

BIG-IP

トラフィックの戻り先決定方法 について

F5ネットワークスジャパン株式会社

トラフィックの戻り先決定方法について

- BIG-IPは、Auto Last Hop 機能、およびLast Hop Pool 機能によって戻りトラフィックの戻り先を決定します。
- BIG-IP System ではDefault で Auto Last Hop 機能が有効になっています。

System » Configuration : Local Traffic : General

Device Local Traffic

Properties

Auto Last Hop	<input checked="" type="checkbox"/> Enabled
Maintenance Mode	<input type="checkbox"/>
VLAN-Keyed Connections	<input checked="" type="checkbox"/> Enabled
Path MTU Discovery	<input checked="" type="checkbox"/> Enabled
Reject Unmatched Packets	<input checked="" type="checkbox"/> Enabled
Reaper High-water Mark	95 %
Reaper Low-water Mark	85 %
SYN Check™ Activation Threshold	16384 connections
Layer 2 Cache Aging Time	300 seconds
Share Single MAC Address	<input type="checkbox"/>
SNAT Packet Forwarding	TCP and UDP Only

Update

SNAT Pool: None

Rate Class: None

Traffic Class: Enabled Available

Connection Limit: 0

Address Translation: Enabled

Port Translation: Enabled

Source Port: Preserve

Clone Pool (Client): None

Clone Pool (Server): None

Last Hop Pool: None

Update Delete

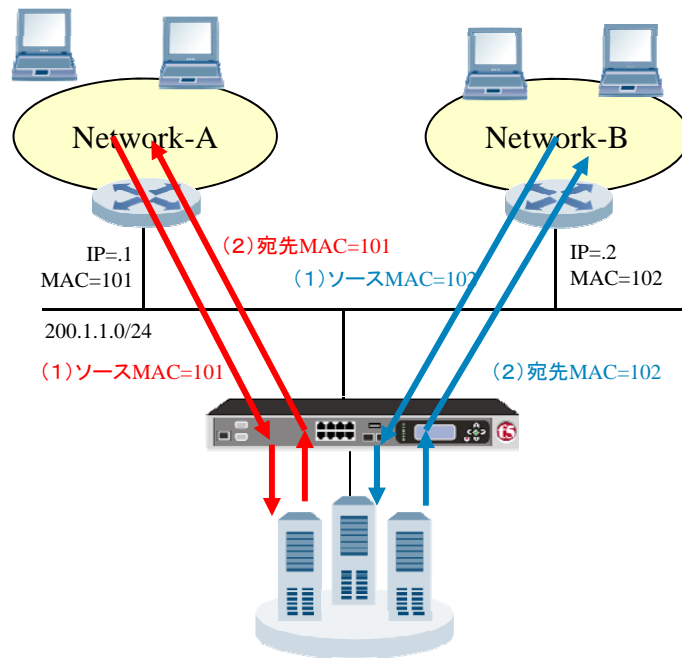
RouterPool
http_pool
https_pool
web01_pool
web02_pool

Auto Last Hop 機能

- Auto Last Hop 機能が有効な場合、戻りトラフィックのフレームの宛先MACのアドレス解決にはARPによる解決は使用せず、送信元MACを覚えておき、戻りトラフィックの宛先MACとします。

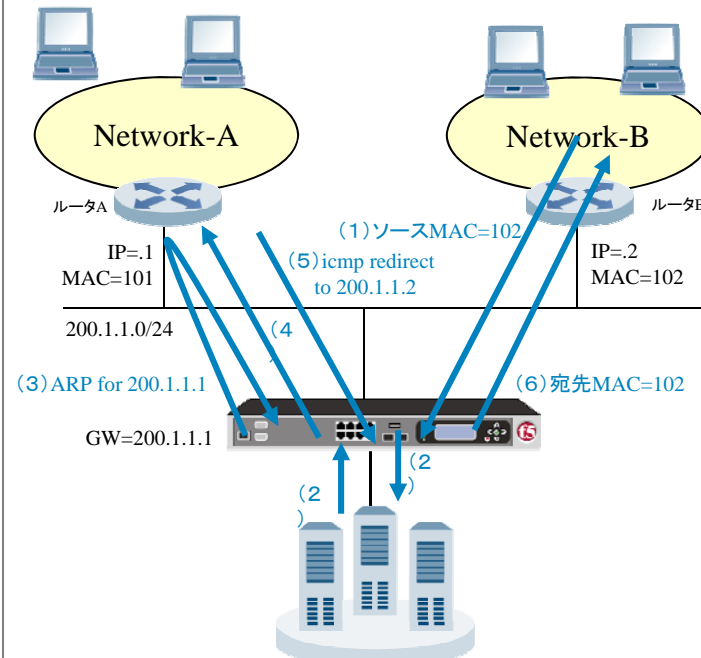
Auto Last Hop が enable の場合

Auto Last Hop 機能が enable の BIG-IP は、(2)の宛先MACアドレスをARPで解決するのではなく、(1)のソースMACより解決します。このため、複数のゲートウェイが存在する環境においても、直接フレームを渡すことができます。



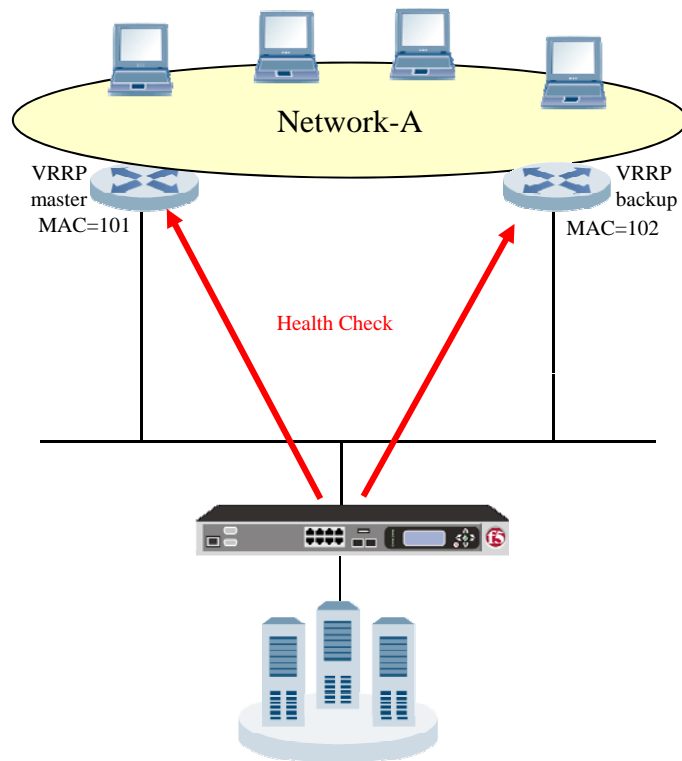
Auto Last Hop が disable の場合

Network-Bからのトラフィックにもかかわらず、BIG-IPは自分のゲートウェイであるルータAをARP解決し、一度ルータAにトラフィックを投げます。ルータAからicmpのリダイレクトメッセージを受け取り、ルータB経由の通信となる。(又は常にルータAがルータBに転送する非効率な経路を通る。)



Last Hop Pool 機能

- Last Hop Pool 機能は、特定のVirtual Server宛ての通信の戻りをBIG-IPが上位ネットワーク機器に渡す際、Auto Last Hop ではなく上位ネットワーク機器のUp/Downの状況を見て、Upしているルータにトラフィックを送信します。



Last Hop Poolとは

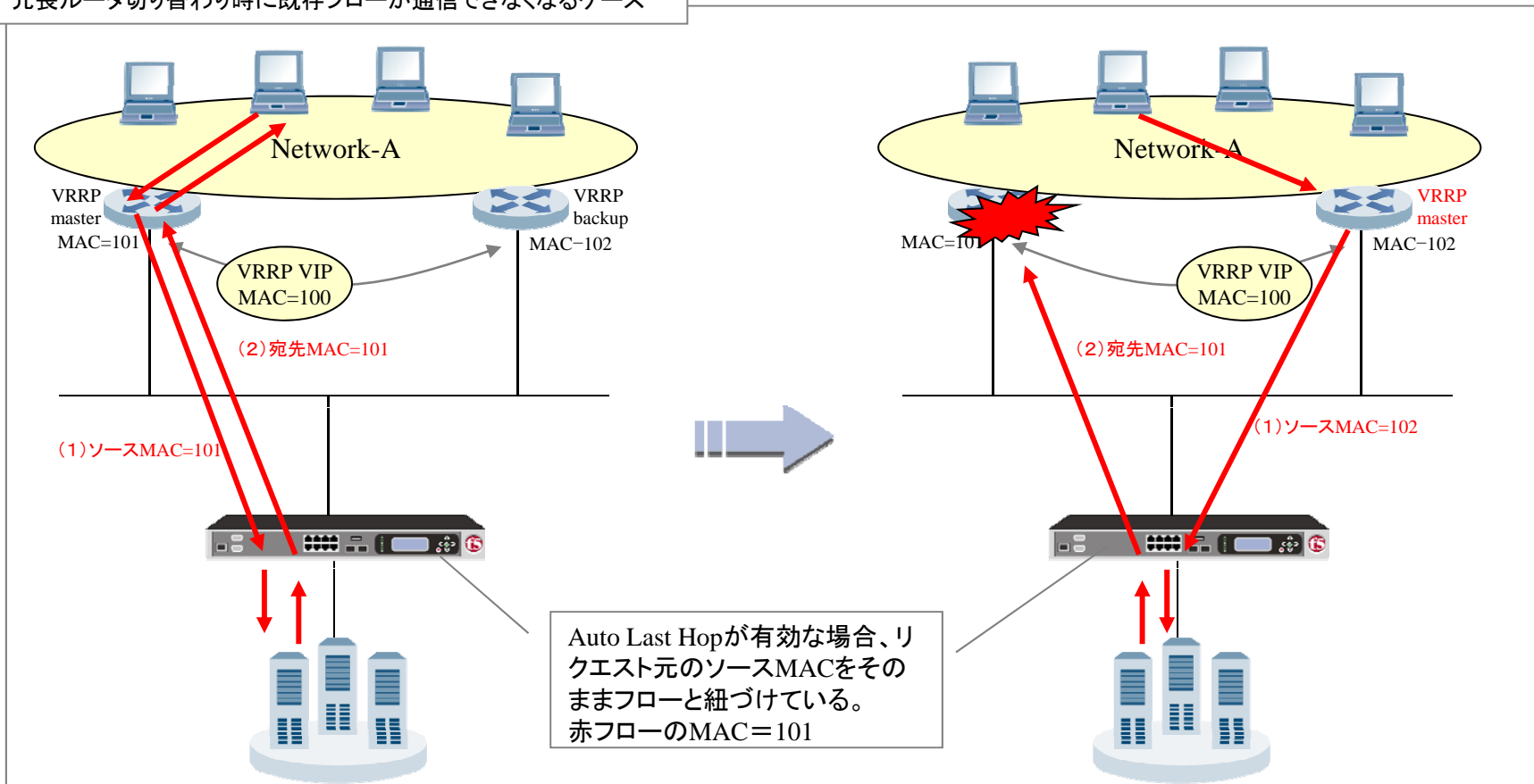
特定のVirtual Server宛ての通信の戻りをBIG-IPがルータに渡す際、Auto Last HopではなくルータのUp/Downの状況を見て、Upしているルータに渡す機能。

ルータのUp/Downを見るために、ルータをPoolメンバー (Last Hop Poolメンバー)として登録します。

Auto Last Hop 機能が問題となるケース

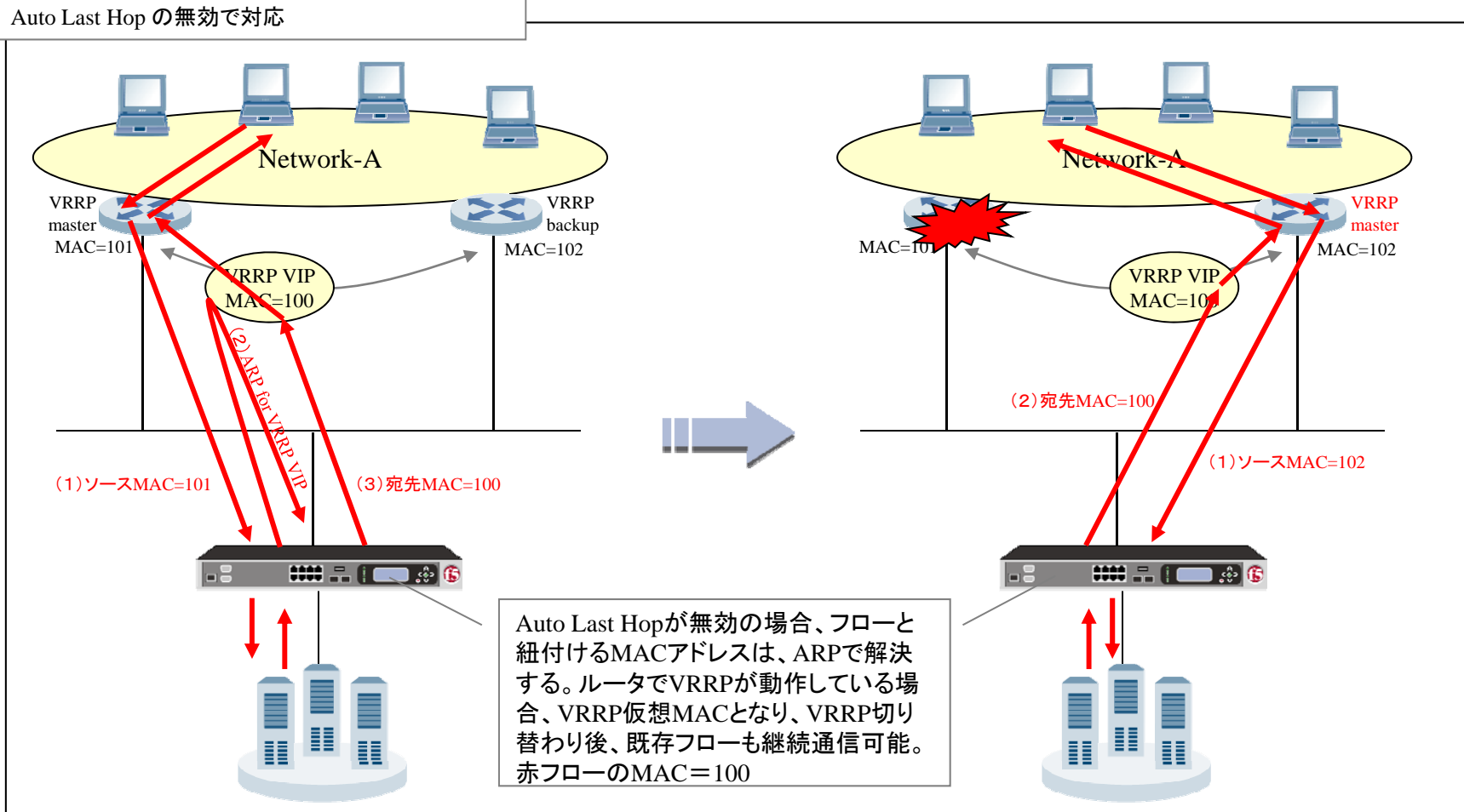
- 上位が冗長ペアかつ、送信に 仮想 MAC を使用しない冗長化方式の場合切り替わり時に既存の通信が出来なくなるケースがあります。

冗長ルータ切り替わり時に既存フローが通信できなくなるケース



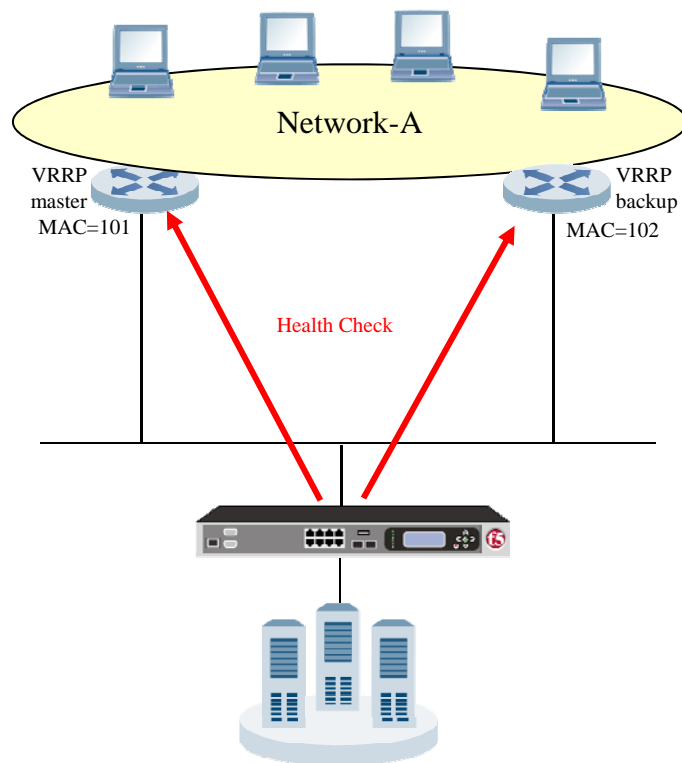
対応策1

■ Auto Last Hop を Disable にすることで対応



対応策2

■ Last Hop Pool 対応



Last Hop Poolとは

特定のVirtual Server宛ての通信の戻りをBIG-IPがルータに渡す際、Auto Last HopではなくルータのUp/Downの状況を見て、Upしているルータに渡す機能。

ルータのUp/Downを見るために、ルータをPoolメンバー（Last Hop Poolメンバー）として登録します。

参考情報

- **sol11796**: Overview of the Auto Last Hop setting

<http://support.f5.com/kb/en-us/solutions/public/11000/700/sol11796.html?sr=13584642>

- **sol2211**: Using last hop pools to correctly return traffic to upstream redundant devices

<http://support.f5.com/kb/en-us/solutions/public/2000/200/sol2211.html?sr=13584678>

- **sol9487**: BIG-IP support for neighboring VRRP/HSRP routers

<http://support.f5.com/kb/en-us/solutions/public/9000/400/sol9487.html?sr=13584754>



IT agility. Your way.

Twitterでコンテンツ更新情報をお知らせします！
@F5TechDepot



本資料に関するご意見、ご要望は、下記のメールアドレス(受信専用)にお願い致します。

F5J-Tech_Depot/atmark/f5.com

※迷惑メール防止のため、「@」を「/atmark/」と表記しています。