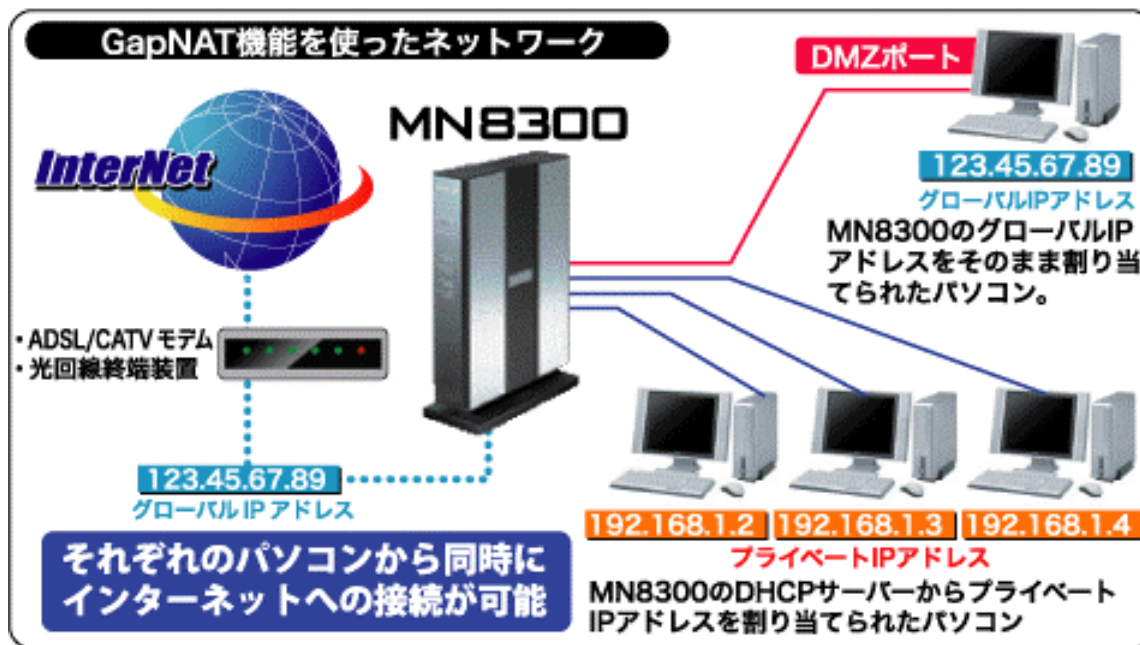


- GapNAT 機能概要 -

GapNAT: Global address proxy with Network Address Translation

プロバイダから取得したグローバルIPアドレスを、LAN側の端末にDHCP機能で割り当てることができます。グローバルIPアドレス端末とプライベートIPアドレス端末の混在ネットワークが構築できます。DMZの構築も簡単。対戦型ネットワークゲームなどに便利です。



平成15年8月

株式会社 エヌ・ティ・ティ エムイー

1.はじめに

MN8300のようなルータを接続するメリットとして主に次の2点が挙げられます。

プロバイダより払出された1つのグローバルIPアドレスを使用して複数端末の同時アクセスが可能になります。

NATによるアドレス変換や、IPフィルタの使用によりセキュリティを意識したネットワーク運用が可能になります。

一方で、プライベートIPアドレスをPCに付与するというNATの仕様上、次のデメリットが発生します。

特定のブロードバンドアプリケーション（対戦型ゲーム、映像/音声通信）が使用出来ないという制限を受けます。

通常NATでこれらのアプリケーションを使用するためには各アプリケーション毎の対応が必要となりますが、それとは異なるアプローチでこの制約を回避するのが「GapNAT」機能になります。

また、LAN型PPPoE接続時（複数グローバルIPアドレス契約）は「マルチGapNAT」を利用して、LAN内にグローバルIPアドレスを持つ端末とプライベートIPアドレスを持つ端末を同時に混在収容させることが可能出来ます。

2.機能概略

MN8300のWAN側に割当てられたグローバルIPアドレスを、LAN側に接続する特定のPCに付与します。こうすることで当該PCは、グローバルIPアドレスを持つ端末として動作することが可能となり使用するアプリケーションの制限を受けません。

LAN側に複数のPCが接続する場合には、ADSLモデムに対して最初にDHCPでアドレス獲得要求を行なったPC、あるいはMN8300にMACアドレスが登録されたPCに対して、グローバルIPアドレスが付与されます。DHCPで付与した場合2台目以降のPCには、従来通りプライベートIPアドレスが付与されます。

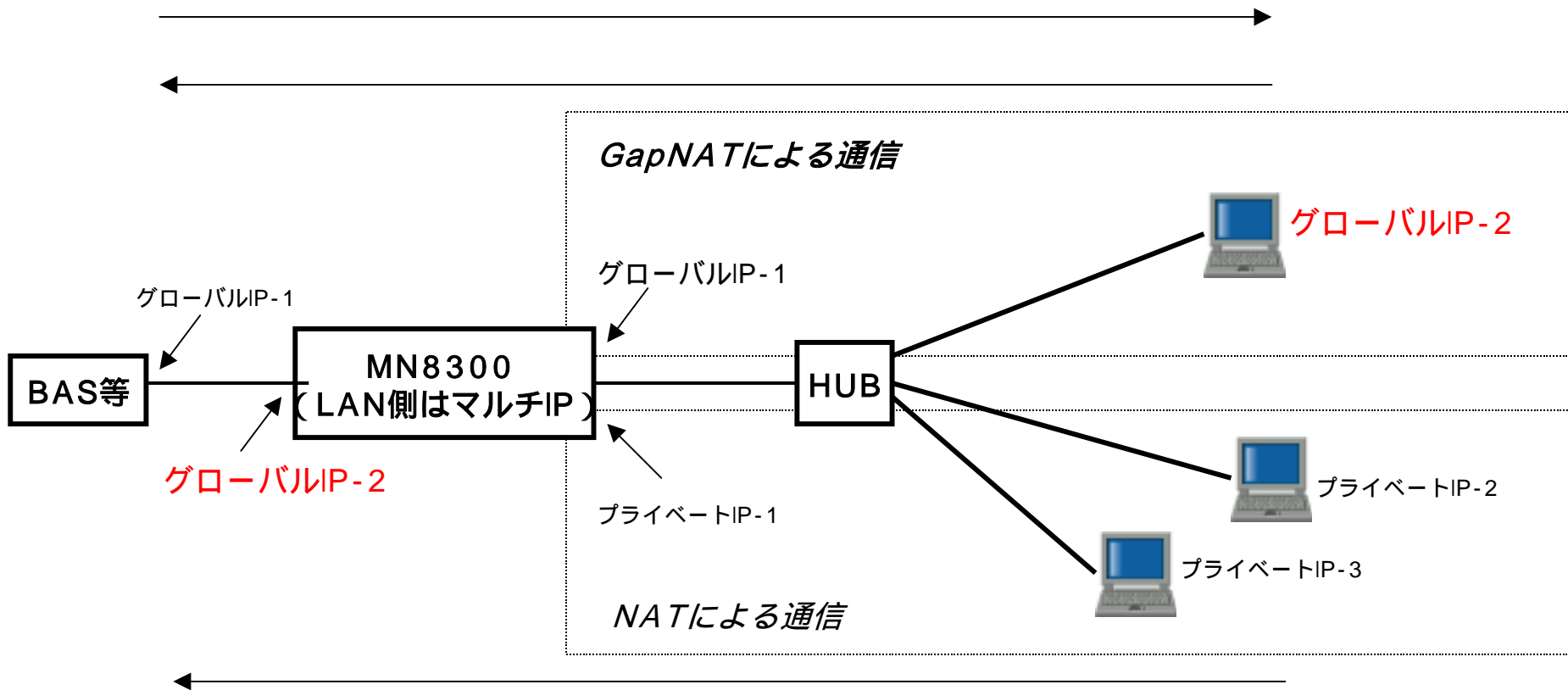
3.制限事項

ネットワークアドレス（ホスト部ALL0）とブロードキャストアドレス（ホスト部ALL1）にあたるアドレスとは、通信出来ません。

同時に使用出来る接続先は1です。

グローバルIPアドレスホストからBASへのPINGには、MN8300が応答します。

【参考1】GapNATを設定した時の、MN8300を通過するパケットの処理について



グローバルIPアドレスを持つパソコンから開始された通信に関するパケットは、内容が書き換えられることなく、そのまま転送されます。

インターネット側から開始された通信に関するパケットは、内容が書き換えられることなくそのまま転送され、結果的にグローバルIPアドレスが設定されたLAN内のパソコンに転送されます。

プライベートIPアドレスを持つパソコンから開始された通信に関するパケットは、NAT変換され、パケット内のIPアドレスおよびポート番号が書き換えられて転送されます。

厳密にはグローバルIPアドレスによる通信は、NAT変換されています。

ただし、同一のIPアドレス/ポート番号に変換されるため、原則として書換えられていないものと判断します。

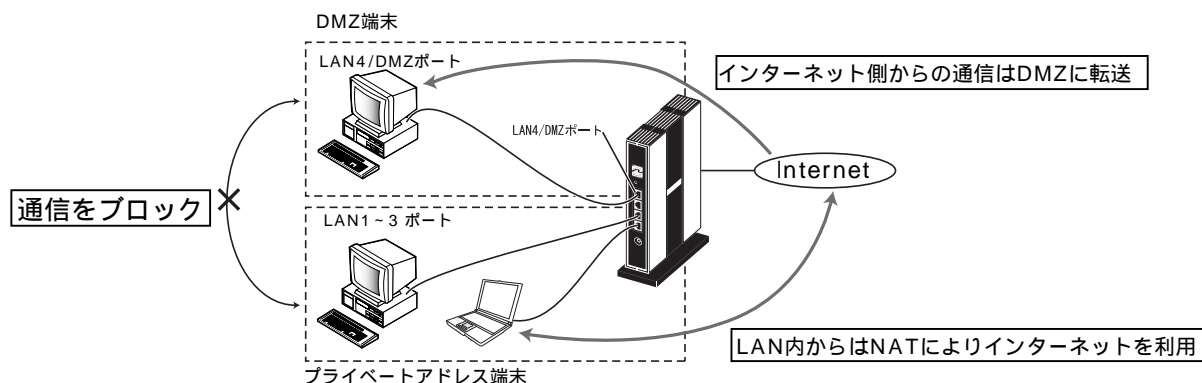
【参考2】LAN4/DMZポートを利用したDMZ環境の構築

LAN内のネットワークと外部ネットワーク間にLAN内への侵入を阻止する目的で設けられるサブネットをDMZと言います。通常、外部に公開するWWWサーバなどをDMZに設置します。本機器ではGapNAT機能を利用して、LAN4ポートをDMZポートをDMZとして運用することができます。DMZは以下のような概念を持つネットワークです。

インターネット側から開始された通信は、DMZネットワークに依存するパソコン（GapNAT使用時は1台、マルチGapNAT使用時は複数台）に転送出来ます。

DMZポートと他のLANポートとは、相互に通信出来ません。

LAN内のパソコンからは、NAT機能によりインターネットを利用出来ます。これらの仕組みにより、インターネット側からDMZへ侵入された場合でも、DMZと他のLANとの通信は遮断されているため、DMZ経由でLANへの侵入は出来ません。これによりインターネット側からの侵入は、DMZまでで食い止めることが出来、外部に公開していない他のLANに存在するパソコンは、侵入者から保護されます。本機器はDMZに対する通信に関して、フィルタリングによる制限を設ける簡易的なファイアウォール機能を搭載しているため、更に安全性が高まります。



MN8300では簡単な設定で、上記のようなDMZ環境を構築できます。