ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Комутаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри КС
В.І. Гостєв
(підпис, ініціали, прізвище)

"___" _____2015_ року

Срібна І.М., Сторчак К.П.
(прізвище та ініціали автора)

ЛЕКЦІЯ

з навчальної дисципліни
Комп'ютерні технології вимірювань в телекомунікаціях
(назва навчальної дисципліни)

Тема 5: Етапи процесу діагностики мережі
(номер і назва теми)
Заняття : Етапи процесу діагностики мережі
(номер і назва заняття)

Навчальний час – 2 години.

Для студентів інституту (факультету):
Навчально-науковий інститут
телекомунікації та інформатизації
факультет Інформаційних технологій,
факультет Телекомунікацій

Навчальна та виховна мета:
Ознайомити студентів з етапами діагностики локальної мережі

Обговорено та схвалено на засіданні
кафедри
"28" серпня 2015 року Протокол №1

Київ – 2015

Зміст

Вступ.
1. Організація процесу діагностики мережі
2. Вимірювання утилізації мережі.
3. Вимірювання числа колізій в мережі.
Заключна частина

Л І Т Е Р А Т У Р А

1.Т.И. Иванова Комп'ютерные технологии в телефонии. Эко-Трендз, 2003 г.
2. Бакланов И.Г. Методы измерений в системах связи. – М.: Эко-Трендз, 1999.
3. Бакланов И.Г. Тестирование и диагностика систем святи. – М.: Эко-Трендз, 2001.

Наочні посібники

Схеми.

Завдання на самостійну роботу

1. Приклади систем комп'ютерної телефонії.
2. Особливості і вимоги до побудови систем комп'ютерної телефонії.

Вступ

Перш ніж приступити до опису методики виявлення "прихованих дефектів", ми хотіли б визначитися з термінами: що, власне, розуміється під локальною мережею, діагностикою локальної мережі і яку мережу слід вважати "хорошою".

Дуже часто під діагностикою локальної мережі мають на увазі тестування тільки її кабельної системи. Це не зовсім вірно. Кабельна система є однією з найважливіших складових локальної мережі, але далеко не єдиною і не найскладнішою з погляду діагностики. Крім стану кабельної системи на якість роботи мережі значно впливає стан активного устаткування (мережевих плат, концентраторів, комутаторів), якість устаткування сервера і налаштування мережевої операційної системи. Крім того, функціонування мережі істотно залежить від алгоритмів роботи експлуатованого в ній прикладного програмного забезпечення (ПЗ).

*Під терміном "**локальна мережа**" ми розумітимемо весь комплекс вказаних вище апаратних і програмних засобів; а під терміном "**діагностика локальної мережі**" - процес визначення причин незадовільної роботи прикладного ПЗ в мережі. Саме якість роботи прикладного ПЗ в мережі є визначальним, з погляду користувачів. Всі інші критерії, такі як число помилок передачі даних, ступінь завантаженості мережевих ресурсів, продуктивність устаткування та ін., є вторинними. "Хороша мережа" - це така мережа, користувачі якої не помічають, як вона працює.*

*Основних причин незадовільної роботи прикладного ПЗ в 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. Так, щоб достовірно визначити, в чому причина незадовільної роботи прикладного ПЗ, локальну мережу потрібно піддати комплексній діагностиці. **Комплексна діагностика** допускає виконання наступних робіт (етапів).*

- *Виявлення дефектів фізичного рівня мережі: кабельної системи, системи електроживлення активного устаткування; наявність 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 (накладання сигналів) 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 спроможності сервера і мережі.*

Розглянемо перші чотири етапи комплексної діагностики локальної мережі, а саме: діагностику канального рівня мережі. Немає доцільності розглядати методику тестування кабельної системи мережі, так як її тестування можливо здійснити лише одним натискання клавіши AUTOTEST на кабельному сканері. Іншого способу не існує. При цьому прилад виконає повний комплекс тестів на відповідність кабельної системи мережі вибраному стандарту.

Хотілося б звернути вашу увагу на два моменти, тим більше що про них часто забувають при тестуванні кабельної системи мережі за допомогою сканера.

Режим AUTOTEST не дозволяє перевірити рівень шуму створюваного зовнішнім джерелом в кабелі. Це може бути шум від люмінесцентної лампи, силової електропроводки, стільникового телефону, потужного копіювального апарату та ін. Для визначення рівня шуму кабельні сканери мають, як правило, спеціальну функцію. Оскільки кабельна система мережі повністю перевіряється тільки на етапі її інсталяції (організації), а шум в кабелі може виникати непередбачувано, немає повної гарантії того, що шум виявиться саме в період повномасштабної перевірки мережі на етапі її інсталяції.

При перевірці мережі кабельним сканером замість активного устаткування до кабелю підключаються з одного кінця - сканер, з іншого - інжектор. Після перевірки кабелю сканер і інжектор відключаються, і підключається активне устаткування: мережеві плати, концентратори, комутатори. При цьому немає повної гарантії того, що контакт між активним устаткуванням і кабелем буде такий же хороший, як між устаткуванням сканера і кабелем. Ми неодноразово зустрічалися з випадками, коли незначний дефект вилки RJ-45 не виявлявся при тестуванні кабельної системи сканером, але виявлявся при діагностиці мережі аналізатором протоколів.

В рамках пропонованої методики ми не розглядатимемо методику попереджувальної діагностики мережі. Не ставлячи під сумнів важливість попереджувальної діагностики, відмітимо тільки, що на практиці вона використовується рідко. Найчастіше (хоч це і неправильно) мережа аналізується тільки в періоди її незадовільної роботи. У таких випадках локалізувати і виправити наявні дефекти мережі потрібно швидко.

1. Організація процесу діагностики мережі

Будь-яка методика тестування мережі істотно залежить від засобів, що є у розпорядженні системного адміністратора. В більшості випадків необхідним і достатнім засобом для виявлення дефектів мережі (окрім кабельного сканера) є ***аналізатор мережевих протоколів***. Він повинен

підключатися до того домена мережі (collision domain), де спостерігаються збої, в максимальній близькості до найбільш підозрілих станцій або сервера (див. Правило 3.3, лекція 6).

Якщо мережа має архітектуру з компактною магістраллю (collapsed backbone) і в якості магістралі використовується комутатор, то аналізатор необхідно підключати до тих портів комутатора, через які проходить аналізований трафік. Деякі програми мають спеціальні агенти або зонди (probes), що встановлюються на комп'ютерах, підключених до віддалених портів комутатора. Зазвичай ***агенти*** (не плутати з агентами SNMP) ***є сервісом або задачею, що працює у фоновому режимі на комп'ютері користувача.*** Як правило, агенти споживають мало обчислювальних ресурсів і не заважають роботі користувачів, на комп'ютерах яких вони встановлені. Аналізатори і агенти можуть бути підключені до комутатора ***двома способами***.

При ***першому*** способі (рисунок 5а) аналізатор підключається до спеціального порту (порту моніторингу або дзеркальному порту) комутатора, якщо такий є, і на нього по черзі спрямовується трафік, зі всіх портів комутатора.

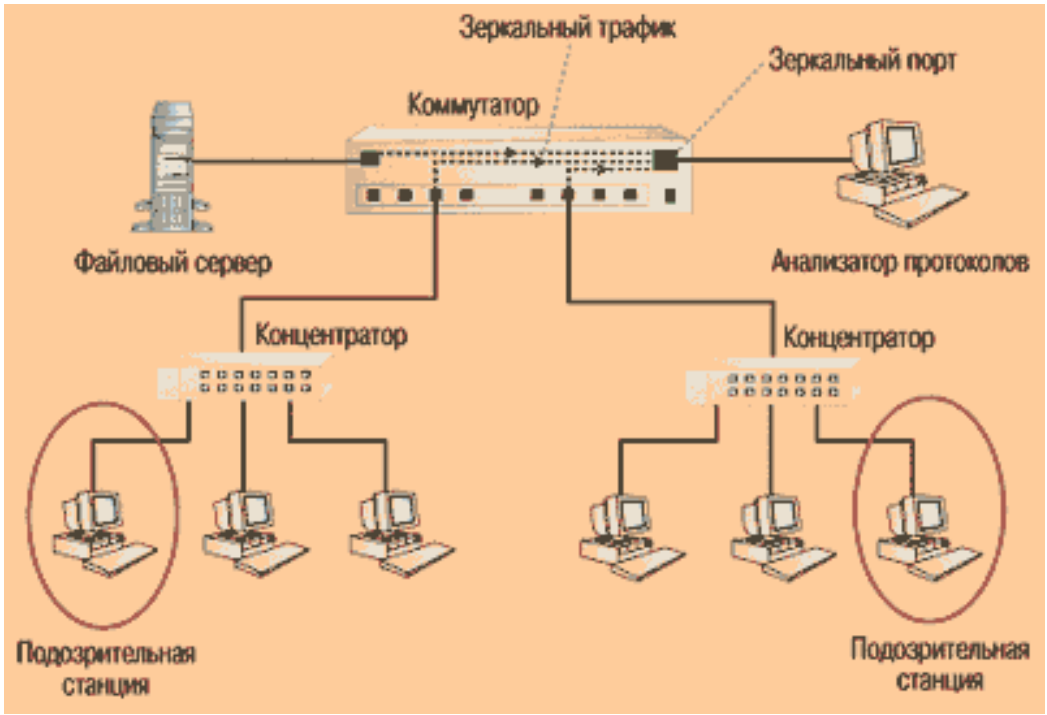

Рисунок 5а - Дзеркальний трафік зі всіх портів комутатора по черзі спрямовується на порт комутатора, до якого підключений аналізатор протоколів

Другий спосіб. Якщо в комутаторі спеціальний порт відсутній, то аналізатор (або агент) слід підключати до портів доменів мережі, що цікавлять, в максимальній близькості до найбільш підозрілих станцій або сервера (рисунок 5б). Іноді це може потребувати використання додаткового

концентратора. Згідно Правилу 3.3 (лекція 6), даний спосіб має перевагу над першим. Виняток становить випадок, коли один з портів комутатора працює в повнодуплексному режимі (тобто дозволяє одночасно передавати інформацію в двох напрямках). Якщо це так, то порт заздалегідь необхідно перевести в напівдуплексний режим (в обох напрямках, але по черзі, а не одночасно).

На ринку є безліч різноманітних аналізаторів протоколів - від чисто програмних до програмно-апаратних. Не дивлячись на функціональну ідентичність більшості аналізаторів протоколів, кожен з них володіє тими або іншими перевагами і недоліками. В зв'язку з цим хотілось би звернути увагу на дві важливі функції, без яких ефективну діагностику мережі провести буде важко.

По-перше, аналізатор протоколів повинен мати вбудовану функцію генерації трафіку (див. Правило 3.4, лекція 6). По-друге, аналізатор протоколів повинен уміти "проріджувати" кадри, що приймаються, тобто приймати не всі кадри підряд, а, наприклад, кожен п'ятий або кожен десятий з обов'язковою подальшою апроксимацією отриманих результатів. Якщо ця функція відсутня, то при сильній завантаженості мережі, якою б продуктивністю не володів комп'ютер, на якому встановлений аналізатор, останній "зависатиме" і/або втрачатиме кадри. Це особливо важливо при діагностиці швидких мереж типу Fast Ethernet і FDDI (розподілений волоконний інтерфейс даних).

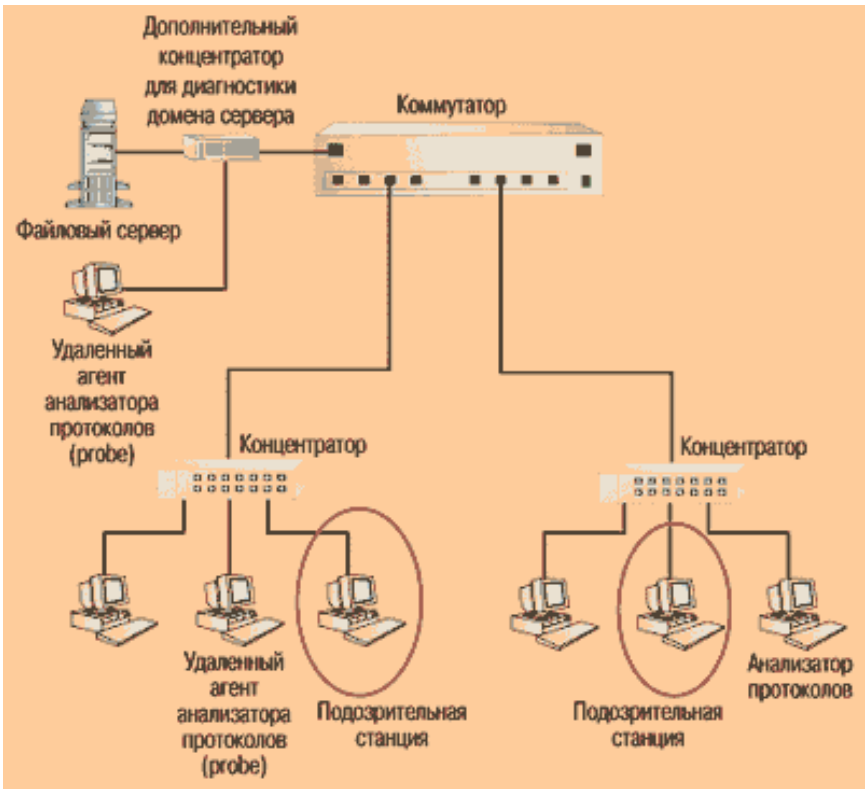

Рисунок 5б - Аналізатор протоколів і віддалені агенти контролюють основні домени мережі. Для діагностики домену сервера використовується додатковий концентратор

Пропоновану методику ілюструватимемо на прикладі використання чисто програмного аналізатора протоколів Observer компанії Network Instruments, що працює в середовищі Windows 95 і Windows NT. На наш погляд, цей продукт володіє всіма необхідними функціями для ефективного проведення діагностики мереж.

Отже, припустимо, що прикладне програмне забезпечення у вашій мережі Ethernet почало працювати повільно, і вам необхідно оперативно локалізувати і ліквідувати дефект.

2. Перший етап - Вимірювання утилізації мережі і встановлення кореляції (зв'язку) між уповільненням роботи мережі і перевантаженням каналу зв'язку

Утилізація каналу зв'язку мережі - це відсоток часу, протягом якого канал зв'язку передає сигнали, або це - частка пропускної спроможності каналу зв'язку, займаного кадрами, колізіями і завадами. Параметр "Утилізація каналу зв'язку" характеризує величину завантаженості мережі.

Канал зв'язку мережі є загальним мережевим ресурсом, тому його завантаженість впливає на час реакції прикладного програмного забезпечення. Першочергове завдання полягає у визначенні наявності взаємозалежності між незадовільною роботою прикладного програмного забезпечення і утилізацією каналу зв'язку мережі.

Припустимо, що аналізатор протоколів встановлений в тому домені мережі (collision domain), де прикладне ПЗ працює повільно. Середня утилізація каналу зв'язку складає 19%, пікова доходить до 82%. Чи можна на підставі цих даних зробити достовірний висновок про те, що причиною повільної роботи програм в мережі є перевантаженість каналу зв'язку? Навряд чи.

Часто можна чути про стандарт де-факто, відповідно до якого для задовільної роботи мережі Ethernet утилізація каналу зв'язку "в тренді" (усереднене значення за 15 хвилин) не повинна перевищувати 20%, а "в піку" (усереднене значення за 1 хвилину) - 35-40%. Приведені значення пояснюються тим, що в мережі Ethernet при утилізації каналу зв'язку, що перевищує 40%, істотно зростає число **колізій** (накладання кадрів) і, відповідно, час реакції прикладного ПЗ. Не дивлячись на те що такі міркування в загальному випадку вірні, безумовне проходження подібним рекомендаціям може привести до неправильного висновку про причини повільної роботи програм в мережі. Вони не враховують особливості конкретної мережі, а саме: тип прикладного ПЗ, протяжність домена мережі, число одночасно працюючих станцій.

Щоб визначити, яка ж максимально допустима утилізація каналу зв'язку у конкретному випадку, рекомендовано використовувати наведені правила.

Правило 1.1 Якщо в мережі Ethernet у будь-який момент часу обмін даними відбувається не більше ніж між двома комп'ютерами, то будь-яка скільки завгодно висока утилізація мережі є допустимою.

Мережа Ethernet влаштована таким чином, що якщо два комп'ютери одночасно конкурують один з одним за захоплення каналу зв'язку, то через деякий час вони синхронізуються один з одним і починають виходити в канал зв'язку строго по черзі. У такому разі колізій між ними практично не виникає.

Якщо робоча станція і сервер володіють високою продуктивністю, і між ними йде обмін великими порціями даних, то утилізація в каналі зв'язку може досягати 80-90% (особливо в пакетному режимі - burst mode). Це абсолютно не уповільнює роботу мережі, а, навпаки, свідчить про ефективне використання її ресурсів прикладним ПЗ.

Таким чином, якщо у вашій мережі утилізація каналу зв'язку висока, постарайтеся визначити, скільки комп'ютерів одночасно ведуть обмін даними. Це можна зробити, наприклад, зібравши і декодувавши пакети в каналі, що представляє інтерес, в період його високої утилізації.

Правило 1.2 Висока утилізація каналу зв'язку мережі тільки в тому разі уповільнює роботу конкретного прикладного ПЗ, коли саме канал зв'язку є "вузькою частиною" для роботи даного конкретного ПЗ.

Окрім каналу зв'язку вузькі місця в системі можуть виникнути через недостатню продуктивність або невірні параметри налаштування сервера, низьку продуктивність робочих станцій, неефективні алгоритми роботи самого прикладного ПЗ.

Якою мірою канал зв'язку відповідає за недостатню продуктивність системи, можна з'ясувати таким чином. Вибравши найбільш масову операцію даного прикладного ПЗ (наприклад, для банківського ПЗ такою операцією може бути введення платіжного доручення), вам слід визначити, як утилізація каналу зв'язку впливає на час виконання такої операції.

Найпростіше це зробити, скориставшись функцією генерації трафіку, що є у ряді аналізаторів протоколів (наприклад, в Observer). За допомогою цієї функції інтенсивність навантаження, що генерується, слід нарощувати поступово, і на її фоні проводити вимірювання часу виконання операції. Фонове навантаження доцільно збільшувати від 0 до 50-60% з кроком не більше 10%.

Якщо час виконання операції в широкому інтервалі фонових навантажень істотно не змінюватиметься, то вузьким мостом системи є не канал зв'язку. Якщо ж час виконання операції істотно мінятиметься залежно від величини фонового навантаження (наприклад, при 10% і 20% утилізацій каналу зв'язку час виконання операції значно розрізнятиметься), то саме канал зв'язку, швидше за все, відповідає за низьку продуктивність системи, і величина його завантаженості критична для часу реакції прикладного ПЗ. Знаючи бажаний час реакції ПЗ, ви легко зможете визначити, якій утилізації каналу зв'язку відповідає бажаний час реакції прикладного ПЗ.

У даному експерименті фонове навантаження не слід задавати більше 60-70%. Навіть якщо канал зв'язку не є вузьким мостом, при таких навантаженнях час виконання операцій може зрости внаслідок зменшення ефективної пропускної спроможності мережі.

Правило 1.3 Максимально допустима утилізація каналу зв'язку залежить від протяжності мережі.

При збільшенні протяжності домену мережі допустима утилізація зменшується. Чим більше протяжність домену мережі, тим пізніше виявлятимуться колізії. Якщо протяжність домену мережі мала, то колізії будуть виявлені станціями ще в початку кадру, у момент передачі преамбули (байту в кадрі, який вказує на початок корисних даних). Якщо протяжність мережі велика, то колізії будуть виявлені пізніше - у момент передачі самого кадру. В результаті накладні витрати на передачу пакету (IP або IPX) зростають. Чим пізніше виявлена колізія, тим більше величина накладних витрат і більший час витрачається на передачу пакету. В результаті час реакції прикладного ПЗ, хоча і трохи, але збільшується.

Висновки. Якщо в результаті проведення діагностики мережі ви визначили, що причина повільної роботи прикладного ПЗ - в перевантаженості каналу зв'язку, то архітектуру мережі необхідно змінити. Число станцій в перевантажених доменах мережі слід зменшити, а станції, що створюють найбільше навантаження на мережу, підключити до виділених портів комутатора.

3. Другий етап - Вимірювання числа колізій в мережі

Якщо дві станції домену мережі одночасно ведуть передачу даних, то в домені виникає колізія. Колізії бувають трьох типів: місцеві, віддалені, пізні.

Колізія це - зіткнення двох або більше кадрів в мережі, що приводить до їх втрати чи спотворення.

Місцева колізія (local collision) - це колізія, що фіксується в домені, де підключений вимірювальний пристрій, в межах передачі преамбули або перших 64 байт кадру, коли джерело передачі знаходиться в домені. Алгоритми виявлення місцевої колізії для мережі на основі витої пари (10BaseT) і коаксіального кабелю (10Base2) відмінні один від одного.

У мережі 10Base2 станція, що передає кадр визначає, що відбулася локальна колізія по зміні рівня напруги в каналі зв'язку (по його подвоєнню). Виявивши колізію, передавальна станція посилає в канал зв'язку серію сигналів про затор (jam), щоб решта всіх станцій домену дізналася, що відбулася колізія. Результатом цієї серії сигналів виявляється поява в мережі коротких, неправильно сформованих кадрів завдовжки менше 64 байт з невірною контрольною послідовністю CRC. Такі кадри називаються фрагментами (collision fragment або runt).

У мережі 10BaseT станція визначає, що відбулася локальна колізія, якщо під час передачі кадру вона виявляє активність на приймальній парі (Rx).

Видалена колізія (remote collision) - це колізія, яка виникає в іншому фізичному сегменті мережі (тобто за повторювачем). Станція дізнається, що відбулася віддалена колізія, якщо вона отримує неправильно оформлений короткий кадр з невірною контрольною послідовністю CRC, і при цьому рівень напруги в каналі зв'язку залишається у встановлених межах (для мереж 10Base2). Для мереж 10BaseT/100BaseT показником є відсутність одночасної активності на приймальній і передавальній парах (Tx і Rx).

Пізня колізія (late collision) - це місцева колізія, яка фіксується вже після того, як станція передала в канал зв'язку перші 64 байт кадру. У мережах 10BaseT пізні колізії часто фіксуються вимірювальними пристроями як помилки CRC.

Якщо виявлення локальних і віддалених колізій, як правило, ще не свідчить про наявність в мережі дефектів, то виявлення пізніх колізій - це явне підтвердження наявності дефекту в домені. Найчастіше це пов'язано з надмірною довжиною ліній зв'язку або неякісним мережевим устаткуванням. Крім високого рівня утилізації каналу зв'язку колізії в мережі Ethernet можуть бути викликані дефектами кабельної системи і активного устаткування, а також наявністю шумів.

Навіть якщо канал зв'язку не є вузьким місцем системи, колізії неістотно, але уповільнюють роботу прикладного ПЗ. Причому основне уповільнення викликається не стільки самим фактом необхідності повторної передачі кадру, скільки тим, що кожен комп'ютер мережі після виникнення колізії повинен виконувати алгоритм «отката» (backoff algorithm): до наступної спроби виходу в канал зв'язку йому доведеться чекати випадковий проміжок часу, пропорційний числу попередніх невдалих спроб.

В зв'язку з цим важливо з'ясувати, яка причина колізій - висока утилізація мережі або "приховані" дефекти мережі. Щоб це визначити, ми рекомендуємо дотримуватися наступних правил.

Правило 2.1 Не всі вимірювальні пристрої правильно визначають загальне число колізій в мережі.

Практично всі чисто програмні аналізатори протоколів фіксують наявність колізії тільки в тому випадку, якщо вони виявляють в мережі фрагмент, тобто результат колізії. При цьому найбільш поширений тип колізій - ***преамбули кадру*** (тобто до початкового обмежувача кадру (SFD)), що відбуваються у момент передачі, - програмні вимірювальні засоби не виявляють, такий вже влаштований набір мікросхем мережевих плат Ethernet. Найточніше колізії виявляють апаратні вимірювальні прилади, наприклад LANMeter компанії Fluke.

Правило 2.2 Висока утилізація каналу зв'язку не завжди супроводжується високим рівнем колізій.

Рівень колізій буде низьким, якщо в мережі одночасно працює не більше двох станцій (див. Правило 1.1) або якщо невелике число станцій одночасно ведуть обмін довгими кадрами (що особливо характерно для пакетного режиму). В цьому випадку до початку передачі кадру станції "видно" несучу в каналі зв'язку, і колізії рідкі.

Правило 2.3 Ознакою наявності дефекту в мережі служить така ситуація, коли невисока утилізація каналу (менше 30%) супроводжується високим рівнем колізій (більше 5%).

Якщо кабельна система заздалегідь була протестована сканером, то найбільш вірогідною причиною підвищеного рівня колізій є шум в лінії зв'язку, викликаний зовнішнім джерелом, або дефектна мережева плата, що неправильно реалізовує алгоритм доступу до середовища передачі (CSMA/CD).

Компанія Network Instruments в аналізаторі протоколів Observer оригінально вирішила задачу виявлення колізій, викликаних дефектами мережі. Вбудований в програму тест провокує виникнення колізій: він посилає в канал зв'язку серію пакетів з інтенсивністю 100 пакетів в секунду і аналізує число виниклих колізій. При цьому суміщений графік відображає залежність числа колізій в мережі від утилізації каналу зв'язку.

Частку колізій в загальному числі кадрів має сенс аналізувати у момент активності підозрілих (повільно працюючих) станцій і лише у разі, коли утилізація каналу зв'язку перевищує 30%. Якщо з трьох кадрів один зіткнувся з колізією, то це ще не означає, що в мережі є дефект.

Правило 2.4 При діагностиці мережі 10BaseT всі колізії повинні фіксуватися як віддалені, якщо аналізатор протоколів не створює трафіку.

Якщо ви пасивно (без генерації трафіку) спостерігаєте за мережею 10BaseT і фізичний сегмент в місці підключення аналізатора (вимірювального приладу) справний, то всі колізії повинні фіксуватися як віддалені.

Якщо проте ви бачите саме локальні колізії, то це може означати одне з трьох:

- фізичний сегмент мережі, куди підключений вимірювальний прилад, несправний;
- порт концентратора або комутатора, куди підключений вимірювальний прилад, має дефект;
- вимірювальний прилад не уміє розрізняти локальні і видалені колізії.

Правило 2.5 Колізії в мережі можуть бути наслідком перевантаженості вхідних буферів комутатора.

Слід пам'ятати, що комутатори при перевантаженості вхідних буферів емулюють колізії, щоб "пригальмувати" робочі станції мережі. Цей механізм називається "Управління потоком" (flow control).

Правило 2.6 Причиною великого числа колізій (і помилок) в мережі може бути неправильна організація заземлення комп'ютерів, включених в локальну мережу.

Якщо комп'ютери, включені в мережу не мають загальної точки заземлення (занулення), то між корпусами комп'ютерів може виникати різниця потенціалів. У персональних комп'ютерах "захисна" земля об'єднана з "інформаційною" землею. Оскільки комп'ютери об'єднані каналом зв'язку локальної мережі, різниця потенціалів між ними приводить до виникнення струму по каналу зв'язку. Цей струм викликає спотворення інформації і є причиною колізій і помилок в мережі. Такий ефект отримав назву ground loop або inter ground noise.

Аналогічний ефект виникає у разі, коли сегмент коаксіального кабелю заземлений більш ніж в одній точці. Це часто трапляється, якщо Т-з′єднувач мережевої плати стикається з корпусом комп'ютера.

Звернемо увагу на те, що установка джерела безперебійного живлення не знімає описаних труднощів. Найбільш детально дані проблеми і способи їх рішення розглядаються в матеріалах компанії APC (American Power Conversion) в "Керівництві по захисту електроживлення" (Power Protection Handbook).

При виявленні великого числа колізій і помилок в мережах 10Base2 перше, що треба зробити, - перевірити різницю потенціалів між обмотками коаксіального кабелю і корпусами комп'ютерів. Якщо її величина для будь-якого комп'ютера в мережі складає більш ніж один вольт по змінному струму, то в мережі не все гаразд з топологією ліній заземлення комп'ютерів.