ネットワーク実験レポート

18NC021 *

カトリ　スザン

天気 (1 週目) 曇り, 25 度, 64%
天気 (2 週目) 曇り, 25 度, 60%

*情報通信基礎実験1

Contents

1 目的

LAN を構築することにより、LAN で用いられるケーブルや機器などの構成要素と機能を理解する。インターネットで使用される TCP/IP プロトコルについて、LAN で用いられるプロトコルの概要を理解する。
また、PC のコマンドなどを用いて、ネットワークの動作状態の確認やトラブルシューティングの方法を理解する。

2 実験 1 LAN ケーブルの作成

2.1 実施事項

- ストレートケーブルの作成

LAN ケーブルを作る作業を体験し、UTP ケーブル内の 4 ペアのツイストの状態と RJ45 プラグを観察することでレイヤ 1 の仕様の概略を理解する。

2.2 使用機器類と構成

CAT5e ケーブル、RJ45 プラグ、プラグブーツ、ニッパー、ストリッパー、圧着工具、ケーブルテスタ

2.3 実施手順

この実験の中で PC をスイッチに接続するために用いるストレートケーブルを作成する。図 1 のように T568B の仕様のピン結線で、CAT5e ケーブルの両端に RJ45 プラグを取り付ける。プラグのピンに対して誤った配線をするとプラグを切り捨てて再度作り直しとなるので、圧着する前に十分に確認すること。
ケーブル先端の撚りをとる長さは、プラグの中で 13mm 程度である。ケーブルのスリーブはプラグの中に収まり、プラグのストッパーの爪により押さえられることを確認する。出来上がったケーブルは、ケーブルテスタで導通とワイヤのペアが正しいことを確認する。ペアが異なると直流では通電するが、LAN ケーブルとしては正常に動作しない。

3 実験 2 Switch を使用した LAN の構築

3.1 実施事項

- ケーブルと機器の接続
- IP アドレスの設定
- ネットワークの動作状態の確認

小規模な LAN を構築するときの装置構成、IP アドレスの設計と設定方法を理解する。また、ネットワークの動作状態の確認方法を理解する。

3.2 使用機器類と構成

switch、PC4 台、作成したストレートケーブル

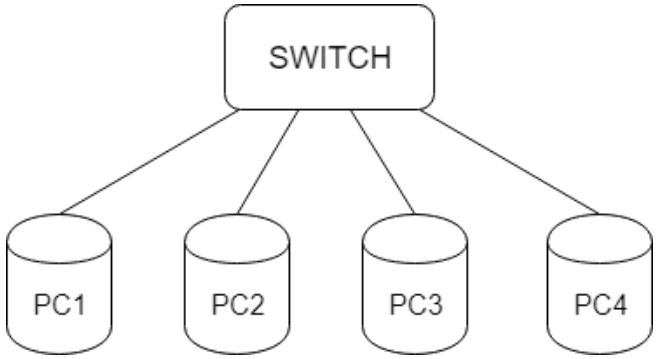

図 1: 実験1回路図

3.3 実施手順

1. ケーブルと機器の接続
   図 1 のように、switch にストレートケーブルを用いて PC と接続する。switch のリンクインジケータが点灯していることを確認する。

2. IP を用いて通信を行うときには、PC などのホストに IP アドレスを付与する必要がある。IP アドレスは手作業で固定的に設定する方法と動的に割り当てて設定する方法がある。現在では DHCP で自動的に設定することが多いが、実験では IP アドレスを手作業で設定する。

   - ホストアドレスとサブネットマスクを各 PC に割り当てる。実験ではクラス C ネットワークの LAN を作るので、次の1つのネットワークアドレスを用いる。ネットワークアドレス　192.168.x.0 サブネットマスク 255.255.255.0
     PC のホストアドレス 192.168.x.1 からホスト部に増加して各 PC に付与
     * ここで、第 3 オクテッドの x は、実験グループごとに割り当てる番号とする。
   - PC のホストアドレスとサブネットマスクを表 1 に記入する。
   - IP アドレスとサブネットマスクを PC に設定する。

   画面左下の［スタートボタン］を右クリックし、［ネットワーク接続］を選択する。
   次に、［ローカルエリア接続 注］のデバイスを右クリックし、［プロパティ］を選択する。
   * 注 :［ローカルエリア接続］は、PC によっては［イーサネット］や［Ethernet］などで表示される。
   ［インターネットプロトコルバージョン4 (TCP/IPv4)］をクリックして選択し、［プロパティ］をクリックする。
   ［次の IP アドレスを使う］にチェックして、IP アドレスの情報を入力する。
   設定の後に、［OK］をクリックして各ウィンドウを閉じる。

3. 設定した IP アドレス情報と MAC アドレスの確認コマンドプロンプトからコマンドを入力して、設定された IP アドレス情報と MAC アドレスを確認する。

   - スタートボタン］を右クリックし、［コマンドプロンプト］を選択してコマンドプロンプトを起動する。
   - prompt コマンドを入力し、プロンプトの表示を時間と PC 名に変更する。　プロンプトを表示させてからコマンドを入力すると、時間が表示されるので記録が整理しやすい。

     C:\Windows> prompt TSPC18GS
     20:12:11.51 PC18>

   - コマンドプロンプトから次のコマンドを入力し、設定された IP アドレス情報と MAC アドレスを確認する。表示された MAC アドレスを表 1 に記入する。

     C:\>ipconfig /all

     表示例　物理アドレス‥‥:00-16-26-F6-1C-30
     IPv4 アドレス‥‥:192.168.1.1
     サブネットマスク‥‥:255.255.255.0

表 1: 各 PC のアドレス情報の値

PC	MAC アドレス	IP アドレス (ホスト)	サブネットマスク
PC1	B0-99-28-D8-11-88	192.168.1.2	255.255.255.0
PC2	E4-7F-B2-11-C3-B8	192.168.1.3	255.255.255.0
PC3	E4-7F-B2-11-C3-77	192.168.1.4	255.255.255.0
PC4	B0-99-28-D8-11-71	192.168.1.5	255.255.255.0

4. ネットワークの動作状態の確認 PC コマンドなどを用いてネットワークの動作確認を行い、その結果を理解する。リンクインジケータ (LED) の点灯を確認することで、レイヤ1の物理的な接続を確認できる。PC から ping コマンドを実行することで、ICMP によるレイヤ3の IP アドレスによる接続の清浄性を確認できる。

   - 各 PC について、LAN への接続状態を確認して表 2 に記入する。
   - ping コマンドをループバックアドレスの 127.0.0.1 に対して実行し、PC の TCP/IP プロトコルが正常に動作していることを確認する。その結果を表3に記入する。

表 2: 各 PC についての接続状態の確認結果

PC	switch/PC のリンクインジケータ (LED) の点灯有無	ループバックへの ping 結果
PC1	有	< 1ms
PC2	有	< 1ms
PC3	有	< 1ms
PC4	有	< 1ms

   - 他の PC に対する ping 結果の確認について、表 3 に記入する。

表 3: 他の PC への接続性の確認結果

下は操作する PC		PC1	PC2	PC3	PC4
PC1	ping	< 1ms	< 1ms	< 1ms	< 1ms
	HTTP	成功	成功	成功	成功
PC2	ping	< 1ms	< 1ms	< 1ms	< 1ms
	HTTP	成功	成功	成功	成功
PC3	ping	< 1ms	< 1ms	< 1ms	< 1ms
	HTTP	成功	成功	成功	成功
PC4	ping	< 1ms	< 1ms	< 1ms	< 1ms
	HTTP	成功	成功	成功	成功

   ブラウザを用いた HTTP による接続の確認により、アプリケーション層まで正常に動作していることが確認できる。

   - ブラウザで他の PC に IP アドレスを指定してアクセスする。HTTP アクセスの成否を確認し、結果を表 3 の HTTP の欄に記入する。
     なお、ブラウザは受け取った情報をキャッシュしてしまい、古い情報や状態を表示し続けることが多いので、F5 を押下するかブラウザを再起動するなどして最新の状態を表示させる。
   - 各 PC で HTTP サーバが起動していない場合は、スタートメニューかデスクトップのアイコンから、HTTP サーバソフトウェアの Apache を起動する。ディスプレイの右下の Apache のアイコンを右クリックし、さらに右クリックをして［Start］を選択して Apache を起動する。

4 実験 3 撚りを解いたケーブルでの通信

4.1 実施事項

- 撚りを解いたケーブルでの通信状態を観察する。

撚りを解いたケーブルの不安定な通信状態と LAN の規格に対して通信可能な距離が短いなどの通信に与える影響を観察して、ツイストペアケーブルの撚りの効果を確認する。

4.2 使用機器類と構成

PC(PC19)、撚りを解いたケーブル (3m, 5m)、100m ストレートケーブル
ケーブル延長アダプタ (ストレートアダプタ、クロスアダプタ)
リンクインジケータ (LED) のない PC の場合は、PC 間に Switch を入れて観察する。

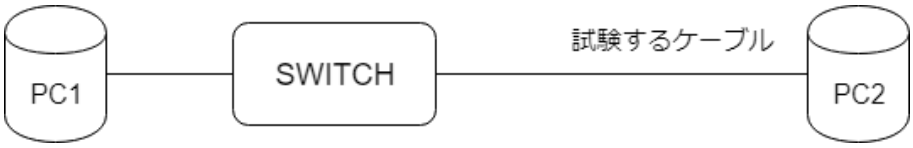

図 2: 実験1回路図

4.3 実施手順

1. IP アドレスの設定の確認
   2 台の PC に設定された IP アドレスとサブネットマスクを確認する。設定については、4.2 を参照のこと。

2. 撚りを解いたケーブルでの通信状態の観察

   - PC 同士を試験するケーブルで接続し、リンクインジケータや ping の結果を用いて通信状態を観察する。

   測定結果を表 4 に記入し、ケーブルの長さと通信の可否などを確認する。結果がケーブルの位置などの状態や PC の個体差により変化するので、複数回試みて不安定な状況や点灯するインジケータの表示の仕方の違いなどを観察して記録する。
   正常なツイストペアケーブルの通信可能な距離を 100BASE-TX の規格を調べて比較する。

表 4: 撚りを解いたケーブルでの通信状態の観察結果

ケーブル長	リンクインジケーターの点灯有無	ping 動作結果	ping 応答がある時の最大時間
3m	時々点灯	失敗	-
5m	時々点灯	失敗	-
10m	時々点灯	失敗	-
100m ツイスト	有	成功	$<$ 1ms

5 実験 4 パケットのモニタリング

5.1 実施事項

- 実験 4 パケットのモニタリング･実施事項
- ARP と ICMP の動作確認

パケットキャプチャソフトを用いてパケットをモニタすることで、フレームとパケットのフォーマットの仕様を確認する。また、フレームとパケットの動きをモニタして TCP/IP 通信のプロトコルの概略を理解する。

5.2 使用機器と構成

パケットキャプチャソフト、Switch、PC 4台

5.3 実施手順

ここでは、Ethernet で実行される ARP の動作と ping コマンドによる ICMP の動作を確認する。また、時間に余裕があれば、HTTP の動作も確認するとよい。

1. IP アドレスの設定の確認
   PC に設定された IP アドレスとサブネットマスクを確認する。設定については、4.2 を参照。
2. モニタリングの準備 windows のプロトコルが TCP/IP の実験のモニタリングの邪魔をしないように windows のプロトコルの動作を止めておく。
   - 左下の [スタートボタン] を右クリックし、[ネットワーク接続] を選択する。
     次に、[ローカルエリア接続] のデバイスを右クリックし、[プロパティ] をクリックする。[インターネットプロトコルバージョン 4(TCP/IPv4)] 以外のチェックを外す。前出の図10を参照のこと。なお、通信する他のプログラムを停止しておくと、ARP と ICMP のトラヒックだけのトラヒックを得やすくなる。
     実施結果のデータは実験グループで共有すればよいが、各自のオリジナルの実験結果を得る場合は、次の ARP テーブルのクリアから のモニタリングまでを、PC1のところを各自が担当する PC ごとに人数分 (PC ごとに) 繰り返して実施すればよい。
   - RP テーブルをクリアする。全 PC で行う。

     C:>arp -d *

   - RP テーブルの内容を表示する。この時点で MAC アドレスの記憶はされていない。

     c:>arp -a
     ARP エントリが見つかりませんでした。
3. モニタリング
   - キャプチャを開始する。操作は 7.3 を参照のこと
   - PC1 から他の 1 台の PCに ping コマンドを実行する。
     これにより、ICMP のパケットが出されるが、それを先行して ARP が行われる。

     C:>ping 192.168.4.2 *PC1 以外の PC に対して行う

   - ARP テーブルを表示し、表 5 に記入する。
     表示された相手の PC の MAC アドレスの値が表2の値に等しいことを確認する。

     C:>arp -a
     ARP テーブルの表示例　インターフェース: 192.168.x.1 -0xe
     インターネット　アドレス　　物理アドレス　　種類
     　　192.168.x.2　　00-1b-8b-79-84-02　動的

     * 第1オクテッドの値が、224 以上のマルチキャストアドレスが表示される場合は、実験ではこれらを無視して取り扱う。

- キャプチャを停止する。
  ARP と ICMP のトラヒックがキャプチャできたら、キャプチャを停止する。

4. ARP と ICMP の動作の確認
   ARP テーブルの表示から ARP テーブルの情報の内容を確認し、キャプチャした結果からフレームとパケットの存在を確認して表 5 に記入する。

表 5: 存在を確認する項目の確認結果

存在を確認する項目	ping した PC	ping された PC	それ以外の PC
ARP テーブルの MAC アドレスと IP アドレスの値	192.168.1.3 E4-7F-B2-11-C3-B8	192.168.1.2 B0-99-28-d8-11-88	- -
ARP request フレーム	有	有	有
ARP reply フレーム	有	有	無
ICMP Echo request	有	有	無
ICMP Echo reply	有	有	無

*ARP テーブルの情報は ARP コマンドの結果から記入し、その他は存在する有無を記入する

キャプチャした結果から ARP フレームの Ethernet ヘッダの内容を分析する。

- 最初のフレームになる ARP request のフレームの内容を表 6 に記入する。
  ARP フレームの宛先の MAC アドレスがブロードキャストアドレスになっている。ping 先の IP アドレスが入っている。また、送信元の IP アドレスと MAC アドレも入っているのでそれに対して返信をすることができる。

表 6: ARP request のフレーム

送信元 MAC アドレス B0-99-28-D8-11-88	宛先 MAC アドレス ff-ff-ff-ff-ff-ff	Ethernet II、Source: 送信元 Destination: 宛先
送信元 IP アドレス 192.168.1.2	問合せの IP アドレス 192.168.1.3	ARP データの Sender IP、 Target IP

*MAC アドレスは 16 進数で記入する

- ARP request の応答である ARP reply のフレームの内容を表 7 に記入する。
  ARP reply には ping 先の PC の MAC アドレスが入っている。また、送信元の MAC アドレスと宛先の MAC アドレスが入れ替わっている。

表 7: ARP reply のフレーム

送信元 MAC アドレス E4-7F-B2-11-C3-B8	宛先 MAC アドレス B0-99-28-D8-11-88	Ethernet II、Source: 送信元 Destination: 宛先
送信元 IP アドレス 192.168.1.3	問合せの IP アドレス 192.168.1.2	ARP データの Sender IP、 Target IP

- ping コマンドが送信する ICMP の Echo request パケットを分析し、表 8 に記入する。ICMP ではレイヤ3の IP パケットの存在と IP パケットの構造を確認する。

ping のパケットには送信元と送信先の IP アドレスが入っている。また、フレームのアドレスには送信元と送信先の MAC アドレスが入っていることを確認する。

表 8: ICMP Echo request のフレームとパケット

送信元 MAC アドレス B0-99-28-D8-11-88	宛先 MAC アドレス E4-7F-B2-11-C3-B8	Ethernet II、Source: 送信元 Destination: 宛先
送信元 IP アドレス 192.168.1.2	問合せの IP アドレス 192.168.1.3	IP ヘッダ, Source: 送信元, Destination: 宛先

- ping コマンドが送信した ICMP の Echo request に対する応答である ICMP の Echo reply パケットを分析し、表 9 に記入する。送信元と宛先が表9と入れ替わっていることを確認する。

表 9: ICMP Echo reply のフレームとパケット

送信元 MAC アドレス E4-7F-B2-11-C3-B8	宛先 MAC アドレス B0-99-28-D8-11-88	Ethernet II、Source: 送信元 Destination: 宛先
送信元 IP アドレス 192.168.1.3	問合せの IP アドレス 192.168.1.2	IP ヘッダ, Source: 送信元, Destination: 宛先

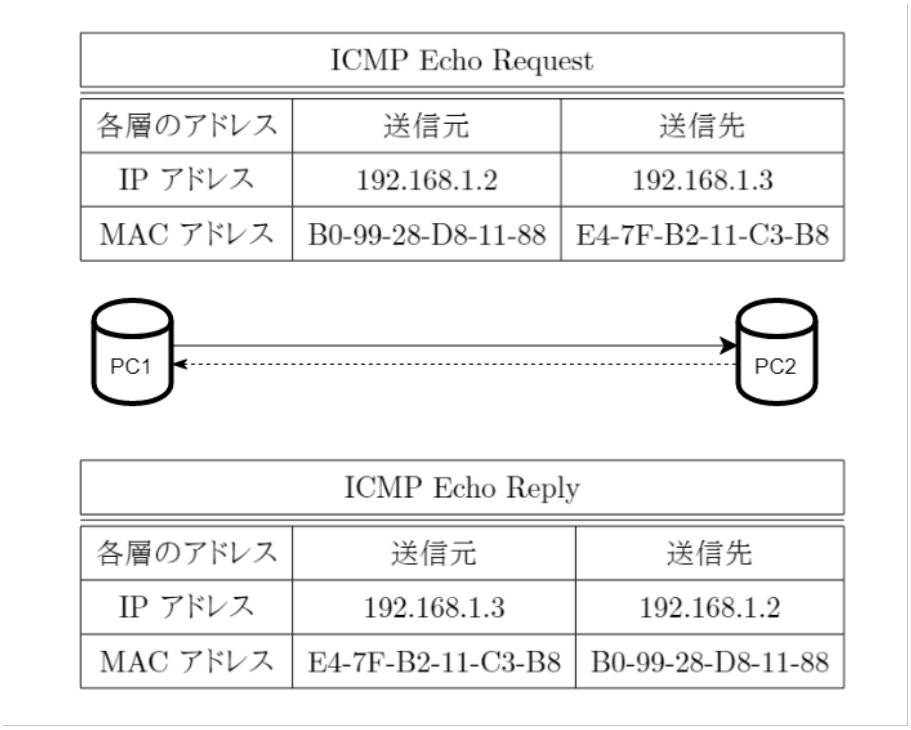

図 3: ICMP のパケット情報

5. キャプチャしたデータの保存

- キャプチャした内容をテキストとしてコピーする。
(File メニュー) から、[Export Packet Dissections] をクリックし、[As Plain Text] をクリックする。ファイル名を指定してテキストファイルとして保存する。このときに画面下部の [Packet Format] の [Packet detail] のチェックをつけて、[All expanded] を指定しておくと詳細な情報を出力できる。

- キャプチャしたデータ形式で保存する。
  キャプチャしたデータ形式で保存するときはキャプチャソフトを終了する前に情報を保存する。このデータは、後日 Wireshark などで詳細に分析したい時などに使用できる。

6 実験 5 ファイアウォールの設定

6.1 実施事項

- パーソナルファイアウォールの設定
- 代表的なプロトコルの理解

ファイアウォールの基本的なパケットフィルタリングの機能により、不正アクセスを軽減する仕組みを理解する。ICMP, HTTP の通過制御を行い、ping コマンドやブラウザを使用した通信を遮断できることを確認する。

6.2 使用機器と構成

2台以上の PC を Switch で接続し、1台はパーソナルファイアウォール (Windows ファイアウォール) によるアクセス制限を行う。
このほかのセキュリティ系ソフトウェアのファイアウォールが動作している場合は、これを一時的に停止しておくこと。

6.3 実施手順

1台の PC において、パーソナルファイアウォールの操作によりパケットの通過を制御する。

- HTTP サーバが起動していることを確認する。
- (スタートボタン) を右クリックし、[コントロールパネル] を選択する。[Windows Defender ファイアウォール] を起動する。

  (Windows Defender ファイアウォールの有効化または無効化) をクリックし、図14のように有効化していることを確認する。

  プロトコルや送信元などの詳細な条件を指定して制御する場合は、[Windows Defender ファイアウォール] の [詳細設定] をクリックして、図15の [セキュリティが強化された Windows Defender ファイアウォール] のウィンドウ内で指定する。

  ICMP の遮断と HTTP の遮断を排他的に行い、ファイアウォールで遮断された PC に対して、他の PC からアクセスする。応答時間やエラーメッセージなどのアクセス状況を表1 0 に記入する。

- ICMP(ping コマンド) の通信を遮断する。
  受信の規則の ICMPv4 のエコー要求を受信する制御条件を選択し、右側の操作で [規則の無効化] をすることで ping に応じなくなる。結果の確認後に、設定を元に戻す。
- Web サーバ側で HTTP を遮断する。
  受信の規則のポート番号 TCP/80 番を受信する制御条件を選択し、右側の操作で [規則の無効化] をすることで HTTP サーバプロセスへのアクセスを遮断する。ブラウザで確認後に、設定を元に戻す。

表 10: 遮断したプロトコルとアクセスの状況

アクセスの方法	ICMP の遮断時	HTTP の遮断時
ping の結果	「要求がタイムアウトしました」	< 1ms
Web アクセスの結果	成功	「アクセスできません」

重要:ファイアウォールの設定は必ず元の [有効]、[許可/ブロック] の設定に戻しておくこと。

オプションで実施:

- ICMP を遮断するときにパケットのキャプチャを行い、どのような動きになっているかを確認する。
- ICMP を遮断したときと、存在しない IP アドレスに ping を行ったときの結果は、どちらも通信ができない。このときの動作の違いをキャプチャして確認する。このときも、ping の前に ARP テーブルのクリアを行うこと。

7 実験 6 IPv6 を使用した通信

7.1 実施事項

- IPv6 アドレスによる PC 間の疎通確認

LAN 内の通信に IPv6 アドレスを使用することで、IPv6 アドレスの仕様と設定などの基本的な操作方法を IPv4 アドレスと比較して理解する。

7.2 使用機器類と構成

実験 2 のケーブルと機器の接続と同じ構成で、IP アドレスだけを IPv6 に変更する。

7.3 実施手順

LAN の物理的接続を行い、PC に IPv6 グローバルユニキャストアドレスを設定して PC 間の疎通の確認を行う。

1. IPv6 アドレスの設定

   - IPv4 と同様に、図16の [インターネット　プロトコル　バージョン6 (TCP/IPv6)] を選択し、IPv6 アドレスを入力する。

     PC に入力する IPv6 アドレス　 2001:db8:x::n/64
     自分が割り当てた IPv6 アドレス　 2001:db8:4::1/64
     * ここで、x は実験グループごとに割り当てる番号とし、n は 1 から増加して各 PC に付与する。

     なお、IPv6 アドレスについての詳細は、JPNIC の Web サイトなどを参照せよ。
     https://www.nic.ad.jp/jp/newsletter/No32/090.html

   - ipconfig コマンドを用いて設定されている IPv6 アドレスを確認し、表 11 の情報を記入する。
     1つのインターフェースに IPv6 アドレス、一時 IPv6 アドレス、リンクローカル IPv6 アドレスなどの複数のアドレスが設定されている。

表 11: IPv6 アドレスの確認結果

PC	IPv6 アドレス	リンクローカル IPv6 アドレス
PC1	2001:db8:1::2	fe80::c0de:8b8b:d02b:bf08
PC2	2001:db8:1::3	fe80::d187:43ad:2c29:263
PC3	2001:db8:1::4	fe80::edb7:230:3966:cc00
PC4	2001:db8:1::5	fe80::e191:a654:b7dd:71fa

2. IPv6 アドレスを使用した通信状況の確認

   - ping コマンドを使用して、PC 間で通信ができることを確認する。

     C:>ping -6 2001:db8:4::2
     2001:db8:4::2 に ping を送信しています　 32 バイトのデータ:
     2001:db8:4::2 からの応答:時間　 < 1ms

- また、宛先にリンクローカル IPv6 アドレスを指定して、ping コマンドにより同様に通信ができることを確認する。
- ブラウザで各 PC から相手側の PC(Web サーバ) の IPv6 アドレスを指定してアクセスし、Web ページが表示されることを確認する。なお、ブラウザなどに IPv6 アドレスを入力するときは、[2001:db8:1::2] のように [] で囲んで入力する。

8 検討事項

8.1 検討事項 1

- WAN と LAN の概要、利用面でのこれらの関係、および設置者 (工事をする者) の違いについて。
  WAN (Wide Area Network) は遠く離れた場所とつながったネットワークのこと。WAN は簡単に言えば LAN と LAN をつないだ大きなネットワークである。
  LAN (Local Area Network) は広くても一施設内程度の規模で用いられるコンピュータネットワークのことである。
  利用面でのこれらの関係
  LAN で構築した小規模のコンピュータネットワーク同士を接続する際に、WAN が使用される。例えば、工場に構築した LAN を他の工場と接続、企業同士の接続などである。
  設置者(工事をする者)の違いについて
  WAN は地理的に離れた場所を接続する必要があるため、利用者個人が配線をすることができず、NTT などの電気通信業者に設置を依頼する必要がある。また WAN の設置だけではインターネットに接続することはできず、別途プロバイダ業者と契約を行う必要がある。LAN は家庭内や企業内など限定された範囲のネットワークのため、一般の人でも構築ができる

8.2 検討事項 2

- リピータ HUB と比較した Switch の機能の特徴について
  スイッチングハブ (switching hub) は宛先の端末にのみ信号を中継するのに対し、リピータハブ (repeater hub) は宛先に関係なく、接続されている全ての端末に信号を中継する。リピータハブは、送信先に関わらず送られてきたパケットをすべてのポートに送信するため、端末 A から端末 B にデータを送信している間は、ほかの端末同士が通信を行うことはできない。一方 Switch は、送られてきたデータを、MAC アドレスをもとに判別することで、送信先の端末にだけデータを送信するため、端末 A から端末 B へデータを送信する場合、データはほかの端末を経由せずに、直接送信先へ届けられる。このため、不要なデータ転送が行われず、ネットワーク全体の負荷が軽くなるという特徴がある。
  また、リピーターバブはすべてのポートにデータを転送するため、もしデータを暗号化せず http などで送信してしまうと、そのデータがハブに接続されているすべて PC で傍受できてしまう。

9 吟味

9.1 実験 1 LAN ケーブルの作成

この実験では LAN ケーブルを実際に作成することで、LAN ケーブル (ツイストペアケーブル) の構造を理解することができた。また、LAN ケーブルは2本のケーブルを撚り合わせて 1 ペアとした形状のものを 4 ペア 8 芯にしたタイプのツイストペアケーブルが主に使われていることが分かった。そして LAN ケーブルはシールドした STP(ShieldedTwistedPairCable) と、シールドの無い UTP(UnshieldedTwistedPairCable) の2種類があり、多く使われているのはシールドされていない UTP だということが分かった。

9.2 実験 2 Switch を使用した LAN の構築

この実験では本来 PC で自動的に割り振られる IP アドレスを手動で任意の IP アドレスに変更する方法やパソコンの物理アドレス (MAC Address) を確認する方法について理解することできた。

9.3 実験 3 撚りを解いたケーブルでの通信

この実験で撚りを解いた3m、5m、10mのケーブルと普通の100mツイストのケーブルで通信状態の確認を行ったところ、100m ツイストケーブルでは通信することができたが、撚りを解いた3m、5m、10mのケーブルを使用した場合は通信出来なかった。この結果からツイストペアケーブルは、1対ごとに線を捻ることでクロストークをキャンセルし、本来の信号のみが流れるようになっており、この撚りを解くとクロストークをキャンセルできなくなり、本来の信号以外のノイズが流れてしまって通信できないということが分かった。

9.4 実験 4 パケットのモニタリング

ARP の request フレームと reply フレームでは、送信元の MAC アドレスと IP アドレスが入れ替わっていることがわかった。また、ICMP の request フレームと reply フレームも同様に入れ替わっていることから、ARP のテーブルに記憶されているアドレスと通信をしていることがわかった。そして LAN につながっている機器が別の機器と通信するためには IP アドレスだけではなく MAC アドレスも必要であり、そのため、ARP デーブルには LAN に繋がっていて、通信したことがある機器の IP アドレスと MAC アドレスをテーブルに保存していて、ある IP アドレスを利用している機器の MAC アドレスを知りたい時はこの ARP テーブルを参照していることが分かった。

9.5 実験 5 ファイアウォールの設定

本実験では実験結果から ICMP を遮断してもデータを送受信できることがわかった。また、ping,traceroute などは IMCP プロトコルの機能であって、ICMP を遮断すると使えなくなるということがわかった。

9.6 実験 6 IPv6 の設定方法

本実験では Windows で IPv6 アドレスを手動で任意のアドレスに変更する方法について理解することができた。

10 参考文献

- LAN と WAN って何が違うの?
  https://flets-w.com/user/point-otoku/knowledge/other/otherl28.html
- Implementing TCP in Rust
  https://youtu.be/bzja9fQWzdA
- マスタリング TCP/IP 入門編第 5 版
  https://www.ohmsha.co.jp/book/9784274068768/