УДК 004.728.4 (045)

Коцюр А.Б.,
Дрововозов В.І., к.т.н.

ОРГАНІЗАЦІЯ ВИСОКОПРОДУКТИВНИХ ОБЧИСЛЮВАЛЬНИХ СТРУКТУР В КОМП'ЮТЕРНИХ СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

izdn_0915@ukr.net

Національний авіаційний університет

Розглянуто проблеми організації високопродуктивних обчислювальних структур у комп'ютерних системах критичного застосування, рекомендації з вибору вигляду і структури інформаційно-обчислювальної підсистеми, питання конфігурації мережі центру управління та обробки даних

Ключові слова: високопродуктивна обчислювальна структура, система критичного застосування, інформаційно-обчислювальна підсистема, мережа центру управління та обробки даних.

Вступ

Комп'ютерна система критичного застосування є системою реального часу (СРЧ), особливістю функціонування якої є строго регламентований час реакції на зовнішні події. Іншою важливою особливістю є одночасна обробка даних – навіть якщо одночасно відбувається декілька подій, система повинна встигнути зреагувати на кожну з них протягом критичного інтервалу часу. Тому до систем реального часу пред'являються жорсткі вимоги: максимальний проміжок часу для виконання будь-якої операції має бути відомий заздалегідь і повинен бути узгоджений з вимогами об'єкта управління; потрібно вибудувати пріоритети задач таким чином, щоб кожна з них встигла з реакцією до свого критичного терміну; підтримка передбачуваних механізмів синхронізації дій; одночасна обробка інформації, яка характеризує зміну процесу кількох подій; можливість безвідмовної роботи протягом тривалого часу. Засоби зв'язку в СРЧ мають гарантувати достовірність доставки необхідної для системи інформації в чітко визначений для неї період часу. Тому комп'ютерна мережа є однією з найважливіших частин систем реального часу і має відповідати жорстким вимогам до часових характеристиках, що пред'являються при передачі даних.

При реалізації систем реального часу складною частиною є вирішення проблеми щодо вибору комп'ютерної мережі та технології передачі даних, що забезпечуватиме високу швидкість та продуктивність функціонування таких систем в режимі реального часу.

Передача інформації між різними застосуваннями, використовуваними в системі організації, центру обробки даних, забезпечується корпоративною мережею.

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи і інші структури, що знаходяться на значному видаленні один від одного. Корпоративна мережа організації має досить важливе значення як для забезпечення ефективного функціонування інформаційної системи критичного застосування.

Важливою обчислювальною структурною одиницею системи критичного застосування є центр управління та обробки даних (ЦУОД), з його мережею, яка відособлена від локальних і глобальних мереж. Він зазвичай служить для взаємодії між собою облаштувань зберігання даних, підключених до одного або більше серверам. ЦОД часто характеризується високими швидкостями передачі даних між зовнішніми облаштуваннями зберігання і своєю високо масштабованою ар-

хітектурою.

Вимоги до обчислювальних мереж для комп'ютерних систем критичного застосування

Головною задачею мережі є забезпечення можливості спільного використання ресурсів у реальному часі. Конкретизуємо вимоги стосовно до задачі забезпечення роботи системи критичного застосування, до якої можна віднести автоматизовану систему управління повітряним рухом (АС УПР). У процесі функціонування АС УПР при великих перепадах інтенсивності повітряного руху можуть спостерігатися різкі перепади обсягів інформації, переданої по комп'ютерних мережах.

Продуктивністю мережі визначаються обсяг переданих даних і час, необхідний на їхню передачу. Для оцінки продуктивності мереж загального призначення використовуються загальноприйняті числові характеристики – час реакції мережі, середня пропускна здатність, максимально можлива пропускна здатність, затримка передачі. Стосовно до систем критичного застосування пропускна здатність задається, безпосередньо виходячи з максимальної очікуваної швидкості протікання процесів у системі, що обслуговується. Надалі вона може змінюватися (як правило, убік збільшення) при зміні вимог до системи в цілому. Наприклад, для АС УПР важливим фактором є максимальна очікувана інтенсивність повітряного руху в зоні відповідальності. Однак при цьому час реакції і затримка передачі даних можуть мінятися в широких межах, що неприпустимо при обслуговуванні повітряного руху, особливо при виникненні позаштатних ситуацій. Тому пріоритетними вимогами до обчислювальної мережі є гранично припустимі значення саме часу реакції і затримки передачі даних.

Безпека означає захист від несанкціонованого доступу до даних і забезпечення надійності і стійкість до навмисних впливів, що руйнують.

Розширюваність – це можливість порівняно легкого додавання нових елементів мережі. Для систем критичного застосування висувається додаткова вимога – можливість модифікації мережі в процесі її функціонування, без зниження експлуатаційних характеристик.

Масштабованість – це можливість нарощування розмірів мережі, у тому числі шляхом приєднання додаткових сегментів.

Прозорість означає можливість використання ресурсів мережі тим самим способом незалежно від їхнього фактичного розміщення – на локальному комп'ютері або в мережі. При цьому користувач як би «не зауважує» мережі, працюючи безпосередньо з ресурсами.

Підтримка різних видів трафіка – можливість сполучення функцій різних мереж, наприклад телефонної, зв'язковий і комп'ютерної.

Керованість – можливість централізованого виявлення й усунення збоїв, несправностей, розподілу ресурсів і повноважень між користувачами. Зупинимося на цій задачі докладніше, оскільки для великої просторово розподіленої корпоративної мережі критичного застосування ефективність керування має найважливіше значення.

Для керування корпоративними комп'ютерними мережами, що включають велику кількість активного устаткування, необхідні складні системи керування, що здійснюють моніторинг, контроль і керування кожним елементом комп'ютерної мережі.

Існуючі системи керування, незважаючи на їхню функціональну надмірність, не мають у своєму складі розвитих інтелектуальних засобів, що дозволяють якісно прогнозувати поводження комп'ютерної мережі. Більшість засобів керування в дійсності мережею не керує, а всього лише пасивно здійснює її моніторинг. Вони стежать за мережею, але не виконують активних дій, при цьому фіксуючи тільки факт збою. Ідеальним рішенням була би розробка системи аналізу, прогнозування і локалізації можливих збоїв у роботі як комп'ютерної мережі в цілому,

так і окремих її елементів. Така властивість системи допоможе заздалегідь виявити можливі вузькі місця і вжити заходів по завчасній їхній ліквідації. Однак така система керування практично нереалізована для роботи в умовах критичного застосування. Тому реальним підходом до рішення даної задачі представляється поточна адаптація деяких підсистем системи в цілому до умов застосування, що змінюються, перерозподіл ресурсів мережі для рішення конкретних пріоритетних задач (наприклад, при виникненні екстремальних ситуацій різного характеру). Такий підхід цілком логічний і природній, якщо врахувати, що будь-яка велика корпоративна мережа складається з окремих сегментів, що порівняно слабко впливають один на одного.

Рекомендації з вибору вигляду і структури інформаційно-обчислювальної підсистеми

Систематизуємо вимоги, що пред'являються до обчислювальних пристроїв і комп'ютерних мереж, за допомогою яких забезпечується робота автоматизованих систем керування критичного застосування (АСУ КЗ). Відзначимо, що обсяг вимог до АСУ КЗ як до такій ширше, ніж просто до СРЧ. Основною відмінністю АСУ КЗ від СРЧ є вимога високої надійності і живучості. Під цим маються на увазі не тільки порівняно великий середній час безвідмовної роботи і збереження своїх функціональних можливостей в екстремальних умовах, зокрема, при впливі техногенних, природних і людських факторів. Для АС УПР як системи критичного застосування найважливішою умовою застосування є збереження працездатності (з відповідним обмеженням обсягу і якості розв'язуваних задач) при повних або часткових відмов елементів, вузлів або навіть підсистем, що входять до її складу. Крім того, час відновлення працездатності в повному обсязі повинне бути мінімальним. Цей час визначається вимогами безперервності обслуговування повітряного руху: інтервали видачі команд і обміну даними звичайно складають одиниці або навіть частки секунд. За цей час система повинна перейти на резервний пристрій або підсистему.

Природно, і устаткування, і програмне забезпечення інформаційно-обчислювальної підсистеми – стандартні комп'ютери або сервери, спеціалізовані обчислювачі, мережне устаткування і лінійно-кабельні обладнання, операційні системи і бази даних, спеціалізовані прикладні програми і т.і. – повинні працювати в реальному часі. Швидкодія інформаційно-обчислювальної підсистеми повинна бути такою, щоб вимога обслуговування АС УПР у реальному часі виконувалося при самому інтенсивному навантаженні. У даному випадку мається на увазі максимальна очікувана інтенсивність повітряного руху для даного аеровузла або аеродрому. Необхідно враховувати ту обставину, що обчислювальні і комунікаційні ресурси устаткування зненацька швидко виснажуються через стрімке зростання обсягів нових послуг і додатків. Отже, при впровадженні нових комп'ютеризованих систем необхідно заздалегідь закладати резерви обчислювальних і комунікаційних потужностей і передбачати можливості розширення і нарощування існуючих систем.

Таким чином, основними вимогами до інформаційно-обчислювальної підсистеми АС УПР як системи критичного застосування, є висока надійність і живучість, ремонтопридатність і поновлюваність. Оскільки АС УПР повинна при цьому працювати в реальному часі, першочерговою вимогою до інформаційно-обчислювальної підсистеми є забезпечення необхідної продуктивності при будь-яких запланованих, у тому числі і пікових навантаженнях.

Звичайно, найпростіше й очевидним є рішення задачі «у чоло»: для підвищення надійності використовувати дорогі високонадійні вузли й елементи, резервувати цілі пристрої і лінійки устаткування; для досягнення необхідної продуктивності – експлуатувати систему на граничних режимах. Ясно, що при цьому одні результати іноді будуть досягатися за раху-

нок інших. Тому потрібно використовувати більш тонкі інструменти керування надійністю і якістю системи. У даному підрозділі зупинимося більш докладно на мережних елементах інформаційно-обчислювальній підсистемі, оскільки вони найчастіше є найбільше «вузьким місцем», і саме від них залежить результуюча продуктивність.

Відповідно до прийнятого в дійсні час класифікацій обчислювальних (комп'ютерних) мереж, інформаційно-обчислювальну підсистему АС УПР можна віднести до корпоративних мереж.

Для досягнення необхідної продуктивності, сумісності мережних технологій і протоколів обміну, масштабованості і розширюваності мережі доцільно використовувати підхід, заснований на еталонній моделі взаємодії відкритих систем (*OSI – Open System Interconnection*).

У рамках моделі *OSI* побудова корпоративної мережі АС УПР є найбільш ефективні і наочним, оскільки полегшуються задачі перетворення інформації в процесі обміну. Представимо, що кожен рівень обслуговується найближчим нижнім рівнем (є клієнтом нижнього рівня), а сам, у свою чергу, обслуговує найближчий верхній рівень (є, відповідно, сервером для верхнього рівня). Тоді ми одержимо багатошарову (багаторівневу) модель мережі АС УПР, з багаторазовим використанням технології «сервер-сервер-клієнт-сервер».

При такій організації мережі контроль, керування і модернізація є децентралізованими. Усі ці процедури спрощуються, а ефективність їхнього виконання і надійність системи в цілому підвищуються.

У рамках запропонованої багатошарової моделі легко логічно і технічно обґрунтувати структуру корпоративної мережі АС УПР. Як відомо, у цифрових конвертованих мережах (або мережах нових поколінь – *NGN*) найбільш розповсюдженими є *ATM* і *IP*-технології. Основними достоїнствами протоколу *IP* є його простота і можливість динамічної фрагментації пакетів. Однак протокол *IP*, будучи, по суті, дейтаграмним протоколом, не дає ніяких гарантій доставки повідомлень. Якщо при цьому на якій-небудь ділянці мережі відбулася втрата пакетів, вузли комутації (або маршрутизатори) починають посилати запити своїм сусідам. Навантаження росте дуже швидко і може взагалі паралізувати даний фрагмент мережі, що для умов критичного застосування неприпустимо.

З іншого боку, *ATM*-технологія гарна тим, що є високошвидкісною (швидкості до 622 Мбіт/с) і забезпечує універсальну обробку різнорідного трафіка в гетерогенній мережі. Крім того, *ATM*-технологія забезпечує гарантоване значення *Qo – quality of service* (якість сервісу).

Тому цілком логічним підходом є створення багаторівневої цифрової архітектури мережі виду *IP/ATM/SDH/DWDM*, де *IP – Internet Protocol* (протокол Інтернет); *ATM – Asynchronous Transfer Mode* (технологія асинхронного режиму передачі або переносу пакетів стандартного розміру 53 байта); *SDH – Synchronous Digital Hierarchy* (синхронна цифрова ієрархія); *DWDM – Dense Wave Division Multiplexing* – оптична технологія високої щільності мультиплексування з поділом по довжині хвилі.

Рекомендації по конфігурації мережі центру управління та обробки даних

У зв'язку із збільшенням обсягу та складності вирішуваних завдань в існуючих та перспективних АС УПР необхідно підвищувати продуктивність мережі і впроваджувати систему контролю якості обслуговування на рівні додатків.

З іншого боку збільшення кількості додатків висуває підвищені вимоги до надійності мережі.

Підвищені вимоги до надійності неминуче тягнуть підвищення уваги до захисту мережі від несанкціонованого доступу.

Крім того, найпотужнішим інструментом для вирішення проблем продук-

тивності, якості обслуговування, надійності та захисту є ефективна система управління мережею.

Таким чином, основними пріоритетами при розвитку мережі ЦУОД стають: підвищення продуктивності і масштабованості мережі, впровадження інтелектуальних сервісів для додатків, впровадження ефективної системи управління мережею, посилення захисту мережі, підвищення надійності мережевої інфраструктури.

Рекомендована конфігурація мережі ЦУОД

Відповідно до проведеного аналізу та згідно особливостям функціонування систем критичного застосування та сформульованим вимогам рекомендована наступна конфігурація мережі ЦУОД (рис.1).

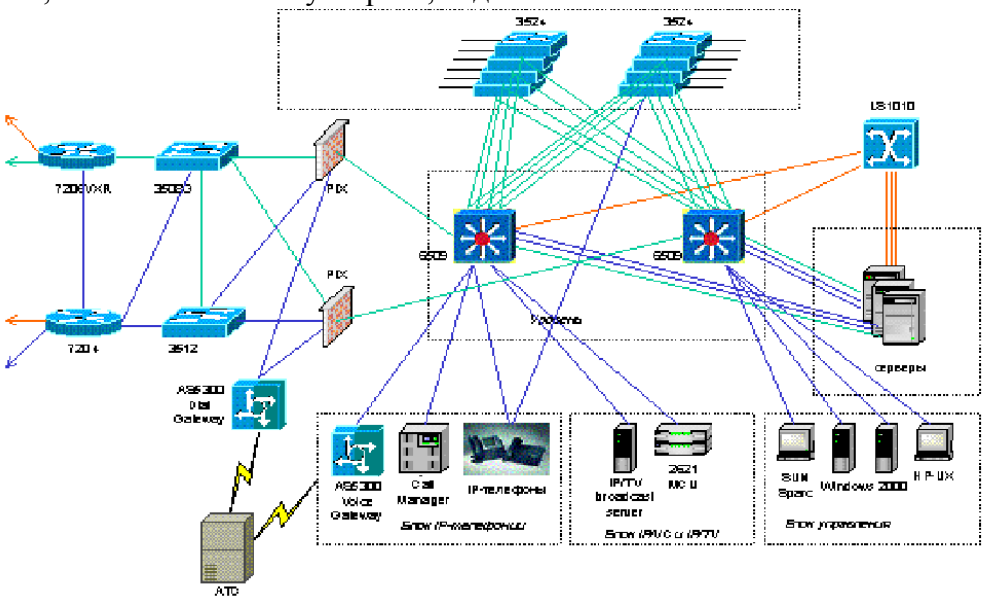

Рис. 1. Конфігурація мережі ЦУОД

Ядро мережі пропонується побудувати на базі двох високопродуктивних багаторівневих комутаторів *Cisco Catalyst* 6509. Пропускна спроможність шини цих комутаторів складає 256 Гбіт/с, а швидкість комутації досягає 150 мільйонів пакетів в секунду. Комутатори будуть обладнані картами маршрутизації в комбінації з модулем управління, що дозволить їм працювати в режимі комутації третього рівня (маршрутизації).

Ці комутатори виконуватимуть завдання високошвидкісної комутації фреймів *Ethernet*, маршрутизації пакетів між віртуальними підмережами (*VLAN*), об'єднання *ATM* і *Ethernet* мереж (*LANE*) і забезпечення якості сервісу для додатків.

Комутатори підключені таким чином, що у разі виходу з ладу будь-якого з них, той, що залишився автоматично бере на себе виконання усіх функцій несправного комутатора. Це дозволяє забезпечити безперервне функціонування ядра мережі.

Внутрішні абоненти повинні підключатися до комутаторів рівня доступу *Cisco Catalyst* 3524. Кожен такий комутатор забезпечує 24 порти *Ethernet* 10/100Мбіт/сек. і 2 порти *Gigabit Ethernet*.

Для забезпечення безперебійної роботи мережі кожен з комутаторів доступу з'єднується з кожним з комутаторів ядра каналами *Gigabit Ethernet*. У разі обриву будь-якого з каналів зв'язку або виходу з ладу одного з комутаторів ядра мережі зв'язок *Catalyst 3524* з ядром здійснюватиметься по резервному каналу.

На рівні доступу не здійснюватиметься ніякій маршрутизації. Головними завданнями комутаторів доступу є: комутація фреймів і підтримка незалежності віртуальних підмереж один від одного.

Підключення кожного сервера здійснюватиметься як мінімум по двох каналах, що дозволить забезпечити велику надійність зв'язку. Для забезпечення зв'язності мережі при виході одного з каналів з ладу передбачається використати протоколи динамічної маршрутизації.

Одним з каналів буде канал існуючої АТМ-мережі, іншим - канал *FastEthernet* або *GigabitEthernet* для високо завантажених каналів.

Канали *Fast* і *Gigabit Ethernet* від серверів підключаються безпосередньо до комутаторів ядра мережі, канали АТМ ОС -3с 155Мбіт/сік підключаються до *LightStream 1010*, який у свою чергу підключається каналами АТМ ОС -12с 622Мбіт/сік до комутаторів ядра мережі.

Видалений доступ до ресурсів можливий двома способами: через маршрутизатори доступу із зовнішніх мереж і по комутованих каналах зв'язку (*Dial - Up*).

Обидва ці шляхи планується контролювати облаштуваннями захисту інформації *Cisco PIX Firewall*. Ці брандмауери сертифіковані по третьому класу захисту і дозволяють значно понизити ризик несанкціонованого доступу.

Доступ із зовнішніх мереж здійснюватиметься через два маршрутизатори доступу. Одним з маршрутизаторів буде використовуваний нині *Cisco 7204*, іншим - *Cisco 7206VXR*, що має достатню продуктивність для обслуговування підключення через гігабітний канал до мережі РАН, що будується. Ці маршрутизатори мають достатні можливості для проведення первинної обробки інформації і завдяки цьому можуть використовуватися разом з *PIX Firewall* для забезпечення захисту інформації.

Для забезпечення видаленого доступу по комутованих каналах планується встановити спеціалізований сервер доступу *Cisco AS5300* з 60 модемами. *Cisco AS5300* повинен підключитися до АТС двома каналами *E1 PRI* і каналами *Fast Ethernet* до *Cisco PIX Firewall* [1-3].

Висновки

В результаті аналізу вимог до обчислювальних структур, що входять до складу систем критичного застосування, встановлено, що для забезпечення ефективного функціонування систем критичного застосування потрібне, по-перше, мати резерв продуктивності обчислювачів, а, по-друге, забезпечувати обмін інформацією між споживачами в реальному часі.

Мережі нових поколінь надзвичайно розширюють можливості інформаційного обміну, особливо в системах критичного застосування. Проте виникає безліч нових проблем. Необхідність поєднання в одних мережевих пристроях і вузлах нових технологій передачі даних з існуючими технологіями вимагає досконалих і дуже складних технологічних і алгоритмічних рішень.

Рекомендації по організації високопродуктивних обчислювальних структур в комп'ютерних системах критичного застосування ґрунтуються на результатах теоретичного аналізу, математичного моделювання і експериментальних досліджень.

Список літератури

1. *Оліфер В.Г., Оліфер Н.А.* Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. 2-е видавництво – СПб.: Пітер, 2003. – 864 с.

2. David Chapman, Andy Fox. Cisco® Secure PIX® Firewalls, Cisco Press, USA, 2001.

3. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с.

Статтю подано до редакції 05.06.2014