"Діагностика локальної мережі" - процес (неперервного) аналізу стану інформаційної мережі. При виникненні несправності мережевих пристроїв фиіксується факт несправності, визначається її місце і вид. Повідомлення про несправність передаєтся, пристрій вимикається і замінюється резервним.

Основних причин незадовільної роботи мережі може бути декілька: пошкодження кабельної системи, дефекти активного устаткування, перевантаженість мережевих ресурсів (каналу зв'язку і сервера), помилки самого прикладного ПЗ. Часто одні дефекти мережі маскують інші. І щоб достовірно визначити, в чому причина незадовільної роботи, локальну мережу потрібно піддати комплексній діагностиці. Комплексна діагностика передбачає виконання таких робіт (етапів).

- Виявлення дефектів фізичного рівня мережі: кабельної системи, системи електроживлення активного устаткування; наявності шуму від зовнішніх джерел.

- Вимірювання поточної завантаженості каналу зв'язку мережі і визначення впливу величини завантаження каналу зв'язку на час реакції прикладного ПЗ.

- Вимірювання числа **колізій** в мережі і з'ясування причин їх виникнення.

- Вимірювання числа помилок передачі даних на рівні каналу зв'язку і з'ясування причин їх виникнення.

- Виявлення дефектів архітектури мережі.

- Вимірювання поточної завантаженості сервера і визначення впливу ступеня його завантаження на час реакції прикладного ПЗ.

- Виявлення дефектів прикладного ПЗ, наслідком яких є неефективне використання пропускної здатності сервера і мережі.

Мережевий адміністратор, на якого найчастіше лягають функції з проведення діагностики, повинен починати вивчати особливості своєї мережі вже на фазі її формування тобто знати схему мережі і докладний опис конфігурації програмного забезпечення із зазначенням всіх параметрів і інтерфейсів. Для оформлення і зберігання цієї інформації підійдуть спеціальні системи документування мережі. Використовуючи їх, системний адміністратор, буде заздалегідь знати всі можливі "приховані дефекти" і "вузькі місця" своєї системи, для того, щоб у разі виникнення нештатної ситуації знати, з чим пов'язана проблема з обладнанням або програмним забезпеченням, пошкоджена програма або до помилки призвели дії оператора.

Мережевому адміністратору слід пам'ятати, що з точки зору користувачів якість роботи прикладного програмного забезпечення в мережі виявляється визначальним. Всі інші критерії, такі як число помилок передачі даних, ступінь завантаженості мережевих ресурсів, продуктивність обладнання і т.д. є вторинними. "Хороша мережа" - це така мережа, користувачі якої не помічають, як вона працює.

У традиційній локальної мережі з розділяючим середовищем передачі аналізатор протоколів або монітор може досліджувати весь трафік даного сегмента мережі.



Малюнок 1.1 - Традиційна локальна мережа з розділяючим середовищем передачі і аналізатором протоколів

Хоча переваги комутованої мережі в продуктивності іноді майже не помітно, поширення комутованих архітектур мало катастрофічні наслідки для традиційних засобів діагностики. У сильно сегментированої мережі аналізатори протоколів здатні бачити тільки одноадресний трафік на окремому порту комутатора, на відміну від мережі колишньої топології, де вони могли ретельно дослідити будь-який пакет в домені колізій. В таких умовах традиційні інструменти моніторингу не можуть зібрати статистику по всіх "діалогах", бо кожна "перемовляючась" пара кінцевих точок користується, по суті, своєю власною мережею.



Малюнок 1.2 - Комутована мережа

У комутованої мережі аналізатор протоколів в одній точці може "бачити" тільки єдиний сегмент, якщо комутатор не здатний дзеркально відображати кілька портів одночасно.

Для збереження контролю над сильно сегментованими мережами виробники комутаторів пропонують різноманітні засоби для відновлення повної "видимості" мережі, однак на цьому шляху залишається чимало труднощів. В поставляючихся зараз комутаторах зазвичай підтримується "дзеркальне відображення" портів, коли трафік одного з них дублюється на раніше незадіяний порт, до якого підключається монітор або аналізатор.

Однак "дзеркальне відображення" має низку недоліків. По-перше, в кожен момент часу видно тільки один порт, тому виявити неполадки, що зачіпають відразу декілька портів, дуже непросто. По-друге, дзеркальне відображення може призвести до зниження продуктивності комутатора. По-третє, на дзеркальному порту зазвичай не відтворюються збої фізичного рівня, а іноді навіть губляться позначення віртуальних локальних мереж. Нарешті, у багатьох випадках не можуть повною мірою дзеркально відображатися повнодуплексні канали Ethernet.

Частковим рішенням при аналізі агрегованих параметрів трафіку є використання можливостей моніторингу агентів mini-RMON, тим більше що вони вбудовані в кожен порт більшості комутаторів Ethernet Хоча агенти mini-RMON не підтримують групу об'єктів Capture із специфікації RMON II, що забезпечують повнофункціональний аналіз протоколів, вони проте дозволяють оцінити рівень використання ресурсів, кількість помилок і обсяг під LGPL.

Деякі недоліки технології дзеркального відображення портів можуть бути подолані установкою "пасивних відгалужувачів", вироблених, наприклад, компанією Shomiti. Ці пристрої являють собою заздалегідь встановлені Y-коннектори і дозволяють відстежувати за допомогою аналізаторів протоколу або іншого пристрою не регенерований, а реальний сигнал.

Наступною актуально проблемою, є проблема з особливостями оптики. Адміністратори корпоративних мереж зазвичай використовують спеціалізоване обладнання діагностики оптичних мереж тільки для вирішення проблем з оптичними кабелями. Звичайне стандартне програмне забезпечення управління пристроями на базі SNMP або інтерфейсу командного рядка здатне виявити проблеми на комутаторах і маршрутизаторах з оптичними інтерфейсами. І тільки деякі мережеві адміністратори стикаються з необхідністю проводити діагностику пристроїв SONET.

Що стосується волоконно-оптичних кабелів, то причин для виникнення можливих несправностей в них істотно менше, ніж у випадку мідного кабелю. Оптичні сигнали не викликають перехресних перешкод, що з'являються від того, що сигнал одного провідника індукує сигнал на іншому - цей фактор найбільш ускладнює діагностичне обладнання для мідного кабелю. Оптичні кабелі несприйнятливі до електромагнітних шумів і індукованих сигналів, тому їх не потрібно розташовувати далеко від електромоторів ліфтів і ламп денного світла, так як із сценарію діагностики всі ці змінні можна виключити.

Сила сигналу, або оптична потужність, в даній точці насправді є єдиною змінною яку потрібно виміряти при пошуку несправностей в оптичних мережах. Якщо ж можна визначити втрати сигналу на всьому протязі оптичного каналу, то можна буде ідентифікувати практично будь-яку проблему. Недорогі додаткові модулі для тестерів мідного кабелю дозволяють проводити оптичні вимірювання.

Підприємствам, які розгорнули велику оптичну інфраструктуру і самостійно її обслуговують, може знадобитися придбання оптичного тимчасового рефлектометра (Optical Time Domain Reflecto-meter, OTDR), що виконує ті ж функції для оптичного волокна, що і рефлектометр для мідного кабелю (Time Domain Reflectometer, TDR). Прилад діє подібно радару: він посилає імпульсні сигнали по кабелю і аналізує їх відображення, на підставі яких він виявляє пошкодження в провіднику або яку-небудь іншу аномалію, і потім повідомляє експерту, в якому місці кабелю слід шукати джерело проблеми.

Хоча різні постачальники кабельних з'єднувачів і роз'ємів спростили процеси терминування та розгалуження оптичного волокна, для цього спочатку потрібно деякий рівень спеціальних навичок, і при розумній політиці підприємство з розвиненою оптичної інфраструктурою змушене буде навчати своїх співробітників. Як би добре не була прокладена кабельна мережа, завжди існує можливість фізичного пошкодження кабелю в результаті якогї-небудь несподіваної події.

При діагностиці бездротових локальних мереж стандарту 802.11b також можуть виникнути проблеми. Сама по собі діагностика, настільки ж проста, як і у випадку мереж Ethernet на базі концентраторів, так як бездротове середовище передачі інформації розділяється між всіма власниками клієнтських радіопристроїв. Компанія Sniffer Technologies першою запропонувала рішення для аналізу протоколів таких мереж з пропускною здатністю до 11 Мбіт / с, і згодом більшість лідируючих постачальників аналізаторів представили аналогічні системи.

На відміну від концентратора Ethernet з дротяними з'єднаннями, якість бездротових клієнтських з'єднань далека від стабільного. Мікрохвильові радіосигнали, що використовуються у всіх варіантах локальної передачі, слабкі і часом непередбачувані. Навіть невеликі зміни положення антени можуть серйозно позначитися на якості з'єднань. Точки доступу бездротової локальної мережі забезпечуються консоллю керування пристроями, і це часто більш дієвий метод діагностики, ніж відвідування клієнтів бездротової мережі і спостереження за пропускною здатністю та умовами виникнення помилок за допомогою портативного аналізатора.

Хоча проблеми синхронізації даних і встановлення пристроїв, що виникають у користувачів персональних цифрових секретарів (PDA), більш природно відповідають завданням групи технічної підтримки, а не обов'язків мережевого адміністратора, неважко передбачити, що в недалекому майбутньому багато таких пристроїв перетворяться з окремих допоміжних засобів, які доповнюють ПК , в повноправних мережевих клієнтів.

Як правило, оператори корпоративних бездротових мереж будуть (або повинні) перешкоджати розгортанню надмірно відкритих систем, в яких будь-який користувач, що знаходиться в зоні дії мережі і володіє сумісною інтерфейсною картою, отримує доступ до кожного інформаційного кадру системи. Протокол безпеки бездротових мереж WEP (Wired Equivalent Privacy) забезпечує аутентифікацію користувачів, гарантію цілісності та шифрування даних, однак, як це зазвичай трапляється, досконала система безпеки ускладнює аналіз причин мережевих неполадок. У захищених мережах з підтримкою WEP фахівці з діагностики повинні знати ключі або паролі, що захищають інформаційні ресурси та контролюючий доступ в систему. При доступі в режимі прийому всіх пакетів аналізатор протоколів зможе бачити всі заголовки кадрів, але у них інформація без наявності ключів буде безглуздою.

При діагностуванні тунельованих каналів, які багато виробників називають віртуальними приватними мережами з віддаленим доступом, виникаючі проблеми аналогічні мають місце при аналізі бездротових мереж з шифруванням. Якщо трафік не проходить через тунельований канал, то причину несправності визначити нелегко. Це може бути помилка аутентифікації, поломка на одній з кінцевих точок або затор в загальнодоступній зоні Internet. Спроба використання аналізатора протоколів для виявлення високорівневих помилок у тунельованому трафіку буде марною тратою сил, тому що зміст даних, а також заголовки прикладного, транспортного та мережевого рівнів зашифровані. Взагалі, заходи, що вживаються з метою підвищення рівня безпеки корпоративних мереж, зазвичай утруднюють виявлення несправностей і проблем продуктивності. Міжмережеві екрани, proxy-сервери і системи виявлення вторгнень можуть додатково ускладнити локалізацію неполадок.

Таким чином, проблема діагностики комп'ютерних мереж є актуальною і в кінцевому рахунку, діагностування несправностей є завданням управління. Для більшості критично важливих корпоративних систем, проведення тривалих відновлювальних робіт не допустимо, тому єдиним рішенням буде використання резервних пристроїв і процесів, здатних взяти на себе необхідні функції негайно після виникнення збоїв. На деяких підприємствах мережі завжди мають додатковий резервний компонент на випадок збою основного, n х 2 компонентів, де n - кількість основних компонентів, необхідне для забезпечення прийнятної продуктивності. Якщо середній час відновлення (Mean Time To Repair, MTTR) досить велика, то може знадобитися ще більша надмірність. Справа в тому, що час усунення несправності передбачити нелегко, а значні витрати протягом непередбачуваного періоду відновлення є ознакою поганого управління.

Для менш важливих систем, резервування може виявитися економічно невиправданим, і в цьому випадку буде доцільно вкладати кошти в найбільш ефективні інструменти (і в навчання персоналу), щоб максимально прискорити процес діагностики та усунення несправностей на підприємстві. Крім того, підтримку певних систем можна довірити стороннім фахівцям, або залучаючи їх на підприємство за контрактом, або користуючись можливостями зовнішніх центрів обробки даних, або звертаючись до провайдерів послуг із супроводу додатків (Application Service Providers, ASP) або провайдерам послуг управління. Крім витрат найбільш значним фактором, що впливає на рішення про звернення до послуг сторонніх організацій, можна вважати рівень компетентності власного персоналу. Мережеві адміністратори повинні вирішити, чи не є деяка конкретна функція настільки тісно пов'язана зі специфічними завданнями підприємства, що від стороннього фахівця не можна буде очікувати більш якісного виконання роботи, ніж це буде зроблено силами службовців компанії.

Майже відразу після того, як були розгорнуті перші корпоративні мережі, надійність яких залишала бажати кращого, виробники і розробники висунули концепцію "самовідновлюючихся мереж". Сучасні мережі, безумовно, надійніше, ніж вони були в 90-х рр., Але не тому, що неполадки стали самоліквідовуватись. Ліквідація збоїв програмного забезпечення та апаратних засобів сучасних мереж все ще вимагають втручання людини, і в найближчій перспективі в такому положенні справ не передбачається ніяких принципових змін. Методи та інструменти діагностики цілком відповідають сучасній практиці і технологіям, але вони ще не досягли такого рівня, який дозволив би значно заощадити час мережевих адміністраторів в їх боротьбі з неполадками мереж і дефіцитом продуктивності.

Інструменти діагностики

Ключовою функцією інструменту діагностики є забезпечення візуального представлення реального стану мережі. Традиційно поставляючі виробниками інструменти візуалізації приблизно відповідають рівням моделі OSI.

Почнемо розгляд з фізичного рівня. Для вирішення проблем на цьому рівні, а також в електричних або оптичних середовищах передачі даних призначені кабельні тестери і спеціалізовані інструменти, такі як тимчасові рефлектометри (Time Domain Reflectometers, TDRs). За більш ніж 15 років інтенсивного розвитку корпоративних локальних мереж у відповідь на потреби професійних мережевих інтеграторів в кабельних тестерах реалізовано безліч функцій, наприклад виконання автоматизованих тестових послідовностей з можливістю друку сертифікаційних документів на підставі результатів тестування. Хоча мережі Ethernet з пропускною здатністю 10 Мбіт / с допускають деякі вільності відносно якості їх прокладки, технології 100BaseT і Gigabit Ethernet з мідним кабелем набагато вимогливіші. Як наслідок, сучасні кабельні тестери досить складні.

У число лідируючих постачальників кабельних тестерів входять компанії Fluke Networks, Microtest, Agilent, Acterna (колишня назва WWG) і Datacom Textron.

Для діагностики проблем на фізичному рівні можна використовувати такі засоби:

1) Роз'єм-заглушку (Hardware loopback) - це роз'єм, який замикає вихідну лінію на вхідну, що дозволяє комп'ютеру передавати дані самому собі. Роз'єм-заглушка використовується при діагностиці обладнання.

2) Розширений тестер кабелю (Advanced cable tester; Cable tester) - спеціальний засіб дозволяє вести моніторинг трафіку мережі і окремого комп'ютера і виявляти певні види помилок, несправний кабель або мережеву плату.

3) Рефлектометр (Time-domain reflectometer) - пристрій, призначений для виявлення дефектів у кабельних лініях локаційним (рефлектометричним) методом. Рефлектометр посилає по кабелю короткі імпульси і виявляє і класифікує розриви, короткі замикання та інші дефекти, також вимірює довжину кабелю і його хвильовий опір і видає результати на екран.

4) Тоновий генератор (Tone generator) - прилад, що генерує в кабелі змінний або безперервний звуковий сигнал, по якому тоновий визначник перевіряє цілісність і якість кабелю. Тоновий визначник - прилад, який визначає цілісність і якість кабелю, на основі аналізу сигналів, що випускаються тоновим генератором.

5) Цифровий вольтметр (Digital voltmeter) - електронний вимірювальни пристрій загального призначення. Вольтметр дозволяє вимірювати напругу струму, що проходить через резистор, і визначати цілісність мережних кабелів.

Для вирішення проблем канального, мережевого і транспортного рівнів традиційним інструментом, який використовується мережевими адміністраторами, є аналізатори протоколів (Protocol analyzer). Ці кошти займаються збором статистики про роботу мережі і визначенням частоти помилок і дозволяють відстежувати і записувати стан об'єктів мережі. Часто мають у своєму складі вбудований рефлектометр.

Недорогі аналізатори зазвичай створюються на основі серійно випускаючихся портативних ПК з використанням стандартних мережевих карт з підтримкою режиму прийому всіх пакетів. Основний недолік аналізаторів протоколів, полягає в тому, що деякі види неполадок на канальному рівні для них залишаються невидимими. Крім того, вони не дозволяють виявити проблеми фізичного рівня в електричних або оптичних кабелях. Разом з тим, з часом в аналізаторах протоколів з'явилася можливість дослідження неполадок прикладного рівня, включаючи транзакції баз даних.

У число лідируючих постачальників аналізаторів протоколів локальних мереж входять Network Associates / Sniffer Technologies, Shomiti, Acterna (прежнее название WWG), Agilent, GN Nettest, WildPackets и Network Instruments.

Третім основним діагностичним інструментом поряд з кабельними тестерами і аналізаторами протоколів є зонд або монітор. Монітор мережі (Network monitor) - програмно-апаратний пристрій, який відстежує мережевий трафік і перевіряє пакети на рівні кадрів, збирає інформацію про типи пакетів і помилок.

 Ці пристрої зазвичай підключаються до мережі на постійній основі, а не тільки у випадку виникнення проблеми та функціонують у відповідності зі специфікаціями віддаленого моніторингу RMON і RMON II. Протокол RMON описує метод збору статистичної інформації про інтенсивність трафіку, помилках, а також про основні джерела і споживачів трафіку. Дані RMON відносяться в першу чергу до канального рівня, тоді як у стандарті RMON II додана підтримка рівнів з третього по сьомий. У протоколі RMON II передбачена можливість збору пакетів або кадрів із збереженням їх у буфер - функція, яка використовується на першому етапі аналізу протоколів. З іншого боку, практично будь-який сучасний аналізатор протоколів збирає більше статистичної інформації, ніж зонд RMON.

Між функціями аналізаторів протоколів і зондами RMON не можна провести чітку межу. Виробники аналізаторів зазвичай рекомендують встановлювати агенти моніторингу та збору даних по всій великої мережі, користувачі ж прагнуть до того, щоб ці розподілені агенти були сумісні з міжнародним стандартом RMON, а не з власним форматом аналізатора. До теперішнього часу постачальники зондів RMON раніше продовжують розробляти свої власні протоколи для програмного забезпечення декодування та експертного аналізу, однак інструменти моніторингу та збору даних, ймовірно, будуть об'єднуватися. З іншого боку постачальники аналізаторів протоколів вважають, що їх програмне забезпечення не призначене для вирішення специфічних завдань RMON, таких, як аналіз трафіку і складання звітів про продуктивність додатків.

Лідируючими постачальниками пристроїв RMON є NetScout, Agilent, 3Com і Nortel. Крім того, виробники комутаторів Ethernet вбудовують підтримку основних функцій RMON в кожен порт. Можна очікувати, що в сучасних умовах найбільш ефективним засобом моніторингу комутованої мережі буде використання наявних на кожному порту вбудованих агентів mini-RMON і доповнення їх можливостей системою з повною реалізацією функцій RMON II або аналізатором протоколів з експертним аналізом.

Ще одним інструментом діагностики є інтегровані діагностичні засоби. Виробники діагностичного обладнання об'єднали функції всіх перерахованих традиційних інструментів в портативних пристроях для виявлення поширених несправностей на декількох рівнях OSI. Наприклад, деякі з цих пристроїв здійснюють перевірку основних параметрів кабелю, відстежують кількість помилок на рівні Ethernet, виявляють дубльовані IP-адреси, здійснюють пошук і підключення до серверів Novell NetWare, а також відображають розподіл в сегменті протоколів третього рівня.

У число лідируючих постачальників інтегрованих діагностичних інструментів входять Fluke Networks, Datacom Textron, Agilent і Microtest. Компанія Fluke кілька років тому представила продукт OptiView Pro, в якому всі компоненти для повномасштабної семирівневої діагностики об'єднані в єдиному портативному пристрої. Фактично Optiview Pro являє собою ПК під управлінням ОС Windows з роз'ємами під плати розширення, де на додаток до вбудованого аналізатору протоколів власної розробки компанії можна встановити інший аналізатор.

Серед програмних засобів діагностики комп'ютерних мереж, можна виділити спеціальні системи управління мережею (Network Management Systems) - централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік, циркулюючому в мережі. Ці системи не тільки здійснюють моніторинг та аналіз мережі, а й виконують в автоматичному чи напівавтоматичному режимі дії з управління мережею - включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.д. Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.

Засоби керування системою (System Management) виконують функції, аналогічні функціям систем управління, але по відношенню до комунікаційного устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку.

Експертні системи. Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі в працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Найпростішим варіантом експертної системи є контекстно-залежна help-система. Більш складні експертні системи являють собою так звані бази знань, що володіють елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron.