ネットワーク構築とファイアウォール関する実験

学籍番号 1250373
溝口 洸熙
グループ 5C

July 24th, 2023

1　目的

本実験では，VLAN とルータを用いて，ネットワークを分割する．また，所属するネットワークに対して NAPT を設定し，特定の通信以外を拒否し，加えてポートフォワーディングを設定する．

1.1　構築する理由

昨今，インターネットが普及し，家庭でも LAN を持つことが普通になっている．たとえば，集合住宅でインターネット回線を引くことを考える．建物全体で 1 つの LAN とし，各戸間でのネットワークを分離しない場合，別戸のネットワーク機器へのアクセスは容易である．各戸間でネットワークの分離することにより，各戸間でのやりとりに制限を設けられる．

また，1 つのスイッチ内に仮想的なスイッチを複数用意し，各ネットワークごとに L2 スイッチを設置せずとも，簡便に LAN を構築できる．

さらに，IPv4 アドレスの枯渇問題に対応すべく，プライベート IP アドレスとグローバル IP アドレスを対応づけて通信し，外部から直接 LAN 内ホストへのアクセスを禁止する．加えて，許可した通信以外を拒否する設定をし，LAN の安全性を高める．

1.2　構築するものの概要

LAN 間のネットワーク分離はルータを用いる．1 台のスイッチ内に仮想的なスイッチを用意する技術を VLAN（Virtual LAN）と呼び，本実験ではこれを採用する．

さらにプライベート IP アドレスとグローバル IP アドレスをポート番号をもとに動的に対応づけるしくみとして NAPT，特定通信以外を拒否するしくみとしてパケットフィルタリング，特定ポートの通信を特定ホストに転送するポートフォワーディングを採用する．ポートフォワーディングを設定することにより，パケットフィルタリングを実現できる．

2　内容

本実験では図 1 のネットワークを作成する．ルーティングの設定や NAPT は図 1 の `router5` に行う．

2.1　スイッチの設定

コンソールへ接続し，`telnet` での操作を可能にするため，L2 スイッチに IP アドレスを付与する．スパニングツリー機能を停止した後 VLAN を用いて，1 台のスイッチ内に 3 つのセグメント（**デフォルトセグメント**，**5C 班セグメント**，**5i 班セグメント**）を作成する．

2.2　ルータの初期設定

コンソールへ接続し，バックボーンの IP アドレス，5C 班のネットワークアドレス，5i 班のネットワークアドレスと各サブネットマスクを決定する．ルータへ IP アドレスを付与した後，ルーティングテーブルを作成する．動的ルーティングは OSPF を用い，デフォルトルートとしてメインルータ（`192.168.0.9`）を設定

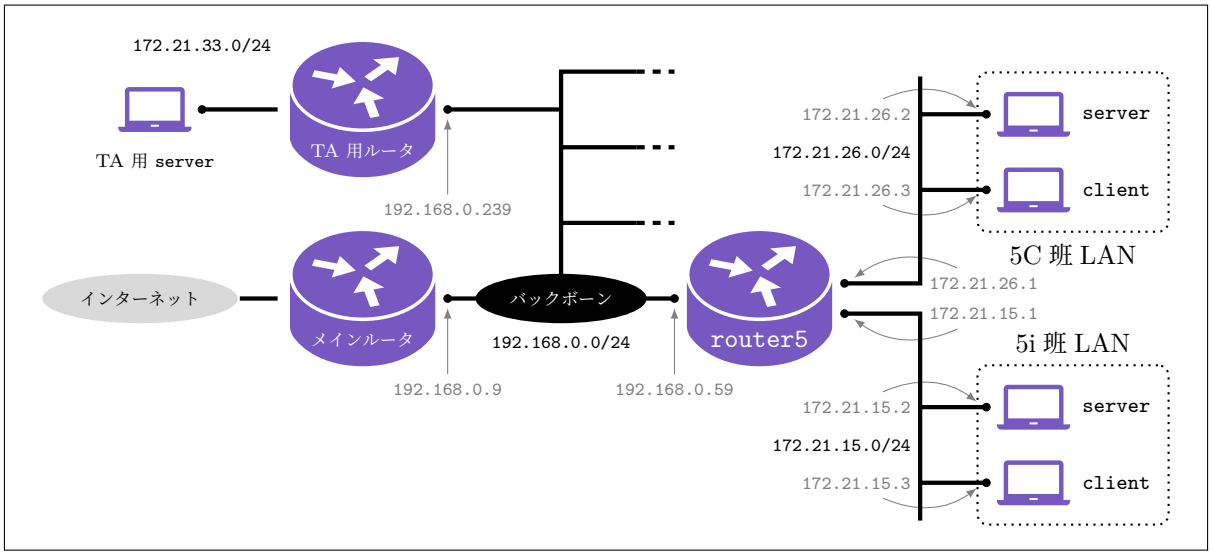


図 1　論理ネットワーク図（L2 スイッチは省略）

し，TA 班用への経路を静的経路として設定する．

2.3　ホストのネットワーク設定

サーバの IP アドレス，DNS ゾーンの設定，Apache の IP アドレス制限の設定を更新する．それに伴い，クライアントのネットワーク設定も更新する．

2.4　NAPT・ポートフォワーディングの設定

5C 班 LAN（内部）からバックボーン（外部），そして外部から内部へのアクセスを，以下のように router5 へ設定する．

- 内部から外部へは，動的 NAPT を用いて任意のアクセスを許可する．
- 外部からサーバ以外ホストへのアクセスを禁止する．
- 外部からサーバへ，静的 NAPT を用いて以下のアクセスを許可する．
  - DNS（TCP，UDP）
    宛先ポート 53 番，転送先ポート 53 番
  - Web（TCP）
    宛先ポート 80 番，転送先ポート 80 番
  - SMTP（TCP）
    宛先ポート 25 番，転送先ポート 25 番
  - SSH（TCP）
    宛先ポート 8022 番，転送先ポート 22 番

3　要素技術

3.1　ルーティングプロトコル

AS（Autonomous System）とは，経路制御に関するルールを決めて，それをもとに運用する範囲を指す．AS 内部の経路制御では IGP（Interior Gateway Protocol），AS 間の経路制御では EGP（Exterior Gateway Protocol）を用いる [1, p.173].

3.1.1　経路制御アルゴリズム

経路制御のアルゴリズムは大きく 2 つある．

■距離ベクトル型　距離と方向によってネットワークやホストの位置を決定し，これらの情報から経路制御表を作成する．処理は比較的簡単だが，ルータ間で交換される情報は距離と向きだけなので，ネットワークが複雑になると，経路の収束*に時間がかかる [1, p.174 - p.175].

■リンク状態型　ルータがネットワーク全体の接続状態を理解して経路制御表を作成する方法．ネットワークの構造は，どのルータにとっても同じなので，すべてのルータが同じ経路制御情報を持つ．ルータ間の経路制御情報をすばやく同期させれば，経路制御を安定させられる．リンク状態型は複雑なネットワークでも安定した経路制御をできるが，欠点としてネットワークトポロジーから経路制御表を作成する計算コストが高い [1, p.175].

3.1.2　主なルーティングプロトコル

主なルーティングテーブルと，方式について説明する．ここでは，RIP と OSPF を取り上げる．

分類	IGP		EGP
プロトコル名	RIP	OSPF	BGP
アルゴリズム	距離ベクトル型	リンク状態型	距離ベクトル型

■RIP　RIP（Routing Information Protocol）は，距離ベクトル型のルーティングプロトコルである．経路制御情報を 30 秒周期でブロードキャストし，情報を伝搬する（図 2）．距離が一番短い，つまりホップ数が最小になる経路を選択する [1, 2, p.276 - p.277, p.132].

■OSPF　OSPF（Open Shortest Path First）は，リンク状態型のルーティングプロトコルで各リンクに重みをつけ，この重みが最小となるような経路を選択する．ホップ数が最小でなくても，コストが最小の経路を選択する．図 3 の例では，ホップ数が最小の経路は Internet VPN でのコストが大きいため，コストが最小となる経路を経路を選択している．OSPF のコスト算出は，最大通信帯域が大きいほど小さな値が設定される [2, p.138].

*経路制御情報が安定すること．

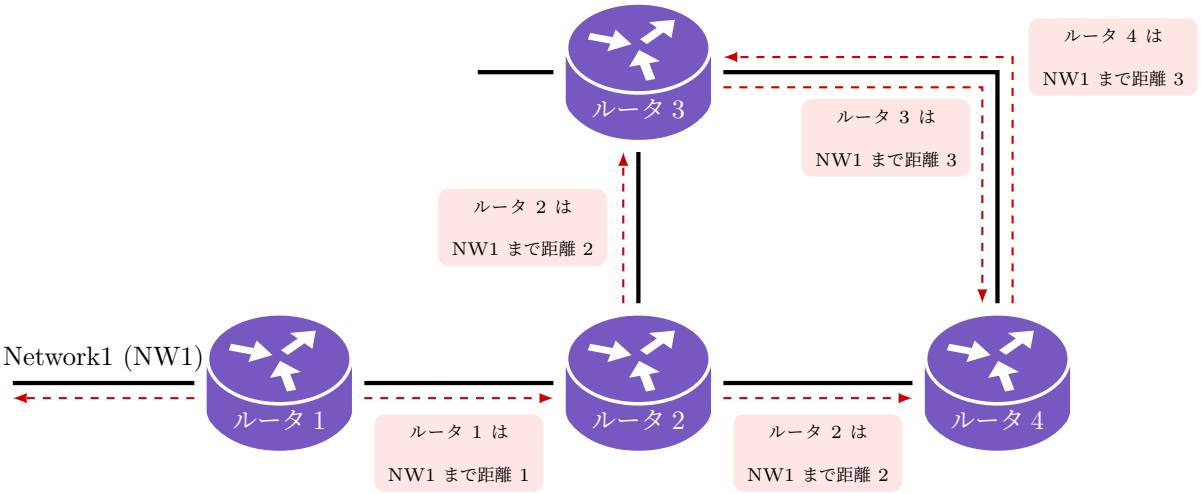
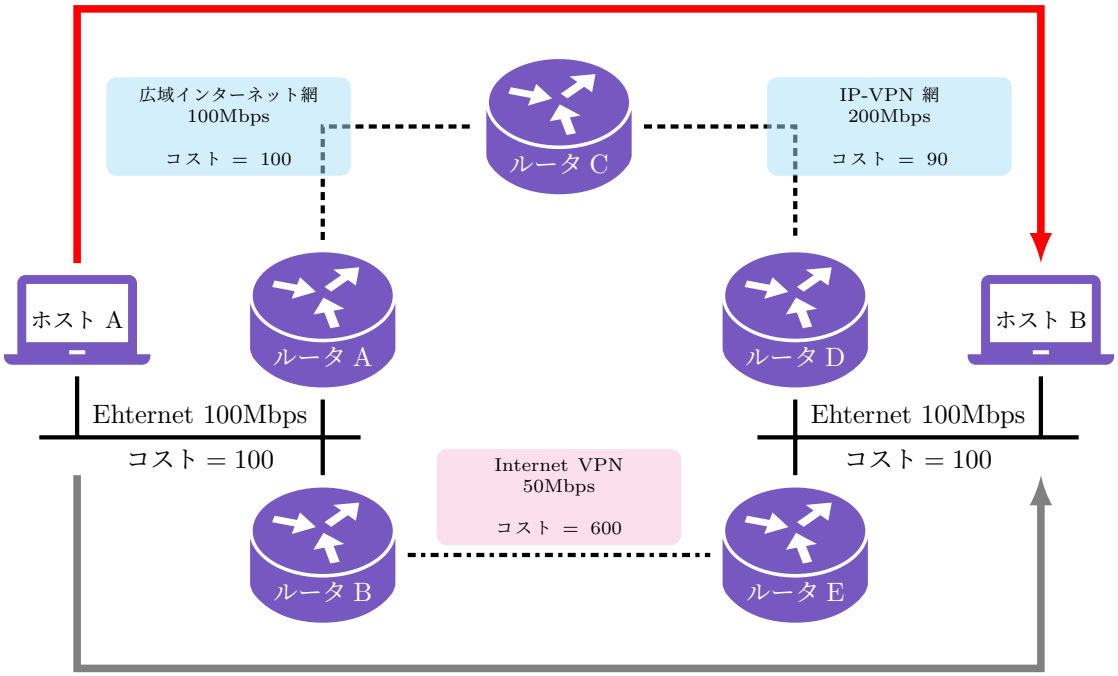


図 2　RIP の経路情報交換

OSPF での経路【ホップ数 = 3，総コスト = 390】



RIP での経路【ホップ数 = 2，総コスト = 800】

図 3　OSPF での経路選択 [1, p.284]

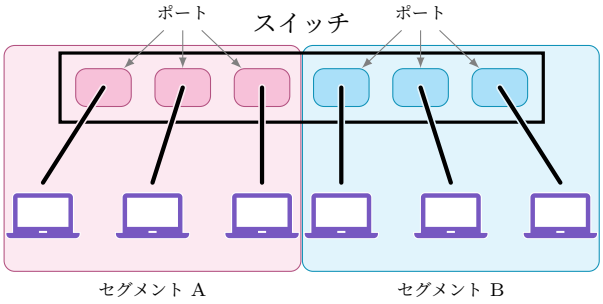


図 4　VLAN

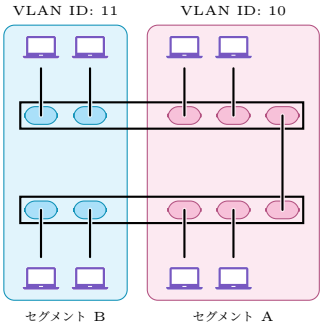


図 5　スイッチをまたいだ VLAN

3.2　VLAN

VLAN（Virtual LAN）とは，1 つの L2 スイッチに接続されていても，異なるセグメントとして設定でき，VLAN どうしの通信を一切遮断する技術である．この技術を用いることで，ポートごとのにセグメントを分割でき，ブロードキャストドメインを区切ることができる．これにより，ネットワーク負荷を軽減でき，安全性が向上する（図 4）．VLAN にはいくつか種類がある．

ポートベース VLAN　“1 台のハブにおいてポート別に VLAN を形成する”[3, p.71]．ここでのハブとは L2 スイッチである．

タグ VLAN　スイッチをまたいだ VLAN の構築（図 5）により，ネットワークの配線を変えずにネットワークの構造を変更でき，機器の節約につながる．この技術はタグ VLAN と呼ばれ，VLAN ID を各セグメントに定義し，Ethernet ヘッダに VLAN ID を付することで，どのセグメントにフレームを転送するか決める [1, p.105 - p.106]．

3.3　パケットフィルタ

パケットフィルタ（パケットフィルタリング）とは，ファイアウォールの一種であり，規定されたパケットのみを通過させるしくみだ．LAN 内の限定的なホストのみを外部から接続可能にすることが，パケットフィルタする目的の 1 つである．例として，ホストとサーバが同一ネットワーク上にあるとき，以下の制限を設ける．

- 外部からホストへのアクセスを禁止する．
- 外部からサーバへ，ポート 80 番でのアクセスのみ許可する．
- 内部から外部へ任意の接続を許可する．

これにより，外部からホストへのアクセスされるリスクが減る．外部からサーバへのポート 80 番以外のアクセスもパケットフィルタによりアクセスできないため，安全性が向上する．TCP コネクションは，`ACK`，`SYN` フラグを確認することで，内部から外部へのコネクション確立要求のみを許可できる．TCP の 3 ウェイ・ハンド・シェイクでの最初の手続き（`SYN` フラグのみが立ったパケット）が外部から来た場合は，そのパケットを破棄することで実現できる [1, p.343]．

3.4 NAPT

> “プライベートアドレスが割り当てられた端末も，外部ネットワークへの出口ルータでグローバルアドレスへの変換処理を行えば，外部インターネットに存在する端末と通信することができる．このアドレス変換を NAT（Network Address Translation）もしくは NAPT（Network Address Port Translation）と呼ぶ．” [4, p.97]

NAT を用いることで，LAN 内の IP アドレスを秘匿にでき，安全性が向上する．

■NAT　NAT とは，LAN 内で使用するプライベート IP アドレスと，インターネットに接続するとき使用するグローバル IP アドレスを変換する技術．しかし，変換先のグローバル IP アドレスが不足する．

■NAPT　IP アドレスだけでなく，TCP や UDP のポート番号も変換する技術．NAT で生じた変換先のグローバル IP アドレスが不足する問題は，NAPT を用いて解決できる．1 つのグローバル IP で複数のプライベート IP アドレスをポート番号により対応づけることで，グローバル IP アドレスを節約できる．NAPT には動的 NAPT と静的 NAPT があり，静的 NAPT は手動で NAT テーブルの変換エントリを登録し，ポートフォワーディングに用いられる．動的 NAPT は，プライベート IP アドレスとポート番号，グローバル IP アドレスとポート番号のテーブルを動的に設定する． [1]

4 作業記録

4.1 スイッチの設定

1. スイッチの電源を切り，スイッチからすべての配線を取り外す．コンソールケーブルをコンピュータの USB 端子に挿入し，/dev/ttyUSB0 が存在するか確認したのち，以下のコマンドを実行する．

```
# chmod 777 /dev/ttyUSB0
```

2. cu をインストールする．

```
# apt install cu
```

3. コンソールケーブルの一端をスイッチに挿入し，スイッチの電源を入れる．コンソールに接続するため，以下のコマンドを実行する．

```
# cu -l ttyUSB0 -s 9600
```

4. コンソールに接続できたら，スイッチのホスト名設定，パスワード設定，パスワードの暗号化，DNS ルックアップの無効化，コンソールの設定をする

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname switch5
switch5(config)# username exp password 0 root00
switch5(config)# service password-encryption
switch5(config)# no ip domain-lookup
```

```
switch5(config)# line console 0
switch5(config-line)# logging synchronous
```

5. VLAN1 へ，スイッチに遠隔ログイン用 IP アドレスを割り当てる．

```
switch5(config)# interface vlan1
switch5(config-if)# ip address 192.168.0.58 255.255.255.0
switch5(config-if)# no shutdown
switch5(config-if)# exit
```

6. telnet の許可設定をする．

```
switch5(config)# line vty 0 4
switch5(config-line)# password 0 root00
switch5(config-line)# login
switch5(config-line)# exit
```

7. スパニングツリーを無効にする．

```
switch5(config)# no spanning-tree vlan 1
```

8. VLAN を定義する．本実験では，1〜8 番ポートをバックボーン用，9〜16 番ポートを 5C 班用，17〜24 番ポートを 5i 班用の VLAN と定義する．また，VLAN 番号は班サブネットの第 3 オクテットとする．

```
switch5(config)# vlan 26
switch5(config-vlan)# name group5c
switch5(config-vlan)# exit
switch5(config)# vlan 15
switch5(config-vlan)# name group5i
switch5(config-vlan)# exit
switch5(config)# interface range fa0/9-16
switch5(config-if-range)# switchport mode access
switch5(config-if-range)# switchport access vlan 26
switch5(config-if-range)# exit
switch5(config)# interface range fa0/17-24
switch5(config-if-range)# switchport mode access
switch5(config-if-range)# switchport access vlan 15
switch5(config-if-range)# exit
```

9. 設定内容を保存する．

```
switch5# copy running-config startup-config
```

4.2 ルータの設定

1. ルータの電源を切り，スイッチからすべての配線を取り外す．コンソールケーブルをコンピュータの USB 端子に挿入し，/dev/ttyUSB0 が存在するか確認したのち，以下のコマンドを実行する．

```
# chmod 777 /dev/ttyUSB0
```

2. コンソールケーブルの一端をスイッチに挿入し，スイッチの電源を入れる．コンソールに接続するため，以下のコマンドを実行する．

```
# cu -l ttyUSB0 -s 9600
```

3. コンソールに接続できたら，ルータのホスト名設定，パスワード設定，パスワードの暗号化，DNS ルックアップの無効化，コンソールの設定をする

```
Router> enable
Router# configure terminal
Router(config)# hostname router5
router5(config)# username exp password 0 root00
router5(config)# service password-encryption
router5(config)# no ip domain-lookup
router5(config)# line console 0
router5(config-line)# logging synchronous
```

4. telnet の許可設定をする．

```
router5(config)# line vty 0 4
router5(config-line)# password 0 root00
router5(config-line)# login
router5(config-line)# exit
```

5. バックボーン側の IP アドレスを 192.168.0.59/24 に設定する．利用するインタフェースは FastEthernet2（FE2）．

```
router5(config)# interface fastEthernet2
router5(config-if)# switchport access vlan 1
router5(config-if)# no shutdown
router5(config-if)# exit
router5(config)# interface vlan1
router5(config-if)# ip address 192.168.0.59 255.255.255.0
router5(config-if)# no shutdown
router5(config-if)# exit
```

6. FastEthernet0 を 5i 班，FastEthernet1 を 5C 班に割り当て，それぞれ IP アドレスを設定する．

```
router5(config)# interface fastEthernet0
router5(config-if)# ip address 172.21.15.1 255.255.255.0
router5(config-if)# no shutdown
router5(config-if)# exit
router5(config)# interface fastEthernet1
router5(config-if)# ip address 172.21.26.1 255.255.255.0
router5(config-if)# no shutdown
router5(config-if)# exit
```

7. ルーティングを設定する．ルーティングプロトコルは OSPF を採用する．

```
router5(config)# router ospf 1
```

```
router5(config-router)# network 192.168.0.0 0.0.0.255 area 0
router5(config-router)# network 172.21.26.0 0.0.0.255 area 0
router5(config-router)# exit
```

8. 静的経路を設定する．デフォルト経路をメインルータ（192.168.0.9），TA 班への経路は TA 班のバックボーン IP アドレスを指定する．

```
router5(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.9
router5(config)# ip route 172.21.33.0 255.255.255.0 192.168.0.239
```

9. NAPT を設定する．内側から外側へ任意のアクセスを許可し，変換後の外側 IP アドレスを定義する．また，NAT の変換ルールを定義する．さらに，NAT の内側・外側を定義する．

```
router5(config)# access-list 1 permit 172.21.26.0 0.0.0.255
router5(config)# ip nat pool ipaddr 192.168.0.56 192.168.0.56 prefix-length
  24
router5(config)# ip nat inside source list 1 pool ipaddr overload
router5(config)# interface vlan1
router5(config-if)# ip nat outside
router5(config-if)# exit
router5(config)# interface fastEthernet1
router5(config-if)# ip nat inside
router5(config-if)# exit
```

10. NAPT を設定する．パケットフィルタ用のアクセスリストを要件に従って設定する．

```
router5(config)# ip nat inside source static tcp 172.21.26.2 25 192.168.0.59
  25
router5(config)# ip nat inside source static tcp 172.21.26.2 53 192.168.0.59
  53
router5(config)# ip nat inside source static udp 172.21.26.2 53 192.168.0.59
  53
router5(config)# ip nat inside source static tcp 172.21.26.2 80 192.168.0.59
  80
router5(config)# ip nat inside source static tcp 172.21.26.2 443 192.168.0.59
   443
router5(config)# ip nat inside source static tcp 172.21.26.2 22 192.168.0.59
  8022
```

11. 設定内容を保存する．

```
switch5# copy running-config startup-config
```

4.3 サーバとクライアントのネットワーク情報更新

各ホストの IP アドレスを図 1 に従って変更する．

■サーバの設定 以下のファイルを編集する．ここで c5.zone ファイルの A レコード server は，サーバの IP アドレスではなく，VLAN1 インタフェースの IP アドレスを入力する．これは，NAT により外から内部

の IP アドレスがわからないからである．クライアントへのアクセスは，外部から許可していないため，A レコード client はクライアントの IP アドレスを入力しても問題ない．

src. 1　/etc/netplan/00-install-config.yaml

```
# This is network config written by 'subiquity'
network:
    version: 2
    ethernets:
        enp0s31f6:
            addresses:
                - 172.21.26.2/24
            routes:
                - to: default
                  via: 172.21.26.1
            nameservers:
                addresses:
                    - 172.21.26.2
            dhcp4: false
```

src. 2　/etc/bind/c5.zone

```
$TTL    100
@       IN      SOA   server.c5.exp.info.kochi-tech.ac.jp. postmaster.c5.exp.info.
  kochi-tech.ac.jp. (
                2023061901
                100
                100
                100
                100  )
        IN      NS      server.c5.exp.info.kochi-tech.ac.jp.
server  IN      A       192.168.0.59
www     IN      CNAME   server
client  IN      A       172.21.26.3
... 略 ...
```

ファイルの書き込みが終われば，以下のコマンドを実行する．

```
# netplan apply
# systemctl restart bind9
# systemctl restart named
```

■クライアントの設定　クライアントのネットワーク設定ウィザードで，IP アドレスを 172.21.26.3 へ設定する．DNS サーバを 172.21.26.2，デフォルトゲートウェイを 172.21.26.1 へ設定する．

4.4　配線

図 6 のように，ルータとスイッチ間を接続し，サーバとクライアントをスイッチと接続する．同じ VLAN 内なら，スイッチ上のどのポートに挿しても良い．

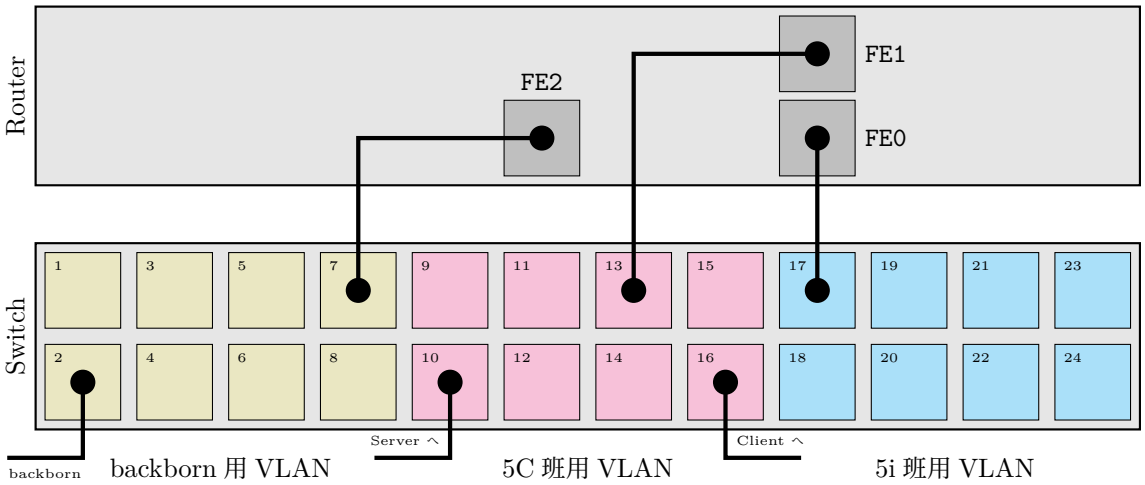


図 6　ルータとスイッチの配線

4.5　動作確認

TA サーバ, メインルータ (192.168.0.9), インターネット (たとえば 8.8.8.8) に ping が通るか確認する. また，TA サーバ上にある，アクセス者の IP アドレスを確認する CGI（http://172.21.33.2/index.cgi）にアクセスし，192.168.0.59 と，バックボーン側の IP アドレスが表示されるか確認する．これは NAPT を通して，5C 班 LAN 内の IP アドレスが秘匿になっていることを示している．最後に，traceroute コマンドで，TA サーバまで，2 台のルータを経由していることを確認する.

4.6　設定確認

src. 3　スイッチの設定情報

```
switch5#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5,
   Fa0/6
                                                 Fa0/7, Fa0/8
15   groupi5                           active    Fa0/17, Fa0/18, Fa0/19, Fa0/20,
  Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
26   groupc5                           active    Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0
  /13
                                                 Fa0/14, Fa0/15, Fa0/16
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
15   enet  100015     1500  -      -      -        -    -        0      0
26   enet  100026     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

src. 4　ルータの設定情報

```
router5#show running-config
Building configuration...

Current configuration : 2632 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname router5
!
boot-start-marker
boot-end-marker
!
enable password 7 071D2E435A5949
!
no aaa new-model
!
!
dot11 syslog
!
!
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
username exp password 7 095E41060D5547
!
```

```
!
archive
 log config
  hidekeys
!
!
!
!
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet0
 ip address 172.21.15.1 255.255.255.0
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.21.26.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 ip address 192.168.0.59 255.255.255.0
 ip access-group 101 in
 ip nat outside
 ip virtual-reassembly
!
```

```
router ospf 1
 log-adjacency-changes
 network 172.21.15.0 0.0.0.255 area 0
 network 172.21.26.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.0.9
ip route 172.21.33.0 255.255.255.0 192.168.0.239
!
!
no ip http server
no ip http secure-server
ip nat pool ipaddr 192.168.0.59 192.168.0.59 prefix-length 24
ip nat inside source list 1 pool ipaddr overload
ip nat inside source static tcp 172.21.26.2 25 192.168.0.59 25 extendable
ip nat inside source static tcp 172.21.26.2 53 192.168.0.59 53 extendable
ip nat inside source static udp 172.21.26.2 53 192.168.0.59 53 extendable
ip nat inside source static tcp 172.21.26.2 80 192.168.0.59 80 extendable
ip nat inside source static tcp 172.21.26.2 443 192.168.0.59 443 extendable
ip nat inside source static tcp 172.21.26.2 22 192.168.0.59 8022 extendable
!
access-list 1 permit 172.21.26.0 0.0.0.255
access-list 101 permit tcp any 172.21.15.0 0.0.0.255 established
access-list 101 permit ip any host 192.168.0.59
access-list 101 permit tcp any host 172.21.15.2 eq domain
access-list 101 permit udp any host 172.21.15.2 eq domain
access-list 101 permit tcp any host 172.21.15.2 eq smtp
access-list 101 permit tcp any host 172.21.15.2 eq www
access-list 101 permit tcp any host 172.21.15.2 eq 443
access-list 101 permit tcp any host 172.21.15.2 eq 22
access-list 101 permit icmp any host 172.21.15.2
access-list 101 permit udp any eq domain host 172.21.15.2
!
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
 line aux 0
line vty 0 4
 password 7 1317181D1F5C54
 login
!
```

```
end

router5#show ip interface brief
Interface                  IP-Address      OK? Method Status
  Protocol
BRI0                       unassigned      YES NVRAM  administratively down down
BRI0:1                     unassigned      YES unset  administratively down down
BRI0:2                     unassigned      YES unset  administratively down down
FastEthernet0              172.21.15.1     YES NVRAM  up                    down
FastEthernet1              172.21.26.1     YES NVRAM  up                    up
FastEthernet2              unassigned      YES unset  up                    up
FastEthernet3              unassigned      YES unset  up                    down
FastEthernet4              unassigned      YES unset  up                    down
FastEthernet5              unassigned      YES unset  up                    down
FastEthernet6              unassigned      YES unset  up                    down
FastEthernet7              unassigned      YES unset  up                    down
FastEthernet8              unassigned      YES unset  up                    down
FastEthernet9              unassigned      YES unset  up                    down
NVI0                       172.21.15.1     YES unset  up                    up
Vlan1                      192.168.0.59    YES NVRAM  up                    up
router5#show access-list
Standard IP access list 1
    10 permit 172.21.26.0, wildcard bits 0.0.0.255 (15 matches)
Extended IP access list 101
    10 permit tcp any 172.21.15.0 0.0.0.255 established
    20 permit ip any host 192.168.0.59 (63 matches)
    30 permit tcp any host 172.21.15.2 eq domain
    40 permit udp any host 172.21.15.2 eq domain
    50 permit tcp any host 172.21.15.2 eq smtp
    60 permit tcp any host 172.21.15.2 eq www
    70 permit tcp any host 172.21.15.2 eq 443
    80 permit tcp any host 172.21.15.2 eq 22
    90 permit icmp any host 172.21.15.2
    100 permit udp any eq domain host 172.21.15.2
router5#show ip nat trans
router5#show ip nat translations
Pro Inside global         Inside local          Outside local         Outside
  global
tcp 192.168.0.59:8022     172.21.26.2:22        ---                   ---
tcp 192.168.0.59:25       172.21.26.2:25        ---                   ---
tcp 192.168.0.59:53       172.21.26.2:53        ---                   ---
udp 192.168.0.59:53       172.21.26.2:53        ---                   ---
tcp 192.168.0.59:80       172.21.26.2:80        ---                   ---
tcp 192.168.0.59:443      172.21.26.2:443       ---                   ---
router5#exit
```

5　考察

昨今，官民問わずサイバー攻撃が後を絶たない．近年は，組織的な犯罪で，金銭を目的とした商業的な，巧妙で対策の難しいサイバー攻撃が増加している [5]．無論，大学というインターネットに比べると小さな規模のネットワークでも，危険は潜んでいる．たとえば，タグ VLAN は，Ethernet ヘッダに VLAN ID を付することで所属するセグメントを認識している．パケットは簡単に書き換えられるので，悪意のあるものが VLAN ID を書き換え，所属する LAN とは別の LAN へパケットが漏れる可能性もある．これは，A 研究室と B 研究室のネットワークを VLAN で区切っている状況下では，A 研究室のホストが B 研究室の LAN へアクセスできることを示唆している．この対策として，VLAN ID をハッシュ化してヘッダに付し，さらに，スイッチ間で VLAN ID を同期し，VLAN ID をフレームごとに変更するワンタイム VLAN ID を導入することで解決できるのではないだろうか．

参考文献

[1] 直也井上, 公保村山, 隆史竹下, 透荒井, 幸雄苅田．マスタリング TCP/IP 入門編（第 6 版）．オーム社, 2019.

[2] 原山美知子．インターネット工学（シリーズ知能機械工学）．シリーズ知能機械工学. 共立出版, 2014.

[3] 村上泰司．ネットワーク工学, 第 2 版. 森北出版, 2014.

[4] 阪田史郎, 井関文一, 小高知宏．情報通信ネットワーク（IT text）．IT text. オーム社, 2015.

[5] 長谷川皓一．動的ネットワーク構成によるサイバー攻撃対策支援手法の研究．PhD thesis, 名古屋大学, 2017.

本レポートで描画した図の一部は，ヤマハ株式会社の公開済図形（`https://network.yamaha.com/support/download/tool/`）を利用している．