УДК 629.735.051:004.7 (043.3)

Нагурный А. А.

ИНФОРМАЦИОННЫЙ КРИТЕРИЙ ПОИСКА НЕШТАТНЫХ СИТУАЦИЙ В СЕТЕВЫХ УЗЛАХ

Нагурний О. О. Інформаційний критерій пошуку нештатних ситуацій у мережних вузлах. Проаналізований стан проблеми виявлення відмов і оперативного відновлення мережних вузлів комутації. Запропонований інформаційний критерій пошуку нештатних ситуацій – відмов, перевантажень, погіршення характеристик мережних сегментів, маршрутів і мережі в цілому. Розроблена стратегія пошуку вузлів з нештатними станами шляхом опитування із змінною частотою.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖНИЙ СЕГМЕНТ, МЕРЕЖНИЙ ВУЗОЛ КОМУТАЦІЇ, НЕШТАТНА СИТУАЦІЯ, ІНФОРМАЦІЙНИЙ КРИТЕРІЙ, ВІДМОВА, ПЕРЕВАНТАЖЕННЯ

Нагурный А. А. Информационный критерий поиска нештатных ситуаций в сетевых узлах. Проанализировано состояние проблемы обнаружения отказов и оперативного восстановления сетевых узлов коммутации. Предложен информационный критерий поиска нештатных ситуаций – отказов, перегрузок, ухудшения характеристик сетевых сегментов, маршрутов и сети в целом. Разработана стратегия поиска узлов с нештатными состояниями путем опроса с переменной частотой.

Ключевые слова: КОРПОРАТИВНАЯ СЕТЬ, СЕТЕВОЙ СЕГМЕНТ, СЕТЕВОЙ УЗЕЛ КОММУТАЦИИ, НЕШТАТНАЯ СИТУАЦИЯ, ИНФОРМАЦИОННЫЙ КРИТЕРИЙ, ОТКАЗ, ПЕРЕГРУЗКА

Nagurnyi O. O. Information criterion for selection of worst-case situations in network nodes. Fault location problem state and efficient network switch recovery is analyzed. Information criterion for selection of worst-case situations – failures, overloads, performance degradation of network segments, routes and network is proposed. Strategy for selection nodes with worst-case states by polling with variable frequency is developed.

Keywords: CORPORATE NETWORK, NETWORK SEGMENT, NETWORK SWITCH NODE, ROUTE, WORST-CASE SITUATION, INFORMATION CRITERION, FAILURE, OVERLOAD

Введение. Одной из важнейших частей информационной инфраструктуры предприятий и организаций являются корпоративные сети передачи данных, которые относятся к системам критичного применения, поскольку выход из строя такой системы фактически означает остановку деятельности всей организации.

Корпоративные сети обладают высокой сложностью в силу территориальной распределенности инфраструктуры, совмещения возможностей собственно передачи данных с возможностями телефонии и видеоконференцсвязи, наличия встраиваемых систем поддержания информационной безопасности, а также резервных и дублирующих элементов, отвечающих за обеспечение надежности и доступности корпоративной сети [1].

Обнаружение отказов и оперативное восстановление относятся к числу сервисов, обеспечивающих высокую доступность (готовность). Управление надежностью и отказоустойчивость опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

Обнаружение отказов и оперативное восстановление может играть по отношению к другим средствам безопасности роль инфраструктурного сервиса, обеспечивая высокую готовность последних. Это особенно важно для межсетевых экранов, средств поддержки виртуальных частных сетей, серверов аутентификации, нормальное функционирование которых критически важно для корпоративной информационной системы в целом.

В корпоративной компьютерной сети любого масштаба необходим постоянный контроль и мониторинг. Нельзя полагаться лишь на внимание системного администратора – необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения об отказах и других проблемах.

Даже случайные сбои аппаратного или программного обеспечения могут привести к серьезным последствиям. Замедление функционирования сетевых сервисов и служб – наименее неприятное из них, хотя и может оставаться незамеченным в течение длительного

времени. Гораздо хуже, когда критично важные службы или приложения полностью прекращают функционирование. Типы же “критичных” служб могут быть весьма разнообразны и для них, соответственно, требуются различные методы мониторинга.

От корректной работы веб-серверов и серверов БД может зависеть работоспособность внутрикорпоративных приложений и важных внешних сервисов для клиентов; сбои и нарушения работы маршрутизаторов могут нарушать связь между различными частями корпорации и ее филиалами; серверы внутренней почты и сетевых мессенджеров, автоматических обновлений и резервного копирования, принт-серверы – любые из этих элементов могут страдать от программных и аппаратных сбоев.

Поскольку полностью исключить возможность отказа или некорректной работы техники невозможно, решение заключается в том, чтобы обнаруживать проблемы на наиболее ранних стадиях, и получать о них наиболее подробную информацию. Для этого, как правило, применяется различное программное обеспечение (ПО) мониторинга и контроля сети, которое способно накапливать статистические данные о стабильности и других параметрах работы серверов, сервисов и служб, доступные для подробного анализа, и своевременно оповещать технических специалистов об обнаруженной проблеме.

Выбор способов и объектов мониторинга сети зависит от множества факторов – конфигурации сети, действующих в ней сервисов и служб, конфигурации серверов и установленного на них ПО, возможностей ПО, используемого для мониторинга и т.п. [2].

В самом общем случае можно говорить о таких элементах системы мониторинга [3]:

– *проверка физической* доступности оборудования;

– *проверка состояния* (работоспособности) служб и сервисов, запущенных в сети;

– *детальный анализ* некритичных, но важных параметров функционирования сети: производительности, загрузки и т.п.;

– *проверка параметров*, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах баз данных, содержимое лог-файлов).

Начальный уровень любой проверки – тестирование физической доступности оборудования (которая может быть нарушена в результате отключения самого оборудования либо отказе каналов связи).

Следующий этап – проверка принципиальной работоспособности критичных служб. Как правило, это означает TCP-подключение к соответствующему порту сервера, на котором должна быть запущена служба, и, возможно, выполнение тестового запроса (например, аутентификации на почтовом сервере по протоколу SMTP или POP или запрос тестовой страницы от веб-сервера).

Помимо времени отклика устройств и служб для различных типов серверов существуют другие принципиально важные проверки: память и загруженность процессора (веб-сервер, сервер баз данных), место на диске (файл-сервер), и более специфические – например, статус принтеров у сервера печати.

Способы проверки этих величин варьируются, но один из основных, доступных почти всегда – проверка по SNMP-протоколу. Помимо этого, можно использовать специфические средства, предоставляемые операционной системой (ОС) проверяемого оборудования.

Наконец, многие окружения требуют специфических проверок – запросов к базам данных (БД), контролирующим работу конкретного приложения; проверка файлов отчетов или значений настроек; отслеживание наличия некоторого специального файла (например, создаваемого при “падении” системы).

Из приведенных выше соображений следует очевидный вывод о необходимости выбора оптимальной программы сбора информации. Критериями оптимизации являются минимальное время опроса, объем данных, которые необходимы для получения достоверной и полной информации о состоянии сети и др.

Стратегия поиска неисправности с использованием информационного критерия. В основе программы опроса лежит определение последовательности проверки элементов контролируемого устройства по максимуму информации о месте неисправности, получаемой на каждом шаге проверки [4].

Последовательность опроса определяется в порядке убывания информации о состоянии объекта

$$I_{\alpha,j+1} = H_{\alpha j} - H_{\alpha,j+1}, \quad \alpha = \left(0,1,...,\alpha_j,...,\alpha_{N-1}\right), \tag{1}$$

где $I_{\alpha,j+1}$ – количество информации о состоянии объекта, полученное на α_{j+1} шаге поиска;

H_{aj} и $H_{\alpha,j+1}$ – средние условные энтропии состояния объекта контроля после α_j и α_{j+1} проверок.

Процесс опроса продолжается до тех пор, пока не будет обнаружен неисправный элемент (энтропия состояния объекта не будет равна (близка) нулю или апостериорная вероятность определения неисправного элемента не будет равна (близка) единице).

Для объектов с последовательным соединением элементов и структурой с несколькими входами и перекрестными связями при равной стоимости проверок и наличии только одной неисправности процедура поиска строится по методу половинного деления на основе использования функции

$$H\left(P\right) = -P\log_2 P - \left(1-P\right)\cdot\log_2\left(1-P\right). \tag{2}$$

Первой следует выбрать проверку элемента под номером *K*, для которого $H(P_k)$ максимальна т.е. $\left|\frac{1}{2} - P_K\right|$ минимальна. Здесь $P_K = \sum_{i=1}^{K} p_i \quad \left(1 \le K \le N-1\right)$, p_i – вероятность неисправности в *i*-ом элементе.

После того, как первая проверка найдена, объект разбивается на две части $b_1, b_2, ..., b_k$ и $b_{K+1}, b_{K+2}, ..., b_N$, вероятности p_i заменяются на

$$\frac{p_i}{P_K}\ \left(1 \le i \le K\right) \quad \text{и} \quad \frac{p_i}{1-P_K}\ \left(K+1 \le i \le N\right).$$

В группе, где обнаружена неисправность, осуществляется аналогичная операция путем контроля элемента *d,* для которого $H(P_d)$ максимальна.

При априорной вероятности *i*-ого элемента p_i, удовлетворяющей соотношению $-K \le \log_2 p_i \le -\left(K-1\right)$, количество проверок, требующихся для установления неисправности этого элемента, меньше или равно *K*.

Для объектов с более сложными внутренними связями поиск неисправного элемента при минимальном количестве опросов может быть осуществлен следующим способом. При заданной функциональной модели объекта контроля и таблицы неисправностей в виде матрицы состояний и выходных параметров проверяемых элементов определяется количество информации, получаемое от контроля каждого элемента. По вычисленным значениям информации составляется последовательность опроса элементов в порядке убывания ее величины.

Численное значение признака (количество условной информации) для определения последовательности поиска имеет вид

$$I_{\alpha_{j+1}} = \left[\frac{m_1}{N} \log_2 \frac{m_1}{N} + \frac{m - m_1}{N} \log_2 \frac{m - m_1}{m} + \frac{m_2}{N} \log_2 \frac{m_2}{N - m} + \frac{N - m - m_2}{N} \log_2 \frac{N - m - m_2}{N - m} \right], \quad (3)$$

где N – число проверяемых функциональных элементов объекта;

m_1 – число единиц в таблице состояний объекта на α_{j+1} шаге контроля относительно m единиц на α_j шаге;

m_2 – число единиц в таблице на α_{j+1} шаге относительно $N - m$ нулей на α_j шаге.

Использование только информационной составляющей для определения последовательности проверок в случае различных их стоимостей (затрат времени) может оказаться недостаточным для достижения минимальной средней стоимости проверок.

Решение может быть найдено за счет максимизации показателя $\gamma_{\alpha_j} = \frac{I_{\alpha_j}}{c_{\alpha_j}}$ отношения информационной составляющей к стоимости на каждом шаге проверки.

Для информационной программы поиска неисправности можно сделать ***следующие выводы.***

1. Последовательность опроса контролируемых элементов в соответствии с принципом получения максимальной информации на каждом шаге проверки обеспечивает достаточно быстрый поиск неисправности за счет минимального количества шагов поиска. Значение среднего времени проверки зависит от распределения значений вероятностей контролируемых элементов.

2. Программа поиска предусматривает одновременную оценку состояния и выходных параметров функциональных элементов объекта как единого целого, что практически выполняется для элемента сети с локально расположенными в нем блоками (для поиска неисправности на втором этапе контроля).

3. Стратегия поиска неисправности учитывается в структуре запросного кода как порядковый номер передачи кода того или иного адреса.

Выбор периодичности контроля. Определим выбор периодичности контроля с позицией минимизации средних потерь из-за затрат на контроль (стоимость каждой проверки равна C_1) и затрат, связанных с простоем аппаратуры с момента её отказа до момента его обнаружения (стоимость единицы времени простоя C_2).

Предположим, что объект проверяется через каждые x единиц времени. Если объект оказал в момент времени t, когда $kx \le t \le (k+1)x$, где $k - k$ -ая проверка, то потери составят

$$C_1(k+1) + C_2[(k+1)x - t].$$

Средние потери равны

$$C_{cp} = \sum_{k+0}^{\infty} \int_{kx}^{(k+1)x} [kC_1 + C_2[(k+1)x - t]dF(t) + C_1,$$

где $F(t)$ – функция распределения времени безотказной работы проверяемого объекта.

Если $F(t) = 1 - e^{-\lambda t}$, где λ - интенсивность отказов, то

$$C_{ср} = \frac{C_1 e^{-\lambda x}}{1-e^{-\lambda x}} + \frac{C_2 x}{1-e^{-\lambda x}} + \frac{C_2}{\lambda} + C_1 \qquad (4)$$

Дифференцируя выражение (4) по x и приравнивая производную к нулю, получим уравнение, связывающее интервал проверки x со средним временем безотказной работы $1/\lambda$ при условии обеспечения минимальных средних потерь $C_{ср\min}$: $e^{\lambda x} - \lambda x = 1 + \lambda \frac{C_1}{C_2}$.

График зависимости $x = f(\frac{1}{\lambda})$ при различных $\frac{C_1}{C_2}$ показан на рис. 1.

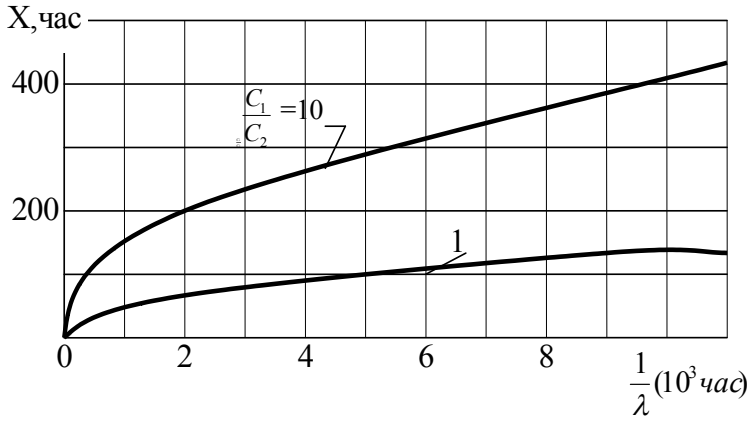

Рис.1. Зависимость частоты проверок от относительной стоимости

Строго периодические графики проверок оказываются оптимальными для систем, отказы в которых подчиняются экспоненциальному распределению с постоянной интенсивностью. В тех случаях, когда известно, что система откажет в заданном интервале времени, можно задать достаточные условия на функцию распределения отказов, при выполнении которых необходимо проводить проверки в конце этого интервала. Если интенсивность отказов возрастает (что свидетельствует о её износе), проверки проводятся с увеличивающейся частотой.

Выводы. Использование стратегии с использованием информационного критерия обеспечивает достаточно быстрый поиск за счет минимального количества шагов и может быть рекомендован на втором этапе определения неисправного блока в найденном отказавшем элементе сети.

Периодичность контроля (частота опроса) определяется характеристиками проверяемого объекта, возможностями системы контроля, потерями из-за простоя аппаратуры от момента её отказа до обнаружения этого отказа. Зависимость частоты опроса от надежности проверяемого элемента при условии обеспечения минимальных средних потерь на условии обеспечения минимальных средних потерь на контроль и затрат из-за простоя показывает: чем выше вероятность появления неисправности, тем чаще должен опрашиваться элемент.

Литература

1. Таненбаум Э. Компьютерные сети / Э. Танненбаум. 4-е изд. – СПб.: Питер, 2003. – 992 с.

2. Andrew S. Tanenbaum, Maarten van Steen. Distributed systems: principles and paradigms. – Pearson Prentice Hall, 2007. - 686 PP.

3. Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление / Бигелоу С. : пер. с англ. – СПб.: БХВ-Петербург, 2005. – 1200 с.

4. Дмитриев В. И. Прикладная теория информации / В. И. Дмитриев. – М.: Высшая школа. – 1989. – 320 с.