???? VLAN ???????? ARP ???? ARP ???????

非常好的问题，你描述的这种双网关同 **VLAN** 场景确实极易引发 **ARP** 异常甚至 **ARP** 风暴，这正是造成堡垒机、SSH 连接卡顿、间歇掉线的高危结构之一。下面我会从原理 → 症状判断 → 排查命令 → 验证与优化方案四个角度带你系统分析。

?????????????????

在 **同一 VLAN（L2 广播域）**中接入了两台路由器（LAN 口），例如：

设备	**IP**	网关角色
Router1	10.2.2.253	默认网关 A
Router2	10.2.2.254	默认网关 B
VM1	10.2.2.11	默认网关 10.2.2.253
VM2	10.2.2.12	默认网关 10.2.2.254
Switch	VLAN 10	同一广播域

这种情况下：

- 两台路由器都会收到广播（ARP、DHCP、NetBIOS 等）；
- 如果虚拟机数量多（尤其是几十台 Hyper-V 虚机），每台虚机在 ARP 解析时会广播；
- 两个路由器的 ARP 缓存中都会出现同一网段的大量 IP；
- 如果路由器或虚机错误响应了对方的 ARP 请求，就会出现：

> **“ARP 抢答”**或**“错误网关 MAC 映射”**
>
> 导致部分主机发出的流量走错路由，从而时通时断。

???????ARP ??? ARP ???????

症状	可能原因
SSH/远程连接延迟剧烈波动	广播/ARP 占用链路

症状	可能原因
`ping` 丢包率高且无规律	同网段多设备争答 ARP
`arp -a` 结果频繁变化，MAC 地址不稳定	存在 ARP 抢答或冲突
交换机 CPU 使用率高	广播/组播风暴
路由器的 ARP 表闪烁、频繁老化	网络中 ARP 过多

?????????

1?? ??????? ARP ?????

```
arp -n
```

观察一段时间:

- 若同一 IP 的 MAC 地址在几秒内频繁变化 → **ARP** 冲突。

Linux 可用:

```
watch -n 1 "ip neigh show dev eth0"
```

2?? ?????????????????

进入特权模式:

```
enable
show interface gigabitEthernet 0/45
```

或:

```
show mac-address-table count
show cpu-usage
show interface counters errors
```

重点看是否有以下特征:

- 接口广播包数量极高;
- MAC 地址表频繁刷新;

- CPU 占用偏高。

3?? ????????????????????

锐捷设备可以查看：

```
show storm-control interface all
```

4?? ??????????????

```
tcpdump -i eth0 arp
```

如屏幕中连续滚动大量 ARP 请求（Request）和应答（Reply），说明网络广播严重。

?????????

? ???? ARP ??

1. 抓包中看到同一 IP 有不同 MAC 地址答复；
2. `arp -n` 中 MAC 地址频繁变化；
3. ping 某个目标时出现间歇通；
4. CPU 利用率升高；

   → 基本可以确认是 **ARP** 风暴 **/ARP** 混乱。

?????????????????

?? 1??? VLAN??????

- Router1、Router2 各自放入不同 VLAN，例如：
  - VLAN 10 → Router1 + VM组 1
  - VLAN 20 → Router2 + VM组 2
- 由交换机三层互通（或路由策略）控制。

□ □□□□□ ARP 冲突，彻底隔离广播域。

⚠ 缺点：需要调整虚拟机网段规划。

?? 2????? ARP ??

在路由器和关键服务器上绑定固定的 IP-MAC:

```
arp -s 10.2.2.254 xx:xx:xx:xx:xx:xx
```

这样即使网络中有错误 ARP 也不会污染表项。

?? 3??????????

```
interface range gigabitEthernet 0/1-48
storm-control broadcast level 1.00
storm-control multicast level 1.00
storm-control unicast level 1.00
```

?? 4??? LACP ????????????????

如果你的初衷是“增加出口带宽”，应考虑:

- **LACP** 链路聚合 或
- 双上联负载均衡（**ECMP**）

而不是在同 VLAN 下增加路由器。

?? 5???????

确认优化后再使用:

```
ping -f <目标IP>
arp -n
show interface counters
```

若延迟稳定、ARP 不再闪烁、CPU 降低 → 问题解决。

? ????

问题	原因	最优解
SSH 延迟、连接困难	同 VLAN 双网关引起 ARP 竞争	拆分 **VLAN**，分别绑定各路由器
间歇性断开	ARP 抢答或错误路由响应	静态 ARP + 广播风暴抑制
链路不稳定	广播风暴或 MAC 抖动	storm-control / VLAN 隔离

如果你愿意，我可以帮你：

- 画出你当前拓扑图；
- 给出基于锐捷交换机的三 **VLAN** 规划 **+**防风暴配置模板；
- 并附上堡垒机上 **tcpdump** 分析脚本，快速判断是否 ARP 风暴。

是否要我帮你生成这套完整分析方案？

好，你在堡垒机上看到 **ARP** 表（**MAC**）没有变化，这一步很重要 — 它基本上把「ARP 抢答 / ARP 风暴」作为主要原因排除掉了（至少对堡垒机自身来说它看到的网关 MAC 是稳定的）。下面我把可能的原因按优先级列清楚，并给出逐步、可执行的排查命令与判断要点 —— 你按顺序跑一遍并把关键输出贴回来，我可以帮你解读并给出解决措施。

????????????

> **ARP** 风暴可能性低（堡垒机看到的 MAC 稳定）。现在需检查：交换机/端口级别的 MAC 表与错误计数、路由路径对称性（asymmetric routing）、连接追踪/防火墙表耗尽、虚拟化网络（Hyper-V）和 SSH 服务本身负载/限制。

??????????????

A. ?????Linux???? — ??????????

1. 查看 CPU / 内存 / IO 是否饱和（SSH 卡顿常见原因）

```
uptime
top -b -n1 | head -n 12
vmstat 1 5
```

```
iostat -x 1 3    # 若未安装 sysstat: apt install sysstat
```

异常判断：CPU 长期 >80%、大量 iowait、swap 使用高 → 性能瓶颈。

2. 查看 sshd 日志与系统日志

```
sudo tail -n 200 /var/log/auth.log
sudo journalctl -u ssh -n 200
sudo dmesg | tail -n 50
```

异常判断：有大量 `sshd: unable to fork`、`connection reset`、权限错误等 → sshd 问题或资源耗尽。

3. 查看网络错误/丢包/速率

```
cat /proc/net/dev
# 或用 ip -s link
ip -s link show eth0
ethtool -S eth0    # 某些驱动支持，看错误计数
```

异常判断：RX/TX errors、drops 非常多 → 物理链路/驱动/duplex 问题。

4. 实时抓包观察 SSH 交互是否被丢包或 reset

```
sudo tcpdump -i eth0 tcp port 22 -w /tmp/ssh_capture.pcap
# 在出现问题时停止并分析: tcpdump -r /tmp/ssh_capture.pcap -tt -n
# 或用实时观察:
sudo tcpdump -i eth0 -n 'tcp port 22 and (tcp[tcpflags] & (tcp-rst) != 0 or tcp[tcpflags] & (tcp-ack) != 0)'
```

观察点：是否有大量 TCP RST、重复 ACK、长时间没有响应等。

5. 检查 conntrack / nf_conntrack（若 NAT 较多会影响）

```
sudo apt-get install -y conntrack    # 若未安装
sudo conntrack -S
sudo conntrack -L | wc -l
cat /proc/sys/net/netfilter/nf_conntrack_max
```

异常判断：表接近或已满（entries≈接近 max）→ 连接被拒或重置，尤其在 NAT-heavy 场景。

6. 检查 IP 层设置（rp_filter 等）

```
sysctl net.ipv4.conf.all.rp_filter
sysctl net.ipv4.conf.eth0.rp_filter
sysctl net.ipv4.tcp_syncookies
```

若开启严格 rp_filter（=1），某些不对称路由返回包会被丢弃；可临时设为 0 测试：

```
sudo sysctl -w net.ipv4.conf.all.rp_filter=0
```

B. ?????????? / ???????? — ?? L2 ?????

> 目标：确认没有 MAC table flapping、接口错误、广播风暴、STP 问题

1. 查看 **MAC** 地址表中关键 **MAC** 是否稳定（查看堡垒机 IP/MAC 与两台路由器 MAC）

```
# 锐捷风格示例
show mac-address-table dynamic
show mac-address-table address <MAC地址>
```

观察点：是否同一 MAC 在不同端口间频繁切换（flapping）。

2. 查看接口错误 / 带宽利用 / 广播计数

```
show interface gigabitethernet 1/0/45   # 路由器1连接口
show interface gigabitethernet 1/0/46   # 路由器1另口（若有）
show interface counters errors
show interface utilization
show cpu-usage
```

异常判断：接口错误（CRC、FCS）、高丢包、接口上下线或高 CPU → 物理链路或风暴。

3. 检查 **STP / loop**

```
show spanning-tree
```

若网内有 loop或 STP频繁变更，会出现间歇性通信问题。

4. 开启或查看 **storm-control / port-security** 配置
   如果没有风暴抑制，建议开启（取决设备语法）。

C. ??????? — ??/ARP/??

> 目标：确认两台路由器不会互相“抢答”或路由方向导致不对称

1. 核对路由器 **ARP** 表与 **MAC**（确认路由器看到的下一跳）
   在两台路由器上分别看 ARP、CAM：

```
show arp
show mac-address-table
```

2. 检查是否有 **proxy-arp**、**NAT** 会话或策略
   如果路由器做了 proxy-arp 或代理，会影响主机的出/入流向。
3. 检查路由器是否对某些会话做了策略路由或 **NAPT**／连接跟踪
   大量 NAT 表或连接跟踪满会导致会话中断。

D. ? Hyper-V / ???????????????

> Hyper-V 下一般是虚拟交换机、vNIC、MAC 模式或 MAC spoofing 导致 MAC 表跳动或桥接问题

1. 在 Hyper-V 宿主机上检查 vSwitch、网卡绑定和 team 配置（PowerShell）

```
Get-VMSwitch
Get-VMNetworkAdapter -VMName <VM名> | Select VMName, SwitchName, MacAddress, MacAddressSpoofing
Get-NetAdapter | Format-Table -Auto
```

异常判断：同一物理口上有多个桥接且开启 Mac Spoofing，或绑定多路径（错误配置）会造成 L2 异常。

2. 检查宿主机网络接口统计 `netstat -i` / `Get-NetAdapterStatistics`，看是否有异常流量或错误。

????????????????????????????????

1. 在堡垒机执行：`top`，`ip -s link show eth0`，`conntrack -S`，`sudo tcpdump -i eth0 tcp port 22`
   （观察是否被重置或大量重传）

→ 若堡垒机资源告急或有大量 RST/重传，优先处理堡垒机。

2. 在交换机执行：`show mac-address-table dynamic | include <堡垒MAC>` 与 `show interface counters errors`
   → 若 MAC 在端口间切换或接口错误高，重点排查物理链路/虚拟交换机配置/网卡驱动。
3. 在两台路由器上查看 `show arp` 与 `show ip route`、NAT/conntrack 状态
   → 若 conntrack 满或 NAT 表很多（/proc/net/nf_conntrack），需要调整或增加连接数限制。
4. 在 Hyper-V 宿主机检查 vSwitch 与 Mac Spoofing
   → 关闭不必要的 MAC 泄露与桥接配置。

???????????????????????????

1. 在堡垒机临时关闭 rp_filter（见上），观察连接是否稳定。
2. 检查/调整 sshd 配置：`MaxStartups`、`UseDNS no`，防止 DNS 延迟影响新连接。
3. 在交换机对服务器和路由器端口启用 storm-control（限制广播），并开启端口优先级/ policer。
4. 对路由器和关键服务器（堡垒）做静态 ARP（仅作为临时手段）：

```
# 在堡垒机
sudo ip neigh replace 10.2.2.254 lladdr aa:bb:cc:dd:ee:ff nud permanent dev eth0
```

（注意：静态 ARP 只适合关键节点用于短期排错）

???????????????????????

请在堡垒机/交换机/路由器/Hyper-V宿主机分别运行并贴回关键输出（或至少贴部分）：

堡垒机

```
top -b -n1 | head -n 12
ip -s link show eth0
cat /proc/net/dev
sudo conntrack -S
sudo conntrack -L | wc -l
sudo tcpdump -n -i eth0 -c 200 tcp port 22 > /tmp/ssh200.pcap
```

交换机（锐捷或等效）

```
show mac-address-table dynamic | include 00:13:5d:02:97:25   # 举例堡垒MAC
show interface gigabitEthernet 1/0/45   # 路由器端口
show interface counters errors
```

```
show cpu-usage
show spanning-tree
```

两台路由器

```
show arp
show ip nat translations count     # 若有 NAT
show conntrack summary              # 或查看 NAT/conntrack 状态
```

Hyper-V 宿主机（ **PowerShell**）

```
Get-VMSwitch
Get-VMNetworkAdapter -VMName <some-vm> | Select VMName, MacAddress, MacAddressSpoofing
Get-NetAdapterStatistics -Name "Ethernet"   # 或具体物理网卡名
```

?????????????????

- 若交换机 `show mac-address-table` 显示 同一 **MAC** 在不同端口不断切换 → 是 L2 问题（可能桥接/虚拟交换机误配置或 loop）
- 若交换机 /接口 `errors` 很多或 CRC/FCS 错误 → 是物理链路或双工错配
- 若 conntrack 数接近上限或 NAT 表大量短时连接（比如大并发外连） → 会导致新 SSH 连接失败 / 重置
- 若 tcpdump 显示大量 RST 或重复 ACK → TCP 层被中断或路由返回路径不稳

????????????????

- 最稳妥 ：把两台路由器 分别放到不同 **VLAN**（推荐）或使用 VRRP/负载均衡方案。
- 临时：对堡垒机做静态 ARP、关闭 rp_filter、检查 sshd 限制、在交换机启用 storm-control 与端口安全。
- 长期：规划出口链路聚合或上层做多 WAN 负载 /策略路由，避免在同一 L2 域并行两网关。

把上述命令的输出贴过来（尤其是 `ip -s link`、交换机的 `show mac-address-table dynamic` 与 `show interface 1/0/45`、以及 `conntrack -S`），我会基于这些结果给出 下一步精确修复 —— 比如如何调整交换机端口、是否需要静态 ARP、或配置 VRRP/策略路由。

非常好的排查数据 ◫

从你贴的这些信息可以得出几个关键结论：

? ????????

从交换机当前状态来看，**ARP** 风暴或二层广播风暴的迹象目前不明显。

我们逐条分析：

1?? **MAC ?????**

```
Dynamic Address Count : 37
```

说明交换机学习到的二层设备数量正常，没有频繁波动，也没有出现同一MAC 地址快速在不同端口间跳转（即MAC flapping），这基本排除了大规模广播/环路的情况。

2?? **??????**

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 output errors, 0 collisions, 0 interface resets
```

说明链路层物理质量良好，无冲突、无丢包。

3?? **?????????????**

```
Received 18236138 broadcasts （72天内）
```

这相当于每天约25 万个广播包，大约每秒2～3 个广播包，对于大规模虚拟机环境是正常的。

? **??**?

当前时段并未发生ARP 风暴，也未发现环路迹象。

但问题可能在高峰期**NAT** 并发**40** 万时才触发，这种情况往往不是单纯ARP 风暴，而是以下几种**“隐性拥塞”**导致。

?? ???????????

你描述的现象：

> 高峰期时堡垒机远程困难、SSH 延迟甚至断连
>
> 而平时正常

说明瓶颈发生在高并发 **+** 同一**VLAN** 多路由出口环境下。重点怀疑以下几点：

1?? ?????????? VLAN??? ARP ????

- 即使你人为区分默认网关（10.2.2.253 / 10.2.2.254），但所有服务器都在VLAN10 同一广播域内。
- 每个虚拟机会定期发ARP 请求，如：

```
who-has 10.2.2.254 tell 10.2.2.x
who-has 10.2.2.253 tell 10.2.2.x
```

- 当虚拟机量很大（上百台甚至上千台）时，会造成**ARP request** 洪泛广播。若路由器的ARP 缓存刷新周期较短（比如60 秒），则在高并发NAT 时会形成持续广播洪流，**CPU** 飙高、**ARP** 表溢出、转发延迟。

□ □□□

- 在两台路由器上手动固定ARP（静态绑定）主机或堡垒机的MAC 地址；
- 调整路由器ARP 表老化时间（例如改为600 秒以上）；
- 让不同网关的主机放在不同**VLAN**（强烈建议）；

> 即 VLAN10 → 走 10.2.2.254
> VLAN20 → 走 10.2.3.254
> 通过三层互通区分出网路径。

2?? NAT ?????? CPU ??

高峰期40 万NAT 并发属于中高强度，如果路由器CPU/NAT 表容量不足（尤其是中低端型号），路由器在处理新建连接时会丢包、重传，导致堡垒机SSH 卡顿。

□ □□□□

在两台路由器上执行：

```
show cpu
show nat session summary
show nat statistics
show log
```

关注是否有：

- NAT 会话数接近最大值；
- CPU 使用率高；
- NAT 端口耗尽；
- 出现ICMP redirect 或NAT 分配失败日志。

3?? **???????? vSwitch ??**

堡垒机往往是 Hyper-V 虚拟机，如果物理网卡队列、vSwitch 绑定、RSS 未调优，在高并发 ARP 或 NAT 回包时容易丢包。

□ □□□

在堡垒机上运行：

```
ethtool -S eth0 | grep -E "drop|err"
ss -s
sar -n DEV 1
```

观察是否有接收丢包、延迟、socket backlog。

? ???????? ARP ?????

??1????????

```
tcpdump -i eth0 arp
```

如果每秒出现大量 `who-has`，且目的 IP 涉及 10.2.2.253 / 10.2.2.254，说明确实存在 ARP 洪流。

??2?????????????

```
show interface counters broadcast
```

（有的锐捷命令为 `show interface traffic`）
若每秒广播帧数超过几百以上持续存在，则为风暴迹象。

??3?????????

如果设备支持，可执行：

```
interface range te0/1-48
storm-control broadcast level 0.5
storm-control action shutdown
```

（限制广播流量占带宽 0.5%）

? ??????????????

优先级	建议措施	说明
◫ 高	VLAN 划分路由出口	10.2.2.x / 10.2.3.x 分离广播域
◫ 高	固定路由器静态 ARP / 提高老化时间	减少广播洪流
◫ 中	检查路由器 NAT 并发与 CPU 负载	防止性能瓶颈
◫ 中	堡垒机抓包验证 ARP 是否异常	实地确认是否风暴
◫ 低	交换机开启广播风暴抑制	预防性措施

如果你方便提供:

- 路由器品牌型号（或 NAT 性能参数）
- 高峰期时 `tcpdump -i eth0 arp` 的抓包数据（10秒左右）
- 路由器 CPU 与 NAT 表使用率

我可以帮你进一步判断到底是 **ARP** 风暴、**NAT** 过载 还是 虚拟交换队列瓶颈。

是否希望我帮你写一套抓包 + 分析命令脚本（堡垒机用）来自动判断是否 ARP洪流?

Revision #2
Created 4 November 2025 04:57:27 by Admin
Updated 4 November 2025 04:58:41 by Admin