

情報ネットワーク論実習（第2回目）

H15,6,25

1. はじめに

前回に引き続き、Ethereal を用いてネットワーク上を流れるパケットの内容を観測し、TCP/IP プロトコルの動作を理解する。

2. ネットワークのモニタ

大学構内サーバのホスト名を指定して ping を実行し、DNS 問合せを観測する(*)。

- ・ 一度キャッシュされるとDNS 問合せは発生せずキャプチャできない。キャプチャに失敗した場合は、ホスト名を変えるか、故意に誤ったホスト名を指定する。
- ・ サーバの例；www.meijo-u.ac.jp , ccant.meijo-u.ac.jp , www-is.meijo-u.ac.jp
- ・ DNS の動き、及びパケットの内容を解析する。

(*)大学外部への ping はファイアウォールで阻止されるため成功しない。

隣人のホスト名を指定して ping を実行し、DNS 問合せおよびARP を観測する。

- ・ クライアントはDNS に登録されていないのでDNS 問合せは不成功に終わる。次に、Windows 固有の問合せシーケンスが走りIP アドレスが解決される。
- ・ 一度キャッシュされるとDNS 問合せ、ARP は発生しない。キャプチャに失敗した場合はホスト名を変える。
- ・ DNS、Windows 問合せ、ARP の動き、及びパケットの内容を解析する。

IE で外部のサイトをアクセスし、WEB アクセスの流れを観測する。

- ・ 外部へのアクセスは必ずプロキシサーバを経由するため、DNS 問合せは発生しない。相手アドレスはプロキシサーバ (IP アドレス ; 202.11.0.9 , ホスト名 ; ccant.meijo-u.ac.jp) となる。ポート番号は 80 ではなく 10080 が使われている。
- ・ TCP の接続手順、パケットの内容などを解析する。

大学構内のサーバを指定して tracert を実行し、その動作をキャプチャする。

- ・ 経路途中に存在するルータのIP アドレスを知ることができる。一部表示されない部分があるが、途中のルータがICMP エラー応答をサポートしていないためと考えられる。
- ・ tracert の動作を解析する。

(*)大学外部への tracert は と同様の理由により成功しない。自宅のPC から tracert を実行してみるとよい。

3. 演習

DNS 問合せのパケットフォーマットを転記し、各フィールドの内容を詳しく説明せよ。

ARP 要求のパケットフォーマットを転記し、各フィールドの内容を詳しく説明せよ。

前回の演習

・ ICMP ECHO のパケットフォーマットを転記し、各フィールドの内容をできるだけ詳しく説明せよ。

