І.Ролік, М.М.Букасов, П.І. Терещенко // Зб. наук. праць ЦНДІ Збройних Сил України. — 2006. — 3 (37).— С. 33—43.

15. Букасов М. М., Ролік О. І., Теленик С. Ф. Технологія управління ІТ-інфраструктурою на основі ресурсного підходу// Вісник ЖДТУ. — 2008.— 4(47). — с. 180—189.

16. Ролик А.И., Соколовский Р.Л. Распределение мобильных компонентов системы управления информационно-телекоммуникационной системой// Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка. — 2007. — 47.— С. 113—124.