ネットワーク構築

細川 夏風

2025 年 11 月 25 日

1 目的

近年，クラウド化の影響のによってネットワークの重要性がより大きくなった．しかし，“Amazon Web Service”(以下:“AWS”) や “Azure”，“Google Cloud Platform” などによってネットワーク内部に触れる機会は大きく減少している．それが引き起こす問題として，この実験直前に起こった “AWS” のシステム障害を起因とする大規模なシステム障害である．これは市場が “AWS” の寡占状態にあったことも問題の一つであるが，ネットワーク内部に触れるエンジニアの割合が市場の規模に適していないからであると私は考えている．そのため，今回のような有事の際にネットワークを構築可能になるためにデファクトスタンダードである “Cisco” 社製のスイッチやルータを用いて LAN 環境の構築やルータのルーティングテーブルの設定を行うことができる様になる必要がある．また，昨今過激化しているサイバー攻撃に対する防衛意識を高めるためにもその玄関口とも言えるネットワークの基礎を学ぶことが重要である．現環境を支えているインフラストラクチャーを知ることがこれからの自身の学びに繋がるのである．

2 内容

今回構築したネットワークは主にレイヤ 3(以下:L3) までの階層で動作する．いくつかの段階からこのネットワークは構築されている．ネットワークの構成図を以下に示す．

(1). デバイス同士で通信を行うために L2 のスイッチ (以下: スイッチ) の MAC アドレステーブルを用いて，Ethernet で通信を行う．ただし，昨今のほとんどでは IP アドレスが用いられている．今回もその例外ではない．そのため，ARP コマンドを用いて IP アドレスから相手の MAC アドレスを調べている [2].

(2). 今実験ではスイッチの数が足りないため，スイッチの VLAN 機能を用いる．この機能でスイッチを仮想的に 2 つに分割する．これにより，異なる VLAN に接続したデバイス同士は通信が行えない．ユーザがポートを選択し，静的にポートをそれぞれの VLAN に割り振る．

(3). その異なる VLAN に接続しているデバイス同士の通信を行うために L3 のルータを用いる．

ルータに存在するルーティング機能を用いて，2 つのセグメントに別れたデバイスに情報を送信する．

(4). 更に上位のルータを用いて，自班のルータのルーティングテーブルに他の班の情報を書き込み，他の班との通信を行う．上位ルータと接続のためにポートを用いるが，その際スイッチのポートの数が足りなくなるため，今実験では `Switch Virtual Interface`(`SVI`，L3 スイッチの機能) を用いる．この機能はルータに `VLAN` の機能を加えたものである．この機能によりルータのスイッチポートに `VLAN` を割り当てることができる [1]． 本大学のネットワーク経由で yahoo.co.jp に接続する。この接続における名前解決には、本大学の DNS サーバーが用いられる．

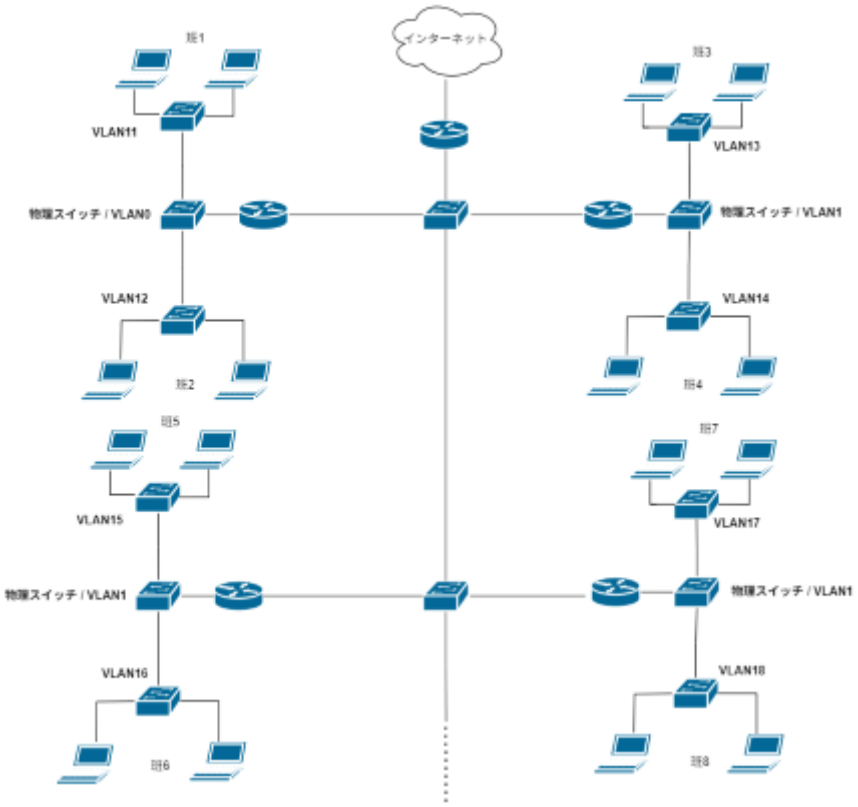

図 1　ネットワークの全体像

3 作業記録

3.1 スイッチの VLAN 構築

```
Switch>en
```

このコマンドで現在のスイッチの設定を確認している.

```
Switch#show running-config
Current configuration : 2901 bytes
! version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
! hostname Switch !
```

確認だけでなく，設定を変更できるようにしている.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch1
```

パスワードの設定

```
switch1(config)#username exp password -0 root00
```

パスワードの暗号化

```
switch1(config)#enable password 0 root00
switch1(config)#service password-encryption
```

DNS ルックアップの無効化 (入力された文字列をドメインと認識し，それについて DNS が検索するのを防ぐ役割)[4]

```
switch1(config)#no ip domain--lookup
switch1(config)#line con 0
switch1(config-line)#logging synchronous
switch1(config-line)#exit
switch1(config)#vlan 11
switch1(config-vlan)#name group1
```

```
switch1(config-vlan)#exit
```

この部分は間違えて “Fa” とコマンドを打つはずだったが “fa” と入力しているため，その後のコマンドで LAN をうまく分割できていない.

```
switch1(config)#int range fa0/9-16
switch1(config-if-range)#swithport mode access vlan 11

switch1(config-if-range)#exit
switch1(config)#no spanning-tree vlan 11
switch1(config)#exit
switch1#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
                                 Fa0/9, Fa0/10,Fa0/11,Fa0/12
                                 Fa0/13,Fa0/14,Fa0/15,Fa0/16
                                 Fa0/17,Fa0/18,Fa0/19,Fa0/20
                                 Fa0/21,Fa0/22,Fa0/23,Fa0/24
11   group1                           active

switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)#int range Fa0/9-16
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 11
switch1(config-if-range)#exit
switch1(config)#exit
switch1#
*Mar  1 00:15:30.942: %SYS-5-CONFIG_I: Configured from console by
   console
switch1#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
                                    Fa0/17,Fa0/18,Fa0/19,Fa0/20
                                    Fa0/21,Fa0/22,Fa0/23,Fa0/24
11   group1           active        Fa0/9, Fa0/10,Fa0/11,Fa0/12
                                    Fa0/13,Fa0/14,Fa0/15,Fa0/16

switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)#vlan 12
switch1(config-vlan)#name group2
switch1(config-vlan)#exit
switch1(config)#int range Fa0/17-24
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 12
switch1(config-if-range)#exit
switch1(config)#no spaning-tree vlan 12
switch1(config)#exit
switch1#show
*Mar  1 00:17:33.290: %SYS-5-CONFIG_I: Configured from console by
   console
switch1#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
11   group1           active    Fa0/9, Fa0/10,Fa0/11,Fa0/12
                                Fa0/13,Fa0/14,Fa0/15,Fa0/16
12   group2           active    Fa0/17,Fa0/18,Fa0/19,Fa0/20
                                Fa0/21,Fa0/22,Fa0/23,Fa0/24
```

3.2 ルータの設定

```
Would you like to enter the initial configuration dialog? [yes/no]:
   no

Press RETURN to get started!
```

```
Router>
Router>en
Router#configure

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain lookup

Router(config)#username exp password 0 root00
Router(config)#enable password 0 root00
Router(config)#hostname router1
router1(config)#exit
router1#
*Jan  1 00:12:34.211: %SYS-5-CONFIG_I: Configured from console by
   console
router1#show running-config

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
! hostname router1 !
! enable password root00 !

router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#service pass
router1(config)#service password-encryption
router1(config)#exit
router1#show
*Jan  1 00:13:52.183: %SYS-5-CONFIG_I: Configured from console by
   console
router1#show run

Current configuration : 1006 bytes
```

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! hostname router1 !
boot-start-marker
boot-end-marker
! enable password 7 111B160A03425B
! no aaa new-model !
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#interface fastEthernet 0
router1(config-if)#ip address
```

ルータのポートに対して IP アドレス (デフォルトゲートウェイに当たる) を割り振る.

```
router1(config-if)#ip address 172.31.10.1 255.255.255.0
router1(config-if)#no shutdown
router1(config-if)#
*Jan  1 00:17:28.631: %LINK-3-UPDOWN: Interface FastEthernet0,
   changed state to up
router1(config-if)#exit
router1(config)#int fa1
```

前述と同様

```
router1(config-if)#ip address 172.31.11.1 255.255.255.0
router1(config-if)#no shutdown
router1(config-if)#exit
*Jan  1 00:18:26.515: %LINK-3-UPDOWN: Interface FastEthernet1,
   changed state to up
```

ここからは SVI の機能を用いて，スイッチポートとの仮想的なポートにデフォルトゲートウェイを割り振っている.

```
router1(config)#int fa2
router1(config-if)#switchport access vlan 1
router1(config-if)#no shutdown
router1(config-if)#exit
```

```
router1(config)#int vlan1
router1(config-if)#ip add

router1(config-if)#ip address 192.168.1.11 255.255.255.0
router1(config-if)#no shutdown
```

デフォルトルートの設定 (静的に設定したルーティングテーブルのどれにも当てはまらない場合に用いられる)

```
router1(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
router1(config)#int vlan1
router1(config)#exit
router1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
           level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
           static route
       o - ODR, P - periodic downloaded static route

;以下上部は省略
Gateway of last resort is not set
router1#conf t
```

ルーティングテーブルの作成 (間違っている)

```
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.12
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.13
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.14
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.15
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.16
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.17
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.18
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.19
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.20
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.21
```

```
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.22
router1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.23
router1(config)#exit
router1#show ip route
*Jan  1 00:30:20.183: %SYS-5-CONFIG_I: Configured from console by
   console
Gateway of last resort is not set

router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#ip route 172.31.12.0 255.255.255.0 192.168.1.12
router1(config)#exit
router1#show ip route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.31.0.0/24 is subnetted, 3 subnets
C       172.31.11.0 is directly connected, FastEthernet1
C       172.31.10.0 is directly connected, FastEthernet0
S       172.31.12.0 [1/0] via 192.168.1.12
C    192.168.1.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.1.1
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#ip route 172.31.12.0 255.255.255.0 192.168.1.13
router1(config)#exit
router1#show ip route
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.31.0.0/24 is subnetted, 3 subnets
C       172.31.11.0 is directly connected, FastEthernet1
C       172.31.10.0 is directly connected, FastEthernet0
S       172.31.12.0 [1/0] via 192.168.1.13
                    [1/0] via 192.168.1.12
C    192.168.1.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

```
router1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.

router1(config)#ip route 172.31.13.0 255.255.255.0 192.168.1.13
router1(config)#ip route 172.31.14.0 255.255.255.0 192.168.1.13
router1(config)#ip route 172.31.15.0 255.255.255.0 192.168.1.13
router1(config)#ip route 172.31.12.0 255.255.255.0 192.168.1.12
router1(config)#ip route 172.31.13.0 255.255.255.0 192.168.1.12
router1(config)#exit
router1#show ip route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.31.0.0/24 is subnetted, 6 subnets
C       172.31.11.0 is directly connected, FastEthernet1
C       172.31.10.0 is directly connected, FastEthernet0
S       172.31.15.0 [1/0] via 192.168.1.13
S       172.31.14.0 [1/0] via 192.168.1.13
S       172.31.13.0 [1/0] via 192.168.1.13
                    [1/0] via 192.168.1.12
S       172.31.12.0 [1/0] via 192.168.1.13
                    [1/0] via 192.168.1.12
C    192.168.1.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.1.1
router1#config
```

この 2 行は間違えたテーブルの部分を削除している.

```
router1(config)#no ip route 172.31.13.0 255.255.255.0 192.168.1.13
router1(config)#no ip route 172.31.12.0 255.255.255.0 192.168.1.13
```

```
router1(config)#exit
router1#
*Jan  1 00:52:58.851: %SYS-5-CONFIG_I: Configured from console by
   consoleshow
router1#show ip route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.31.0.0/24 is subnetted, 6 subnets
C       172.31.11.0 is directly connected, FastEthernet1
C       172.31.10.0 is directly connected, FastEthernet0
S       172.31.15.0 [1/0] via 192.168.1.13
S       172.31.14.0 [1/0] via 192.168.1.13
S       172.31.13.0 [1/0] via 192.168.1.12
S       172.31.12.0 [1/0] via 192.168.1.12
C    192.168.1.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.1.1
router1#config
router1(config)#ip route 172.31.16.0 255.255.255.0 192.168.1.14
router1(config)#ip route 172.31.17.0 255.255.255.0 192.168.1.14
router1(config)#ip route 172.31.18.0 255.255.255.0 192.168.1.15
router1(config)#ip route 172.31.19.0 255.255.255.0 192.168.1.15
router1(config)#ip route 172.31.20.0 255.255.255.0 192.168.1.16
router1(config)#ip route 172.31.21.0 255.255.255.0 192.168.1.16
router1(config)#ip route 172.31.22.0 255.255.255.0 192.168.1.17
router1(config)#ip route 172.31.23.0 255.255.255.0 192.168.1.17
router1(config)#ip route 172.31.24.0 255.255.255.0 192.168.1.18
router1(config)#ip route 172.31.25.0 255.255.255.0 192.168.1.18
router1(config)#ip route 172.31.26.0 255.255.255.0 192.168.1.19
router1(config)#ip route 172.31.27.0 255.255.255.0 192.168.1.19
router1(config)#ip route 172.31.28.0 255.255.255.0 192.168.1.20
router1(config)#ip route 172.31.29.0 255.255.255.0 192.168.1.20
router1(config)#ip route 172.31.30.0 255.255.255.0 192.168.1.21
router1(config)#ip route 172.31.31.0 255.255.255.0 192.168.1.21
router1(config)#ip route 172.31.32.0 255.255.255.0 192.168.1.22
router1(config)#ip route 172.31.33.0 255.255.255.0 192.168.1.22
router1(config)#ip route 172.31.34.0 255.255.255.0 192.168.1.23
router1(config)#exit
router1#
*Jan  1 00:59:22.743: %SYS-5-CONFIG_I: Configured from console by
   console
router1#show ip route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.31.0.0/24 is subnetted, 25 subnets
S       172.31.34.0 [1/0] via 192.168.1.23
S       172.31.33.0 [1/0] via 192.168.1.22
S       172.31.32.0 [1/0] via 192.168.1.22
S       172.31.19.0 [1/0] via 192.168.1.15
S       172.31.18.0 [1/0] via 192.168.1.15
S       172.31.17.0 [1/0] via 192.168.1.14
S       172.31.16.0 [1/0] via 192.168.1.14
S       172.31.23.0 [1/0] via 192.168.1.17
S       172.31.22.0 [1/0] via 192.168.1.17
S       172.31.21.0 [1/0] via 192.168.1.16
S       172.31.20.0 [1/0] via 192.168.1.16
S       172.31.27.0 [1/0] via 192.168.1.19
S       172.31.26.0 [1/0] via 192.168.1.19
S       172.31.25.0 [1/0] via 192.168.1.18
S       172.31.24.0 [1/0] via 192.168.1.18
S       172.31.31.0 [1/0] via 192.168.1.21
S       172.31.30.0 [1/0] via 192.168.1.21
S       172.31.29.0 [1/0] via 192.168.1.20
S       172.31.28.0 [1/0] via 192.168.1.20
C       172.31.11.0 is directly connected, FastEthernet1
C       172.31.10.0 is directly connected, FastEthernet0
S       172.31.15.0 [1/0] via 192.168.1.13
S       172.31.14.0 [1/0] via 192.168.1.13
S       172.31.13.0 [1/0] via 192.168.1.12
S       172.31.12.0 [1/0] via 192.168.1.12
C    192.168.1.0/24 is directly connected, Vlan1
S*   0.0.0.0/0 [1/0] via 192.168.1.1
router1#
router1#
router1#show ip route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```
     172.31.0.0/24 is subnetted, 25 subnets
S       172.31.34.0 [1/0] via 192.168.1.23
S       172.31.33.0 [1/0] via 192.168.1.22
S       172.31.32.0 [1/0] via 192.168.1.22
S       172.31.19.0 [1/0] via 192.168.1.15
S       172.31.18.0 [1/0] via 192.168.1.15
S       172.31.17.0 [1/0] via 192.168.1.14
S       172.31.16.0 [1/0] via 192.168.1.14
S       172.31.23.0 [1/0] via 192.168.1.17
S       172.31.22.0 [1/0] via 192.168.1.17
S       172.31.21.0 [1/0] via 192.168.1.16
S       172.31.20.0 [1/0] via 192.168.1.16
S       172.31.27.0 [1/0] via 192.168.1.19
```

以上のログについては必要のない部分を一部削除しています.

4 考察

今回は静的にルーティングテーブルを作成したが，一般にそのような方法が取られているケースは少ない．それぞれのデバイスとルータで通信を行い経路情報を交換し，ルーティングテーブルを作成するダイナミックルーティングという方法が取られている．これは静的ルータィングと違ってデバイスに多少がかかるが，基本的に複雑化しやすいルーティングの管理を簡単にするためだ．そのルーティングについて現在は “Border Gateway Protocol(以下:BGP)” という手法が用いられている．これには “Autonomous System(以下:AS)” と呼ばれる ISP:Internet Service Provider や地域ネットワークを組織をひとまとまりにしたものが用いられている [3]．これにはセキュリティに関する重大な問題があり，“BGP” には IP アドレスと AS の整合性を確かめる方法を持っていない．そのため，ある IP アドレスに対して攻撃者の所属している AS を指定すれば，場合により世界中のルータがこれまでの対応関係を無視してルーティングを行う．これにより，ハイジャックされたサイトの URL もしくは IP を入力すると，攻撃者のサーバまで届いてしまう．これに対して “Resource Public-Key Infrastructure(RPKI)” という技術が用いられている．これは IP アドレスと AS の登録に電子署名を用いる方法である．これにより不正な登録によるハイジャックは成功しなくなってきている [5]．しかし，この技術も完璧ではない．正当な AS までのパスの途中に攻撃者を書き足すことでこれを回避できる．それに対するさらなる対策として文献 [5] 内で Autonomous System Provider Authorization(ASPA) が紹介されている．これは送られてくる AS についてのホワイトリストを作り，そのホワイトリスト内にない AS から送られてくると，不正な通信であると検知するシステムである．これはまだ実用段階にないため，その効果については議論できない．

参考文献

[1] CiscoLAN スイッチの教科書 著者: シスコシステムズ合同会社，基盤技術グループ 発行所: 株式会社インプレス 発行年:2017 年 5 月 1 日

[2] ネットワークはなぜつながるのか 著者: 利根勤 発行所: 日経 BP 社 発行年:2003 年 1 月 17 日

[3] マスタリング TCP/IP 入門篇 第 5 版 著者: 竹下 隆史，松山 公保，荒井 透，苅田 幸雄 発行所: 株式会社オーム社 発行年:2014 年 5 月 20 日

[4] コンピュータネットワーク入門 著者: 小口 正人 発行所: 株式会社サイエンス社 発行年:2023 年 9 月 15 日

[5] “RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins,” in *Proceedings of the Internet Measurement Conference (IMC '19)*, Amsterdam, Netherlands: ACM, 2019, pp. 406–419 著者:Taejoong Chung，Balakrishnan Chandrasekaran，Bruce M. Maggs，John Rula，Emile Aben，David Choffnes，Alan Mislove，Tim Bruijnzeels，Dave Levin，Roland van Rijswijk-Deij，Nick Sulliva