

フレーム衝突実験

1. ネットワーク情報

《実験1》 ネットワーク情報を破棄する(動的 IP アドレスの解放)

DHCP サーバーから取得したネットワーク情報を一旦破棄する実験です。

コマンドプロンプト(通称 dos 窓)を開き、ネットワークコマンド ipconfig /release を実行する。コマンド実行後に、ブラウザで任意 Web サイトを閲覧できないことを確認する。

```
C:¥>ipconfig /release
```

このときのネットワーク情報を、コマンドプロンプトを開き、ネットワークコマンド ipconfig /all を実行して確認する。確認した以下のネットワーク情報①～⑥を実験ノートに記録する。※①～⑥の表示しているものだけでよい。

- ①物理アドレス ②DHCP 有効 ③IPv4 アドレス
④ サブネットマスク ⑤デフォルトゲートウェイ ⑥DNS サーバー

```
C:¥>ipconfig /all
Windows IP 構成
イーサネット アダプター ローカル エリア接続:
① 物理アドレス. . . . . : ??-??-??-??-??-??
② DHCP 有効. . . . . : ?
自動構成有効. . . . . : はい
③ IPv4 アドレス. . . . . : ?.?.?.? (優先)
④ サブネット マスク. . . . . : ?.?.?.?
⑤ デフォルト ゲートウェイ. . . . . : ?.?.?.?
⑥ DNS サーバー. . . . . : ?.?.?.?
```

この情報を記録する

《実験2》 ネットワーク情報を再取得する(動的 IP アドレスの再取得)

一度破棄したネットワーク情報を DHCP サーバーから再び取得する実験です。

コマンドプロンプト(通称 dos 窓)を開き、ネットワークコマンド ipconfig /renew を実行する。コマンド実行後に、ブラウザで任意 Web サイトを閲覧できることを確認する。

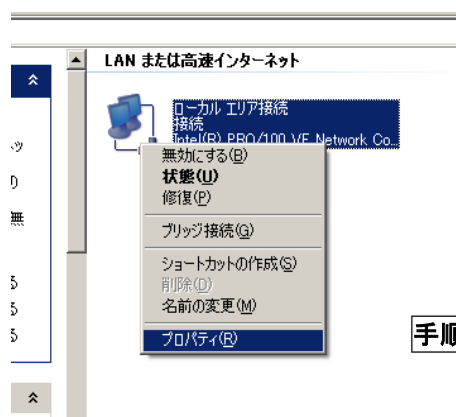
```
C:¥>ipconfig /renew
```

このときのネットワーク情報を、コマンドプロンプトを開き、ネットワークコマンド ipconfig /all を実行して確認する。確認した情報①～⑥を実験ノートに記録する。※①～⑥の表示しているものだけでよい。

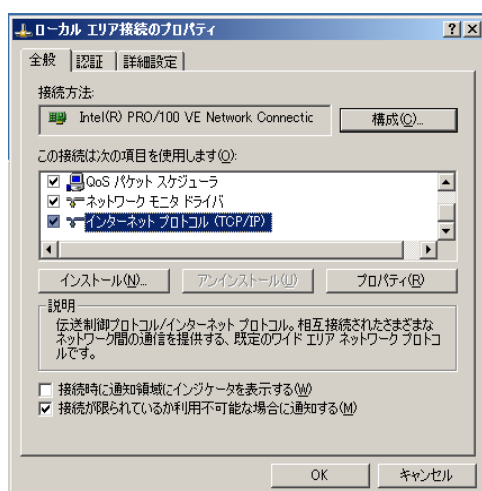
- ①物理アドレス ②DHCP 有効 ③IPv4 アドレス
④ サブネットマスク ⑤デフォルトゲートウェイ ⑥DNS サーバー

《実験3》ネットワーク情報を静的に設定する

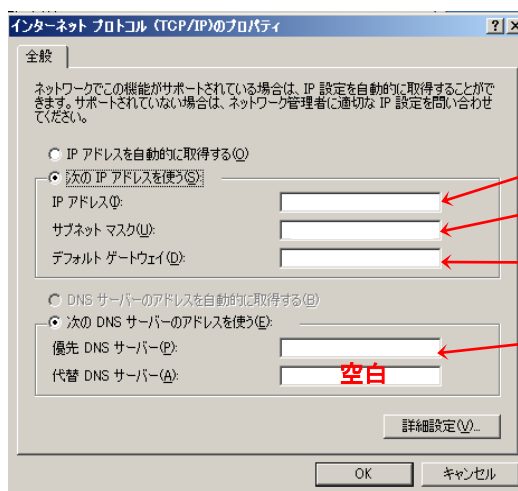
《実験2》で表示したネットワーク情報のうち、③IP アドレス、④サブネットマスク、⑤デフォルトゲートウェイ、⑥DNS サーバー を、下図のネットワーク情報の設定(静的 IP アドレス)に従って、自分の PC(iMac)に設定する。設定完了後、ブラウザで任意 Web サイトを**閲覧できる**ことを確認し、閲覧可否を実験ノートに記録(可/否)する。



手順 1 ローカルエリア接続を右クリックした後、プロパティを左クリックする



手順 2 インターネットプロトコルでプロパティボタンを押す



③IP アドレス
④サブネットマスク
⑤デフォルトゲートウェイ
⑥DNS サーバー

手順 3「次の IP アドレスを使う」「次の DNS サーバーのアドレスを使う」にチェックをいれて、各情報を入力する

<ネットワーク情報の設定(静的 IP アドレス)>

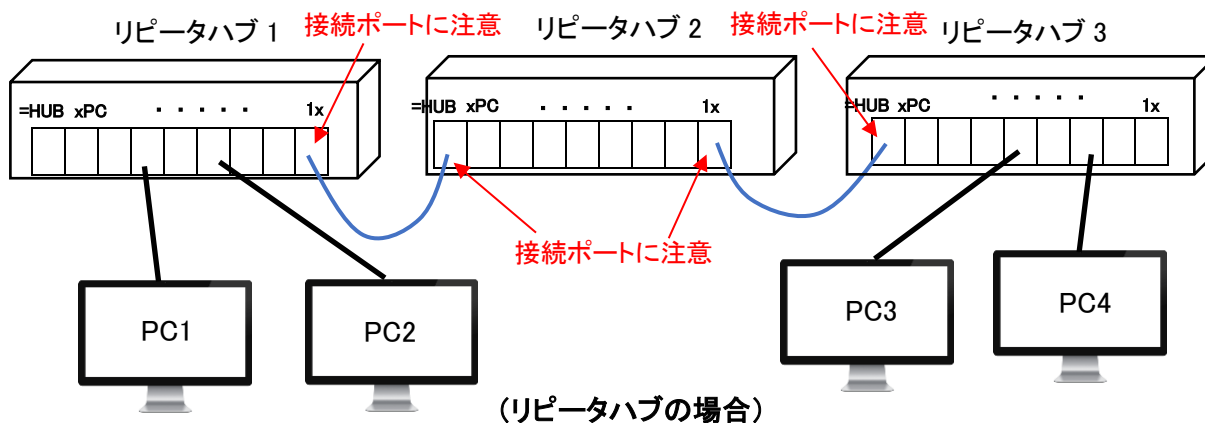
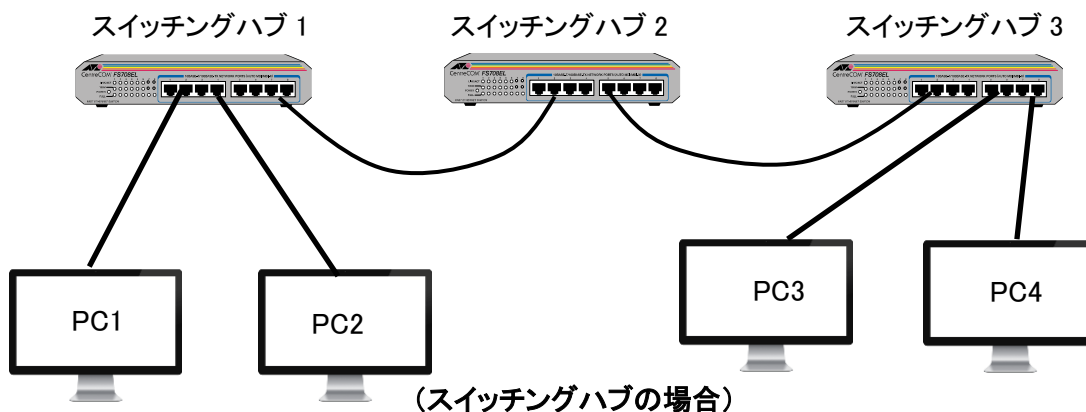
2. ネットワーク構築

3 機の(リピータまたはスイッチング)ハブを使って、テーブル上の全 PC(2 台~4 台)を接続し、PC 間でパケットが転送できるようにする。

《実験4》ネットワークを構築する

下図(ネットワーク構成 1)のように 3 機のハブと PC1~PC4(ここでは、4 台で説明する)を接続する。図中で指定したネットワーク情報(ネットワークアドレス、サブネットマスク)に従って、PC1~PC4 にホストアドレス、サブネットマスクを設定する。このときの以下に示す①~③のネットワーク情報をノートに記述する。※デフォルトゲートウェイと優先 DNS サーバーは空白。

- ① ネットワーク構成図(ハブと PC1~PC4 の接続図)
- ② PC1~PC4 の IP アドレス(自分の PC 以外のもすべて)※自分の PC には○印をつける
- ③ PC1~PC4 のサブネットマスク(自分の PC 以外のもすべて)※自分の PC には○印をつける



<ネットワーク構成1>

ネットワークアドレス: **172.17.0.0**
 サブネットマスク: **255.255.255.0**

《実験5》ネットワークの動作を確認する ※《実験5》以降では Windows のファイアーウォールを無効(OFF)にする
 《実験4》で構築したネットワークが、正しく動作しているかを確認する。自分の PC から各 PC(自分の PC 除く)に
 検査用パケット(ICMP)を送り、その応答を確認する。コマンドプロンプトを開き、ネットワークコマンド ping を実行する。

宛先 PC のアドレス

```
C:\>ping 172.17.0.2

Pinging 172.17.0.2 with 32 bytes of data:

Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(宛先 PC(172.17.0.2)が応答した時)

```
C:\>ping 172.17.0.2

Pinging 172.17.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(宛先 PC(172.17.0.2)が応答しない時)

<ping の応答 1>

応答しない場合は、問題を解決して再度実行する。ネットワークコマンド ping を実行後に表示する情報①～⑪を実験ノートに記録する。※記録する項目は、下図の四角(□)で囲んだ項目。

```

C:\>ping 172.17.0.2

Pinging 172.17.0.2 with 32 bytes of data:

Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

①宛先 PC の IP アドレス
 ②パケットサイズ
 ③パケット生存時間
 ④応答(往復)時間
 ⑤送信パケット数 ⑥受信パケット数 ⑦消失数 ⑧消失割合
 ⑨応答(往復)時間の最小時間 ⑩最大時間 ⑪平均時間

<ping 応答 2>

3. フレーム衝突実験

《実験6》フレームの衝突を確認する(スイッチングハブのカスケード接続)

<ネットワーク構成 1>(スイッチングハブの場合)のネットワークで、以下の<フレーム衝突 1>の操作例に従って、自分の PC から各 PC(自分の PC 除く)へ連続して検査用パケット(ICMP)を送って応答を確認する。このとき、スイッチングハブの背面(または前面)のいずれかのランプが一瞬赤色に変化するか否かを確認する。

いずれかのランプが緑色から赤色に一瞬でも変化すれば、転送中にフレームが衝突していることが確認できる。このランプの変色(緑色→赤色)が“起こった/起こらなかった”を実験ノートに記録する。

```

C:\>ping -t 172.17.0.2

Pinging 172.17.0.2 with 32 bytes of data:

Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
Reply from 172.17.0.2: bytes=32 time<1ms TTL=128
途中省略

Ping statistics for 172.17.0.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Ctrl+C
^C
C:\>
  
```

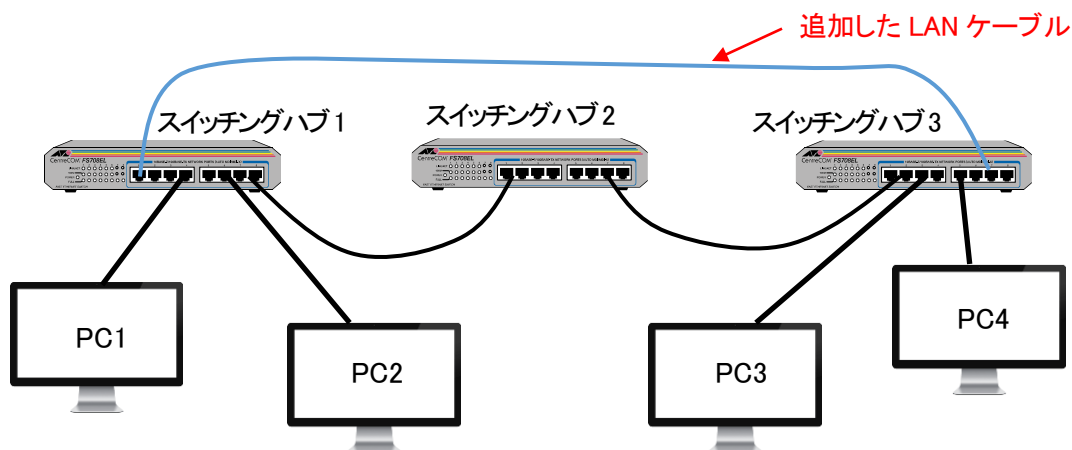
連続実行: ping -t 宛先 ip address
 停止: Ctrl キーと C キーを同時に押す

<フレーム衝突 1>

《実験7》フレームの衝突を確認する(リピータハブのカスケード接続)

＜ネットワーク構成 1＞(リピータハブの場合)のネットワークで《実験6》と同様の実験を行い、リピータハブのランプの変色(緑色→赤色)が“起こった/起こらなかった”を実験ノートに記録する。

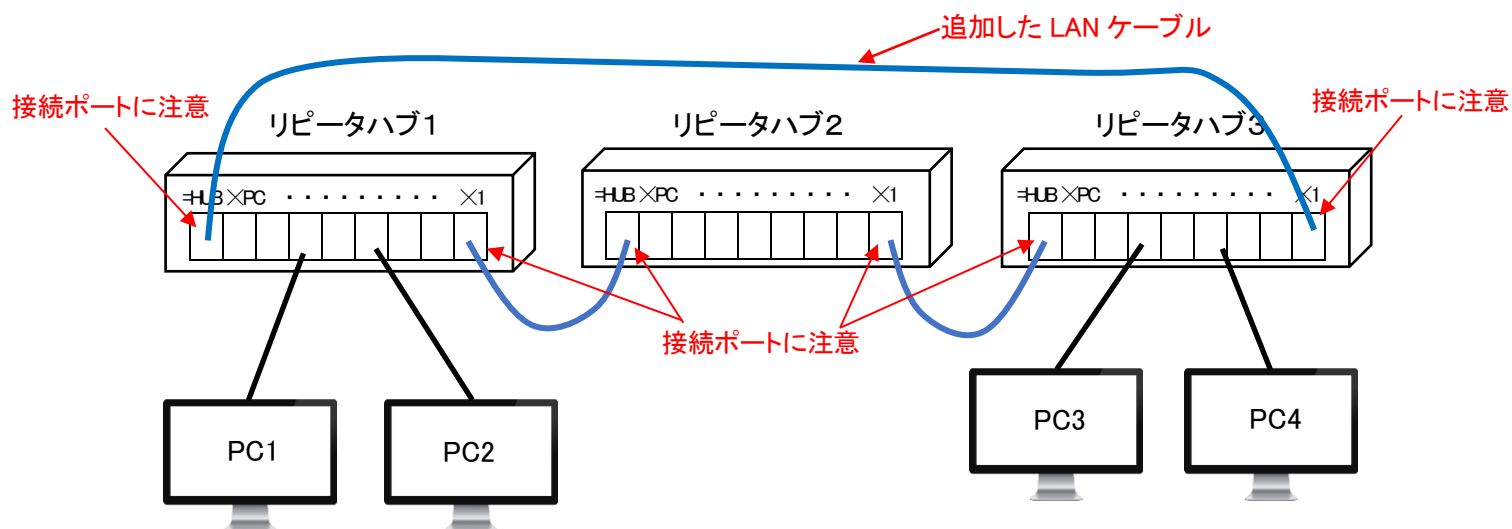
《実験8》フレームの衝突を確認する(スイッチングハブのループ接続)



＜ネットワーク構成 2＞(スイッチングハブの場合)

＜ネットワーク構成 1＞(スイッチングハブの場合)において、スイッチングハブ 1 とスイッチングハブ 3 を LAN ケーブルで接続して、上記の＜ネットワーク構成 2＞(スイッチングハブの場合)のように再構成する。この構成で《実験 6》と同様の実験を行い、スイッチングハブのランプの変色(緑色→赤色)が“起こった/起こらなかった”を実験ノートに記録する。

《実験9》フレームの衝突を確認する(リピータハブのループ接続)



＜ネットワーク構成 2＞(リピータハブの場合)

＜ネットワーク構成 1＞(リピータハブの場合)において、リピータハブ 1 とリピータハブ 3 を LAN ケーブルで接続して、上記の＜ネットワーク構成 2＞(リピータハブの場合)のように再構成する。この構成で《実験6》と同様の実験を行い、リピータハブのランプの変色(緑色→赤色)が“起こった/起こらなかった”を実験ノートに記録する。