

## 各章末の演習問題

※記述式の解答については、理解を促すために本文とはあえて別の書き方をしており、さらにその語の初出以降の内容等も含めた書き方をしています。ただし、同じでないから不正解ではなく、内容（意味）が合致していれば正解で大丈夫です。

### 第1章

1. 次の10進数を2進数に変換せよ。

(1) 14→1110

(2) 75→1001011

(3) 135→10000111

(4) 237→11101101

2. 次の2進数を10進数に変換せよ。

(1) 100111→39

(2) 10011101→157

(3) 11000011→195

(4) 10000000→128

(5) 11000000→192

(6) 11100000→224

(7) 11110000→240

(8) 11111000→248

3. 次の2進数2つの論理積を取れ。

(1) 10010101 と 11010001→10010001

(2) 01000101 と 11011010→01000000

4. 次の10進数2つの論理積を取れ。答えは10進数で答えよ。

(1) 127 と 63→01111111 と 00111111→00111111→63

(2) 167 と 52→10100111 と 00110100→00100100→36

(3) 95 と 237→01011111 と 11101101→01001101→77

(4) 193 と 165→11000011 と 10100101→10000001→129

5. 次のIPアドレス（前の番号）とサブネットマスク（後の番号）の論理積を取るとどうなるか答えよ。

① 192.168.2.4 と 255.255.255.252→192.168.2.4

② 172.24.236.192 と 255.255.224.0→172.24.224.0

③ 124.156.223.145 と 255.192.0.0→124.128.0.0

6. ルータは第3層、スイッチは第2層など、ネットワーク機器はなぜ2層や3層に分類されるのか説明せよ。

ルータはIPアドレスを使ってデータを送受信し、スイッチはMacアドレスを使ってデータを送受信することから、第3層で扱うのがIPアドレス、第2層で扱うのがMacアドレスであることより、ネットワーク機器をどのようなアドレスを扱っているかで層で分類される。

7. 次のカッコ内を埋めよ。カッコ内に文字が書いてあるものはどちらか○をせよ。

① プロトコルとは（通信での約束事）のことである。

② MACアドレスは（WAN LAN）で使われるアドレスであり、（16）進数の（12）桁で表現され、2進数では（48）ビットで表現される。またMACアドレ

スは物理アドレスとも呼ばれ、書き換えることができない。

- ③ IP アドレスは ( WAN LAN ) で使われるアドレスであり、一般に 10 進数を 3 つのドットで 4 つに区切って表現される。その区切られた部分には 10 進数で (0) から (255) までの値が入る。IP アドレス全体は 2 進数で (32) ビットで表現される。また IP アドレスは論理アドレスとも呼ばれ、書き換えることができる。
- ④ IP アドレスは、(ネットワーク) 部と (ホスト) 部に分かれる。

8. 次の IP アドレスに関する事柄について答えよ。

- ① ネットワークアドレスとは何か (どのような役割があるか) 説明せよ。  
そのアドレス群を代表するアドレス、またそのアドレス群全体を表すアドレス、さらにルータで使うアドレス。
- ② サブネットマスクとは何か (どのような役割があるか) 説明せよ。  
IP アドレスからネットワークアドレスを抽出するためのもの。IP アドレスとこのマスクを論理積することに寄ってネットワークアドレスが抽出できる。
- ③ デフォルトゲートウェイとは何か (なぜ設定する必要があるのか) 説明せよ。  
※3 章で出てくる内容でした。その内容を踏まえれば、LAN につながっているネットワークにあるルータのインターフェイスのことで、別のネットワークアドレスを持つネットワークへの入り口の役目をするために、(別のネットワークアドレスを持つネットワークに送信する場合には設定する必要がある (P.))
- ④ IP アドレスにおいて、クラス A か B か C かというのにはどのような違いがあるのか説明せよ。
  - ・配布できる IP アドレスに違いがある。クラス A では約 16700 万個、クラス B では 65536 個、クラス C では 256 個である。
  - ・ネットワーク部とホスト部の長さが違う。クラス A はネットワーク部が第 1 オクテットのみの 1 オクテット (8 ビット) に対し、ホスト部は第 2~4 オクテットの 3 オクテット (24 ビット) であり、同様にクラス B ではネットワーク部とホスト部がいずれも 2 オクテット (16 ビット)、クラス C ではネットワーク部が 3 オクテット (24 ビット) でホスト部が 1 オクテット (8 ビット) である。
  - ・第 1 オクテット目を 2 進数にした際に、先頭が 0 なのがクラス A, 10 なのがクラス B, 110 なのが C である。
- ⑤ グローバルアドレスおよびプライベートアドレスについて説明せよ。  
インターネットに接続する為に必要な IP アドレスをグローバルアドレス、また研究や実験、インターネットにつながらない、またはインターネットから隔離されているネットワークを構築する時に使う IP アドレスをプライベートアドレスという。
- ⑥ ネットワークアドレスおよびブロードキャストアドレスについて説明せよ。  
クラス A, B, C いずれの場合でも、最初の IP アドレスをネットワークアドレスと呼び、そのアドレス群を代表するものである。また最後の IP アドレスをブロー

ドキャストアドレスと呼び、そのアドレス群全てのホスト（PC等）にデータを届けるためのものである。

9. 次のネットワーク機器の機能（役割）をそれぞれ説明せよ。同じような用途の機器の場合は、それぞれの違いを明確にして答えること。

① リピータ

PC同士をつなぐ機器。HUBと違い、ポートが2つしかなく、データを遠い所へ送るために使われる。

② HUB（ハブ）

PC同士をつなぐ機器。HUBと違い、ポートが3つ以上ある。スイッチと異なり、データを入れて来たポート以外のポート全てに送信する。

③ スイッチ

PC同士をつなぐ機器、HUBと違い、MACアドレスを使い、データを宛先のポートのみに送信する。

④ ルータ

ルータ同士をつなぐ機器。IPアドレスを使って、データを送受信する。

10. IPアドレスに関する次の事柄について答えよ。

① グローバルアドレスおよびプライベートアドレスについて説明せよ。

インターネットに接続をするために必要なIPアドレスをグローバルアドレスと呼び、世界で唯一で重複してはいけない。またインターネットと隔離されたり、インターネットと直接接続しないようなネットワークを構築する場合に使われるIPアドレスをプライベートアドレスと呼び、指定された範囲のものを利用する。

② ネットワークアドレスおよびブロードキャストアドレスについて説明せよ。

そのネットワークのアドレスの範囲の最初のアドレスをネットワークアドレスと呼び、そのネットワークを代表するアドレスを意味し、ルータのルーティングテーブルで利用される。そのネットワークのアドレス範囲の最後のアドレスをブロードキャストアドレスと呼び、そのアドレス範囲の全てのアドレスと通信するために利用される。

11. カプセル化とは何か説明せよ。

ISO7層モデルにおいて、7層から1層へデータが作成される際に、IPアドレスやMacアドレス等を付けていくことが、カプセルをかぶせていくかのようになることから、このデータの作成の過程をカプセル化という。

12. 次のTCP/IPに関する問いに答えよ。

① TCPとUDPの信頼性について、コネクション型・コネクションレス型という言葉を用いるべく使って説明せよ。

TCPは送信したデータが相手に到着したかを確認するコネクション型の通信を利用してデータの信頼性を保つのにに対し、UDPは到着を確認しないコネクションレ

ス型の通信をするのでデータの信頼性は低い。

- ② TCP/UDP におけるポート番号とは何か，説明せよ。

受信したデータをどのプロトコルに受け渡すかを区別するために，プロトコルごとに番号を付けている。この番号のことをポート番号という。

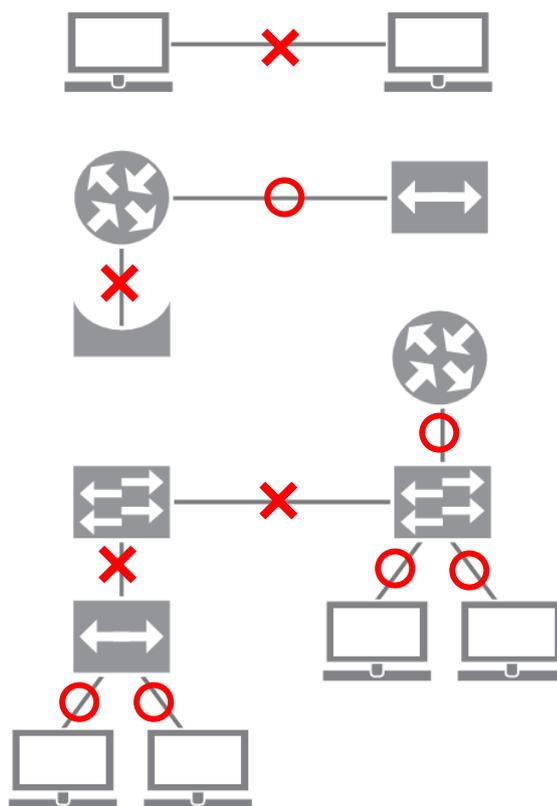
- ③ TCP/IP モデルとは何か，OSI 参照モデルと対応させながら説明せよ。

OSI 参照モデルが一般的なネットワーク（でのデータの変化）を表しているのに対し，TCP/IP モデルは現在の WAN や LAN（でのデータの変化）を表しているものである。

## 第2章

1. 次の機器群を LAN ケーブルで配線したい。それぞれ，ストレートケーブル，クロスケーブルのどちらで配線すべきか。ストレートケーブルの場合には線上に○を，クロスケーブルの場合には線上に×を全ての配線について書け。

例 ストレート  クロス 



2. なぜ LAN ケーブルには「ストレート」と「クロス」の区別があるのか説明せよ。

ネットワーク機器は、その種類によって送信ポートと受信ポートの位置が異なっている。そのため、そのままつないでも送信ポートと受信ポートが直接つながる場合は「ストレート」ケーブルを使い、直接つながらない場合はつながるようにケーブルを交差させる「クロス」ケーブルを使う必要があるため、ストレートとクロスの区別がある。

- よく使われている LAN ケーブルは最大何メートル先の PC やネットワーク機器にデータを届けることができるか、答えよ。 **100m**
- 各ネットワーク機器間を LAN ケーブルで接続する場合、ストレートとクロスのどちらを接続すべきかが分かる“図”を書け。 : P.45 図 2. 10 を参照して下さい。

### 第 3 章

- 次の図から情報を読み取り、以下の空欄を埋めよ。④については説明をせよ。ただし、いずれの場合もサブネットマスクはデフォルトのサブネットマスク（クラス B の場合は 255.255.0.0, C の場合は 255.255.255.0）が設定されているとする。

#### ①PC0（左側の PC）の

ネットワークアドレス (172.16.0.0)

ブロードキャストアドレス (172.16.255.255)

デフォルトゲートウェイ (172.16.255.254)

※ただし、デフォルトゲートウェイは有効な IP アドレスの一番最後の IP アドレスに設定されている。

#### ②PC1（右側の PC）の

ネットワークアドレス (192.168.2.0)

ブロードキャストアドレス (192.168.2.255)

デフォルトゲートウェイ (192.168.2.2)

#### ③Router0 のルーティングテーブル

| アドレス           | インターフェイス |
|----------------|----------|
| 192.168.1.0/24 | S0       |
| 192.168.2.0/24 | S0       |
| 172.16.0.0/16  | fa0      |

- 前問③のルーティングテーブルで、データがなぜ的確にルーティングされるのかを説明せよ（例えば、192.168.2.1宛のデータが、③のルーティングテーブルでなぜルーティングできるのかを説明すればよい）。

192.168.2.1宛でのデータが Router0 に受信された場合、(ネットワーク) アドレス欄に

書かれているサブネットマスクと論理積され、その結果/24 と論理積した結果である 192.168.2.0 に対応したインターフェイスである S0 ヘルパーティングすることで、宛先である 192.168.2.1 方向へデータを送ることができる。

#### 第4章

1. MAC アドレステーブルとはどんなものか、説明せよ。

スイッチにおいて、宛先 MAC アドレスがあるポートにデータを出すために、接続されている PC 等の MAC アドレスとポート（インターフェイス）の対応が掲載されている表のことである。

2. MAC アドレステーブルはどのように“自動的に”学習がなされるのか、具体的な例を示して説明せよ。

スイッチに入ってきたフレームの送信元 MAC アドレスを、MAC アドレステーブルにそのフレームが入ってきたポート（インターフェイス）と共に記録することで、自動的に学習される形となる。

3. 次のスイッチの方式の名称を答えよ。

- ① 受信フレームの宛先 MAC アドレスを受信時に読み取った時点でフォワーディングを行う。カットスルー
- ② フレームの最初の 64 バイトを受信してエラーチェックを行った上でフレームを転送する。フラグメントフリー
- ③ フレーム全体をチェックしてアドレスを調べる一方、エラーの有無をチェックする。：ストア&フォワード

#### 第5章

1. ルーティングプロトコルとは何か、またなぜ必要か説明せよ。

ルーティングテーブルを自動的に構築するためのプロトコルをルーティングプロトコルと呼ぶ。ルーティングプロトコルはこのように管理者が手動で構築する必要がない他、ルートが使えなくなったりまた新しいルートが使えるようになったりした場合も自動的に最適なルートを使えるようにするため、手間がかからないという観点から必要となる。

2. スタティックルーティングの特徴をダイナミックルーティングと対比して説明せよ。

ルーティングテーブルを自動で構築するダイナミックルーティングに対し（管理者が）手動で構築することをスタティックルーティングと呼ぶ。またダイナミックルーティングはルートが変化しても自動的にルーティングテーブルを変更するが、スタティックルーティングでは手動で変更しなければならない。しかしながら、ダイナミックルーティングはメモリ、CPU、帯域を使うのに対してスタティックルーティングはこれらをあまり使わないため高速にルーティングできるというメリットがある。

3. ダイナミックルーティングの特徴をスタティックルーティングと対比して説明せよ。  
スタティックルーティングはルーティングテーブルを手動で作成する必要があるが、ダイナミックルーティングは自動で作成することができる。またルートが変化した時も自動でルーティングテーブルを変更することができる。しかしながら、スタティックルーティングに比べてCPUやメモリ、帯域幅をつかってしまうというデメリットもある。
4. あるルータで「show ip route」を行った時、次のような表示となった（一部を抜粋）。
- ① 最初の「C」や「R」は何を意味しているか。直接接続（C）かどのルーティングプロトコル（RはRIP）でそのルートを学習したかを意味している。
  - ② 「172.21.0.0/16 [120/1] via 172.17.1.1, 00:00:07, FastEthernet0/0」の次のものはそれぞれ何を意味しているか説明せよ。
    - (ア) 172.21.0.0/16：ネットワークアドレス
    - (イ) via 172.17.1.1：そのネットワーク（アドレス）がどのIPアドレスを経由して到達できるか
    - (ウ) FastEthernet0/0：そのネットワークアドレスが接続しているインターフェイス
- ※P.51の説明も参照
5. 自律システム及び自律システム番号とは何か説明せよ。  
自律システムは会社や学校などの組織のことを指し、自律システムはその自律システムに振られている番号のことである。
6. ディスタンスベクタ型のルーティングプロトコルとはどういうものか説明せよ。  
距離と方向で経路を決定するルーティングプロトコルである。ただし、回線速度を考慮しないため、遅い回線を選んでしまう可能性がある。
7. リンクステート型のルーティングプロトコルとはどういうものか説明せよ。  
回線の速度を考慮するほか、ネットワーク全体の地図を持つようなルーティングプロトコルである。ただし、CPUやメモリ、帯域を使ってしまうというデメリットもある。
8. ダイナミックルーティングで使用しているAD値（アドミニストレーティブディスタンス値）とはどのようなものか説明せよ。  
複数のルーティングプロトコルが利用されている場合、複数のルートが選ばれる場合がある。このような時、各ルーティングプロトコルに優先度のような数値を付けて、その数値が低いものを優先して選ぶようにする時に使うこの数値をAD値と呼ぶ。
9. 次のルーティングプロトコルのAD値を答えよ。
- 直接接続（ 0 ） スタティックルート（ 1 ） RIP（ 120 ）  
EIGRP（ 90 ）

10. メトリック値とは何か。説明せよ。

そのルータから宛先ネットワークまで到達するのに必要な“コスト”となる値のことをメトリック値と言う。RIP はルータの数、OSPF は回線の速さをメトリック値としており、これらが小さいものが良いルートとして選ばれる。

11. 次のルーティングプロトコルをディスタンスベクタ型、リンクステート型、ハイブリッド型に分類せよ。

EIGRP (ハイブリッド型) OSPF (リンクステート型) RIP (ディスタンスベクタ型)

12. 経路集約とは何か説明せよ。

ルーティングテーブルを小さくする目的で、ルーティングに支障がない形で、ルートをまとめること。例えば、同じインターフェイスに送信すれば良い 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 の3つのネットワークアドレスを 192.168.0.0/16 のように1つにすることで、ルーティングテーブルを小さくできる。

13. 以下の図のルータの接続において OSPF が動作するとして、次の問に答えよ。

- ①このネットワークにおける OSPF を設定するコマンドを書け。ただし、いずれもサブネットマスクは/24 である (2つめの解答は2行にわたって書いてもよい)

Router(config)#

router ospf 1

Router(config-router)#

network 202.251.172.0 0.0.0.255 area 0

- ②DR ルータと BDR ルータとなるルータを選出せよ。

DR ルータ : R4

BDR ルータ : R3

## 第6章

1. ARP について、なるべく簡潔に説明せよ。その際、「ARP 要求」「ARP 応答」「ブロードキャスト」「ユニキャスト」という言葉を使って説明せよ。

ARP は、IP アドレスからそれに対応する MAC アドレスを調べるために使われるプロトコルである。実際には、MAC アドレスを調べたい PC 等からブロードキャストで「この IP アドレスに対応する MAC アドレスは何番か」のような“ARP 要求”を“ブロードキャスト”により送信する。それを受け取った対応する PC 等は「MAC アドレスは\*\*番です」のような“ARP 応答”として“ユニキャスト”により送信した PC に送り出す。

## 第7章

1. コリジョンおよびコリジョンドメインとは何か，説明せよ．また，コリジョンドメインを分割する機器・しない機器についても説明せよ．

コリジョンとは，複数の PC 等から同時にデータが送信された場合に，ネットワーク内でそれらデータが衝突してしまうことを指す．またこのコリジョンが起こる可能性がある範囲のことをコリジョンドメインと呼ぶ．ハブはコリジョンドメインを分割しないが，スイッチやルータは分割する．

2. ブロードキャストおよびブロードキャストドメインとは何か，説明せよ．またブロードキャストドメインを分割する機器・しない機器についても説明せよ．

ブロードキャストは全ての PC 等にデータを送信することを指す．またこのブロードキャストが届く範囲のことをブロードキャストドメインと呼ぶ．ハブやスイッチはブロードキャストドメインを分割しないが，ルータは分割する．

3. 次の各ネットワークにはコリジョンドメイン及びブロードキャストドメインはいくつあるか答えよ．

コリジョンドメイン : (A) 2 (B) 5 (C) 4  
ブロードキャストドメイン : (A) 1 (B) 3 (C) 1

4. イーサネットおよび IEEE 802.3 で使われている CSMA/CD (キャリア検知多重アクセス/衝突検出) 方式とはどういうものか説明せよ．

通信を行いたい PC はケーブル内にデータが通信されていないかどうかを調べ (CS に相当)，通信していなければデータを送信する．この状態ではどの PC からでも通信が可能である (MA に相当)．もし同時にデータが送信された場合にはコリジョンが起きるためそれを検出し (CD に相当)，もしコリジョンが起きたらそれを検知した送信元 PC がジャム信号を送信し，ネットワーク全体にそれを通知する．このジャム信号を受信した PC はバックオフアルゴリズムを行い，ランダムな時間待機させ，この待機が終了した PC からデータを送信させることでコリジョンが起こらないようにする．  
※説明としては CS,MA,CD と CD が起こった際の動作の要点について説明するのが良い．

5. 全二重と半二重とは何か説明せよ．

送信と受信を同時に行うことができることを全二重といい，逆に送信か受信かどちらか一方しかできないことを半二重という．

## 第8章

1. 192.168.1.0/24 のアドレスを 8 分割する場合を，“表”の形で作成せよ．

| サブネットマスク | ネットワークアドレス   | 有効アドレス最初     | 有効アドレス最後     | ブロードキャストアドレス |
|----------|--------------|--------------|--------------|--------------|
| /27      | 192.168.1.0  | 192.168.1.1  | 192.168.1.30 | 192.168.1.31 |
| /27      | 192.168.1.32 | 192.168.1.33 | 192.168.1.30 | 192.168.1.31 |

|     |               |               |               |               |
|-----|---------------|---------------|---------------|---------------|
| /27 | 192.168.1.64  | 192.168.1.65  | 192.168.1.62  | 192.168.1.63  |
| /27 | 192.168.1.96  | 192.168.1.97  | 192.168.1.126 | 192.168.1.127 |
| /27 | 192.168.1.128 | 192.168.1.129 | 192.168.1.158 | 192.168.1.159 |
| /27 | 192.168.1.160 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 |
| /27 | 192.168.1.192 | 192.168.1.193 | 192.168.1.126 | 192.168.1.127 |
| /27 | 192.168.1.224 | 192.168.1.225 | 192.168.1.254 | 192.168.1.255 |

2. 172.16.0.0/16 のアドレスを 16 分割する場合を、“表”の形で作成せよ.

| サブネットマスク | ネットワークアドレス   | 有効アドレス最初     | 有効アドレス最後       | ブロードキャストアドレス   |
|----------|--------------|--------------|----------------|----------------|
| /20      | 172.16.0.0   | 172.16.0.1   | 172.16.15.254  | 172.16.15.255  |
| /20      | 172.16.16.0  | 172.16.16.1  | 172.16.31.254  | 172.16.31.255  |
| /20      | 172.16.32.0  | 172.16.32.1  | 172.16.47.254  | 172.16.47.255  |
| /20      | 172.16.48.0  | 172.16.48.1  | 172.16.63.254  | 172.16.63.255  |
| /20      | 172.16.64.0  | 172.16.64.1  | 172.16.79.254  | 172.16.79.255  |
| /20      | 172.16.80.0  | 172.16.80.1  | 172.16.95.254  | 172.16.95.255  |
| /20      | 172.16.96.0  | 172.16.96.1  | 172.16.111.254 | 172.16.111.255 |
| /20      | 172.16.112.0 | 172.16.112.1 | 172.16.127.254 | 172.16.127.255 |
| /20      | 172.16.128.0 | 172.16.128.1 | 172.16.143.254 | 172.16.143.255 |
| /20      | 172.16.144.0 | 172.16.144.1 | 172.16.159.254 | 172.16.159.255 |
| /20      | 172.16.160.0 | 172.16.160.1 | 172.16.175.254 | 172.16.175.255 |
| /20      | 172.16.176.0 | 172.16.176.1 | 172.16.191.254 | 172.16.191.255 |
| /20      | 172.16.192.0 | 172.16.192.1 | 172.16.207.254 | 172.16.207.255 |
| /20      | 172.16.208.0 | 172.16.208.1 | 172.16.223.254 | 172.16.223.255 |
| /20      | 172.16.224.0 | 172.16.224.1 | 172.16.239.254 | 172.16.239.255 |
| /20      | 172.16.240.0 | 172.16.240.1 | 172.16.255.254 | 172.16.255.255 |

3. 172.16.0.0/16 のアドレスを 512 分割する場合を、“表”の形で作成せよ. ※

| サブネットマスク | ネットワークアドレス     | 有効アドレス最初       | 有効アドレス最後       | ブロードキャストアドレス   |
|----------|----------------|----------------|----------------|----------------|
| /25      | 172.16.0.0     | 172.16.0.1     | 172.16.0.126   | 172.16.0.127   |
| /25      | 172.16.0.128   | 172.16.0.129   | 172.16.0.254   | 172.16.0.255   |
| /25      | 172.16.1.0     | 172.16.1.1     | 172.16.1.126   | 172.16.1.127   |
| /25      | 172.16.1.128   | 172.16.1.129   | 172.16.1.254   | 172.16.1.255   |
| .....    | .....          | .....          | .....          | .....          |
| /25      | 172.16.254.0   | 172.16.254.1   | 172.16.254.126 | 172.16.254.127 |
| /25      | 172.16.254.128 | 172.16.254.129 | 172.16.254.254 | 172.16.254.255 |
| /25      | 172.16.255.0   | 172.16.255.1   | 172.16.255.126 | 172.16.255.127 |
| /25      | 172.16.255.128 | 172.16.255.129 | 172.16.255.254 | 172.16.255.255 |

4. 10.0.0.0/8 のアドレスを 2048 分割する場合を、“表”の形で作成せよ. ※

※この問題は表にすると多くの行を要するので、表の前 2~4 行、後ろ 2~4 行を書けば良い.

| サブネットマスク | ネットワークアドレス   | 有効アドレス最初     | 有効アドレス最後       | ブロードキャストアドレス   |
|----------|--------------|--------------|----------------|----------------|
| /19      | 10.0.0.0     | 10.0.0.1     | 10.0.31.254    | 10.0.31.255    |
| /19      | 10.0.32.0    | 10.0.32.1    | 10.0.63.254    | 10.0.63.255    |
| /19      | 10.0.64.0    | 10.0.64.1    | 10.0.95.254    | 10.0.95.255    |
| /19      | 10.0.96.0    | 10.0.96.1    | 10.0.127.254   | 10.0.127.255   |
| .....    | .....        | .....        | .....          | .....          |
| /19      | 10.255.128.0 | 10.255.128.1 | 10.255.159.254 | 10.255.159.255 |
| /19      | 10.255.160.0 | 10.255.160.1 | 10.255.191.254 | 10.255.191.255 |

|     |              |              |                |                |
|-----|--------------|--------------|----------------|----------------|
| /19 | 10.255.192.0 | 10.255.192.1 | 10.255.223.254 | 10.255.223.255 |
| /19 | 10.255.224.0 | 10.255.224.1 | 10.255.255.254 | 10.255.255.255 |

5. 次の IP アドレスが有効アドレスか無効アドレスか判別せよ。できればその理由も答えよ。

- ① 192.168.1.72/29    ② 172.16.17.0/20    ③ 10.128.0.0/9    ④ 172.24.254.255/24

① 192.168.1 .01001000

255.255.255.11111000

⇒サブネットマスクの 0 の部分がすべて 0 なので無効アドレス (ネットワークアドレス)

② 172.16 .00010001.00000000

255.255.11110000.00000000

⇒サブネットマスクの 0 の部分がすべて 0 や 1 ではないので有効アドレス

③ 10 .10000000.00000000.00000000

255.10000000.00000000.00000000

⇒サブネットマスクの 0 の部分がすべて 0 なので無効アドレス (ネットワークアドレス)

④ 172.24.11111110.11111111

255.255.11111111.00000000

⇒サブネットマスクの 0 の部分がすべて 1 なので無効アドレス (ブロードキャストアドレス)

## 第9章

1. CDP とはどんなプロトコルか説明せよ。

隣接する Cisco 社のルータやスイッチの型番やインターフェイスの情報を取得することができるプロトコルである。

2. Cisco 以外のルータやスイッチで CDP と同様の機能を持つプロトコルの名称を答えよ。 : LLDP

3. tracert コマンドがどのようなもので、その仕組み (なぜそのようなことができるか) を説明せよ。

tracert は、宛先 IP アドレスまでの過程、特に途中で通過するルータの IP アドレスを知ることができる。tracert は icmp の TTL が 0 になると送信元に TimeExceeded エラーが送られることを利用し、TTL を 1, 2・・・と設定して送信することで、TTL が 0 になったルータの IP アドレスを知ることができるため、通過したルータの IP アドレスを知ることができる。

## 第 10 章

1. アクセスリストとはどのようなものか説明せよ。

ルータで送信・受信 IP アドレスやポート番号、Ping などで許可/拒否をするために記述するリストのことである。

2. 標準アクセスリストと拡張アクセスリストの違いについて説明せよ。

標準アクセスリストは送信元 IP アドレスしか指定できないが、拡張アクセスリストは加えて宛先 IP アドレス、ポート番号や Ping を指定することができる。

3. 標準アクセスリストと拡張アクセスリストをルータのインターフェイスに設定する場合に基本的な基準（ルール）がある。それを説明せよ。できればなぜそのようなルールが存在するのかを説明せよ。

標準アクセスリストは宛先近くのインターフェイスで設定をし、拡張アクセスリストは送信元近くのインターフェイスで設定をする。これは、標準アクセスリストは送信元しか指定できないため、送信元近くで設定してしまうと宛先以外のネットワークも許可や拒否をしてしまう可能性がある。また拡張アクセスリストは宛先 IP アドレスを指定できるため、送信元近くに設定しても他の送信データを許可/拒否しない他、データを早く許可/拒否できるので余計な通信をさせないメリットもある。

4. 次のネットワークにおいて、次のような制限および許可ができるようにアクセスリストを作成し、どのルータのどのインターフェイスに設定するかを決定せよ。ただし、標準アクセスリスト、拡張アクセスリストのどちらでもできる場合はその 2 つを答え、拡張アクセスリストでしかできない場合はその 1 つを答えよ。

※いずれの問題も別解（別の書き方）があるので、そのあたりはご判断いただきたい

- ① 172.16.1.0 ネットワークからサーバ 0 (172.16.5.0 ネットワーク) への全ての通信を拒否し、それ以外の通信は全て許可する。

標準アクセスリスト：Router 2 で access-list 1 deny 172.16.1.0 0.0.0.255

インターフェイス：Router2 の 172.16.5.0 側インターフェイスの outbound で

拡張アクセスリスト：Router0 で access-list 100 deny ip 172.16.1.0 0.0.0.255 172.16.5.0 0.0.0.255

インターフェイス：Router0 の 172.16.1.0 側インターフェイスの inbound で

- ② 172.16.3.0 ネットワークからサーバ 0 (172.16.5.0 ネットワーク) とサーバ 1 (192.168.1.0 ネットワーク) への全ての通信を拒否し、それ以外の通信は全て許可する。

標準アクセスリスト：①Router 2 で access-list 1 deny 172.16.3.0 0.0.0.255

インターフェイス：Router2 の 172.16.5.0 側インターフェイスの outbound で

②Router1 の access-list 1 deny 172.16.3.0 0.0.0.255

インターフェイス：Router1 の 172.16.1.0 側インターフェイスの outbound で

拡張アクセスリスト：Router1 で access-list 100 deny ip 172.16.3.0 0.0.0.255 172.16.5.0 0.0.0.255

access-list 100 deny ip 172.16.3.0 0.0.0.255 172.16.1.0 0.0.0.255

インターフェイス：Router0 の 172.16.3.0 側インターフェイスの inbound で

- ③ PC1 からサーバ 0 への一切のアクセスはできないがそれ以外の通信はすべて許可する。

標準アクセスリスト：Router 2 で access-list 1 deny 172.16.1.2 0.0.0.0

インターフェイス：Router2 の 172.16.5.0 側インターフェイスの outbound で

(※この場合、サーバ 0 だけでなく 172.16.5.0 ネットワークへの通信が全て拒否される)

拡張アクセスリスト：Router0 で access-list 100 deny ip 172.16.1.1 0.0.0.0 172.16.5.1 0.0.0.255

インターフェイス：Router0 の 172.16.1.0 側インターフェイスの inbound で

- ④ PC3 からの全ての WEB サーバへの閲覧を禁止し、それ以外の通信は許可する。

拡張アクセスリスト：Router1 で access-list 100 deny tcp 172.16.3.2 0.0.0.0 172.16.5.1 0.0.0.0 eq 80

access-list 100 deny tcp 172.16.3.2 0.0.0.0 192.168.1.1 0.0.0.0 eq 80

インターフェイス：Router1 の 172.16.3.0 側インターフェイスの inbound で

- ⑤ セキュリティ対策として、サーバ群の全ての ping を拒否したい。その他の全ての通信は拒否しない。

拡張アクセスリスト：Router1 で access-list 100 deny icmp any 172.16.5.1 0.0.0.0 echo

access-list 100 deny icmp any 192.168.1.1 0.0.0.0 echo

インターフェイス：Router2 の 172.16.4.0 側インターフェイスの inbound で

- ⑥ 172.16.3.0 ネットワークからは、172.16.1.0 ネットワークへのネットワークアクセスのみを許可し、それ以外のネットワークへのアクセスは全て拒否する。

拡張アクセスリスト：Router1 で access-list 100 permit ip 172.16.3.0 0.0.0.255 172.16.1.0 0.0.0.255

インターフェイス：Router1 の 172.16.3.0 側インターフェイスの inbound で

(標準アクセスリストでも可能であるが、複雑になるので省略)

5. 前問の①を、名前付きアクセスリストで実現せよ。

標準アクセスリスト：Router 2 で ip access-list standard std1

deny 172.16.1.0 0.0.0.255

インターフェイス：Router2 の 172.16.5.0 側インターフェイスの outbound で(ip access-group std1 out)

拡張アクセスリスト：Router0 で ip access-list extended ext1

deny ip 172.16.1.0 0.0.0.255 172.16.5.0 0.0.0.255

インターフェイス : Router0 の 172.16.1.0 側インターフェイスの inbound で(ip access-group ext1 in)

## 第 11 章

1. 次の NAT に関する問いに答えよ.

① NAT および PAT のような技術がなぜ必要なのか説明せよ.

NAT は内部の IP アドレスを外部に出さないことからセキュリティが向上し、また ISP の移行時には内部の IP アドレスを変更する必要がないことから移行が楽になる。特に PAT を利用すると多くの内部の IP アドレスを 1 つのグローバル IP アドレスで代替できることから、近年の IPv4 アドレスの枯渇問題を解決することができる。

② NAT における「ダイナミック変換」と「スタティック変換」について説明せよ.

スタティック変換は内部の IP アドレスと外部の IP アドレスを一対一で対応させるもので、その対応は変化しないが、ダイナミック変換はアドレスプールと呼ばれる IP アドレス群の中から適当に選ばれ対応させるもので、内部と外部の IP アドレスの対応は一対一ではなく変化する。

③ PAT とは何か、NAT との共通点・相違点を明らかにしながら説明せよ.

PAT は NAT 同様に、内部と外部の IP アドレスを変換するものであるが、NAT は一般的にそれらを一対一あるいは複数の内部アドレスを複数の外部アドレスに変換するが、PAT はポート番号を用いて全ての内部アドレスを 1 つの外部アドレスに変換することで、グローバル IP アドレスを節約することができる。

④ ルータで NAT (ダイナミック変換) を設定しようとする。指示された設定をするためのコマンドを空欄の中に埋めよ。空欄の下のアドレス等は、上のコマンドに続くものである。

○パブリック IP アドレスプールの定義 (プール名 : cutt)

```
Router(config)# ip nat pool cutt  
199.99.9.40 199.99.9.45 netmask 255.255.255.224
```

○内部プライベート IP アドレスに一致するアクセスリストの定義 (リスト番号 : 2)

```
Router(config)# access-list 2 permit  
10.10.10.0 0.0.0.255
```

○内部リストから外部プールへの NAT 変換の定義 (アクセスリストとアドレスプールの対応付け)

```
Router(config)# ip nat inside source  
list 2 pool cutt
```

○内部・外部インターフェイスの指定 (イーサネット側 : 内部, シリアル側 : 外部)

```
Router(config)# interface serial 0
```

```
Router(config-if)# ip nat outside
```

---

```
Router(config-if)# interface fastethernet 0
```

```
Router(config-if)# ip nat inside
```

---

⑤次の図中のルータで PAT が設定されている場合、PC から WWW サーバへデータを送信する際の次のアドレスはそれぞれどれか。表の空欄を埋めよ。

| 内部ローカルアドレス   | 内部グローバルアドレス  | 外部ローカルアドレス  | 外部グローバルアドレス |
|--------------|--------------|-------------|-------------|
| 172.24.105.5 | 202.23.32.45 | 202.23.32.1 | 202.23.32.1 |

## 第 12 章

### 1. DHCP とは何をするプロトコルか、説明せよ。

IP アドレスやサブネットマスクなどを、サーバからの情報で自動的に設定するためのプロトコル。

### 2. DHCP でなぜ IP アドレスを自動的に振ることができるのか、その仕組み（動作）について説明せよ。

- ① PC から DHCP を探すためのフレームをブロードキャストで（DHCP サーバに）送信する
- ② ①のデータを受け取った DHCP サーバは IP アドレス等のデータのフレームをブロードキャストで（PC に）送信する
- ③ ②を受け取った PC はこの IP アドレス等を受け入れるというフレームをブロードキャストで（DHCP サーバに）送信する
- ④ ③を受け取った DHCP サーバはこの受入を承認するというフレームをブロードキャストで（PC に）送信する。

## 第 13 章

### 1. VLAN とは何か説明せよ。

スイッチのポートを番号で管理し、番号が同じポート間では通信できるが、違うポート間では通信できないようにして、あたかも複数のスイッチかのように使う方法。

### 2. VLAN におけるトランキング（トランク）とは何か説明せよ。

複数のスイッチで VLAN を設定する場合、そのままだと（最低でも）VLAN の数だけポートを消費してしまうため、ポートがそれだけ減ってしまう。そのため、1つのポートのみを全て

の VLAN のデータを流すことで、ポートを消費することを防ぐことができるポートをトランクという。

2. の問題に関連し、スイッチ間で異なる VLAN 番号のデータを流す場合、スイッチ間では何が行われているか（どのようにして異なる VLAN 番号のデータを 2. で伝送するのか）説明せよ。

トランクにおいてどの VLAN のデータが流れているかを示すために、データにタグを付けてデータを通信している

- VTP とはどのようなものか、説明せよ。

VLAN (番号) のデータを複数のスイッチで共有するためのプロトコル。

- 次の図のように Switch\_A で作成した VLAN 情報を Switch\_B でもそのまま利用したい。このことを実現するために、以下の空欄を埋めよ。ただし、Switch\_A での VLAN の作成、スイッチの各ポートの VLAN の設定やトランクの設定などはすでに行われているとする。また、必要であるのに示されていない事柄については、適当に決めて良いが、デフォルトで設定されていて設定が必要ないと思われる内容についても設定を行うこと。

○Switch\_A の設定

```
Switch_A(config)# vtp domain cutt
```

```
Switch_A(config)# vtp mode server
```

```
Switch_A(config)#exit
```

○Switch\_B の設定

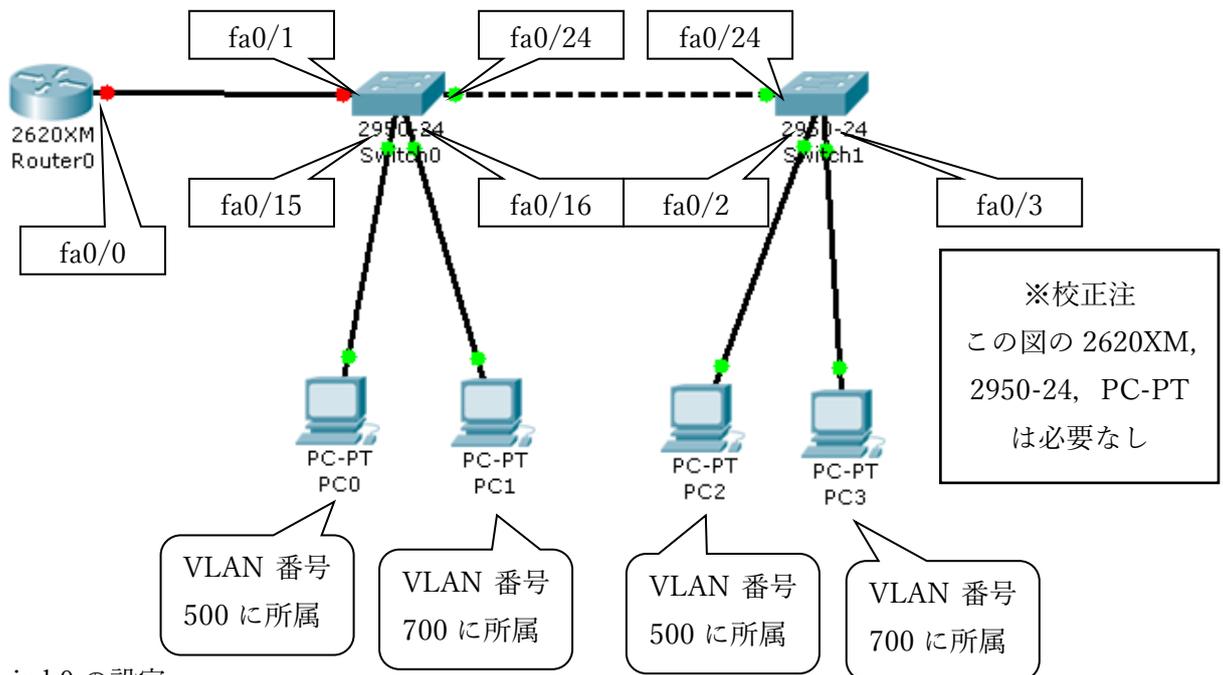
```
Switch_B(config)# vtp domain cutt
```

```
Switch_B(config)# vtp domain client
```

```
Switch_B(config)#exit
```

※ 「cutt」の部分はどのような名前でも良い

- 次の図のようにスイッチを使って VLAN を構成し、さらに各 VLAN 間で通信ができるようにする場合に、必要な設定をするためのコマンドで不足している部分の最初の大きな空欄および下線部を埋めよ。ただし各 PC は適切に設定されているものとする。スイッチの名称は左が「Switch0」、右が「Switch1」である。ルータは「Router0」である。さらに、VLAN 番号 500 では 192.168.10.0/24 ネットワークを、VLAN 番号 700 では 192.168.20.0/24 ネットワークを使っているものとする。



○Switch0 の設定

Switch>enable

Switch#conf t

VLAN を登録するコマンドを書いて下さい  
(複数行になります)

```

vlan 500
vlan 700

```

```

Switch(config)#int fa0/1
Switch(config-if)# switchport mode trunk
Switch(config)#int fa0/24
Switch(config-if)# switchport mode trunk
Switch(config)#int fa0/15
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 500
Switch(config)#int fa0/16
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 700

```

○Switch1 の設定 (省略 (Switch0 と同様に適切に設定されている))

◎ルータの設定

```
Router>enable
Router#conf t
Router(config-if)# int fa0/0.500
Router(config-subif)# encapsulation dot1q 500
Router(config-subif)# ip address 192.168.10.254
Router(config-subif)# int fa0/0.700
Router(config-subif)# encapsulation dot1q 700
Router(config-subif)# ip address 192.168.20.254
Router(config)#int fa0/0
Router(config-if)#no shutdown
```

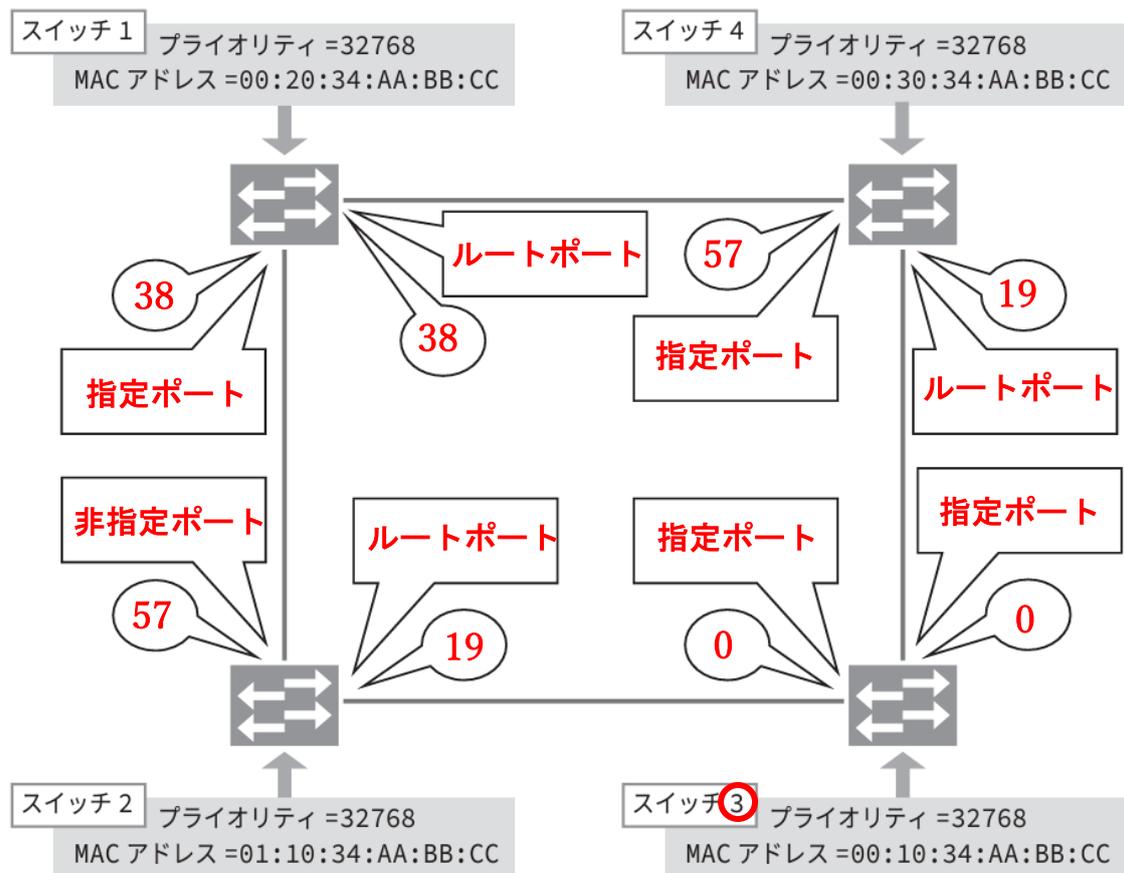
※int fa0/0.500 および fa0/0.700 の 500 と 700, ip address 192.168.10.254 および 20.254 の 254 については, 有効な範囲であればいくつでも正解です.

7. 図 13. 7 で, トランクリンクを使わずに同じ機能を実現するにはどうすればよいか, 答えよ.

各スイッチに (トランクではなく) 必要な VLAN 番号のポートを作成し, 接続することで実現できる (P.204 の図 13.6(a)参照)

## 第 14 章

- 冗長構成をしようとしてスパニングツリーなどの機能のないスイッチで LAN を構成した場合に起こりえる「ブロードキャストストーム」について説明せよ.  
ブロードキャストは全てのポートからデータを送り出すため, 円形にスイッチがつながっている冗長構成ではそのデータがそのネットワークを回り続けるだけでなく, データがコピーし続けるために多くのデータが回り続けてしまうことを嵐 (ストーム) になぞらえてブロードキャストストームという.
- スパニングツリープロトコルとは何か説明せよ.  
ループ状にスイッチが配置されているためにデータが回り続けてしまうため, ループができないようにポートの一部を使えなくするようにするプロトコルをスパニングツリープロトコルという.
- 次の図のようにスイッチを配置した場合, スパニングツリープロトコルが行う動作について次の問いに答えよ.
  - ルートブリッジはどれか. 該当するスイッチの番号に○を書け.
  - 各ポートのルートパスコストを○括弧内に書け. ただし, すべてのリンクの帯域幅は 100Mbps で, そのパスコストは「19」である.
  - それぞれのポートは「ルートポート」「指定ポート」「非指定ポート」のいずれになるか, □括弧内にそのいずれかを書け.



## 第 15 章

1. ある管理者がスイッチの Fa0/1 ポートを以下のように設定した。次の問いに答えよ。
  - ① (a)の設定は何をしようとしているか、説明せよ。 : そのポートに Mac アドレスを登録できる最大数を 1 とする
  - ② (b)の設定は何をしようとしているか、説明せよ。 : 最初に接続された PC 等の Mac アドレスを登録する
  - ③ (c)の設定は何をしようとしているか、説明せよ。 : 未登録の MAC アドレスが通信した場合、ポートを shutdown して違反通知をする
  - ④ 上記の設定で Fa0/1 ポートに違法な PC が接続された場合、そのポートを復帰させるにはどうしたらよいか答えよ。 : shutdown した後、no shutdown を行う
  - ⑤ この管理者はポート Fa0/1 をどのようにしたいと考えて上のような設定をしたのか、説明せよ。 : fa0/1 には指定された PC 等のみを接続させることとし、その他の PC 等が接続された場合には、それを通信させないと同時に、管理者等が操作をしないと復帰をさせないようにしようとしている
2. スイッチにおいて、あるタイミングで「show mac-address」コマンドを実行したら図(a)の

ようになった。一定時間経過後、同様のコマンドを実行したら図 (b) のように変化した。

| Switch#show mac-address |                |         |       | Switch#show mac-address |                |         |       |
|-------------------------|----------------|---------|-------|-------------------------|----------------|---------|-------|
| Mac Address Table       |                |         |       | Mac Address Table       |                |         |       |
| Vlan                    | Mac Address    | Type    | Ports | Vlan                    | Mac Address    | Type    | Ports |
| 1                       | 0004.9acc.77e0 | STATIC  | Fa0/1 | 1                       | 0004.9acc.77e0 | STATIC  | Fa0/1 |
| 1                       | 0060.5c10.b57a | DYNAMIC | Fa0/2 | 1                       | 00e0.a368.64ec | DYNAMIC | Fa0/3 |
| 1                       | 00e0.a368.64ec | DYNAMIC | Fa0/3 |                         |                |         |       |

(a)

(b)

- ① 図中 Fa0/1 はなぜ Type が「STATIC」となっているのか、その理由を述べよ。：ポートセキュリティを有効にしている (MAC アドレスを STATIC で登録してもこのようになる)
- ② なぜ (a) と比べて (b) は 1 つ減ったのか、その理由を述べよ。ただし、PC 等は撤去・電源 OFF をされていないこととする。：PC 等は撤去・電源 OFF をしていなくても、通信しないと MAC アドレステーブルから削除されるため、それが起こった。

3. スイッチを図のように設置して次のことを実習せよ。：実際に実習してみてください。

## 第 16 章

1. 次の VLSM についての問いに答えよ。

- ① VLSM とは何か説明せよ。

複数のサブネットに、異なるサブネットマスクを設定できる方法。このことにより、各サブネットで必要な数の IP アドレスを確保できるとともに、無駄な IP アドレスを確保せず将来のために残すこともできる。

- ② あるサイトは 192.168.2.0/24 のネットワークアドレスを持つ。VLSM が使える環境であるとして、以下の条件を満たすように、VLSM の技術を用いて①～⑧の各セグメントに (サブ) ネットワークアドレスおよびサブネットマスクを割り当てるよう。解答せよ (\*.\*.\*./\*の形式で書く)。ただし、「ip subnet-zero」は有効になっているものとする。また解答の⑥～⑧は省略する。

条件1 : 各 LAN 用セグメントには、示されているだけの台数のネットワーク機器をつなげられるように IP アドレスを確保する。また、将来を考えて未使用の IP アドレスを多く確保する。

条件2 : 各シリアルリンクセグメントにはなるべく少ない IP アドレスを確保する。

条件3 : ネットワーク番号は①→②→③…の順で小さい番号（若い番号）を振ることとする。

① 192.168.2.0/25

② 192.168.2.128/27

③ 192.168.2.160/28

④ 192.168.2.176/29

⑤ 192.168.2.184/30

⑥ 192.168.2.184/30

⑦ 192.168.2.188/30

⑧ 192.168.2.192/30

## 第 17 章

次の問いに答えよ。

1. 次の図中の WAN テクノロジで用いられるネットワーク機器および施設の名称を答えよ（図中の①～④を空欄内に名称を記入）。ただし、適切なものであれば日本語・カタカナ・英字略称どれで答えてもよい。

①セントラルオフィス(CO)

②分界点

③顧客宅内装置 (CPE)

④ローカルループ

2. 上の図の②はどのような意味があるか、説明せよ。：通信事業者側と顧客側との責任の境界
3. PAP と CHAP はどこで使われる技術で、それぞれの違いは何か説明せよ。：PPP の認証で使われる技術で、パスワードが平文のものを PAP、パスワードが暗号化されているものを CHAP と言う。
4. 次の（ ）に語句を埋めよ。

① HDLC や PPP, フレームリレーは OSI 7 層モデルで言うと（データリンク（第 2））層のプロトコルである。

② PPP はリンクの確立や維持・切断を行うプロトコルである（LCP）とマルチプロトコルな上位層との通信を行うためのプロトコルである（NCP）の 2 つの層を持っている。

## 第 18 章 IPv6

1. IPv6 は (128) ビットで構成されている。また IPv6 アドレスで「0」が連続する場合には省略できる。IPv6 アドレスである「2001:0000:23fb:0000:0000:0400:000e:6000」を省略形で書くと、(2001:0:23fb::400:e:6000) となる。

## 第 20 章 無線 LAN

1. 無線 LAN におけるアドホックモードとインフラストラクチャモードとはどんなものか、AP (アクセスポイント) という言葉を使って説明せよ。

ネットワーク機器間において、アクセスポイントを介して通信をする方式をインフラストラクチャモード、アクセスポイントを介さず直接一対一で通信する方式をアドホックモードという。