

них, позволяют решать задачи распределения ресурсов, администрирования и безопасности. В статье дана классификация объектов, событий и критериев аудит-контроля, а также предложена процедура оценки состояния системы с возможностью прогноза на определенный период времени.

Комментарий. Работа выполнена под руководством доц. Саенко В.И.

Литература. 1. Саенко В.И. Администрирование, управление и мониторинг в компьютерных сетях // АСУ и приборы автоматики. 1998. №.108. С. 251-258. 2. Ценк А. Novell Netware 4.x. К.: BHV,1996. 784 с.

Поступила в редколлегию 12.05.98

УДК 681.324

АДМИНИСТРИРОВАНИЕ, УПРАВЛЕНИЕ И МОНИТОРИНГ В КОМПЬЮТЕРНЫХ СЕТЯХ

САЕНКО В.И.

Рассматривается формальный анализ базовых задач, их взаимосвязанность и особенности реализации в реальном масштабе времени. К ним относятся задачи: управления сетевыми объектами, администрирования, мониторинга.

1. Актуальность

Важным моментом развития информационных технологий является переход от концепции сосредоточенных локальных систем к системам распределенным, предполагающим распределенность не только ресурсов транспортной системы, но и ресурсов самой информационной системы, например распределенность баз данных и обрабатывающих модулей. Эти аспекты, прежде всего, затрагивают вопросы организации управления проектируемой и существующих систем. Для распределенной системы характерно наличие множества задач, разобщенных топологически, но близких по функциям. Представляется актуальным формализация основных задач, обеспечивающих эффективность функционирования распределенных информационных систем.

2. Описание проблемы

Распределенную информационную систему рассматриваем как совокупность функционально однородных, связанных виртуальных сетей, функционирующих на фиксированной транспортной струк-

туре компьютерной сети. Число виртуальных сетей p может быть произвольным. Компьютерная p -я виртуальная сеть обеспечивает решение p -й группы функционально однородных задач $\{X_j\}_{j \in X^p}$, $p=1, \dots, p$, $X^p M X^0$, где множество всех задач системы $X^0 = \bigcup_p X^p$, p – число виртуальных сетей (групп).

Объединение всех функциональных сетей представляет собой многослойную топологическую структуру, в которой транспортные функции обеспечивают два нижних слоя: транспортная физическая сеть (слой 1), образованная аппаратными устройствами и каналами связи, и транспортная информационная виртуальная сеть (слой 2), образованная программными системами поддержки процессов передачи информации.

Остальные слои образуют специализированные информационные виртуальные сети (слой 3), образованные специализированными программными системами поддержки решения функциональных задач группы 1 и покрывающие транспортную сеть (V – VII уровни модели OSI).

Пример таких сетей – сети Extranet, использующие в качестве транспортной сеть Internet.

Любой из слоев сети представляется множеством элементов, каждый из которых может быть ресурсосодержащим и ресурсопотребляющим. Схемы информационных потоков представляют собой схемы, связывающие ресурсосодержащие и ресурсопотребляющие элементы для каждого слоя сети. В компьютерной сети можно выделить несколько базовых задач, связанных с обеспечением ее функциональности. К ним относятся задачи: управления сетью и ее элементами, администрирования и мониторинга. Перечисленные задачи решаются в реальном масштабе времени в уже существующей системе.

Повышение эффективности функционирования информационной системы подразумевает в первую очередь повышение эффективности ее управления. Эффективность функционирования системы рассматриваем по отношению к каждому слою в отдельности и ко всей системе в целом. Наиболее правильным является слоевое рассмотрение проблемы. В этом случае эффективность функционирования системы для заданного слоя p характеризуется набором выходных параметров $W^p = (w_1, w_2, \dots, w_n)^p$ и функциональной полнотой управления в смысле обеспечения (покрытия) всех задач управления $\{X_j\}_{j \in X^p}$, $X^p M X^0$, X^0 – полное множество задач, $j=1, \dots, k_p$, k_p – число задач в p -м слое. Для каждой задачи управления X_j существует соответствующий критерий эффективности $Y_j = Y_j(W)$, функционально связанный с W . Пусть система описывается через $X = \{x_i\}$ – параметры состояния (x_i – контролируемые) и каждый выходной параметр $w_i \in W$ функционально связан с векто-

ром параметров состояния, т.е. $w_t = f(X)$. В системе имеются управляемые переменные U , которые могут быть изменены (изменение X достигается через изменение U). Каждое $x_t \in X$ функционально связано с U и имеет в явном или неявном виде аналитическое выражение связи $x_t = x_t(U)$. Базовые задачи могут быть формализованы в терминах параметров и характеристик, описывающих сеть. Такая формализация позволяет сформировать единую концепцию обеспечения эффективности функционирования существующей и проектируемой систем.

3. Управление

Решения задач управления рассматриваются, прежде всего, по отношению к конкретному объекту в сети. Объект должен быть элементом распределенной информационной системы, оказывать косвенное или прямое влияние на ее эффективность, иметь параметры, отражающие его индивидуальные характеристики, и параметры, приводящие к целенаправленному изменению его состояния. Будем выделять (не претендуя на полноту) следующие объекты: ресурсы (R), конфигурацию (C), трафик (T), сервис (A), безопасность (J), базы данных (D), пользователи (U), задачи (X), программы (P), службы (B), $\langle \text{РИУС} \rangle = \{R, C, T, A, J, D, X, U, P, B\}$.

Проблемы управления рассматриваются по отношению к конкретной задаче $X_j, j=1, \dots, k_p$; k_p – число задач системы. Считаем, что система задается набором внутренних управляемых параметров U , контролируемых параметров X , внешних параметров W , набором задач $\{X_j\}$, набором функций, обеспечивающих решение этих задач $\{F_j\}$, критериев оптимальности Y_j . В $[i]$ -й момент система описывается как $(\{X_j\}, \{F_j\}\{Y_j\}, W, X, U) [i]$ или $(\{X_j\}[i], \{F_j\}, \{Y_j\}[i], W[i], X[i], U[i])$.

Тогда для достижения условия оптимальности функционирования системы достаточно обеспечить выполнение условия $Y_j \in O(Y'_j)$ или $Y_j \in O(Y')$, где $O(Y'_j)$ – окрестность оптимального значения критерия Y_j , $O(Y'_j) \in O(Y')$, $O(Y')$ – множество окрестностей оптимальных значений локальных критериев, и найти такое DU , при котором $U[i+1] = U[i] + DU$, $X[i+1] = X(U[i+1])$, $W[i+1] = W(X[i+1])$, $Y_j[i+1] = Y_j(W[i+1])$, $\forall j, j=1, \dots, k_p$; $Y_j[i+1] \in O(Y')$, $U[i]$ – состояние вектора в момент $[i]$.

При управлении распределенной информационной системой будем выделять следующие типовые задачи:

А) управление ресурсами, Б) управление конфигурацией, В) управление трафиком, Г) управление сервисом, Д) управление безопасностью, Е) управление базами данных, Ж) управление пользователями, З) управление задачами, И) управление программами, К) управление службами.

Каждая из типовых задач управления может быть разбита на две подгруппы: первая — установочные задачи; вторая — задачи оперативного управления. Первая подгруппа представлена, в свою очередь, как: а) формирование проблемных задач $\{X_j\}^p \in X^p$, $X^p \subset X^\circ$, где X° — общее множество задач системы, а X^p — группа задач слоя p ; б) формирование критериев Y ; в) формирование показателей качества W , $W_j \in W$; г) формирование параметров состояния X ; д) формирование управляемых параметров U .

Вторая подгруппа представлена пятью задачами: 1) контроль состояния объекта, т.е. контроль $X=(x_1, x_2, \dots, x_n)$ и их оценивание; 2) оценка отклонения текущего состояния объекта от заданного $\text{dist}(X[i], X')$; 3) определение (расчет) состояния системы (X', Y, W) , оптимального с точки зрения некоторого критерия, и системы ограничений, где $Y_j[i+1]=Y_j(W(X'[i+1]))$, $Y_j[i+1] \in O(Y')$, $X'=(x'_1, x'_2, \dots, x'_n)$, $x'_i=x'_i(U)$, $U \in W$, W — ограничения; 4) формирование управляющего воздействия DU , $U[i+1]=U[i]+DU$ для перевода объекта из состояния A в состояние B : $X[i+1]=X(U[i+1])$, $A()=(X[i+1])$, $B()=(X(U[i+1]))$; 5) физическая реализация воздействия $(U[i+1])$ по переводу объекта в заданное состояние.

Таким образом, под функциональностью системы будем понимать обеспечение решения типовых задач $A) - K)$ по отношению к объектам $\{R, C, T, A, J, D, X, U, P, B\}$ при условии, что каждая типовая задача представлена, в свою очередь, задачами $\{a, б, в, г, д; 1, 2, 3, 4, 5\}$. Решение групп задач рассматривается по отношению к каждому слою в отдельности и ко всей сети в целом. Эффективная реализация решения задач управления может быть достигнута только при условии наличия достоверной информации о состоянии системы и безошибочной реализации процедур формирования DU . Поэтому проблемой является также построение и реализация средств контроля за состоянием системы (средств мониторинга).

4. Оценка эффективности сети

Понятие эффективности для сети с учетом сказанного выше рассматриваем только как эффективность сетевых процессов в отдельном слое. Возможен вариант межслоевой оптимизации для всей сети, но в работе он не рассматривается.

Для каждого слоя сети вводим основной параметр — время выполнения фиксированной транзакции. Транзакция — последовательность элементарных операций, требуемых для выполнения макроопераций. Фиксированная транзакция формируется как тестовый набор операций, отражающих специфику функционирования сети по отношению к определенной прикладной задаче.

Задача оптимизации рассматривается на трех уровнях: для отдельного объекта, для отдельного слоя и по всем слоям.

При решении задачи оптимизации для объекта из $\{R, C, T, A, J, D, X, U, P, B\}$ формируем функционал критерия близости текущего значения параметра оптимизации к оптимальному значению. Особенность функционирования объектов в сети связана с тем, что для них нельзя решать оптимизационную задачу по достижению абсолютного оптимума. В сети присутствует множество объектов и в этом случае задача сводится к разрешению компромисса. Предлагается более простое решение (как обычно на практике и делается): вводится значение по параметру оптимизации, которое считается наилучшим (значение вводится администратором сети). Если администратор допускает ошибку при выборе значения, то в соответствии с механизмом управления сервисом в последующем эта ошибка будет устранена. Для выбранного значения вводится интервал допустимых отклонений $\pm Dw$, который позволяет сформировать окрестность оптимальных значений. Оценивается текущее значение и рассчитывается его мера близости с наилучшим $r = \text{dist}(W, W')$. Оптимальным считается значение, при котором $r \leq Dw$. Реальная оценка получается как

$$s = \begin{cases} r/dw - 1, & \text{если } r/dw > 1, \\ 0, & \text{если } r/dw < 1. \end{cases} \quad (1)$$

Оценка параметра r в каждом конкретном случае рассматривается отдельно. Например, это может быть $r = |t' - t[i]|$, если используется в качестве параметра время выполнения транзакции (оптимальное t' и текущее $t[i]$).

Функционал критерия оптимальности для объекта запишется как

$$Y_1 = s = (\text{dist}(W, W')/Dw) - 1 \rightarrow 0 \quad (2)$$

с учетом условий, приведенных выше, или в более простой форме:

$$Y_1 = r = \text{dist}(W, W') \rightarrow 0.$$

При решении задачи оптимизации для слоя возможны два варианта:

– формирование критерия на основе критериальных оценок группы или всех объектов:

$$\Psi_s = \sum_i \sum_j b_{ij} \Psi_{ij} \rightarrow 0, \quad (3)$$

где i – тип группы однородных объектов; j – номер объекта в группе; b_{ij} – весовой коэффициент;

– формирование критерия на основе понятия транзакции

$$Y_s = (t[i] - t')^2 \rightarrow 0. \quad (4)$$

Здесь $t[i]$, t' – время выполнения транзакции, квадрат обеспечивает положительную определенность.

При оптимизации всей сети формируется обобщенный критерий оптимизации на основании функционалов слоев с весовыми коэффициентами

$$Y = a_1 Y_1 + a_2 Y_2 + \dots + a_m Y_m \rightarrow 0, \quad (5)$$

где a_j – весовой коэффициент; Y_p – функционал p -го слоя.

Оптимизацию по всей сети проводить нецелесообразно.

5. Администрирование

Администрирование характеризуется набором задач X управления при отклонении конфигурационных настроечных параметров серверов и системы в целом (регламента) в различных режимах функционирования системы. Будем различать администрирование для штатного и для аварийного режимов.

Состояние системы в штатном режиме администрирования описывается набором X и показателями эффективности W , охватывая контроль состояния каждого ресурса и ресурсосодержащего элемента, контроль распределения прав на ресурсы, контроль бюджетов пользователей и их прав, мониторинг состояния конфигураций, элементов и ресурсов, сетевой анализ и диагностику, контроль доступа и аудит, обеспечение достоверности данных, модификацию конфигурации о маршрутизации и конфигурации настроек сервера.

Задача управления при администрировании в штатном режиме сводится к переустановке прав и бюджетов в соответствии с формируемыми внешними требованиями (заявками) или в соответствии с текущей ситуацией в сети ($X[i]$). Эта задача не требует оперативности и не имеет жестких ограничений на время.

Задача управления в аварийном режиме имеет жесткие ограничения на время ее решения и на сохранение целостности системы в период устранения возмущающего воздействия, она возлагается на администраторов систем и сети.

Для администрирования сформировались три концепции: администрирование для сетей, работающих на платформах операционной системы NetWare 4.x фирмы Novell (протоколы IPX/SPX) [2]; для сетей, работающих на платформах операционной системы Windows NT фирмы Microsoft (протоколы NetBEUI, TCP/IP) [3]; для сетей, работающих на платформах UNIX-подобных операционных систем (протоколы TCP/IP) [3].

Критериальные условия Y_j по оптимизации каких-либо показателей эффективности W_j при администрировании не учитываются для формирования управляющих воздействий, а обеспечивают качественную оценку администрирования за какой-либо период, т.е. $Y_j = Y_j(W[i]) \mid i = i_1, \dots, i_2; [i_1, i_2]$ – период отчетности.

Таким образом, в аварийном режиме изменения DU вносятся администратором в случае нарушения условия $W[i+1] = W(X[i+1])$. В

штатном режиме изменения DU приводят к переходу системы в новое состояние $X[i+1]=X(U[i+1])$, характеризующее новыми значениями $W[i+1]$.

Задачи решаются для каждого слоя в отдельности. Наиболее удачное решение получается, если в системе имеются для каждого слоя администраторы доступа или администраторы задач.

6. Мониторинг

Мониторинг рассматривается как обеспечивающая система для решения задач управления и администрирования. Он позволяет осуществить достоверный сбор данных о состоянии сетевой системы, создать статистические выборки значений контролируемых параметров и отследить динамику изменения выборочных параметров в заданном интервале времени. Фактически мониторинг обеспечивает функции контроля для всех слоев компьютерной сетевой системы. Одним из примеров решения задачи мониторинга является анализ транспортных процессов [1]. Анализ процессов позволяет выявить источники и причины возникновения временных участков, на которых сеть находилась в состоянии частичной потери функциональности, и участков, соответствующих полной потере функциональности. Мониторинг и администрирование позволяют свести к минимуму суммарную величину этих участков.

Основная проблема решения задач мониторинга связана со сложностью проведения в реальном масштабе времени анализа протоколов передачи данных на всех уровнях сетевой модели. В большинстве случаев структуры пакетов и кадров в протоколах сетевых модулей оказываются закрытыми для внешних программ.

Другой проблемой мониторинга является обеспечение полной независимости информационной нагрузки, создаваемой тестовыми процедурами контроля, от существующей наблюдаемой системы.

Системы мониторинга обеспечивают для компьютерной сети контроль управляемых параметров U и параметров состояния X , контроль внешних параметров W и их связь с задачами X_j системы, оценку критериев оптимальности Y_j и накопление статистических выборок по заданному параметру в определенные $[i]$ -е моменты времени.

Существенное упрощение решения задач мониторинга при сборе данных о состоянии транспортной системы для 1-го и 2-го слоев можно достичь, используя средства network management (управление сетевым оборудованием). Технология основана на реализации всех функций оперативного управления интеллектуальными устройствами в сети. Реализация функций осуществляется в фоновом по отношению к основному информационному процессу режиме. На настоящий момент доминируют два стандарта: SNMP (Simple

Network Management Protocol) и DMI (Desktop Management Interface). Оба стандарта перекрывают основные функции мониторинга и управления независимо от типа операционных систем. Стандарт SNMP несколько проще DMI и обеспечивает управление интеллектуальными сетевыми устройствами в локальной сети. Стандарт DMI, обеспечивающий управление серверами и рабочими станциями в сетях любого масштаба, в настоящее время становится базовым стандартом компьютерных систем.

Мониторинг слоев информационных виртуальных сетей решается либо с использованием средств существующих операционных систем сетевых платформ, например, через механизм аудирования, либо с использованием оригинальных инструментальных средств.

7. Выводы

Задачи управления, администрирования и мониторинга сети составляют единое целое и могут быть реализованы в рамках общей постановки задачи. В то же время они должны решаться применительно к каждому слою сети. Следует отметить, что близкие между собой формальные описания решения задач на самом деле предполагают совершенно различные механизмы и процедуры обработки данных. Например, оценка состояния сетевой системы для каждой из базовых задач подразумевает совершенно различную процедуру сбора данных и наполнение информацией.

Литература: 1. *Саенко В.И., Панченко А.В.* Анализ транспортных процессов в локальных сетях// АСУ и приборы автоматики.1998. №108. С.226–234.
2. *Чапелл Л., Хейкс Д.* Анализ локальных сетей NetWare. М.: Лори, 1995. 596 с.
3. *Рули Д. и др.* Сети Windows NT. К.: BHV, 1997. 798 с.

Поступила в редколлегия 10.10.98