Wireshark を利用した専攻共通計算機室ネットワークトラブル対応

○鬼頭良彦 A)、藤原冨未治 A)

A) 工学系技術支援室　情報通信技術系

概要

現在担当している業務の中に専攻共通計算機室の管理がある。共通計算機室は専攻関連の学生、教職員が自由に利用できる Windows パソコンと専攻のメールや Web 等のサーバがセキュリティの関連でローカルの同一ネットワークで運用されている。

その環境下でおきるトラブルでハード関連やログが残るものについては対応が容易であるが、ネットワークの遅延等のログを調査しても原因が特定できないといった場合には対応に時間がかかることがあった。

そのような場合にフリーソフトの Wireshark を利用してパケットキャプチャーを行い、ネットワークの状況を観察することによって原因究明の手掛かりとなることがあるのでその報告をする。

1　はじめに

専攻共通計算機室は Windows Server 2003 と Windows Server 2008 のサーバで管理を行い、クライアントとしては Windows7 が 20 台、WindowsXP が 4 台、Windows2000 が 5 台で学生実験やレポート作成用に自由に利用できる環境となっている。ネットワーク的には全てローカル内で運用されており、同じネットワークに専攻のメールサーバ、Web サーバ等も配置されている。その為、ネットワーク内でおきたトラブルについてはメール等専攻全体に影響を及ぼすので早期の原因究明が必要となる。

2　Wireshark とは

フリーのネットワークアナライザでパソコンベースで簡単に利用ができ、ネットワークに流れるパケットのチェック、またデータを保存しておけば後で詳細分析も可能である。そのためノートパソコンにインストールしておけば様々な場所でネットワークの状況が確認できる。最新バージョンは 1.8.5 で次のサイトからダウンロードが可能である。

Wireshark Web ページ：　http://www.wireshark.org/download.html

3　Wireshark の使用方法

パケットキャプチャを行う場合、ネットワーク全体を観察するか、個別機器の状況を観察するかで別途器具が必要となるが、Wireshark の使用方法は変わらない。ネットワーク全体の場合は HUB に Wireshark をインストールしたパソコンを接続することで観察可能であり、サーバ等の個別機器のアクセス状況を観察したい場合は図 1 のようにパケットのミラーリング可能なスイッチング HUB を利用する。我々のところでは CenterCOM FS808TP V1 という携帯に便利な

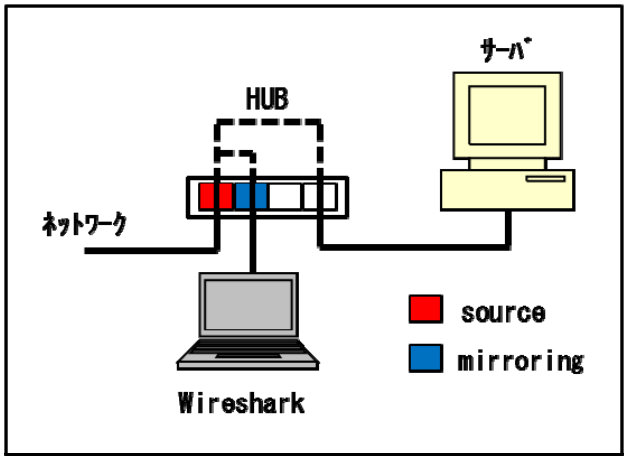

図 1．個別機器のパケット観察

HUB を利用している。

3.1　パケットのキャプチャ方法

Wireshark を起動すると図２の起動画面が表示される。

キャプチャを開始するには起動画面上部メニューの Capture から Options を選択する。Option メニューで図３に表示の項目にチェックをいれて Start ボタンを押すとキャプチャが開始される。チェック項目の説明は次の通りである。

・Capture all in promiscuous mode：NIC に届いたフレームを全てキャプチャする

・Update list of packets in real time：キャプチャしたパケットをリアルタイム表示する。

・Automatic scrolling in live capture：パケット一覧表示を自動的にスクロールする。

・Hide capture info dialog：別画面で表示されるキャプチャ情報画面を非表示にする。

・Enable transport name resolution：プロトコルのポート番号をプロトコル名に変換する。

また、長時間の観察が必要な場合は Capture File の設定を行うことによって保存ファイルの分割を行うことができる。

図４にキャプチャが開始された時の画面を示す。画面上部がパケット一覧部でパケットデータがリアルタイムで表示され、自動スクロールされる。画面中央がパケット詳細部、画面下部がパケットデータ部になる。ある程度キャプチャを行ったところで停止させ、パケット一覧部、詳細部でトラブルのチェックを行う。

図２．Wireshark 起動画面

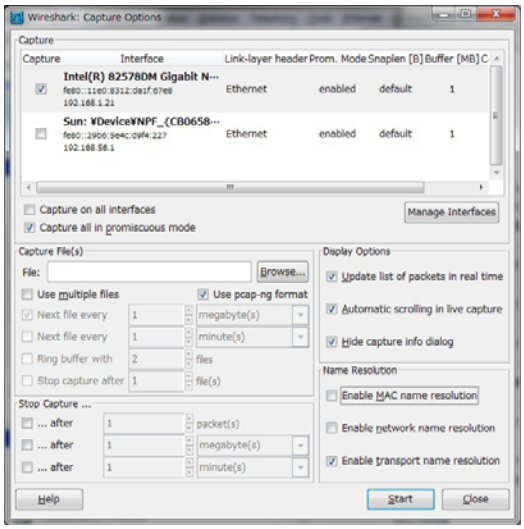

図３．Capture Options 画面

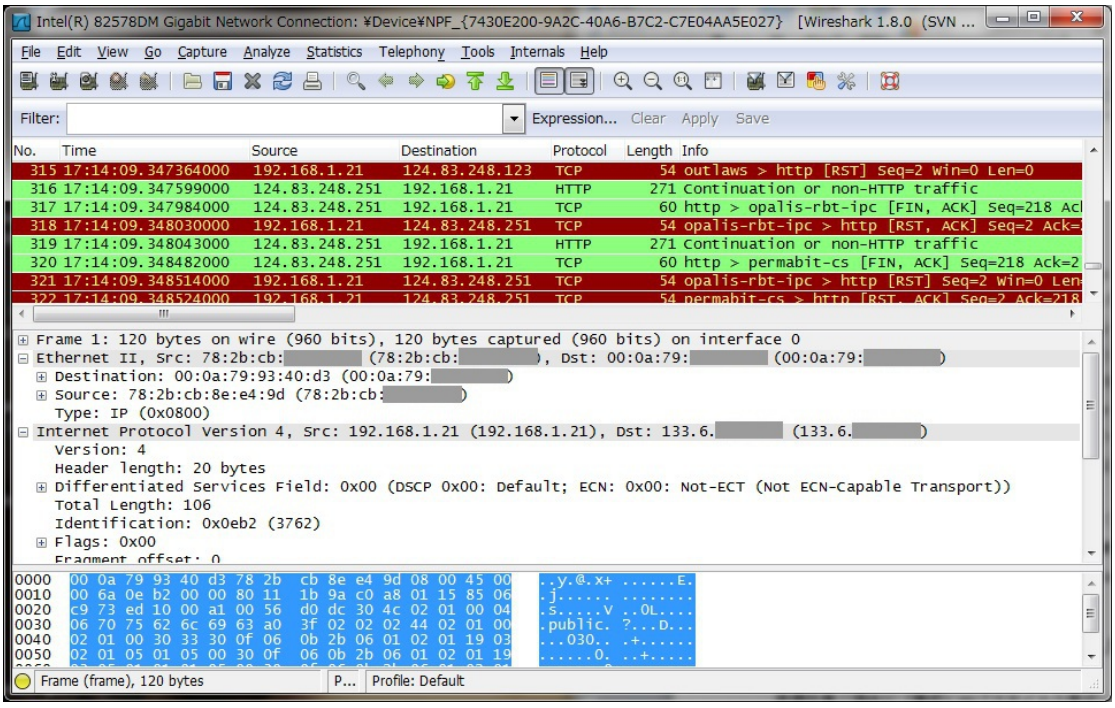

図４．パケットキャプチャ画面

3.2　キャプチャデータの分析方法

分析方法としては分析目的によって手法が違ってくるが、我々のところでは主にトラブル究明のヒントとして利用するため、図４の上部メニューの Statistics から Flow Graph を選択し、データ全体をラダー表示させて通信の流れをチェックしている。図５に Flow Graph 画面を示す。左側に時間、中央部に送受信の方向、右側にコメントが掲載されている。この画面から注目すべきプロトコルや Mac アドレス等があれば図４のメニューの下にある Filter でデータの絞り込みを行い、再度 Flow Graph でチェックを行い、最後に図４中央のパケット詳細部で詳細データのチェックを行う方法をとっている。

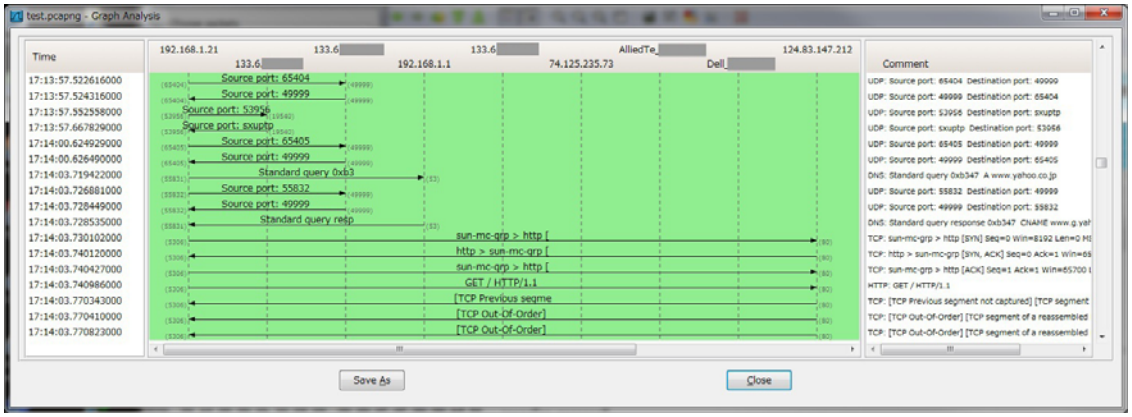

図５．Flow Graph 画面

4　トラブル事例紹介

次に専攻共通計算機室でおきたネットワークトラブルの事例を二つ照会する。

4.1　事例１（ブロードキャストストーム）

専攻のメールや Web へのアクセスができなくなったとの連絡があり、各サーバを調べると稼働はしており、ログにはサーバ間の通信がタイムアウトとなりマウントが切れたとの記録があった。サーバ室のネットワーク機器を調べたが故障が見つからず原因が不明であった。そこで Wireshark でネットワーク上のパケットを調べると図６のように同じパケットが大量に流れており、ブロードキャストストームの状態が確認できた。そこでクライアント室を調べ、異常点滅をしている HUB を停止させるとブロードキャストストームが収まった。原因は HUB の故障と思われたが、調べるとパソコンに接続されていたネットワークケーブルが何らかの理由で外され、HUB に差し戻されていたためブロードキャストストームがおきたと思われる。

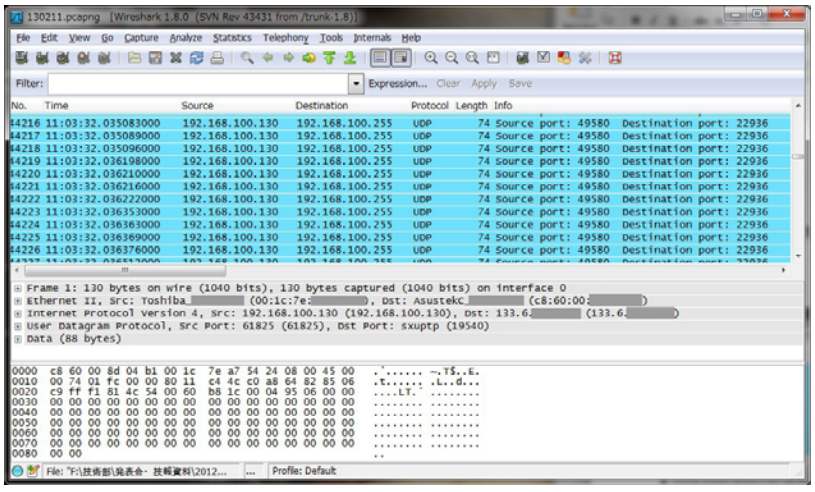

図６．ブロードキャストストーム例

4.2　事例２（Web サーバへのアクセス調査）

専攻 Web サーバはグローバル側にルータを入れて Web サーバはローカルネットワークで運用している。そのルータより同一建物内の同一機器からの定期的アクセスログが排出されたが、ルータの機能として簡易的なログしか排出されずプロトコルのような詳細データは残っていない。そこで状況確認の為、図１で示したミラーリング用 HUB を使用して１日中キャプチャを行いパケットの分析を行った。分析の際に今回はアクセス機器が特定されているので、その Mac アドレスを Filter で絞り込んだ結果、図７のように ARP の問い合わせが１０分間隔程度で定期的に行われていると判明した。

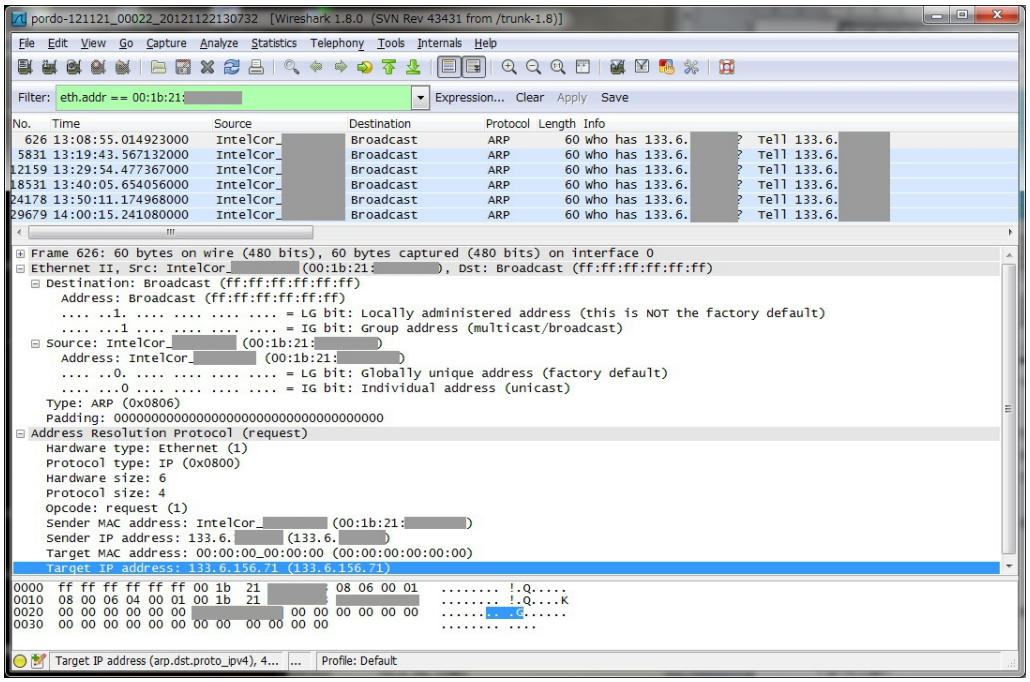

図７．APR の問い合わせ

5　まとめ

ネットワークトラブルの対応はサーバログのチェックで原因が判明する場合が多いが、ログはサーバ等で起きたトラブルの記録のためネットワーク全体に異常が起きた場合には判断が難しい。その場合にネットワークの状況を観察することによって原因が判明する場合があるので、ノートパソコン等にインストールした Wireshark でネットワーク全体か、機器単体のトラブルなのかの切り分けすることによって原因追求が早まる場合もあると思われる。

Wireshark は現在専攻共通計算機室のトラブル時のみに利用しているが機能としては様々な分析が行えるため、Snort 等の監視ソフトとの併用でセキュリティチェックにも利用が可能と思われる。

参考文献

[1]　竹下 恵, “パケットキャプチャ入門－LAN アナライザ Wireshark 活用術”, リックテレコム, 2007.2.15

[2]　竹下 恵, “パケットキャプチャ実践技術－Wireshark によるパケット解析応用編”, リックテレコム, 2009.2.6

[3]　Chris Sanders 著, 高橋基信･宮本久仁男監訳, “実践パケット解析－Wireshark を使ったトラブルシューティング第 2 判”,オライリー・ジャパン, 2012.11.21