学内ネットワークのサブネット化について

教育学部　出口　憲，久保　仁

The Subnetting of the TOKOHA Gakuen University Network

Ken DEGUCHI and Masashi KUBO

Abstract

We report on the subnetting of the TOKOHA Gakuen University (TGU) network. A subnetting changes a network to a more manageable and secure one. We have challenged to build subnets. We have used the Windows NT servers as routers and then divided the TGU network into the subnets, where the routing information between the subnets has been resolved by the proxy ARP server. In addition, we have configured the DHCP servers for an easy maintenance of client computers on the subnet.

1　なぜサブネット化を行うのか？

ネットワークがある程度の規模となってくると管理が非常に繁雑となる．例えば，従来の設定を変更する場合，全てのコンピュータの設定を変更せねばならないので著しい負担となることは明らかである．そこで，ネットワークを小さなネットワークに分割し，管理するコンピュータの台数を減らすという方法が考えられる．これがサブネットの基本的な考え方である [1–3].

本学においても，教室，研究室及び事務関係のコンピュータ台数が 300 台[1]以上となっており，もはや実態を把握することさえ困難になりつつある．設定がおかしかったり故障しているコンピュータや機器がネットワークに接続されている可能性は大きく，最近頻繁に生じているネットワーク障害[2]をもたらす原因になっていると思われる．どこにどのようなコンピュータを導入するかということについての情報を集約すべき方法が確立されていなかったこと，将来にわたるネットワーク構築の展望が欠けていたことに原因がある．無計画にコンピュータの台数を増やせば，ネットワークは

[1]短大 (静岡，菊川) を合わせると 500 台近い規模となる．

[2]ネットワークへの負荷が大きくなるとパケットの転送ができなくなるトラブルが頻繁に発生している．故障している機器が存在するためと思われる．

確実に破綻する．このような観点からもネットワークを再編しサブネット化を行うことは極めて有意義である．

サブネット同士の通信はルータあるいはブリッジを介して行うことになるため，直接接続されている場合に比べて余分な情報が流れない．このため，ネットワークにトラブルが拡がることを防止できるだけでなく，サブネットをまたいで情報を覗き見することもできなくなりセキュリティの観点からいっても望ましい．

以下の章では，TCP/IP ネットワークの基本的な仕組，サブネット化に当たっての検討事項，サブネット化の手順について述べ，最後に今後のネットワーク管理をどのように行っていくべきかということについて言及する．

2 TCP/IP ネットワークの基本的な事項

まず，TCP/IP を用いたネットワークにおいて，どのように情報の交換が行われているかを簡単に述べることにする．

2.1 パケット

ネットワークで送られる情報は，ある程度のパケット (packet，束) として送られている．一般に一つの情報は複数のパケットに分けられて送られる．パケット交換をするということに TCP/IP ネットワークの特徴の一つがある．

2.2 IP アドレス

ネットワーク上でコンピュータの区別をするために用いられるものが IP アドレスである．10 進表記をすると，IP アドレスは，

172.16.128.100

という形であらわされる．10 進表記の数字では，0〜255 までの数字が使われる．“.” が区切りをあらわしているので，$256^4 = 2^{32} \simeq 4 \times 10^9$ の組み合わせが存在することになるが，インターネットに接続する組織が増えたため，IP アドレスは不足し始めている[3]．インターネット上で IP アドレスの重複が起きてはならないので，組織ごとに IP アドレスの割り当て範囲が決められている．

IP アドレスの中でも表 1 に示すものはプライベート IP アドレスと呼ばれ，インターネット上には存在せず，インターネットに直接接続されていないコンピュータには，このプライベート IP アドレスを割り当てることが推奨されている [4]．

[3]IP アドレスは連続的に使われているわけではなく，所々使われていないものが存在する．

IP アドレスの範囲	サブネットマスク	説明
10.0.0.0〜10.255.255.255	255.0.0.0	1 個のクラス A
172.16.0.0〜172.31.255.255	255.255.0.0	16 個のクラス B
192.168.0.0〜192.168.255.255	255.255.255.0	256 個のクラス C

表 1: プライベート IP アドレスの割り当て

2.3 MAC アドレス，ARP

ネットワークカード固有の MAC アドレス (ハードウェアアドレス) と IP アドレスを用いて，ネットワークに接続されたコンピュータは識別されている．MAC アドレスは，16 進表示で `00:00:4c:21:9a:f0` のようにあらわされ，出荷時にネットワークカードごとに書き込まれており通常変更することはできない．組み合わせ数は，8bit $\times$ 6 = 48 bit，すなわち，$2^{48} \simeq 2.5 \times 10^{14}$ もあるため不足することはないと思われる．

一方，IP アドレスは自由に変更できる．一般に，ネットワーク上での情報のやり取りは IP アドレスによって行われるが，その際に MAC アドレスと IP アドレスの対応表が必要になる．あるコンピュータが「これこれの IP アドレスを持っているコンピュータの MAC アドレスを教えてくれ」という要求を出すと，他のコンピュータが MAC アドレスを教える仕組で実現されている．この仕組を ARP (Address Resolution Protocol)[3, 5] という．

2.4 ネットマスク

表 1 のサブネットマスクとは，同じネットワークに存在する IP アドレスの範囲を示すものである．IP アドレスの割り当て範囲を示す方法として，172.16.0.0/16，あるいは 172.16.0.0/255.255.0.0 という表記を用いる．これは，/以降がサブネットマスクをあらわしており，先頭の 16bit (今の場合，172.16 の部分) を固定して，172.16.0.0〜172.16.255.255 までの IP アドレスが同一ネットワークに存在することをあらわす[4]．例えば，172.16.1.3 と 172.16.4.6 は同じネットワーク上に存在しているので直接通信を試みるが，172.17.1.100 の場合は別のネットワークに存在するため直接的な通信はできない．

[4]ただし，172.16.0.0 はネットワークそのものをあらわし，172.16.255.255 はブロードキャストといって 172.16.0.0/16 に属する全てのコンピュータに対しての一斉通知に使われる特別なものとして使われるので IP アドレスとして使うことはできない．

2.5 ルータ

コンピュータはそれ自身が持っている情報 (IP アドレスとサブネットマスク) をもとにパケットの送り先を判断している．しかし，パケットの送り先が不明の場合，パケットは指定されたルータ (デフォルトゲートウェイ) に送られる．ルータはパケットを送る経路を決める装置で，パケットの行き先を確認し適切な経路へとパケットを再送信する．これを繰り返すと異なるネットワーク間の通信が可能になる．

例えば，図 1 のような，192.168.1.0/24 (すなわち，192.168.1.0〜192.168.1.255) と 192.16.168.2.0/24 (すなわち，192.168.2.0〜192.168.2.255) という異なるネットワーク (表 1 のクラス C に相当する) を考える．

192.168.1.20 が 192.168.1.30 と通信する場合 サブネットマスクから同じネットワークに存在すると判断できるので，192.168.1.20 は 192.168.1.30 と直接通信を試みる．

192.168.1.20 が 192.168.2.40 と通信をする場合 サブネットマスクから同じネットワークに存在しないと判断されるので，192.168.1.20 と 192.168.2.40 はルータを介して通信を行なおうとする．

ところで，192.168.1.0/24 に属するコンピュータは，192.168.1.0/24 に属するものとしか通信できない．同様に，192.168.2.0/24 に属するコンピュータは，192.168.2.0/24 属するものとしか通信できない．このため，図 1 のようにルータは複数の IP アドレスを持っており，その間でパケットの中継を行えるように設定されている．192.168.1.0/24 に属するコンピュータのデフォルトゲートウェイを 192.168.1.254，192.168.2.0/24 に属するコンピュータのデフォルトゲートウェイを 192.168.2.254 と設定してあれば，ルータを介したネットワーク間の通信が可能となる．つまり，192.168.1.20 が 192.168.2.40 と通信するときは，192.168.1.20 ↔ 192.168.1.254 ↔ 192.168.2.254 ↔ 192.168.2.40 というようにパケットが送られる．

3 サブネット化に当たっての検討事項

サブネット化の前に検討したことは以下の 5 点である．

- ネットワークの分離．
- ルータの確保．
- DHCP (Dynamic Host Configuration Protocol)[6] を用いたネットワーク管理．
- ルーティングの設定．
- NetBIOS[7, 8] 名の解決．

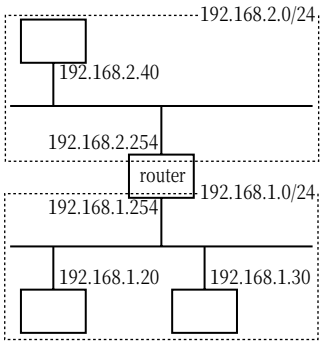


図 1: 192.168.1.0/24 と 192.168.2.0/24 の接続図.

3.1 ネットワークの分離

まず，サブネット化を行う上で一番念頭に置くことは，教室と研究室・事務室を分離することである．これは，教職員が使用するコンピュータを学生の使用するコンピュータから直接見えないようにするための処置で，セキュリティ面からも重要である[5]．例えば，Windows のネットワークコンピュータを開くと学内のコンピュータが見える．これは，Windows が自分の存在を一斉通知を用いてアナウンスしている[6] ためであるが，ネットワークを分離することで見えないようになる．(あくまでも見えなくなっただけで，アクセスは可能であることに注意．)

3.2 ルータの確保

すでに述べたようにネットワークを分離するためにルータを用いる．教室にある Windows NT サーバを用いればルータを構築できるので，新しい機器を購入する必要はない.

3.3 DHCP を用いたネットワーク管理

コンピュータ教室が増えたこともあり管理が非常に繁雑となってきているので，DHCP を用いる方法に切り替える．DHCP とは，IP アドレス，DNS サーバ，ドメイン名，デフォルトゲートウェイなどの情報をサーバから動的に取得するもので，通常

[5]以前は，学生用のコンピュータから研究室・事務室のコンピュータが丸見えであった.

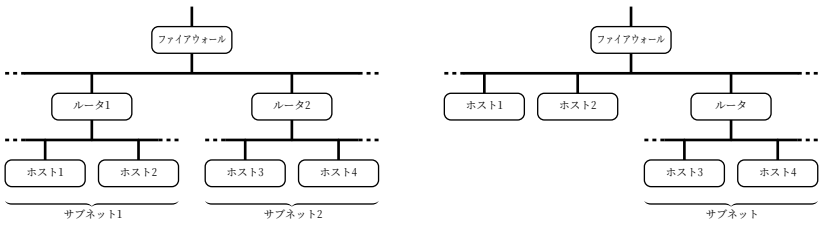
[6]Windows NT 及び Windows 9x などは，NetBIOS という仕組を用いてファイル共有などを行っている．NetBIOS は，インターネットへの接続には全く必要ないということを強調しておく．不用意に設定をするとインターネットから不正なアクセスを受けたり，ネットワークを混乱させる原因にもなるので注意が必要である．特に，ファイル共有は他のコンピュータから自分のコンピュータを操作される危険がある.

はノートパソコンなどをネットワークで移動運用するために用いる．教室のようにコンピュータの台数が多い場合でも，個々のコンピュータを設定する必要はなく，サーバのみの集中管理ができ都合がよい．また，MAC アドレスを用いれば固定 IP アドレスを与えることもできるため，IP アドレスからコンピュータが特定できなくなるというトラブルも避けられる．

3.4 ルーティングの設定

サブネット化を行なった場合, ルーティングをどのように実装するかはケースバイケースである．一般にサブネット化といっても図 2-a のように特定のサーバ類を除いて全てのホストが完全にサブネット内にある場合と, 図 2-b のように一部のホストがサブネット外にある場合とがある．前者についてはサブネットを仕切っているルータがルーティングを行なうので[7], 各ホストのデフォルトゲートウェイを適切に設定するだけでよい[8].

図 2-b のようなサブネットに含まれないホストがある場合は問題が発生する．サブネット内のホストからのパケットは, そのホストのデフォルトゲートウェイが適切に設定されていれば, どのホストへも到達する．ところがサブネット外のホストからサブネット内のホストへは, ARP 要求がルータを通過しないためパケットを送信できない．UNIX サーバなどの場合は各ホストがルーティングテーブルを保持することで対処できるが, Windows や Macintosh といった通常デフォルトゲートウェイのみを設定するホストでは現実的ではない．一般にこの問題は Proxy ARP[9] による透過型ネットワーク[9]を構築することで対処する．



(a) 完全なサブネット化　　(b) 部分的なサブネット化

図 2: サブネットの種類

ルータではなくブリッジを用い，ネットワークを物理的に分離する方法もある．ブ

[7]各ルータのルーティング情報は RIP を用いて共有するのが一般的である．
[8]図 2-a の場合, ホスト 1, 2 のデフォルトゲートウェイはルータ 1 に, ホスト 3, 4 のデフォルトゲートウェイはルータ 2 に設定する．
[9]付録 A 参照

リッジはルーティングを行なわないため，セグメント中に挿入しても論理上単一セグメントのままとなる[10]．大抵のブリッジには簡易なパケットフィルタリング機能が備わっているので，適切にこれを設定することにより不要なパケットを切り落とし，ネットワーク負荷の軽減およびセキュリティの向上を図ることができる．

3.5 NetBIOS 名の解決

NetBIOS 名とは，Windows 関連のネットワーク特有のもので，通常ネットワークコンピュータを開いた際に表示されているコンピュータの名前のことである．これは，通常使われる TCP/IP 上での名前 (DNS) とは異なる．プリンタやファイルの共有を行う際 NetBIOS 名の解決が出来ないと問題が生じるが，同じネットワークに属するコンピュータに対してはブロードキャスト (一斉通知) で情報が送られるため同一ネットワーク内では名前解決に特別な手段はいらない．しかし，ネットワーク外のコンピュータからルータを越えて共有を行う場合，ブロードキャストはルータを越えて流れないために NetBIOS 名の解決が出来なくなる．ルータ越しの NetBIOS 名の解決方法としては，

1. WINS サーバを設置する．
2. lmhosts ファイルを使う．
3. DNS を用いる．

といったものがある．

4 サブネット化の手順

検討の結果，図 3 のような構成のネットワークを構築した．以下はその手順である．

4.1 ルータの構築

コンピュータ教室には Windows NT Server があるので，それをルータとして活用することにした．1 台のコンピュータにネットワークカードを 2 枚挿し，それぞれに教室内部で用いる IP アドレスと教室外部で用いる IP アドレスを与える．次に，2 枚のカード間で IP パケットの転送ができる様にしてやればルータの構築は終了である．これらの作業はコントロールパネルから設定可能であり，それほど手間のかかるものではない[11]．

[10] 逆にネットワークの論理構造を変更しないので従来の設定をそのまま利用できる．
[11] 詳細に関しては，Windows NT リソースキット [10] を参照．

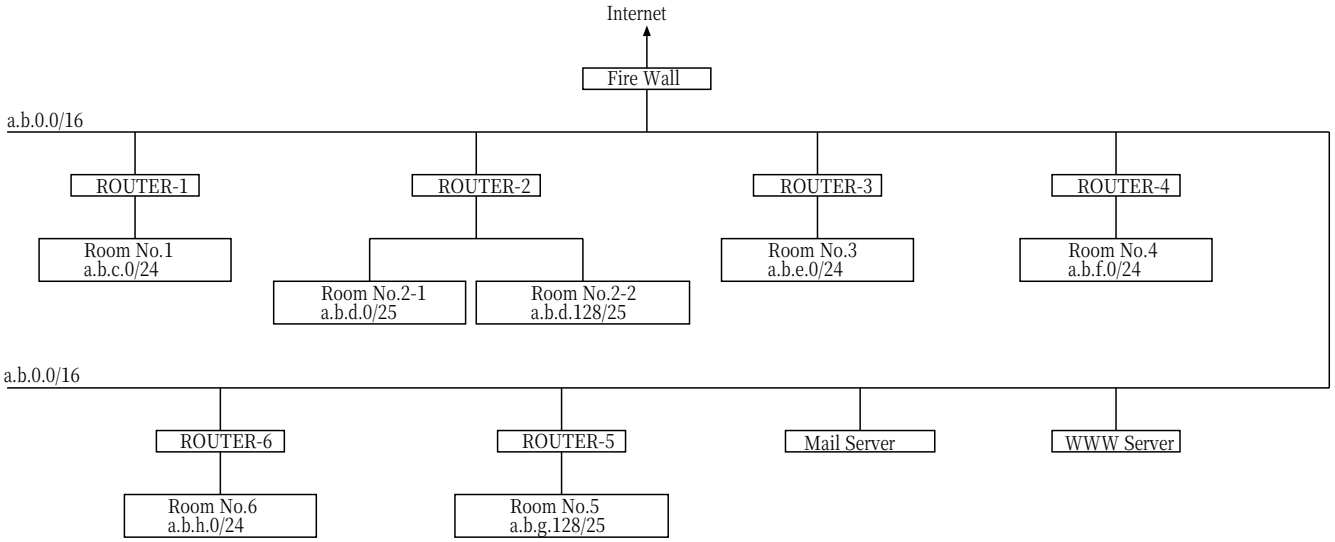


図 3: 学内ネットワークのサブネット化.

・各サブネット内はDHCPにより固定IPアドレスを供給.
・Room No.2-2，Room No.5は学生がパソコンを持ちこめるようにDHCPにより動的にIPアドレスを供給.
・パケットフィルタリングも可能だが何も設定していない.
・セキュリティ保持のためIPアドレスは伏せてある.

4.2 DHCP サーバの構築

教室にある Windows NT Server に DHCP サーバをさせることにした．サブネット化してしまえば，誤って教室外部のコンピュータに IP アドレスを貸し出す心配はない．

Windows NT Server 標準の DHCP サーバは GUI による管理しかできないため，教室コンピュータをまとめて登録する方法がなく大変な作業になるかと思われた．しかし，幸いなことに Windows NT リソースキット [10] に一括登録できるコマンド dhcpcmd があったので作業は簡単に終了することが分かった．

4.3 MAC アドレスの取得

固定 IP アドレスを供給するため，ping と arp コマンドを組み合わせる方法でコンピュータ教室のコンピュータ及びプリンタの MAC アドレスを収集した．収集した IP アドレスと MAC アドレスを基に登録用バッチファイルを作成した．プリンタは DHCP に対応していないものがあること，及びトラブルが起きる可能性は低く台数も少ないので，DHCP による IP アドレスの供給はせず従来のままとした．

4.4 教室コンピュータの設定

DHCP により IP アドレスなどのネットワーク情報を取得できるように設定を変更した．Windows は，コントロールパネルのネットワークアイコンを利用して変更可能である．

4.5 ルーティング情報の設定

今回の事例では，以下の理由により部分的なサブネット化を行なうこととした．

- サーバ類を除いた殆んどのホストでデフォルトゲートウェイが適切に設定されていない[12].
- 配線上, 物理的に完全なサブネット化を行なうことが不可能であり, 部分的なサブネット化以上のメリットがない.
- 使用する機器の関係からソフトウェアブリッジが動作しない.

以下概略を述べる．

[12]従来学内は単一ネットワークであり, また学外へのパケットはかならず Proxy サーバや SOCKS サーバを経由するため不要であった.

Proxy ARP サーバの OS には FreeBSD 3.4-RELEASE[13]を利用した．ARP 情報は各ホストでキャッシングするため，Proxy ARP サーバへの負荷はあまりない．そこで 1 台ですべての教室のサービスを行なうよう設定した．なお，ルータそのものに Proxy ARP を行なわせる試みは残念ながら成功しなかった[14]．

4.6 NetBIOS 名の解決

必要に応じて lmhosts ファイルを使うことにした．特に，図書館 2 階のネットワークをサブネット化する際に変則的な方法を取らざるを得なかった[15]ので，lmhosts ファイルにより NetBIOS 名の解決を図った．

もしも，今まで共有できていたコンピュータが共有できなくなった場合，lmhosts ファイルを適切に設定すれば共有できる[16]が，将来的には，NetBIOS 名の解決のため WINS サーバを動かした方がよいと思われる．

5 今後の課題

教室のサブネット化は完了したが，大学と常葉短大 (静岡校舎)，大学と橘小学校，大学と学園本部の間は一つのネットワークとなっている．別の組織であるから本来ならばネットワークを分けるべきである．ネットワークが一つになっていると，どこかで起きたトラブルが全体に波及し，セキュリティ的にも決して良い状態とはいえない．このように大学のみならず全体のネットワークを見直す作業を進めなければならない．

学内 LAN からインターネットへの出口の問題も考えておかなければならない．現状では出口が 2 つしか存在しないためサーバが負荷に耐えられず，授業などにも支障が出ている．過負荷ゆえにネットワークのトラブルも発生していると思われる．また，UDP パケットも SOCKS サーバを抜けられず，Real Audio などのサービスを受けられず外国語学部の授業に支障が出ている．

「情報化を進める=コンピュータを増やせばよい」という考え方は危険である．トラブルはコンピュータの台数が増えると飛躍的に増大する．例えば，ネットワークのスピードは低下するし，管理の行き届かないコンピュータは確実に増える．結局，コンピュータを増やしても，使えないネットワーク，使えないコンピュータが増えるだけになってしまう．

これらの問題を回避するために，

[13]FreeBSD については，http://www.jp.FreeBSD.ORG/を参照．
[14]Windows NT 標準の arp コマンドでは不可能である．
[15]図書館 2 階のコンピュータからルータを越えて Windows NT の共有リソースを利用するために必要であった．
[16]ただし，lmhosts ファイルの内容を反映させるためには，Windows の再起動が必要である．

- コンピュータの導入について協議する場を設ける．導入する側と管理する側が必ず出席し，どのような必要性があって導入するのか[17]，どのような問題点があるのかを議論しておく．現状のように「いつの間にか導入されている」という事態は避けねばならない．協議する場を開けないというなら導入する側の責任でコンピュータの管理を行ってもらうより他ない．

- 予算を気にしすぎると使えないネットワークができてしまう．

  予算を節約するなら徹底的に節約する．節約するからにはOSなどはフリーのものを用いてサーバを構築する．フリーのものの方が様々な情報が公開されているため管理は容易であるし，信頼性の点でも通常の使用では商用のものに劣っているわけではない．

  予算をかけるならある程度以上の額を出すことが重要である．予算をかけないとメーカーのサポートが受けられず信頼性は低下する．中途半端なサポートでは役に立たないと考えるべきである．

- 今後の展望をしっかりと持つ．ネットワークの肥大化を過小評価してはならない．何を行うのかをはっきりさせ，それに応じた計画を立てる．少なくとも3年程度先を見越したネットワークの構築をする．

- 定期的に小学校や短大とも協議の場を設ける．同じネットワークを共有している以上必要である．ネットワークの状態の把握，及び教育内容について有益な議論ができる．

とにかく,「情報化の流れに乗らなければ」という理由だけで導入を急ぐことは「百害あって一利なし」ともなりかねない．十分な時間をかけ，将来のことも考えた計画を練ることが，後の管理を容易にし，余分な出費を押さえることに結びつくのである．

[17]コンピュータを使うと効率があがる仕事かどうかを見極めることが大切である．何でも使えばいいというものではない．

付録 A　Proxy ARP のしくみ

Windows や Macintosh など, デフォルトゲートウェイ以外のルーティングテーブルを持たないホスト host-a から, host-b へパケットを送出する際は図 4 のようなアルゴリズムが用いられる．同一ネットワークのホストに対しては直接パケットを送出し, 別ネットワークのホストに対しては一次到達先としてデフォルトゲートウェイを選択するわけである．host-a のデフォルトゲートウェイが適切に設定されていない場合, host-a はネットワーク内にサブネットが存在しないものとし, 直接 host-b への ARP 要求を行なう．だが, host-b がサブネット内にある場合, この ARP 要求がサブネットを仕切っているルータによって切り落とされるため host-b へは届かず, 通信が行なえなくなってしまう．

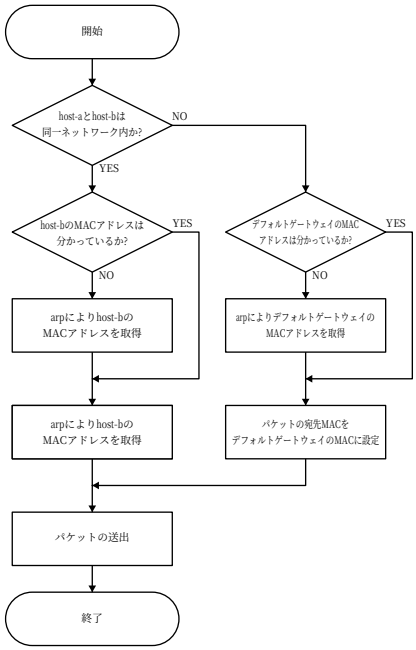
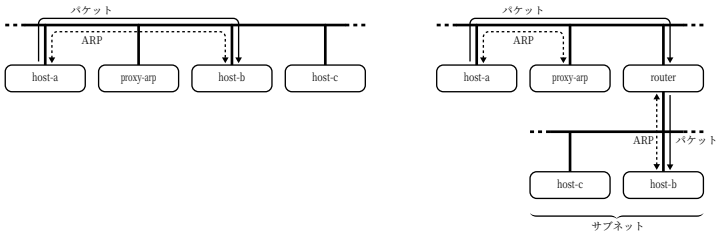


図 4: パケット送出のアルゴリズム

Proxy ARP はこの問題を回避するためのもので, host-b への ARP 要求に対し代理でルータの MAC アドレスを返答する機能である．Proxy ARP サーバを host-a と同一のネットワークに設置することにより, host-b へのパケットはすべてルータへと送られるようになり, 正常に通信を行うことができる．ホストがサブネットを仕切るルータの存在を知覚していないため, 透過型ネットワークと呼ばれる．



(a) 単一ネットワーク　　(b) Proxy ARP 利用

図 5: ARP ブロードキャストとパケットの経路

参考文献

[1] GADS, “Towards an Internet Standard Scheme for Subnetting”, RFC-940, Network Information Center, SRI International, April 1985.

[2] J. Mogul and J. Postel, “Internet Standard Subnetting Procedure”, RFC-950, Stanford University and USC/Information Sciences Institute, August 1985.

[3] W. Richard Stevens 著/井上尚次 監訳/ 橘康雄 訳，詳解 TCP/IP，ソフトバンク (1997)，サブネットについては 47 ページから，ARP については 59 ページからを参照.

[4] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot and E. Lear, “Address Allocation for Private Internets”, RFC-1918, Cisco Systems, Chrysler Corp., RIPE NCC and Silicon Graphics, Inc., February 1996.

[5] D. C. Plummer, “An Ethernet Address Resolution Protocol”, RFC-826, November 1982.

[6] R. Droms, “Dynamic Host Configuration Protocol”, RFC-2131, Bucknell University, March 1997.

[7] NetBIOS Working Group, “Protocol Standard For a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods”, RFC-1001, March 1987.

[8] NetBIOS Working Group, “Protocol Standard For a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications”, RFC-1002, March 1987.

[9] S. Carl-Mitchell and J. S. Quarterman, “Using ARP to Implement Transparent Subnet Gateways”, RFC-826, Texas Internet Consulting, November 1982.

[10] Microsoft Corporation 著/株式会社アスキー・ネットワーク・テクノロジー 監修/株式会社富士通ラーニングメディア 訳，Windows NT 4.0 Server リソースキット，アスキー (1997)

[11] 加藤浩樹，Windows NT 管理の落とし穴，名古屋大学大型計算機センターニュース第 126 号，Vol.31-2, 135-169 (2000).

[12] 加藤浩樹，大量の PC 群による Windows NT ネットワークの取り扱い，名古屋大学大型計算機センターニュース第 127 号，Vol.31-3, 281-303 (2000).