

情報学群実験4C 第2回レポート  
ネットワーク分割

学籍番号 1190319

楠田 健太

グループ4

平成29年7月9日

## 1 目的

1つのネットワークは Ethernet のブロードキャストドメインの範囲に収まっている必要があることから、物理的な伝送量は 1 本である。仮にルータやスイッチを用いたネットワークの分割を行わない場合、100 台、200 台規模でホストが接続されると、送受信される通信量が増加し、遅延時間や CPU への負荷が増加する。また、通信量の他にも IP アドレスの利用率の問題やルーティングテーブルの肥大化問題などの様々な問題が生じる [5]。

本文書では、これらの問題を解決するためにルータ、スイッチを用いてネットワークの分割を行う。具体的にはルータを用いた物理的手法による分割に加えて、より細かく分割するために L2 スイッチの VLAN 機能を用いた論理的手法による分割についても行なう。

## 2 内容

まずは、ルータを用いた物理的手法によってネットワークを分割する。自グループの LAN とバックボーンを接続するルータについて、静的ルーティングテーブルを構築することによって、自グループと他グループおよびバックボーンとの通信が行えるように環境を設定する。今現在の環境では、全端末が同一ネットワークとなっているため、サブネット分割を行うことで、各グループごとにネットワークを分割する。クラス B のアドレスを 256 個のサブネットに分割し、図 1 のように、各 LAN に割り当てる。

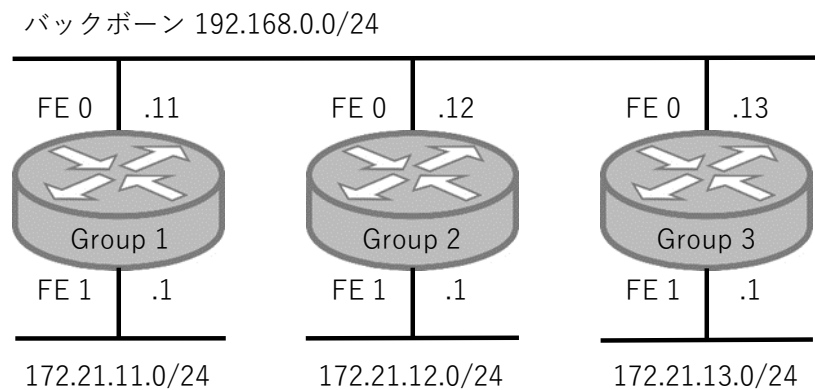


図 1: サブネット割り当て

また、各 LAN 内での IP アドレスは表 1 のように割り当てる。

表 1: サブネット内の IP アドレス

Router サブネット内 I/F	1 番小さい IP アドレス
Server	2 番目に小さい IP アドレス
Linux Client PC	3 番目に小さい IP アドレス
Windows Desktop PC	4 番目に小さい IP アドレス
Mac	6 番目に小さい IP アドレス
Note PC	6 番目に小さい IP アドレス
Reserved	7 番目に小さい IP アドレス

次に L2 スイッチの ポート VLAN 機能を用いて論理的手法によってネットワークを分割する。図 2 のように、スイッチの VLAN 機能を用いて、自グループの VLAN, ペアグループの VLAN, タグ VLAN を作成する。

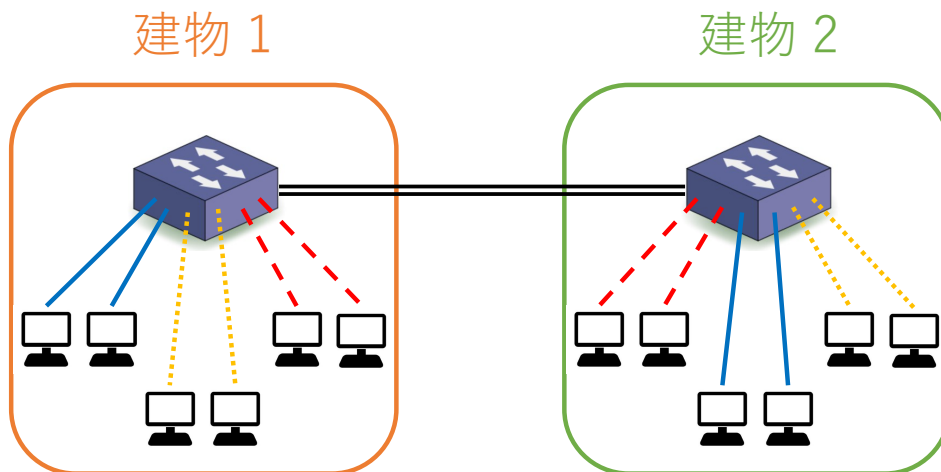


図 2: サブネット割り当て

### 3 要素技術

#### 3.1 ルーティング

ルーティングは OSI 参照モデル第 3 層 (ネットワーク層) の機能である。データを宛先に配送する過程において、個別のアドレスが必要になるまでは複数のアドレスを束ねて 1 つの単位として扱う階層的な仕組みを持っており、ある端末から別の端末に至る最も効率の良いパスを探すプロセスである。主にルーターがそのプロセスにおいて役割を果たす [1]。ルーターはルーティングテーブルを参照することでパケットの転送を行うことができる。受け取ったパケットの宛先 IP アドレスとルーティングテーブルを比較し、次に送信されるルーターが決定される。ルーティングテーブルの中に誤った情報が入っている際は、パケットが目的のホストへ届かないこともある [2]。

実際にルーティングテーブルを作成，管理する方法としてスタティックルーティングとダイナミックルーティングが挙げられる．スタティックルーティングは，ルーターやホストに固定的に経路情報を設定する手法である．しかし，大多数の経路情報を扱う場合，管理者に大きな負担をかけることとなる．また，緊急の場合においても，手作業で迂回するような書き換えが必要となる．これに対して，ダイナミックルーティングとは，ルーティングプロトコルを動作させることにより，自動的に経路情報の設定を行なう．ルーターの数が増えるほど効果的な手法であるが，ルータ間で定期的に情報のやり取りを行う必要があるため，ネットワークには常に，負荷がかかることとなる．このように，それぞれにメリットとデメリットが存在する．これらは組み合わせて利用することもできる [2]．

### 3.2 VLSM

サブネットマスクによるネットワーク部のビット数は，全サブネットワークで統一した方がネットワーク全体を簡単に構成可能であるが，アドレスを有効活用するという点を考慮すると，接続されるホスト数に応じて，サブネットごとに異なるサブネットマスクを利用する方が好ましい．これを実現する技術を VLSM(Variable Length Subnet Mask) という [3]．

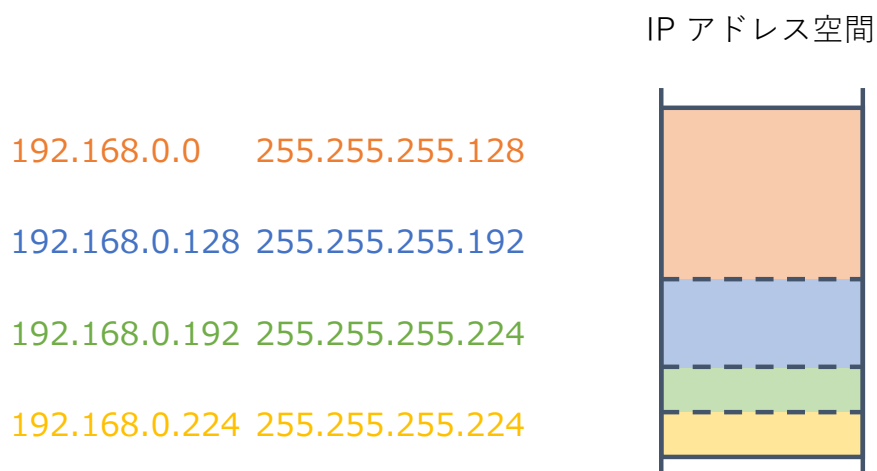


図 3: VLSM

### 3.3 VLAN

VLAN とは，L2 スイッチが備えている機能の一つであり，管理者が中継する範囲を設定することによって，データリンク内に仮想的な LAN が複数構築することが可能となる技術である．スイッチのフォワーディングテーブルの設定により，接続されているノードをグループ化し，グループ外へのブロードキャストフレームの転送を行なわないようにしたものである．なお，VLAN 間の通信については，物理的なネットワークの分割の場合と同様に，ルータを介する必要がある．以下に異なる 3 種類の VLAN について紹介する [3]．

### 3.3.1 ポートベース VLAN

最も簡単な形態の VLAN であり，L2 スイッチの各ポートごとにグループを設定する．スイッチの設定により，各ポートと VLAN の対応付けを行なう [3]．

### 3.3.2 MAC アドレスベース VLAN

ホストに設定された MAC アドレスごとに VLAN を対応させ，L2 スイッチの MAC アドレステーブルに VLAN の識別情報が加えられる．各コンピュータに所属する VLAN が割り当てられることによって，アプリケーション側から見た構成としては，シンプルに見える．しかし，管理者は各 L2 スイッチ への設定を行なう必要があるため，負担がかかる．実際には，ポートベース VLAN と VLAN ごとに ID を付与を行なう Tagging 機能 を用いて，タグ VLAN を利用することによって，多種多様に対応可能であるため，アドレスベースの VLAN は使われなくなってきている [3]．

### 3.3.3 プロトコルベース VLAN

L3 のプロトコルに応じて VLAN をグループ付けすることで，無駄なトラフィックを抑えることが可能である．主に，ルータや L3 スイッチの処理能力を補うために利用される．特定のプロトコルについて，L2 スイッチでブリッジを動作させることによって，ルータや L3 スイッチにかかる負荷を分散させることが可能である [3]．

## 3.4 STP

STP とはスパンニングツリープロトコルの略であり，ブリッジで構成されたネットワークで冗長経路を準備し，そこから有用であるものを用いてネットワークを再編成する手順として規定されている．ループが構成されないように，ブリッジ同士で連携し，不必要となった経路を切断するものである．この手順を踏むことにより，ブロードキャストストームを防ぐことが可能となる．また，アクシデントに対応し，自動的に再編成を行うことから，冗長経路を備えたネットワークを構築することが可能となる．具体的には，物理的な LAN 間のブリッジ接続をツリー状の論理的な形態に変換する．頂点に位置するルートブリッジを先頭に，各ブリッジの優先順位などを考慮した，経路の切断を行う [3]．

適用する場合の注意点を以下に記述する．

1. ブリッジ間において接続の状態を求めるフレームが出現するため，ブリッジの台数を考慮しなければ，帯域について問題が生じることがある．
2. 経路が確定する前に，ブリッジが中継を行うことはないため，ブリッジをノードへ直結させる場合には，ポートの STP 機能をオフにしておく．

## 4 作業記録

### 4.1 IOS ルータ設定

IOS ルータを設定する.

1. インタネットエクスプローラーを開いた.
2. URL 検索窓にて, ftp://192.168.0.1/pub/Windows/putty-gdi-20120211.zip と入力し, 検索ボタンをクリックした.
3. 保存するかどうか尋ねられたため, 「保存」をクリックし, 保存先として「デスクトップ」を指定した.
4. URL 検索窓にて, ftp://192.168.0.1/pub/drivers/usbrs232r\_300v.exe と入力し, 検索ボタンをクリックした.
5. 保存するかどうか尋ねられたため, 「保存」をクリックし, 保存先として「デスクトップ」を指定した.
6. ダウンロードしたフォルダ「usbrs232r\_300v.exe」をダブルクリックした.
7. セキュリティの警告が表示されたため, 「実行」をクリックした.
8. 展開するかどうか尋ねられたため, 展開（解凍）先フォルダが「c:\¥corega」であることを確認し, 「展開」をクリックした.
9. スタートメニュー>コンピュータ>ローカルディスク> corega > usbrs232\_300 と進み, win7\_64bit\_Driver をダブルクリックした.
10. ユーザーアカウント制御が現れたため, 「はい」をクリックした.
11. 「InstallShield Wizard」ウインドウにて「次へ」をクリック>「インストール」をクリック>「Windows セキュリティ」ウインドウが現れるので, 「インストール」をクリックした.
12. インストール後, 「完了」をクリックし, 「InstallShield Wizard」ウインドウを閉じた.
13. USB シリアルを接続した.
14. スタートメニュー>コントロールパネル>ハードウェアとサウンド、デバイス マネージャーと進んだ.
15. ポート（COM と LPT）の項目に, 「CG-USBR232R COM PORT（COM3）」の表示を確認した.
16. ダウンロードした「putty-gdi-20120211.zip」をダブルクリックした.
17. 展開先が尋ねられるため, デスクトップになっていることを確認した後, 「展開」をクリックした.
18. フォルダ「putty-gdi-20120211」>アプリケーション「putty」をダブルクリック>セキュリティの警告にて, 「実行」をクリックした.

19. 「PuTTY Configuration」 ウィンドウが現れるため、「Connection」 カテゴリーの「Serial line」欄にて「COM3」と入力、「Connection type」にて「Serial」を指定した。
20. 「Session」 カテゴリー内ログ「Session logging」にて「All session output」を指定＞「log file name」にてログファイル名を入力「Browse…」をクリック＞参照先としてデスクトップを指定した。
21. コンソールケーブル（水色）で、ルータの CONSOLE 端子と USB シリアルを接続した後、ルータの電源を入れた。
22. 「Open」をクリックし、ルータの設定に入った。
23. 「Would you like to enter initial configure dialog?」と表示された。これは初期設定メニューに入るか否かを確認している。今回はマニュアルで設定するため、「no」を入力した。
24. 「Router# configure terminal」と入力し、設定モードへ移行した。
25. 「Router(config)# no ip domain lookup」と入力し、DNS の逆引き設定を無効化した。
26. 「Router(config)# line con 0」と入力後、「Router(config-line)# logging synchronous」と入力し、ログ表示とコマンド入力画面を分離した。
27. 「Router(config-line)# exit」と入力し、CONSOLE 画面の設定を終了した。
28. 「Router(config)# username root privilege 15 secret 0 root00」と入力し、ユーザを追加した。
29. 「Router(config)# hostname router4」と入力し、ホスト名を設定した..
30. 「router4(config)# exit」と入力し、設定確認を行なうため、設定モードから抜けた。
31. 「router4# show running-config」と入力し、入力した内容が設定に反映されていることを確認した。

## 4.2 IP アドレス割り当て

1. 「router4# conf t」と入力し、設定モードへ移行した。
2. 「router4(config)# interface fastethernet 0」と入力し、I/F の設定を行なった。
3. 「router4(config-if)# ip address 192.168.0.14 255.255.255.0」と入力し、IP アドレスとサブネットマスクを設定した。
4. 「router4(config-if)# no shutdown」と入力し、インターフェースを有効化した。
5. 「router4(config-if)# exit」と入力し、I/F の設定を抜けた。
6. 「router4(config)# interface fastethernet 1」と入力し、I/F の設定を行なった。
7. 「router4(config-if)# ip address 172.21.14.1 255.255.255.0」と入力し、IP アドレスとサブネットマスクを設定した。
8. 「router4(config-if)# no shutdown」と入力し、インターフェースを有効化した。
9. 「router4(config-if)# exit」と入力し、I/F の設定を抜けた。

### 4.3 ルーティング

1. 「router4# show ip route」と入力し、現在のルーティングテーブルを確認した。
2. 「router4# conf t」と入力し、設定モードへ移行した。
3. 「router4(config)# ip route 172.21.11.0 255.255.255.0 192.168.0.11」と入力し、グループ 1 へのルートを設定した。
4. 「router4(config)# ip route 172.21.12.0 255.255.255.0 192.168.0.12」と入力し、グループ 2 へのルートを設定した。
5. 「router4(config)# ip route 172.21.13.0 255.255.255.0 192.168.0.13」と入力し、グループ 3 へのルートを設定した。
6. 「router4(config)# ip route 172.21.14.0 255.255.255.0 192.168.0.14」と入力し、グループ 4 へのルートを設定した。
7. 「router4(config)# ip route 172.21.15.0 255.255.255.0 192.168.0.15」と入力し、グループ 5 へのルートを設定した。
8. 「router4(config)# ip route 172.21.16.0 255.255.255.0 192.168.0.16」と入力し、グループ 6 へのルートを設定した。
9. 「router4(config)# ip route 172.21.17.0 255.255.255.0 192.168.0.17」と入力し、グループ 7 へのルートを設定した。
10. 「router4(config)# ip route 172.21.18.0 255.255.255.0 192.168.0.18」と入力し、グループ 8 へのルートを設定した。
11. 「router4(config)# ip route 172.21.19.0 255.255.255.0 192.168.0.19」と入力し、グループ 9 へのルートを設定した。
12. 「router4(config)# ip route 172.21.20.0 255.255.255.0 192.168.0.20」と入力し、グループ 10 へのルートを設定した。
13. 「router4(config)# ip route 172.21.21.0 255.255.255.0 192.168.0.21」と入力し、グループ 11 へのルートを設定した。
14. 「router4(config)# ip route 172.21.22.0 255.255.255.0 192.168.0.22」と入力し、グループ 12 へのルートを設定した。

以上より、IOS ルータの設定は完了である。

### 4.4 クライアント IP アドレス再割り当て

クライアント IP アドレス を再度割り当てる。



#### 4.4.1 Ubuntu

1. 「\$ ifconfig -a」と入力し、現在のインターフェース設定を確認した。
2. 表示を確認したところ、ens2s0 と ens3s0 の 2 つのネットワークインタフェースと コンピュータの内部間通信に使用される lo(ループバック) 用のインターフェースの計 3 つが確認できた。今回は、その中から、 ens2s0 を選択し、利用した。
3. 「\$ sudo su」と入力し、ユーザを管理ユーザ root へと変更した。
4. 「ifconfig ens2s0 inet 172.21.14.2 netmask 255.255.255.0 up」と入力し、IP アドレスとネットマスクを設定した。
5. 「\$ ethtool ens2s0」と入力し、IP アドレスとサブネットマスクが正しく設定されているかを確認した。
6. 「\$ route add default gw 192.168.0.1」と入力し、デフォルトゲートウェイの設定を行なった。

#### 4.4.2 CentOS

1. 「System Tools(システム)」>「Setting(設定)」>「Network(ネットワーク接続)」>「Wired(有線)」の順に進んだ。
2. 設定のボタン (歯車のようなボタン) から、IPv4 の設定を行なった。
3. 「Addresses」を「Manual(手動)」にして、「Address」:172.21.14.3,「Netmask」:255.255.255.0,「Gateway」:192.168.0.1,「DNS server」:192.168.0.1 と入力した。
4. 「Identity」>「make available to other users ()」にチェック>「適用」をクリックした。
5. 「Wired(有線)」がオフになっている場合は、オンへと切り替える。

#### 4.4.3 Windows 10

1. スタートメニュー>コントロールパネル>ネットワークとインターネット>ネットワークと共有センター>アダプターの設定の変更>ローカルエリア接続>プロパティ>「インターネット プロトコル バージョン 4 (TCP/IPv4)」をダブルクリックした。
2. 「次の IP アドレスを使う」にチェックを入れ、IP アドレス:172.21.14., サブネットマスク:255.255.255.0, デフォルトゲートウェイ:192.168.0.1 をそれぞれの欄に入力した。
3. 次の DNS サーバのアドレスを使うにチェックを入れ、優先 DNS サーバ:192.168.0.1 と入力した。
4. 「OK」をクリックし、TCP/IPv4 ウィンドウを閉じた。
5. 「OK」をクリックし、ローカルエリア接続のプロパティを閉じた。
6. ネットワークの場所の設定を促されるため、社内ネットワークをクリックした。

#### 4.4.4 MacOS X

1. 画面の左上にあるリンゴのアイコンをクリック>「システム環境設定」をクリック>「インターネットとワイヤレス」をクリック>「ネットワーク」をクリックした
2. Ethernet 欄の「IPv4 の構成」を手入力へ変更した。
3. IP アドレス:172.21.14.5, サブネットマスク:255.255.255.0, ルーター:192.168.0.1, DNS サーバー:192.168.0.1 をそれぞれの欄に入力した。

#### 4.4.5 Windows 7

1. スタートメニュー>コントロールパネル>ネットワークとインターネット>ネットワークと共有センター>アダプターの設定の変更>ローカルエリア接続>プロパティ>「インターネット プロトコル バージョン 4 (TCP/IPv4)」をダブルクリックした。
2. 「次の IP アドレスを使う」にチェックを入れ、IP アドレス:172.21.14.6, サブネットマスク:255.255.255.0, デフォルトゲートウェイ:192.168.0.1 をそれぞれの欄に入力した。
3. 次の DNS サーバのアドレスを使うにチェックを入れ、優先 DNS サーバ:192.168.0.1 と入力した。
4. 「OK」をクリックし、TCP/IPv4 ウィンドウを閉じた。
5. 「OK」をクリックし、ローカルエリア接続のプロパティを閉じた。
6. ネットワークの場所の設定を促されるため、社内ネットワークをクリックした。

以上より、クライアントの IP アドレス再割り当ては完了である。

#### 4.5 ルータを用いて物理的に LAN 分割した際の動作確認

ルータを用いて物理的に LAN 分割した際の動作を確認する。

1. スタートメニュー>コマンドプロンプトを開いた。
2. 「ping 172.21.22.1」と入力し、グループ 12 のルータへの通信を確認した。
3. 「ping 172.21.22.2」と入力し、グループ 12 のサーバへの通信を確認した。

以上より、ルータを用いた、物理的に LAN 分割した際の動作確認は完了である。

#### 4.6 IOS スイッチ設定

IOS スイッチを設定する。

1. USB シリアルを接続。
2. フォルダ「putty-gdi-20120211」をダブルクリック>アプリケーション「putty」をダブルクリックし、起動した。

3. 「PuTTY Configuration」ウインドウが現れるため、「Connection」カテゴリーの「Serial line」欄にて「COM3」と入力、「Connection type」にて「Serial」にチェックを入れた。
4. 「Session」カテゴリー内ログをクリック>「Session logging」にて「All session output」にチェック、「log file name」にてログファイル名を入力、「Browse…」をクリックし、参照先としてデスクトップを選択した。
5. コンソールケーブル（水色）で、スイッチの CONSOLE 端子と USB シリアルを接続し、スイッチの電源を入れた。
6. 「Open」をクリックし、スイッチの設定に入った。
7. 「Would you like to enter initial configure dialog?」と表示され、初期設定メニューに入るか否かを尋ねられるため、「no」と入力し、マニュアルで設定を行なう。
8. 「Switch > enable」と入力し、特権モードへ移行した。
9. 「Switch# sh run」と入力し、現在のスイッチ設定を表示した。
10. 「Switch# show interface status」と入力し、現在のポートの状態を確認した。今回は Fa0/3, Fa0/5, Fa0/7, Fa0/9, Fa0/11, Fa0/13 の Status が connected であることを確認した。
11. 「Switch# conf term」と入力し、設定モードへ移行した。
12. 「Switch(config)# vlan 4」と入力し、VLAN を作成、グループ番号として 4 を付与した。
13. 「Switch(config-vlan)# name group4」と入力し、グループ番号 4 の VLAN に「group 4」と名前を付与した。
14. 「Switch(config-vlan)# exit」と入力し、VLAN の設定を抜けた。

以上より、IOS スwitchの設定は完了である。

## 4.7 ポート VLAN

ポート VLAN を設定する。

1. 「Switch(config)# int range fa0/1-16」と入力し、range 記述を用いることで、ポート 1-16 の設定に入った。
2. 「Switch(config-if-range)# switchport mode access」と入力し、ポート 1-16 をポート VLAN 用ポートに設定した。
3. 「Switch(config-if-range)# switchport access vlan 4」と入力し、ポート 1-16 を VLAN 4 に設定した。
4. 「Switch(config-if-range)# exit」と入力し、ポート 1-16 の設定を終了した。
5. 「Switch(config)# int range fa0/17-20」と入力し、range 記述を用いることで、ポート 17-20 の設定に入った。

6. 「Switch(config-if-range)# switchport mode access」と入力し，ポート 17-20 をポート VLAN 用ポートに設定した．
7. 「Switch(config-if-range)# switchport access vlan 1」と入力し，ポート 17-20 をペアのグループの VLAN 番号 1 に設定した．
8. 「Switch(config-if-range)# exit」と入力し，ポート 17-20 の設定を終了した．
9. 「Switch(config)# int range fa0/21-22」と入力し，range 記述を用いることで，ポート 21-22 の設定に入った．
10. 「Switch(config-if-range)# switchport mode trunk」と入力し，ポート 21-22 を VLAN トランクポートに設定した．
11. 「Switch(config-if-range)# switchport trunk allowed vlan 4, 4」と入力し，自グループ用 VLAN 4 と他グループ用 VLAN 1 を設定した．
12. 「Switch(config-if-range)# exit」と入力し，ポート 21-22 の設定を修了した．
13. 「Switch(config)# int range fa0/23」と入力し，ポート 23 の設定に入った．
14. 「Switch(config-if-range)# shutdown」と入力し，23 のインターフェースを安全のためシャットダウンした．
15. 「Switch(config)# int range fa0/24」と入力し，ポート 24 の設定に入った．
16. 「Switch(config-if-range)# shut」と入力し，24 のインターフェースを安全のためシャットダウンした．

以上より，ポート VLAN の設定は完了である．

#### 4.8 ケーブルの接続

適切にケーブルを接続する．

1. タグ VLAN ポートとペアグループのタグ VLAN ポートをケーブル 1 で接続した．
2. 自グループの機器を自グループのスイッチの自グループ VLAN へ接続した．
3. 自グループのノート PC は，ペアグループのスイッチの自グループ用 VLAN へ接続した．
4. 他グループのノート PC は，自グループのスイッチのペアのグループ用 VLAN へ接続した．

以上より，ケーブルの接続は完了である．

#### 4.9 スイッチの VLAN を用いて論理的に LAN 分割した際の動作確認

自グループサーバ，ペアグループサーバ，メインサーバ，に対して，接続ポートを変更しながら ping コマンドと tracert コマンドを実行することで，LAN の分割を確認した．

#### 4.9.1 自グループ用ポート同士の通信

1. 「ping 172.21.11.2」を入力したところ、通信不可能であった。
2. 「ping 172.21.14.2」を入力したところ、通信可能であった。
3. 「tracert 198.168.0.1」を入力したところ、172.21.14.1 > 192.168.0.1 のルートを辿っていることを確認した。
4. 「tracert 172.21.11.2」を入力したところ、172.21.14.1 > 192.168.0.11 > 172.21.11.2 のルートを辿っていることを確認した。
5. 「tracert 172.21.14.2」を入力したところ、172.21.14.1 > 172.21.14.1 のルートを辿っていることを確認した。

#### 4.9.2 自グループのノート PC を他グループ用ポートに接続した通信

1. 「ping 172.21.11.2」を入力したところ、通信可能であった。
2. 「ping 172.21.14.2」を入力したところ、通信不可能であった。
3. 「tracert 198.168.0.1」を入力したところ、172.21.11.1 > 192.168.0.1 のルートを辿っていることを確認した。
4. 「tracert 172.21.11.2」を入力したところ、172.21.11.1 > 172.21.11.2 のルートを辿っていることを確認した。
5. 「tracert 172.21.14.2」を入力したところ、172.21.11.1 > 192.168.0.14 > 172.21.14.2 のルートを辿っていることを確認した。

#### 4.9.3 自グループの機器とペアグループの自グループ用ポートに接続したノート PC との間で通信

1. 「ping 172.21.11.2」を入力したところ、通信不可能であった。
2. 「ping 172.21.14.2」を入力したところ、通信可能であった。
3. 「tracert 198.168.0.1」を入力したところ、172.21.14.1 > 192.168.0.1 のルートを辿っていることを確認した。
4. 「tracert 172.21.11.2」を入力したところ、172.21.14.1 > 192.168.0.11 > 172.21.11.2 のルートを辿っていることを確認した。
5. 「tracert 172.21.14.2」を入力したところ、172.21.14.1 > 172.21.14.2 のルートを辿っていることを確認した。

#### 4.9.4 シャットダウンポートを利用した通信

1. 「ping 172.21.11.2」を入力したところ、通信不可能であった。
2. 「ping 172.21.14.2」を入力したところ、通信不可能であった。
3. 「tracert 198.168.0.1」を入力したところ、通信不可能であった。
4. 「tracert 172.21.11.2」を入力したところ、通信不可能であった。
5. 「tracert 172.21.14.2」を入力したところ、通信不可能であった。

## 5 考察

スイッチの VLAN 機能は、ルータによって分けられたネットワークをさらに細かく分割できる、という考え方を学んだ。しかし、ルータの数がどうしても足りない場合、スイッチの数がどうしても足りない場合に、緊急措置として、互いの役割を補うことはできないかを考える。

まずは、スイッチが足りない場合に、ルータを利用できないかを考えてみる。ルータはたどり着きたいネットワークまで導いてくれるが、ネットワーク内に辿りついてしまうと、MAC アドレスを参照できないため、ノードを特定できない。したがって、パケットをホストへ届けることができないため、代用不可能である。

次に、ルータが足りない場合に、スイッチを利用できないかを考えてみる。バックボーンにスイッチをつなぎ、そのスイッチと異なるネットワーク内のスイッチの間にケーブルを接続すると、タグ VLAN を設定可能である。ただし、バックボーンにつながれたホストはネットワークと同等に IP アドレスを当てる必要があるため、IP アドレスの利用効率は非常に悪くなる。したがって、スイッチに関しても可能な限り代用すべきではない。

また、L3 スイッチでは、ルータと L2 スイッチ両方の役割を担うことが可能である。

## 参考文献

- [1] シスコシステムズ, "シスコ ネットワーキングアカデミー CCNA1 受講ガイド," ソフトバンクパブリッシング株式会社, 2005.
- [2] 竹下隆史, 村山公保, 荒井透, 荻田幸雄, "マスタリング TCP/IP ― 入門編― 第 5 版," 株式会社オーム社, 2014. .
- [3] 宮越健, 角田浩二, "図解標準 最新 LAN ハンドブック", 株式会社秀和システム, 2002.
- [4] Stephen A. Thomas, "次世代 TCP/IP 技術解説," 日経 BP 社, 1997.
- [5] 宇野俊夫, "独習 TCP/IP ネットワーキング編 IPv6 対応," 翔泳社, 2012.