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 6

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

Тема 5: Етапи процесу діагностики мережі
(номер і назва теми)
Заняття : Лекція №6 Третій етап 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

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.

6.1 Вимірювання числа помилок на канальному рівні мережі

У мережах Ethernet найбільш поширеними є наступні типи помилок.

Короткий кадр - кадр завдовжки менше 64 байт (після 8-байтної преамбули) з правильною контрольною послідовністю. Найбільш ймовірна причина появи коротких кадрів - несправна мережева плата або неправильно конфігурований або зіпсований мережевий драйвер.

Останнім часом спостерігається велике число помилок цього типу на повільнодіючих комп'ютерах (486/SX), що працюють під Windows 95 з мережевими платами NE2000. Причина невідома.

Довгий кадр (long frame) - кадр довше 1518 байт. Довгий кадр може мати правильну або неправильну контрольну послідовність. У останньому випадку такі кадри зазвичай називають jabber. Фіксація довгих кадрів з правильною контрольною послідовністю указує найчастіше на некоректність роботи мережевого драйвера; фіксація помилок типу jabber - на несправність активного устаткування або наявність зовнішніх перешкод.

Помилки контрольної послідовності (CRC error) - вірно оформлений кадр допустимої довжини (від 64 до 1518 байт), але з невірною контрольною послідовністю (помилка в полі CRC).

Помилка вирівнювання (alignment error) - кадр, що містить число бітів, не кратне числу байт.

Відблиски (ghosts) - послідовність сигналів, відмінних по формату від кадрів Ethernet, що не містить розподілювача (SFD) і завдовжки більше 72

байт. *Вперше даний термін був введений компанією Fluke з метою диференціації відмінностей між видаленими колізіями і шумами в каналі зв'язку.*

Відблиски є найбільш підступною помилкою, оскільки вони не розпізнаються програмними аналізаторами протоколів з тієї ж причини, що і колізії на етапі передачі преамбули. Виявити відблиски можна спеціальними приладами або за допомогою методу стресового тестування мережі.

Відповідно до загальноприйнятого стандарту де-факто число помилок канального рівня не повинне перевищувати 1% від загального числа переданих по мережі кадрів. Як показує досвід, ця величина перекривається тільки за наявності явних дефектів кабельної системи мережі. При цьому багато серйозних дефектів активного устаткування, що викликають численні збої в роботі мережі, не виявляються на канальному рівні мережі (див. Правило 3.8).

Правило 3.1. Перш ніж аналізувати помилки в мережі, з'ясуйте, які типи помилок можуть бути визначені мережевою платою і драйвером плати на комп'ютері, де працює ваш програмний аналізатор протоколів.

Робота будь-якого аналізатора протоколів заснована на тому, що мережева плата і драйвер переводяться в режим прийому всіх кадрів мережі (promiscuous mode). У цьому режимі мережева плата приймає всі кадри, що проходять по мережі, а не тільки широкомовні і адресовані безпосередньо до неї, як в звичайному режимі. Аналізатор протоколів всю інформацію про події в мережі отримує саме від драйвера мережевої плати, що працює в режимі прийому всіх кадрів.

Не всі мережеві плати і мережеві драйвери надають аналізатору протоколів ідентичну і повну інформацію про помилки в мережі. Мережеві плати 3Com взагалі ніякої інформації про помилки не видають. Якщо ви встановите аналізатор протоколів на таку плату, то значення на всіх лічильниках помилок будуть нульовими.

EtherExpress Pro компанію Intel повідомляють тільки про помилки CRC і вирівнювання. Мережеві плати компанії SMC надають інформацію тільки про короткі кадри. NE2000 видають майже повну інформацію, виявляючи помилки CRC, коротких кадрів, помилки вирівнювання, колізії.

Мережеві карти D-Link (наприклад, DFE-500TX) і Kingstone (наприклад, KNE 100TX) повідомляють повну, а за наявності спеціального драйвера - навіть розширену, інформацію про помилки і колізії в мережі.

Ряд виробників аналізаторів протоколів пропонують свої драйвери для найбільш популярних мережевих плат.

Правило 3.2. Звертайте увагу на "прив'язку" помилок до конкретних MAC-адрес станцій.

При аналізі локальної мережі ви, напевно, звертали увагу, що помилки зазвичай "прив'язані" до певних MAC-адрес станцій. Проте колізії, події в адресній частині кадру, відблиски, нерозпізнані ситуації типу короткого кадру з нульовою довжиною даних не можуть бути "прив'язані" до конкретних MAC-адрес.

Якщо в мережі спостерігається багато помилок, які не пов'язані з конкретними MAC-адресами, то їх джерелом швидше за все є не активне устаткування. Найімовірніше, такі помилки - результат колізій, дефектів кабельної системи мережі або сильних зовнішніх шумів. Вони можуть бути також викликані низькою якістю або перебоями живлення. Якщо більшість помилок прив'язані до конкретних MAC-адрес станцій, то постарайтеся виявити закономірність між місцезнаходженням станцій, передавальних помилкових кадрів, розташуванням вимірювального приладу (див. Правила 3.3, 3.4) і топологією мережі.

Правило 3.3. В межах одного домена мережі (collision domain) тип і число помилок, протоколів, що фіксуються аналізатором, залежать від місця підключення вимірювального приладу.

Іншими словами, в межах сегменту коаксіального кабелю, концентратора або стека концентраторів картина статистики по каналу може залежати від місця підключення вимірювального приладу.

Багатьом адміністраторам мереж дане твердження може виявитися абсурдним, оскільки воно суперечить принципам семирівневої моделі OSI. Одна і та ж перешкода може викликати фіксацію помилки CRC, відблиску, видаленій колізії або взагалі не виявлятися залежно від взаємного розташування джерела завад і вимірювального приладу. Одна і та ж колізія може фіксуватися як видалена або пізня залежно від взаємного розташування конфліктуючих станцій і вимірювального приладу. Кадр, що містить помилку CRC на одному концентраторі стека, може бути не зафіксований на іншому концентраторі того ж самого стека.

Наслідком наведеного правила є той факт, що програми мережевого моніторингу на основі протоколу SNMP не завжди адекватно відображають статистику помилок в мережі. Причина цього в тому, що вбудований в активне устаткування агент SNMP завжди стежить за тим, з чого складається мережа тільки з однієї точки. Так, якщо мережею є декілька стеків "не інтелектуальних" концентраторів, підключених до "інтелектуального" комутатора, то SNMP-агент комутатора може іноді не бачити частини помилок в стеку концентраторів.

Підтвердження приведеного правила можна знайти на серверах Web компаній Fluke (www.fluke.com) і Net3 Group (www.net3group.com).

Рекомендаціям по дозволу описаного феномена присвячені Правила 3.4 і 3.5.

Правило 3.4. Для виявлення помилок на канальному рівні мережі вимірювання необхідно проводити на тлі генерації аналізатором протоколів власного трафіку.

Генерація трафіку дозволяє загострити наявні проблеми і створює умови для їх прояву. Трафік повинен мати невисоку інтенсивність (не більше 100 кадрів/с) і сприяти утворенню колізій в мережі, тобто містити короткі (<100 байт) кадри.

При виборі аналізатора протоколів або іншого діагностичного засобу увагу слід звернути перш за все на те, щоб вибраний інструмент мав вбудовану функцію генерації трафіку інтенсивності, що задавалася. Ця функція є, зокрема, в аналізаторах Observer компанії Network Instruments і NetXray компанії Cinco (нині Network Associates).

Правило 3.5. Якщо спостережувана статистика залежить від місця підключення вимірювального приладу, то джерело помилок, швидше за все, знаходиться на фізичному рівні даного домена мережі (причина - дефекти кабельної системи або шум зовнішнього джерела). Інакше джерело помилок розташоване на канальному рівні (або вище) або в іншому, суміжному, домені мережі.

Правило 3.6. Якщо частка помилок CRC в загальному числі помилок велика, то слід визначити довжину кадрів, що містять даний тип помилок.

Як ми вже відзначали, помилки CRC можуть виникати в результаті колізій, дефектів кабельної системи, зовнішнього джерела шуму, несправних трансиверів. Ще однією можливою причиною появи помилок CRC можуть бути дефектні порти концентратора або комутатора, які додають в кінець кадру декілька "порожніх" байтів.

При великій частці помилок CRC в загальному числі помилок доцільно з'ясувати причину їх появи. Для цього помилкові кадри з серії треба порівняти з аналогічними справними кадрами з тієї ж серії. Якщо помилкові кадри будуть істотно коротші справних, то це, швидше за все, результати колізій. Якщо помилкові кадри будуть практично такої ж довжини, то причиною спотворення, найімовірніше, є зовнішня перешкода. Якщо ж зіпсовані кадри довше справних, то причина криється, найімовірніше, в дефектному порту концентратора або комутатора, які додають в кінець кадру "порожні" байти.

Порівняти довжину помилкових і правильних кадрів найпростіше за допомогою збору в буфер аналізатора серії кадрів з помилкою CRC.

Правило 3.7. Якщо ви вперше діагностуєте свою мережу і в ній спостерігаються проблеми, то не слід чекати, що у вашій мережі дефектний тільки один компонент.

Таблиця 6.1 систематизує причини помилок і колізій для етапів 2 і 3.

Таблиця 6.1 - Типи помилок і колізій, що фіксуються ВИМІРЮВАЛЬНИМ ЗАСОБОМ

Причина помилок	Локальні колізії	Видалені колізії	Пізні колізії	Короткий кадр	Довгий кадр	Jabber	Помилка CRC
Дефектна мережева плата	>5% при U<30%	>5% при U<30%	Є	Є	Є	Є	Є
Дефектний драйвер плати				Є	Є	Є	Є
Дефектний концентратор, повторитель, трансивер	>5% при U<30%	>5% при U<30%	Є			Є	Є
Неправильне підключення	>5% при	>5% при	Є			Є	

Таблиця 6.1 - Типи помилок і колізій, що фіксуються ВИМІРЮВАЛЬНИМ ЗАСОБОМ							
Причина помилок	Локальні колізії	Видалені колізії	Пізні колізії	Короткий кадр	Довгий кадр	Jabber	Помилка CRC
активного устаткування	U<30%	U<30%					
Дуже довгий кабель			Є				Є
Більше 4 повторювачів або об'єднаних в каскад концентраторів			Є				
Неправильне заземлення комп'ютерів або коаксіального кабелю	>5% при U<30%	>5% при U<30%	Є			Є	Є
Дефекти кабельної системи і пасивного устаткування	>5% при U<30%	>5% при U<30%	Є			Є	Є
Джерело шуму поряд з кабельною системою	>5% при U<30%	>5% при U<30%	Є			Є	Є
Примітка. U - утилізація каналу зв'язку							

Найбільш надійним способом локалізації дефектів є почергове відключення підозрілих станцій, концентраторів і кабельних трас, ретельна перевірка топології ліній заземлення комп'ютерів (особливо для мереж 10Base2).

Якщо збої в мережі відбуваються в непередбачувані моменти часу, не пов'язані з активністю користувачів, перевірте рівень шуму в кабелі за допомогою кабельного сканера. За відсутності сканера візуально переконаєтеся, що кабель не проходить поблизу сильних джерел електромагнітного випромінювання: високовольтних кабелів, люмінесцентних ламп, електродвигунів, копіювальної техніки та ін.

Правило 3.8. Відсутність помилок на канальному рівні ще не гарантує того, що інформація у вашій мережі не спотворюється.

На початку даного розділу вже згадувалося, що вплив помилок канального рівня на роботу мережі сильно перебільшений. Наслідком помилок нижнього рівня є повторна передача кадрів. Завдяки високій швидкості мережі Ethernet (особливо Fast Ethernet) і високій продуктивності сучасних комп'ютерів, помилки нижнього рівня не надає істотного впливу на час реакції прикладного ПЗ.

Ми дуже рідко зустрічалися з випадками, коли ліквідація тільки помилок нижніх (канального і фізичного) рівнів мережі дозволяла істотно поліпшити час реакції прикладного ПЗ. В основному проблеми були пов'язані з серйозними дефектами кабельної системи мережі.

Значно більший вплив на роботу прикладного ПЗ в мережі надають такі помилки, як безслідне зникнення або спотворення інформації в мережевих платах, маршрутизаторах або комутаторах при повній відсутності інформації про помилки нижніх рівнів. Ми вживаємо слово "інформація", оскільки у момент спотворення дані ще не оформлені у вигляді кадру.

Причина таких дефектів в наступному. Інформація спотворюється (або зникає) "в надрах" активного устаткування - мережевої плати, маршрутизатора або комутатора. При цьому прийомо-передавальний блок цього устаткування обчислює правильну контрольну послідовність (CRC) вже спотвореної раніше інформації, і коректно оформлений кадр передається по мережі. Ніяких помилок в цьому випадку, природно, не фіксується. SNMP-агенти, вбудовані в активне устаткування, тут нічим допомогти не можуть.

Іноді окрім спотворення спостерігається зникнення інформації. Найчастіше воно відбувається на дешевих мережевих платах або на комутаторах ETHERNET-FDDI. Механізм зникнення інформації в останньому випадку зрозумілий. У ряді комутаторів ETHERNET-FDDI зворотний зв'язок швидкого порту з повільним (або навпаки) відсутній, в результаті інший порт не отримує інформації про перевантаженість вхідних/вихідних буферів швидкого (повільного) порту. В цьому випадку при інтенсивному трафіку інформація на одному з портів може пропасти.

Досвідчений адміністратор мережі може заперечити, що окрім захисту інформації на канальному рівні в протоколах IPX і TCP/IP можливий захист інформації за допомогою контрольної суми.

Повною мірою на захист за допомогою контрольної суми можна покластися, тільки якщо прикладне ПЗ як транспортного протоколу задіє TCP або UDP. Тільки при їх використанні контрольною сумою захищається весь пакет. Якщо як "транспорт" застосовується IPX/SPX або безпосередньо IP, то контрольною сумою захищається лише заголовок пакету.

Навіть за наявності захисту за допомогою контрольної суми описане спотворення або зникнення інформації викликає істотне збільшення часу реакції прикладного ПЗ.

Якщо ж захист не встановлений, то поведінка прикладного ПЗ може бути непередбачуваною.

Крім заміни (відключення) підозрілого устаткування виявити такі дефекти можна ***двома способами***.

Перший спосіб полягає в захопленні, декодуванні і аналізі кадрів від підозрілої станції, маршрутизатора або комутатора. Ознакою описаного дефекту служить повторна передача пакету IP або IPX, якою не передує помилка нижнього рівня мережі. Деякі аналізатори протоколів і експертні системи спрощують завдання, виконуючи аналіз траси або самостійно обчислюючи контрольну суму пакетів.

Другим способом є метод стресового тестування мережі.

Висновки. Основне завдання діагностики канального рівня мережі - виявити наявність підвищеного числа колізій і помилок в мережі і знайти взаємозв'язок між числом помилок, ступенем завантаженості каналу зв'язку, топологією мережі і мостом підключення вимірювального приладу. Всі вимірювання слід проводити на тлі генерації аналізатором протоколів власного трафіку.

Якщо встановлено, що підвищене число помилок і колізій не є наслідком перевантаженості каналу зв'язку, то мережеве устаткування, при роботі якого спостерігається підвищене число помилок, слід замінити.

Якщо не вдається виявити взаємозв'язку між роботою конкретного устаткування і появою помилок, то треба провести комплексне тестування кабельної системи, перевірте рівень шуму в кабелі, топологію ліній заземлення комп'ютерів, якість живлячої напруги.

6.2 Методика попереджувальної діагностики мережі

Методика попереджувальної діагностики полягає в наступному. Адміністратор мережі повинен безперервно або протягом тривалого часу спостерігати за роботою мережі. Такі спостереження бажано проводити з моменту її установки. На підставі цих спостережень адміністратор повинен визначити:

по-перше, як значення спостережуваних параметрів впливають на роботу користувачів мережі;

по-друге, як вони змінюються протягом тривалого проміжку часу: робочого дня, тижня, місяця, кварталу, року і так далі.

Спостережуваними параметрами зазвичай є:

- ***параметри роботи каналу зв'язку мережі*** - утилізація каналу зв'язку, число прийнятих і переданих кожною станцією мережі кадрів, число помилок в мережі, число широкомовних і багатоадресних кадрів та. ін.;
- ***параметри роботи сервера*** - утилізація процесора сервера, число відкладених (чекаючих) запитів до диска, загальне число кеш-буферів, число "брудних" кеш-буферів і тому подібне.

Знаючи залежність між часом реакції прикладного ПЗ і значеннями спостережуваних параметрів, адміністратор мережі повинен визначити максимальні значення параметрів, допустимі для даної мережі. Ці значення вводяться у вигляді порогів (thresholds) в діагностичний засіб. Якщо в процесі експлуатації мережі значення спостережуваних параметрів перевищать порогові, то діагностичний засіб проінформує про цю подію адміністратора мережі. Така ситуація свідчить про наявність в мережі проблеми.

Спостерігаючи достатньо довго за роботою каналу зв'язку і сервера, ви можете встановити тенденцію зміни значень різних параметрів роботи мережі (утилізації ресурсів, числа помилок і т. п.). На підставі таких спостережень адміністратор може зробити висновки про необхідність заміни активного устаткування або зміни архітектури мережі.

У разі появи в мережі проблеми, адміністратор у момент її прояву повинен записати в спеціальний буфер або файл ***дамп*** (інформацію про стан системи) канальної траси і на підставі аналізу її вмісту зробити висновки про можливі причини проблеми.