

ネットワーク基礎

- 1 ルータの役割
- 2 ハブの役割
- 3 データの通り道 経路について
- 4 ルーティングテーブル
- 5 Windowsでのネットワーク確認
- 6 デフォルトゲートウェイ
- 7 DHCPとは
- 8 DNSとは
- 9 Windowsでのネットワーク設定
- 10 ポート番号
- 11 アクセスコントロールリスト
- 12 IPアドレス
- 13 IPアドレス計算
- 14 光ケーブル

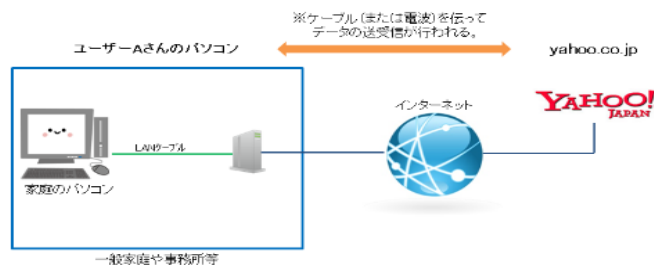
1 ルータの役割



ルータはその名の通り**通信のルート（道）を整理する役割**を担っています。

私達はインターネットで例えばyahoo!JAPANにアクセスする際、それまでの道を作ってあげる必要があります。

下の図は一般的な家庭のパソコンからyahoo!JAPANにアクセスした場合のイメージです。

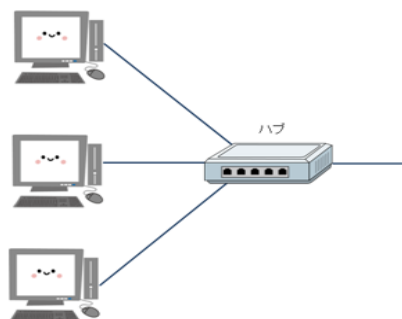


私達はインターネットを利用する時、必ず（どんな形でも）アクセスしたい住所を指定します。これをインターネット用語で「URL」とか言ったりします。

データの通り道を作るのがルーター

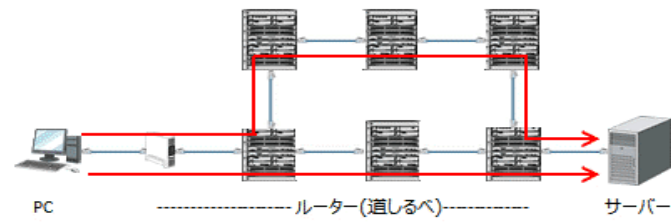
2 ハブの役割

ハブにも様々な種類がありますが、一般的な家庭で使用されるハブは単純に1本のLANケーブルを分配する役割を持っています。



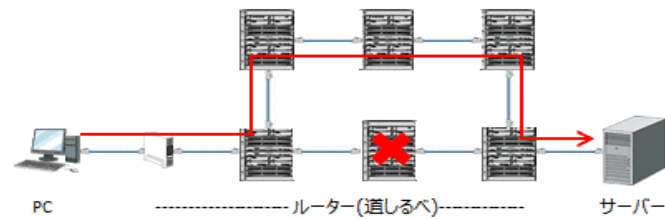
3 データの通り道 経路について

最短経路を進む

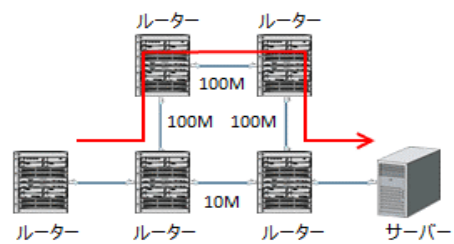


真ん中下のルーターがダウン

Windowsでのネットワーク確認



経路制御はその経路までコストの合計が一番小さいルートが選択されます。



ダイナミックルーティング、ルーター間で教え合う、

RIPはダイナミックルーティングを実現するルーティングプロトコルの1種です。

OSPF

4 ルーティングテーブル



Routing Table

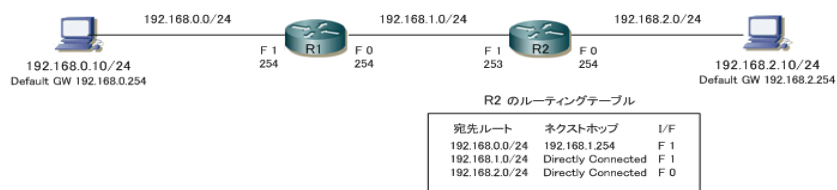
ルーティングテーブルとは、ルータに記録される経路情報で、ルーティング処理を行う際に参照する。作成方法には、スタティックルーティングとダイナミックルーティングの2種類がある。

あるネットワークの端末Aから別のネットワークの端末Bへデータを転送するとき、中継するルータは端末Bが所属するネットワークへ届けるための経路、つまりルートを経由してルーティングテーブルから参照して転送する。

ルーティングテーブルの見方

Windowsでのネットワーク確認

ここではCisco機器を例にして、ルーティングテーブルを詳細に見ていきます。Cisco機器でルーティングテーブルを確認するためには、show ip routeコマンドを入力する必要があります。



このルーティングテーブルの詳細を、以下で見てみましょう。

```
COM4:9600baud - Tera Term VT
ファイル(E) 編集(E) 設定(S) コントロール(Q) ウィンドウ(W) 漢字コード(K) ヘルプ(H)
Router#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

Gateway of last resort is not set
R 192.168.0.0/24 [120/1] via 192.168.1.254, 00:00:06, FastEthernet1
C 192.168.1.0/24 is directly connected, FastEthernet1
C 192.168.2.0/24 is directly connected, FastEthernet0
Router#
```

項番	各項目	説明
①	ルートの情報源	そのルートがどのようにルーティングテーブルに追加されたのかを示すコード。直接接続ルートの場合「C」、スタティックルートの場合「S」、ダイナミックルートの場合はルーティングプロトコルによりコードが異なる。今回はルータでRIPを有効にしているので、ルーティングテーブル上では「R」が表示されている。
②	宛先ルート、サブネットマスク	宛先ネットワークを示すアドレスとサブネットマスクの情報。サブネットマスクはネットワークアドレスの区切りを示し、ロングストマッチの際に参照される情報源。
③	アドミニストレーティブ ディスタンス	ルーティングテーブル上に、プレフィックス長が同じ宛先ルートが複数ある場合このアドミニストレーティブディスタンス(AD)の値が参照される。AD値が小さい宛先ルートがルーティングテーブルに追加される。RIPは、AD値が 120 となる。
④	メトリック	ダイナミックルーティングにおいて、宛先ルートに対し複数のルートが存在する場合に最適経路を選択するために使用される値。このメトリック値は、使用しているダイナミックルーティングプロトコルにより値の意味が異なる。
⑤	ネクストホップアドレス	受信したパケットを宛先ネットワークに転送するために次にパケットを転送する隣接ルータのIPアドレスのこと。今回は、192.168.0.0/24の宛先ルートに対しては192.168.1.254がネクストホップアドレスであることが分かる。viaは「～経由」の意味であり、192.168.1.254経由で192.168.0.0/24のルートが学習されたと分かる。directly connected は直接接続ルートであることからネクストホップは存在しない。
⑥	宛先ルートの学習時間	ダイナミックルーティングにおいて、宛先ルートが追加されてからの経過時間。上図の場合、「192.168.0.0/24」のルート情報を受信してから6秒経過している。
⑦	出カインターフェース	受信パケットを宛先ネットワークに転送するための出カインターフェースを表示。上図「192.168.0.0/24」宛のパケットはR2の「FastEthernet 1」から転送される。

ルータのルーティングテーブルにルート情報を追加するためには、以下の3通りの方法があります。

ルート情報の追加方法	説明
直接接続ルート	ルータの自身のI/FにIPアドレスを設定して、I/Fを有効化することで追加されるルータのこと。前提として、そのインターフェースがリンクアップして "up/up" の状態である必要がある。
スタティックルート	管理者が宛先ネットワークへの最適なルートを手動で設定したルータのこと。
ダイナミックルート	ルータで設定されたルーティングプロトコルにより、自動的に追加されるルータのこと。

5 Windowsでの ネットワーク確認

コマンドプロンプト表示

Cortanaで cmd を入力します。

ipconfig

Window10版のipconfigの結果は日本語で表示されており、比較的分かりやすくなっています。

```
管理: コマンドプロンプト
C:\WINDOWS\system32>ipconfig /all

Windows IP 構成

ホスト名 . . . . . : ...①
プライマリ DNS サフィックス . . . . . : ...②
ノード タイプ . . . . . : ハイブリッド ...③
IP ルーティング有効 . . . . . : いいえ ...④
WINS プロキシ有効 . . . . . : いいえ ...⑤
DNS サフィックス検索一覧 . . . . . : wi2.ne.jp ...⑥

イーサネット アダプター イーサネット:

メディアの状態 . . . . . : メディアは接続されていません ...⑦
接続固有の DNS サフィックス . . . . . : ...⑧
説明 . . . . . : ...⑨
物理アドレス . . . . . : ...⑩
DHCP 有効 . . . . . : はい ...⑪
自動構成有効 . . . . . : はい ...⑫

Wireless LAN adapter ローカル エリア接続* 1:

(項目内容は同上のため、中略)

Wireless LAN adapter Wi-Fi:

接続固有の DNS サフィックス . . . . . : ...⑬
物理アドレス . . . . . : ...⑭
DHCP 有効 . . . . . : はい ...⑮
自動構成有効 . . . . . : はい ...⑯
リンクローカル IPv6 アドレス . . . . . : ...⑰
IPv4 アドレス . . . . . : ...⑱
サブネット マスク . . . . . : ...⑲
リース取得 . . . . . : 2016年11月1日 12:46:39 ...⑳
リースの有効期限 . . . . . : 2016年11月1日 13:47:05 ...㉑
デフォルトゲートウェイ . . . . . : ...㉒
DHCP サーバー . . . . . : ...㉓
DHCPv6 IAID . . . . . : ...㉔
DHCPv6 クライアント DUID . . . . . : ...㉕
DNS サーバー . . . . . : ...㉖

NetBIOS over TCP/IP . . . . . : 有効 ...㉗
```

(1) ホスト名

自分のホスト名 (コンピュータ名)

(2) プライマリDNSサフィックス

最優先のDNSサフィックス (このホストが所属するDNSドメイン)

(3) ノードタイプ

名前解決の方法

- ・ブロードキャスト…ブロードキャストで名前解決を行う
- ・ピアツーピア…WINSサーバで名前解決を行う
- ・混合…ブロードキャストでダメな場合はWINSサーバで名前解決を行う
- ・ハイブリッド…WINSサーバでダメな場合はブロードキャストで名前解決を行う

(4) IPルーティング有効

複数NICが接続されている場合、NIC間でのルーティングの有効/無効を設定

(5) WINSプロキシ有効

WINSサーバと直接通信できないホストがある場合、仲介機能の有効/無効を設定

(6) DNSサフィックス検索一覧

ネットワーク毎にDNS一覧を表示

(7) メディアの状態

メディアの接続有無

(8) 接続固有のDNSサフィックス

接続されているNIC固有に指定したDNS一覧

(9) 説明

アダプタの説明 (型番など)

(10) 物理アドレス

MACアドレス (NIC固有の番号) を表示。IPv4の識別子

(1 1) DHCP有効

DHCP (Dynamic Host Configuration Protocol) 機能の有効／無効を設定

(1 2) 自動構成有効

APIPA (Automatic Private IP Addressing) 機能の有効／無効を設定

(1 3) リンクローカルIPv6アドレス

IPアドレス (IPv6) を表示

(1 4) IPv4アドレス

IPアドレス (IPv4) を表示

(1 5) サブネットマスク

ホストが使用しているサブネットマスクを表示

(1 6) リース取得

DHCPサーバからIPをリースされた時刻

(1 7) リースの有効期限

DHCPサーバからのIPのリースが終了する予定時刻

(1 8) デフォルトゲートウェイ

デフォルトゲートウェイのIPアドレスを表示

(1 9) DHCPサーバ

DHCPサーバのIPアドレスを表示

(2 0) DHCPv6 IAID

IAID (Identity Association ID) 。IPv6の識別子

(2 1) DHCPv6 クライアント DUID

DUID (DHCP Unique Identifier) 。IPv6の識別子

(2 2) DNSサーバ

DNSサーバのIPアドレスを表示

(2 3) NetBIOS over TCP/IP

るNetBIOSをTCP/IPネットワーク上で利用するためのプロトコルの有効／無効を設定

ping

pingとはネットワークの疎通確認ツール

```
選択管理者: コマンドプロンプト
C:\WINDOWS\system32>ping 127.0.0.1

127.0.0.1 に ping を送信しています 32 バイトのデータ:
127.0.0.1 からの応答: バイト数 =32 時間 <1ms TTL=128
127.0.0.1 からの応答: バイト数 =32 時間 <1ms TTL=128
127.0.0.1 からの応答: バイト数 =32 時間 <1ms TTL=128
127.0.0.1 からの応答: バイト数 =32 時間 <1ms TTL=128

127.0.0.1 の ping 統計:
    パケット数: 送信 = 4, 受信 = 4, 損失 = 0 (0% の損失)、
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 0ms、最大 = 0ms、平均 = 0ms

C:\WINDOWS\system32>
```

(1) コマンドの対象ホストと、送信されるパケットのサイズが表示される。

(2) コマンドの途中経過 (送信したパケットのバイト数、応答にかかった時間、TTL (Time To Live、生存時間)) が表示される。指定した要求の数 (指定していない場合は4回) だけ繰り返される。

(3) 送信・受信したパケット数や損失率など、最終結果が表示される。

6 デフォルトゲートウェイ

デフォルトゲートウェイは、簡単に言えばネットワークの玄関口です。たとえばインターネット上のWebページなど、自分が所属するネットワーク以外が宛先として指定された場合、そのままでは、直接その相手と通信することができませんので、玄関となるデフォルトゲートウェイ宛てに通信を転送し、デフォルトゲートウェイとして指定された機器がその通信を処理します。

デフォルトゲートウェイは、一般的な家庭であれば、ISPからレンタルしたホームゲートウェイや無線LANルーターになります。よって、大抵の場合は“デフォルトゲートウェイ=ルーターのIPアドレス（LAN側）”と考えて問題ありませんが、ネットワークの構成によってはそうならない場合もあるので注意が必要です。

7 DHCPとは

ワーク確認

コンピュータにIPアドレスを自動割り当てする仕組みのこと。

IPアドレスやサブネットマスク、ドメイン名などのTCP/IPの設定情報をダイナミックに割り付けるためのプロトコル。DHCPサーバは、主にクライアントのブート時などに、クライアントPCが自身のIPアドレスを自動設定するために用いられる。

DHCPではそれに加えて、割り当てられたIPアドレスに利用可能期間（リース期間）を設定できる。また、クライアントに使用させたいDNSサーバやデフォルトゲートウェイのIPアドレスも自動設定できるのが大きな特徴となっている。

8 DNSとは

DNSは、Domain Name Systemの略で、その名前が示すようにインターネット上でドメイン名（ドメインネーム^{③1}）を管理・運用するために開発されたシステムです。DNSはインターネットを利用するうえでなくてはならない存在であり、現在のインターネットにとって、必要不可欠なシステムの一つとなっています。


では、DNSとはどのようなものなのでしょうか。

インターネットに接続している機器には「IPアドレス」という固有の番号が必ず割り当てられます。そして、インターネット上におけるすべての通信は、相手先のIPアドレスが指定されることにより行われます。例えば、JPNIC Web（<http://www.nic.ad.jp/>）をWebブラウザで見る場合、実際にはwww.nic.ad.jpのIPアドレスである202.12.30.144という宛先IPアドレスに対して通信が行われることになります。そのため<http://www.nic.ad.jp/>を指定するかわりに<http://202.12.30.144/>とすることも可能です^{③2}。

しかし、このようにIPアドレスで相手先を直接指定することは、インターネットを利用する各ユーザーが、該当するWebサーバ等のIPアドレスをなんらかの方法ですべて記憶しておく必要があり、現実的ではありません。また、なんらかの理由により相手先ネットワークの構成が変更された場合、IPアドレスはしばしば付け直されたり、変更される場合があります。このような場合、以前記憶していたIPアドレスでは接続できなくなってしまう。

そのため、より人間が覚えやすく使いやすい「名前」で指定できるようにするためのしくみが必要となります。DNSはそれを実現するためのシステムです。

9 Windowsでの ネットワーク設定

スタートボタン()を**右クリック**します。

[**ネットワーク接続**]を選択します。



ルータの役割

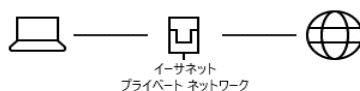
Windowsでのネットワーク確認

「アダプタのオプションを変更する」を選択します。



状態

ネットワークの状態



インターネットに接続されています

制限付きのデータ通信プランをお使いの場合は、このネットワークを従量制課金接続に設定するか、またはその他のプロパティを変更できます。

[接続プロパティの変更](#)

[利用できるネットワークの表示](#)

ネットワーク設定の変更



アダプターのオプションを変更する

ネットワーク アダプターを表示して接続設定を変更します。

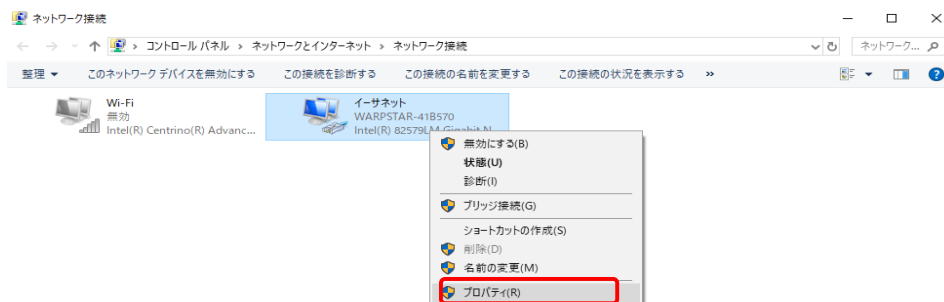


共有オプション

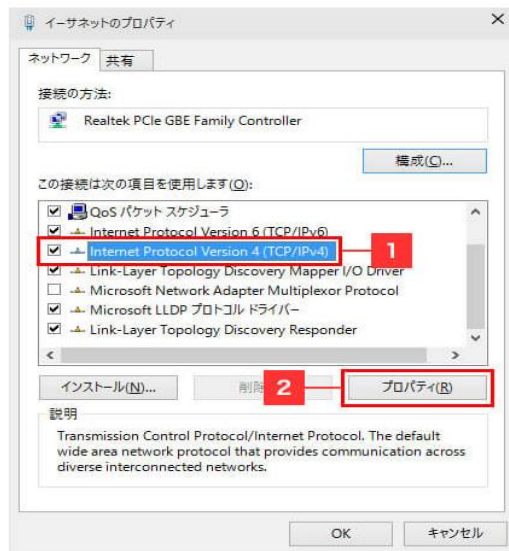
接続先のネットワークについて、何を共有するかを指定します。

▲ ネットワークのトラブルシューティング ツール。

「イーサネット」を右クリックし、「プロパティ」を選択します。

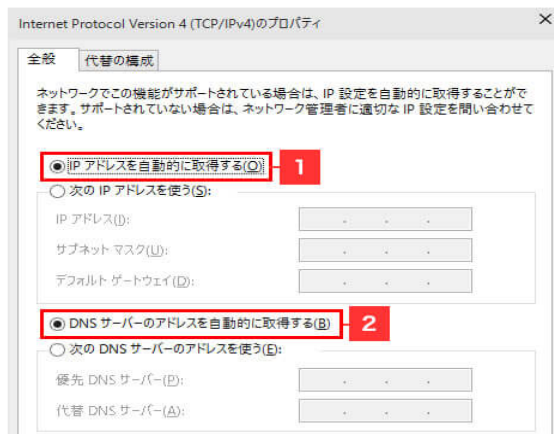


- 1 [インターネット プロトコル バージョン 4 (TCP/IPv4)]を選択します。
- 2 [プロパティ]をクリックします。

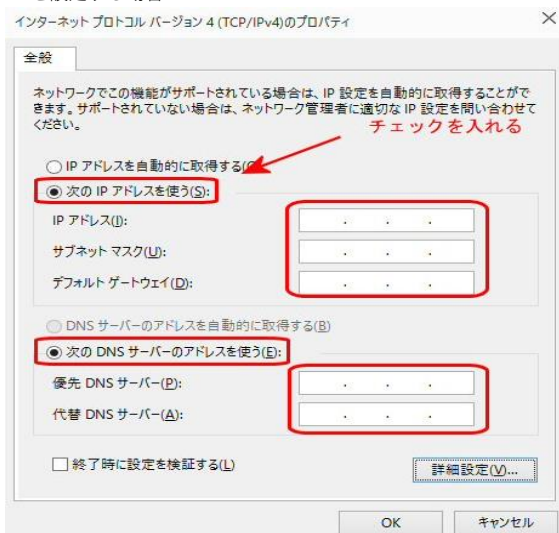


DHCPサーバのサービスを受ける場合

- 1 [IP アドレスを自動的に取得する]と
- 2 [DNS サーバーのアドレスを自動的に取得する]を選択し、



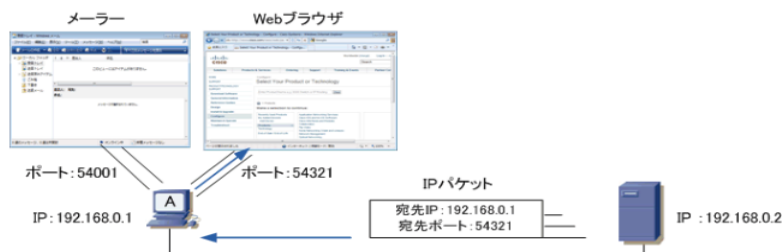
IPを設定する場合



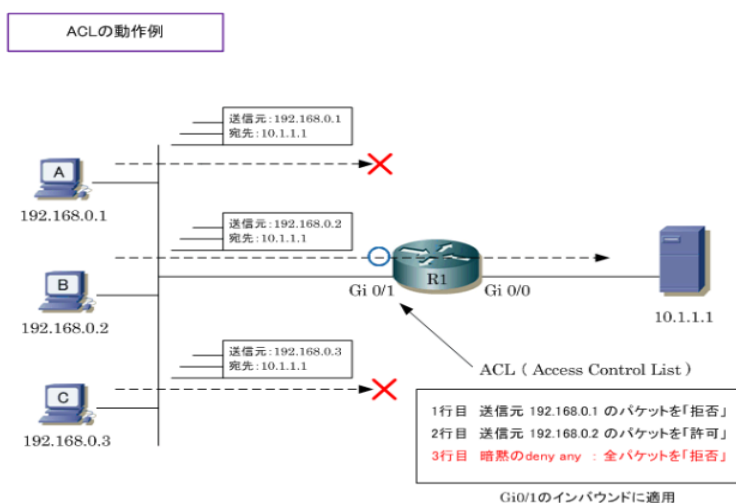
10 ポート番号

ポート番号とは、コンピュータが通信を行うために通信先のアプリケーションを特定するための番号のこと。コンピュータ間の通信で通信する宛先のIPアドレスが分かれば、そのIPアドレスにデータを送信できますがそのデータを受信したコンピュータが、どのアプリケーションでそれを受信するのか判断するために必要です。

例えば下図の通り、コンピュータ上でWebブラウザとメールを起動させていたとします。Webブラウザでインターネットの閲覧をするために、コンピュータ内でデータをWebブラウザに送り届ける必要があります。TCPヘッダにポート番号情報が付加することで、どのアプリケーションなのかを識別しこれを実現しています。



11 アクセスコントロールリスト



上図では2行のACLを適用しています。3行目は設定してなくても自動的に暗黙のdenyが追加されます。このACLをルータ (R1) のインターフェース (G0/1) のインバウンド (IN) で適用しています。つまり、このACLは、R1のGi0/1に着信してくるパケットを対象にしてフィルタリングしていることを意味します。

ホストAからの着信パケットは送信元アドレスが「192.168.0.1」のため、ACL1行目に合致して拒否されホストBからの着信パケットは送信元アドレスが「192.168.0.2」のため、ACL1行目には合致しないのでACLの2行目に合致して許可されます。ホストCからの着信パケットは、送信元アドレスが「192.168.0.3」のため、ACLの1行目、2行目には合致せず、表示されない3行目の暗黙のdeny anyに合致し拒否されます。

◇ 標準ACLの制御例

- 送信元IPアドレス「192.168.0.1」からのパケットを許可、拒否
- 送信元IPアドレス「192.168.0.0/24」のネットワークからのパケットを許可、拒否
- 全ての送信元IPアドレスからのパケットを許可、拒否

◇ 拡張ACLの制御例

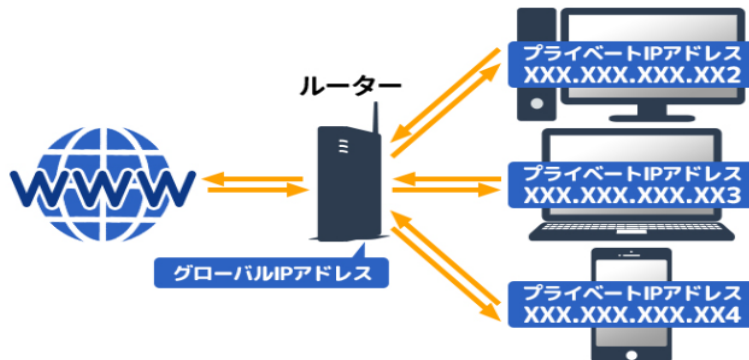
- 送信元IPアドレス「192.168.0.1」から宛先IPアドレス「10.1.1.1」へのパケットを許可、拒否
- 送信元IPアドレス「192.168.0.0/24」から宛先IPアドレス「10.1.1.0/24」へのパケットを許可、拒否
- 全ての送信元IPアドレスから宛先IPアドレス「10.1.1.0/24」へのパケットを許可、拒否
- 送信元IPアドレス「192.168.0.1」から宛先IP「10.1.1.1」へWebアクセス (ポート80) を許可、拒否
- 送信元IPアドレス「192.168.0.1」から宛先IP「10.1.1.1」へICMP通信 (プロトコル番号1) を許可、拒否

12 IPアドレス

IPアドレスの種類

次に、用途別にIPアドレスを分類します。この場合、用途とは以下の二点です。

- 1 インターネットに接続するタイプ(グローバルIPアドレス)
- 2 インターネットに接続しないタイプ(プライベートIPアドレス)

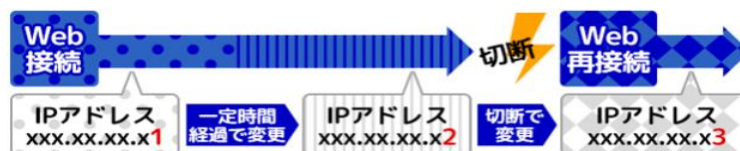


それぞれの特徴は、以下の通りです。

グローバルIPアドレス

グローバルIPアドレスとは、インターネットに接続するタイプのIPアドレスです。さらに、動的IPアドレス、静的IPアドレス(固定IPアドレス)の二つに分かれます。一つひとつ説明していきます。

動的IPアドレス



IPアドレスが変動する場合、動的IPアドレスに分類されます。一般的な事例として、家庭でインターネット・サービス・プロバイダー(ISP)に接続する場合があります。

静的IPアドレス(固定IPアドレス)



一方、静的IPアドレス(固定IPアドレス)とは、言葉の通り変動しないIPアドレスです。では、どのような利用場面が想定されるでしょうか。一言で言えば、接続のたびにコロコロ変わって欲しくない場合に、導入が必須となっています。

例えば、ホームページの公開サーバーや、メールの送受信のためのメールサーバーの場合です。

プライベートIPアドレス

英語表記: Private IP Address

読み: プライベート・アイビー・アドレス

プライベートIPアドレスとは、ホームネットワークや企業内ネットワークなどのLAN (Local Area Network: 閉じたネットワーク) でそれぞれの機器は判別するのに使うために用意されたIPアドレス。通常10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255, 192.168.0.0~192.168.255.255の範囲が標準化団体のRFCによってプライベートIPアドレスとして予約されている。ローカルIPアドレスとも言う。

IPアドレスには、IPv4 (32bit)とIPv6(128bit)があります。

■ IPv4アドレス

現在、世界中で広く使用されているIPアドレスがこのIPv4です。IPv4アドレスは32bitの正整数値と定められており、2進数表記で表すと

11000000101010000001011111111101 ?のようになっています。

ただ、これでは人間にとって理解しにくいので、以下のように、32bitを8bitずつドットで区切って4つに分けて、さらに10進数に直した表記を一般に使用します。

■ 本来の表記

11000000101010000001011111111101

↓

■ 8bitずつ4つに分ける

11000000.10101000.00010111.11111101

↓

■ 10進数に直す

192.168.23.253

サブネットマスクとは？

サブネットマスク(subnet mast)は、ネットワークの範囲を定義するために使用します。

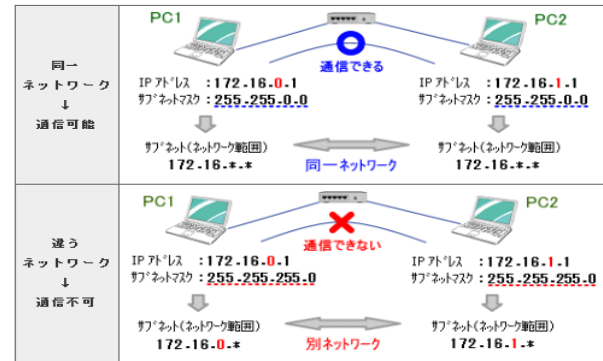
IPアドレスとサブネットマスクを組み合わせることで、ネットワークの範囲(サブネット)を指定することができます。

たとえば、IPアドレス:172.16.0.1を使用している場合、サブネットの値でネットワーク範囲(サブネット)も異なります。

IPアドレス / サブネットマスク	ネットワーク範囲(サブネット)	パソコン等の数(注1)
172.16.0.1 / 255.255.255.0	172.16.0.0～172.16.0.255	254
172.16.0.1 / 255.255.0.0	172.16.0.0～172.16.255.255	65,534

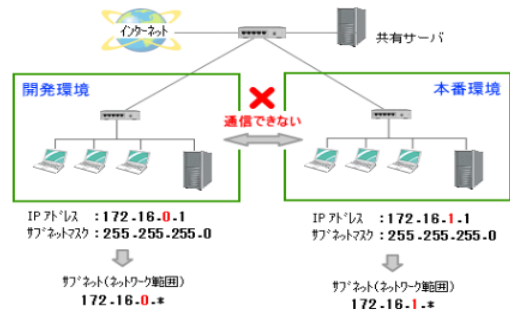
パソコン等を接続できる台数は「ネットワーク範囲 - 2」となる。先頭のアドレスは「ネットワークアドレス」・最終のアドレスは「ブロードキャストアドレス」となり利用できません

ネットワークが同一のパソコンやサーバは容易に通信することができます。逆にネットワークが同一でないパソコンやサーバは、ルータやネットワーク機器(L3など)を使用してネットワークを切り替えて通信する必要があります。



サブネットマスクの分割は、一般的に以下のような場合に利用されます。

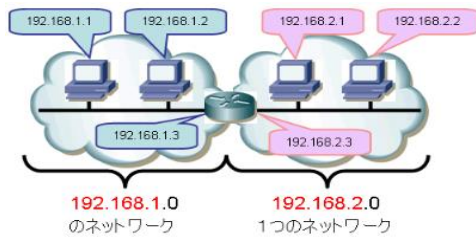
- ・ 会社の部署間でデータの参照を制限する場合
- ・ パソコンやサーバの台数が多く分割して管理する場合
- ・ 開発環境と本番環境を分けるなど、環境を切り離す場合



ネットワークアドレス

◦ホストアドレス部分が全て“0”のIPアドレス

ホストアドレス部分が全て“0”のIPアドレスを「ネットワークアドレス」といいます。



ブロードキャストアドレス

◦ホストアドレス部分が全て“1”のアドレス

ホストアドレス部分が全て“1”のアドレスは、

“ディレクテッド・ブロードキャストアドレス”

と呼ばれます。

192.168.1.0/24の場合のディレクテッド・ブロードキャストアドレスは、

192.168.1.255

となります。

“ディレクテッド・ブロードキャストアドレス”は、そのネットワークに所属するすべてのホストに対して通信したい時に使用するアドレスです。

ディレクテッド・ブロードキャストアドレス宛に通信を行った場合、そのメッセージはネットワーク内の全てのホストに届きます。

2進、10進、サブネットマスク

2進数と10進数の対応表												
10進数	0	1	2	3	4	5	6	7	8	9	10	...
2進数	0	1	10	11	100	101	110	111	1000	1001	1010	...

2進数と10進数の対応表								
10進数	1	2	4	8	16	32	64	128
2進数	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

10進数の基準値	128	64	32	16	8	4	2	1
2進数	0	0	1	0	1	0	1	0

・ワーク確認

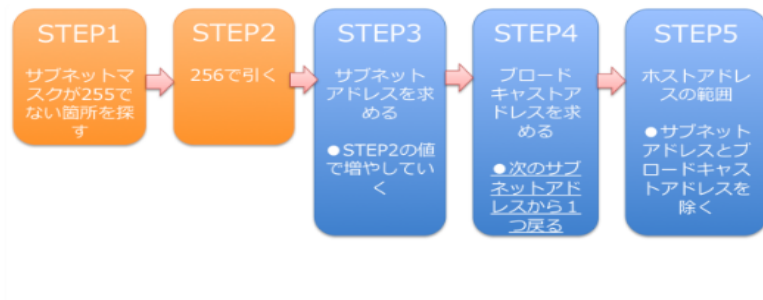
32 + 8 + 2 = 42

サブネットマスクの算出方法		
CIDR表記	10進数表記	2進数表記
/24	255.255.255.0	11111111.11111111.11111111.00000000
/25	255.255.255.128	11111111.11111111.11111111.10000000
/26	255.255.255.192	11111111.11111111.11111111.11000000
/27	255.255.255.224	11111111.11111111.11111111.11100000
/28	255.255.255.240	11111111.11111111.11111111.11110000
/29	255.255.255.248	11111111.11111111.11111111.11111000
/30	255.255.255.252	11111111.11111111.11111111.11111100
/31	255.255.255.254	11111111.11111111.11111111.11111110
/32	255.255.255.255	11111111.11111111.11111111.11111111

13 IPアドレス計算

■問題1

192.168.5.17 255.255.255.248のサブネットアドレスとブロードキャストアドレス、ホストアドレスの範囲は？



ク確認

STEP1 サブネットマスクが255以外を探す

255.255.255.248 なので、第4オクテットの248です。

STEP2 256で引く

$256 - 248 = 8$ です。

STEP3 サブネットアドレスを算出する

STEP2で算出した8ごとにサブネットアドレスが変わります。

1つ目：192.168.5.0

2つ目：192.168.5.8 ←+8

3つ目：192.168.5.16 ←+8

4つ目：192.168.5.24 ←+8

(..続く)

192.168.5.17は、192.168.5.16～192.168.5.24の間です。ですので、3つ目のサブネットに所属します。答えは、**192.168.5.16** です。

STEP4 ブロードキャストアドレスを算出する

次のサブネットアドレスから1つ戻るだけです。

4つ目のサブネットアドレスは、192.168.5.24です。1つ戻ると、答えは、**192.168.5.23** です。

STEP5 ホストアドレスを算出する

サブネットアドレスとブロードキャストアドレス以外がホストアドレスです。

答えは、**192.168.5.17～22**になります。

- 192.168.5.16 サブネットアドレス
- **192.168.5.17～22 ホストアドレス**
- 192.168.5.23 ブロードキャストアドレス

■ 問題2

172.16.30.48 255.255.240.0のサブネットアドレスとブロードキャストアドレス、ホストアドレスの範囲は？

求め方

解き方は、全く同じです。

STEP1 サブネットマスクが255以外を探す

255.255.240.0 なので、第3オクテットの240です。

STEP2 256で引く

$256 - 240 = 16$ です。

STEP3 サブネットアドレスを算出する

この**16**ごとにサブネットアドレスが変わります。今回は、第3オクテットが対象です。

1つ目：172.16.**0.0**

2つ目：172.16.**16.0** ←+16

3つ目：172.16.**32.0** ←+16

4つ目：172.16.**48.0** ←+16

(..続く)

172.16.30.48は、2つ目のサブネットに所属します。答えは、**172.16.16.0** です。

STEP4 ブロードキャストアドレスを算出する

次のサブネットアドレスから**1つ戻るだけです**。

3つ目のサブネットアドレスは、172.16.**32.0**です。1つ戻ると、答えは、**172.16.31.255** です。

STEP5 ホストアドレスを算出する

サブネットアドレスとブロードキャストアドレス以外がホストアドレスです。

答えは、**172.16.16.1～172.16.31.254**になります。

- 172.16.16.0 サブネットアドレス
- **172.16.16.1～172.16.31.254** ホストアドレス
- 172.16.31.255 ブロードキャストアドレス

■ 問題3

10.248.30.150 255.192.0.0のサブネットアドレスとブロードキャストアドレス、ホストアドレスの範囲は？

求め方

解き方は、全く同じです。

STEP1 サブネットマスクが255以外を探す

255.1920.0 なので、第2オクテットの192です。

STEP2 256で引く

$256 - 192 = 64$ です。

STEP3 サブネットアドレスを算出する

この**64**ごとにサブネットアドレスが変わります。今回は、第2オクテットが対象です。

1つ目 : 10.**0**.0.0

2つ目 : 10.**64**.0.0 ←+64

3つ目 : 10.**128**.0.0 ←+64

4つ目 : 10.**192**.0.0 ←+64

X5つ目 : ~~10.256.0.0~~ ← **10.255**までなのでX

全部で4つのサブネットです。

10.248.30.150 は、4つ目のサブネットに所属します。答えは、10.192.0.0 です。

STEP4 ブロードキャストアドレスを算出する

次のサブネットから**1つ戻る**だけです。ただ今回は次のサブネットがないので、一番最後です。

一番最後は、**10.255.255.255** です。

STEP5 ホストアドレスを算出する

サブネットアドレスとブロードキャストアドレス以外がホストアドレスです。

答えは、**172.16.16.1**～**172.16.31.254**になります。

- 10.192.0.0 サブネットアドレス
- **10.192.0.1** ～**10.255.255.254** ホストアドレス
- **10.255.255.255** ブロードキャストアドレス

光ケーブル

光ケーブルは一般家庭のインターネット回線向けとしても普及してきて馴染み深いものになってきました。本項では光ケーブルの特徴、種類等を説明します。

光ケーブルの特徴

光ケーブルはケーブルの中に光が通るように作られていて、光をチカチカして通信しています。実際にケーブルのコネクタを覗くと光が見えます。※目を傷めるので見ない方がいいらしいです。

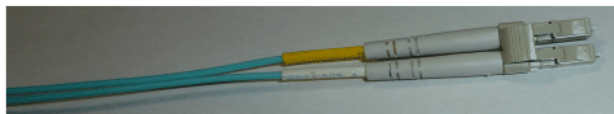
屋外にケーブルを敷設して落雷があっても影響を受けません。又、km単位の距離を接続可能なため、主として建屋内の階を跨ぐ時、屋外に敷設する時に使われます。

光ケーブルのコネクタ

光ケーブルのコネクタには複数種類がありますが、主なものはSCコネクタとLCコネクタです。SCコネクタはGBIC、LCコネクタはSFPに接続されます。

ルーター等の装置は内部で電気信号で動作していますが、GBIC、SFPが光に変換してくれます。通常はルーターやスイッチ等にGBICやSFPを挿入し、光ケーブル用のインターフェースとして使います。

GBICは形状が大きく古いタイプです。SFPは形状が小さく新しいタイプです。このため、最近ではSFPとLCコネクタの組み合わせが主流です。



LCコネクタ

GBIC+SCコネクタ-----LCコネクタ+SFPといった接続も可能です。

尚、10G(10,000Mbps)に対応したSFP+というのもあり、これもLCコネクタで接続します。

ケーブルの種類

ケーブルの種類には大きく分けて2種類あります。マルチモードファイバとシングルモードファイバです。

マルチモードファイバはGIケーブルと略されます。接続距離は規格にも寄りますが2km等です。このため、建屋内の階を跨る機器間の接続や隣接した建屋間の機器での接続に使われます。マルチモードファイバにはコア径50μmのものと62.5μmのものがあります。

シングルモードファイバはSMケーブルと略されます。接続距離は規格にも寄りますが10km等で、場合によってはもっと遠距離の接続が可能です。このため、建屋間、都市間等を結ぶために使われます。

GBIC / SFP (MiniGBIC)

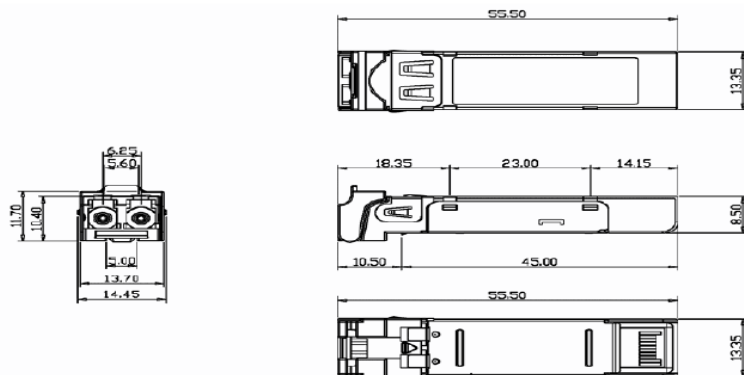
光伝送モジュール(活線挿抜:ホットスワップ型)

概要

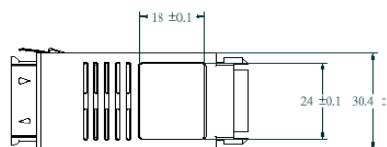
新しい時代のギガビットイーサネット対応のレイヤ 2/3 スイッチは、メーカーに依存しない標準的なギガビットイーサネットの共有型伝送モジュールを利用できる装置が数多くリリースされています。MiniGBIC(SFP)モジュールは、他社のレイヤ 2/3 ギガビットスイッチの標準インターフェースとしてもご利用頂けます。この伝送モジュールの変更だけで、サーバエリアネットワーク、キャンパスエリアネットワーク、そしてメトロエリアネットワークなど幅広い応用が可能になります。距離の異なる伝送モジュール、波長の異なる(CWDM/DWDM)伝送モジュールが豊富にあります。

* MSA(マルチソース・アグリーメント)で I/F は世界共通ですが機器メーカーによっては使用できない場合がありますのでご注意ください。

MiniGBIC 外形寸法図(単位:mm)

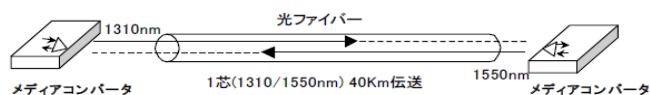


GBIC 外形寸法図(単位:mm)

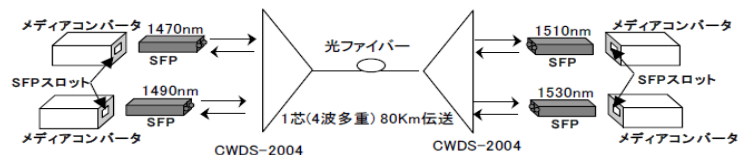


■ 光フィルター多重接続を可能にする

I, 内蔵フィルタ多重 SFP



II, 外付光フィルタ多重 SFP



SFP (Mini-GBIC)

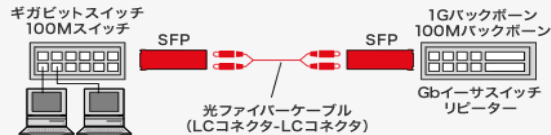
SFPとは？

SFP (Small Form Factor Pluggable) は、1000Base-T/SX/LX/ZXの通信を行う際に通信機器側に実装する物理層の仕様を著述可能な形でまとめたモジュールです。
SFPは同様な用途の GBIC (Gigabit Interface Converter) と比較して大きさが半分以下と小型なことからmini-GBICとも呼ばれています。

- ネットワーク機器のSFPポートに挿入して光信号に変換するモジュール。
- 2芯のLCコネクタ付き光ファイバケーブルを接続し、長距離での高速通信を可能に。
- SX (MMF)、LX (SMF)、1000BASE-Tの3種類をラインナップ。
- 工場出荷時に全品動作チェックを行う万全の品質体制。
- リンクダウンの原因となる光ファイバケーブルの汚れを除去する専用クリーナー付き。
- 通電中のプラグイン/プラグアウトが可能なホットスワップ機能対応。

使用例

<LAN-SFPGSX>



ギガビットスイッチ等のネットワーク機器のSFPポートにSFPを挿入し、光ファイバケーブルで接続します。
シスコ (SX) 他、各メーカーに対応しています。

製品一覧



マルチ
モード 1000
BASE SX

SFP (mini GBIC) コンバータ

LAN-SFPGSX

オープン価格

コネクタ	対応ファイバコア径	波長
機器側/SFPポート、 ネットワーク側/LCコネクタ (デュプレックス)	50/125ミクロン	850nm

アッテネータ(減衰器)

光の伝送装置や TXの送信レベルでRX受けれるレベル範囲より強い場合など
信号を適切な信号レベルに減衰させるときに使用する。



アッテネータ(減衰器)は、信号を適切な信号レベルに減衰させる製品です。光伝送の送受信間距離の差から発生する光パワーの差や光の反射は伝送装置に対して悪影響を及ぼす可能性があります。この為、光パワーレベルを調整する必要性がありアッテネータを使用します。

- ✓ シングルモードを0dBから10dBまでお客様の接続環境に合わせて1dBステップごとに減衰量を選択可能
- ✓ Duplex(双重)のパッチコードなどで減衰器を使用したい場合にスペーサーとして有効な0dBのアッテネータをご用意
- ✓ 使用頻度の高いSC、LCコネクタのUPC研磨(各1dB～10dB)を在庫しており即納対応も可能