NSX-T Data Center - Proxy ARP



Table of contents

Proxy ARP introduction	3
Proxy ARP use case with NSX-T	4
Proxy ARP Support and Summary	6
Proxy ARP implementation in NSX-T Data Center – Active Standby architecture	6
Proxy ARP implementation in NSX-T Data Center – Active Active architecture	14

Proxy ARP introduction

Proxy ARP is a method that consist of answering an ARP request on behalf of another host. This method is performed by a layer 3 networking device (usually a router). The purpose is to provide connectivity between 2 hosts when routing wouldn't be possible for various reasons.

To illustrate that introduction, we will consider the following network diagram:

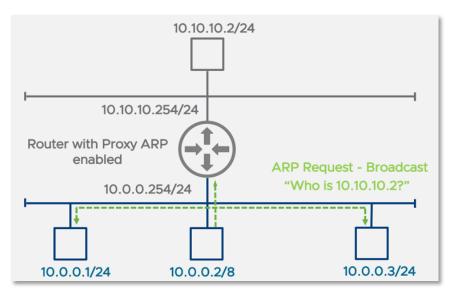


Figure 1 - Proxy ARP - ARP Request

In the following example, we will assume that the source host with the IP address 10.0.0.2 is configured with a subnet mask of 255.0.0.0. The destination host is configured with an IP address of 10.10.10.2 with a subnet mask of 255.255.255.0.

Based on its subnet mask, the source host thinks that the destination host is in the same subnet and therefore will need to have knowledge of its MAC address.

The source host will then send an ARP request (broadcast) that will reach the entire broadcast domain. It is crucial to note that the ARP request is not received by the destination host since it sits on a different broadcast domain from a router point of view.

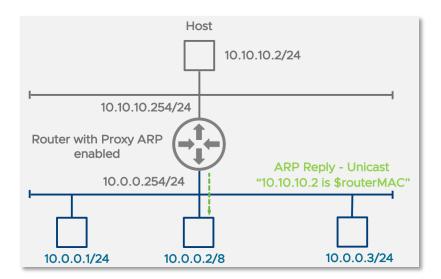


Figure 2 - Proxy ARP - ARP Reply

The Router has the "Proxy ARP" feature enabled and will reply with a unicast ARP reply to the source host on behalf of the destination host because it has a valid directly connected path to the requested IP. The MAC address specified in the ARP reply message is owned by the router physical interface.

After that sequence, the source host has knowledge of the destination host MAC address and a new entry in its ARP table has been added. The IP address of the destination host is mapped to the MAC Address of the router with Proxy ARP enabled. IP traffic can now be exchanged between the hosts.

Proxy ARP use case with NSX-T

In this case, the virtual machine connected to the NSX overlay segment is in a different subnet than the virtual machine connected to the VLAN segment.

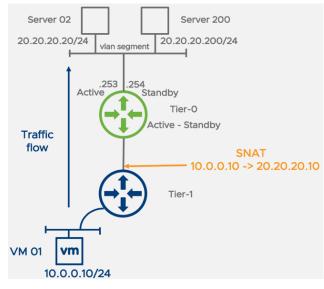
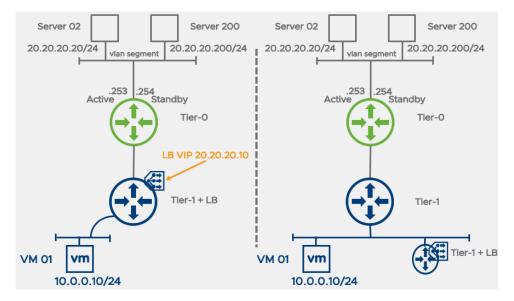


Figure 3 - Proxy ARP use case.

By enabling proxy-ARP, hosts on the overlay segments and hosts on a VLAN segment can exchange network traffic together without implementing any change in the physical networking fabric.





Proxy ARP is automatically enabled when a NAT rule or a load balancer VIP uses an IP address from the subnet of the Tier-O gateway uplink.

Figure 4 - Proxy ARP load balancer topologies.

Proxy ARP can be considered in environments where IP subnets are limited and where it is problematic to use new subnets easily and rapidly (either by using static routes or BGP).

Proof of concepts and VMware Enterprise PKS environments are usually using Proxy-ARP to simplify the network topology.

For production environment, VMware recommends implementing proper routing between a physical fabric and the NSX-T Tier-O by using either static routes or Border Gateway Protocol with BFD. If proper routing is used between the Tier-O gateway and the physical fabric, BFD with its sub-second timers will converge faster.

In case of failover with proxy ARP, the convergence relies on gratuitous ARP (broadcast) to update all hosts on the VLAN segment with the new MAC Address to use. If the Tier-0 gateway has proxy ARP enabled for 100 IP addresses, the newly active Tier-0 SR needs to send 100 Gratuitous ARP packets.

With such a mechanism, we can conclude that convergence time depends on the number IP addresses enabled for proxy ARP.

Proxy ARP Support and Summary

Proxy ARP on the NSX-T edge node is a feature supported since NSX-T 2.4.

The following table summarizes the design option and support for the Proxy ARP feature:

NSX-T PROXY ARP SUPPORT	
MODE	SUPPORT
Active / Standby	Supported ¹
Active / Active	Not Supported

Proxy ARP implementation in NSX-T Data Center – Active Standby architecture

We will be using the following diagram to illustrate this topology. In our demonstration, we will configure the SNAT rule on the Tier-1 SR Gateway.

Virtual Machine 01 is connected to the overlay segment and has an IP address of 10.0.0.10/24.

Server 02 and Server 200 are connected to the VLAN segment with an IP address of 20.20.20.20/24 and 20.20.200/24 respectively.

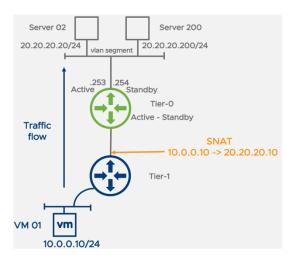


Figure 5 - Proxy ARP - Multi Tier Architecture.

In our example, the traffic is initiated by the virtual machine on the overlay segment. In order to enable the Proxy-ARP feature on the Tier-O gateway uplinks, a Source NAT (SNAT) rule must be implemented on the Tier-1 (or Tier-0) gateway as described in the diagram above.

If the traffic is initiated by the server on the VLAN segment, a Destination NAT (DNAT) rule must be implemented on the Tier-1 gateway.



¹ In case of 1:1 SNAT, ICMP echo sent by the host on the VLAN segment will be answered by the Tier-0 SR gateway.

The overlay segment is connected to the Tier-1 gateway. The route advertisement statements must include the "NAT IPs" to redistribute these routes from the Tier-1 gateway to the Tier-0 gateway.

VM NSX-T						1	Q L	(? ~ a	idmin 🕓
Home Networking Se	curity Inventory	Plan & Troubleshoot System						POLICY	MANAGER
Network Overview Network Topology			DGE BRIDGE PROFILES METAD	DATA PROXIES				CLEAR	⑦ ☆ ×
Connectivity		Segment Name	Connectivity	Transport Zone	Subnets	Ports	Admin State	Status (j)	Alarms
🔁 Tier-O Gateways	: > 00	Tenant-PROXY-ARP-T0-Overlay	Tenant-PROXY-ARP-T1 Tier1	nsx-overlay-transportzone Overlay	10.0.0.254/24	1	🔴 Up	● Suc C	0
Tier-1 Gateways Segments	: > 00	Tenant-PROXY-ARP-T0-Uplink	None	LAB-01-nsx-uplinks-vlan- transportzone VLAN	Not Set	0	● Up	🌒 Suc 🕐	0

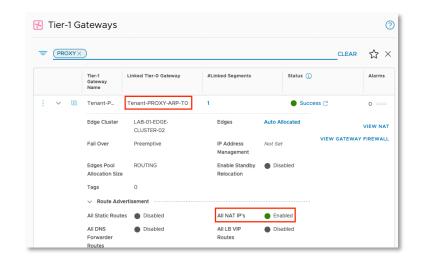


Figure 6 - Active Standby - Segments

Figure 7 - Active/Standby - Tier-1 Configuration.

	eways Tenant-PRO (#1	nterfaces 2		COLLAPSE ALL	Q Search
	Name	Туре	IP Address / Mask	Connected To(Segment)	Status
· ~	Uplink-PROXY-ARP-EN-03	External	20.20.20.253/24	Tenant-PROXY-ARP-T0- Uplink	🕒 Success 🤁 🕕
	Edge Node	LAB-01-EDGE-03	MTU	9000 (1)	VIEW STATISTIC
	Tags	0	PIM	Disabled	
	ND Profile	default	URPF Mode	Strict	
~	Uplink-PROXY-ARP-EN-04	External	20.20.20.254/24	Tenant-PROXY-ARP-T0- Uplink	🕒 Success 🤆 🕕
	Edge Node	LAB-01-EDGE-04	MTU	9000 (1)	VIEW STATISTIC
	Tags	0	PIM	Disabled	
	ND Profile	default 🚯	URPF Mode	Strict	

Figure 8 - Active/Standby - Tier-O Uplink Interfaces

Assuming that the Source NAT rule is not yet configured, the following output demonstrates that Proxy ARP is not enabled on the uplink. The Tier-0 SR will not answer to the ARP requests on the VLAN segment that are needed to reach 20.20.20.10.



lab-01-edge-03> get logical-router Logical Router					
JUID	VRF	LR-ID	Name	Туре	Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666	0	0		TUNNEL	4
52510271-dbbb-4a84-a8a3-e5f28146c926	1	22	SR-Tenant-PR0XY-ARP-T0	SERVICE_ROUTER_TIER0	5
5b05770-78a9-4a36-b018-2bd8ae81c067	3	24	DR-Tenant-PROXY-ARP-T1	DISTRIBUTED_ROUTER_TIER1	4
3bc5b902-d446-4aac-a8cb-43e75bc77631	4	34	SR-Tenant-PROXY-ARP-T1	SERVICE_ROUTER_TIER1	5
c5ff5633-c4f3-459c-bf31-f6b013243e15	5	21	DR-Tenant-PROXY-ARP-T0	DISTRIBUTED_ROUTER_TIERØ	4

Figure 9 - Finding the VRF ID on the Tier-O Service Router

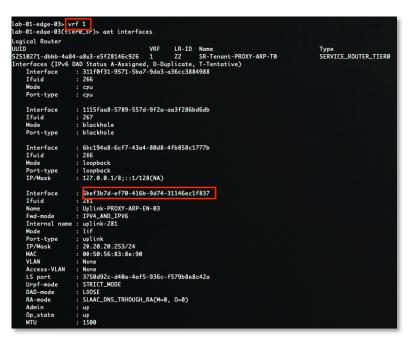


Figure 10 - Finding the Interface UUID for the Tier-O uplink

interface	: 6bef3b7d-ef70-416b-9d74-31146ec1f837
ifuid	: 310
VRF	: 52510271-dbbb-4a84-a8a3-e5f28146c926
name	: Uplink-PROXY-ARP-EN-03
mode	: lif
IP/Mask	20.20.253/24
Fwd-mode	: IPV4_AND_IPV6
MAC	: 00:50:56:83:8e:90
VLAN 1-edge	2000
LS port	: 3750d92c-d40a-4af5-936c-f579b8e8c42a
urpf-mode	: STRICT_MODE
admin	: upef3b7d-ef78-416b-9d74-31146ec1f837
op_state	: up
MTU	: 1500 271 dbbb 4a84-a8a3 e5 F28146c926
lab-01-edge	2-03> get logical-router interface 6bef3b7d-ef70-416b-9d74-31146ec1f837 arp-proxy
interface	: 6bef3b7d-ef70-416b-9d74-31146ec1f837
ifuid	: 310 AND TPV6
VRF	: 52510271-dbbb-4a84-a8a3-e5f28146c926
name	: Uplink-PROXY-ARP-EN-03
mode	: lif/0d92c-d48a-4af5-936c-f579b8e8c42aF
MAC	: 00:50:56:83:8e:90
admin	: up
op_state	: up
arp_proxy	

Figure 11 - Active Tier-O Interfaces CLI output before NAT rule configuration

The next step is to configure the source NAT rule that matches the specific host 10.0.0.10. According to the rule, the Tier-01 SR will translate the source IP address of every packet sent by VM 01 with a new



value of "20.20.20.10".

→ NAT									
Gateway	Tenant-PROXY-ARP-T1		NAT Rules 1		'iew	NAT	<u> </u>		
ADD NAT RULE							COLLAPSE ALL	Filter by Nam	ne, Path and more
	Name	Action	Mat	ch	Translated		Apply To	Enabled	Status
			Source	Destination					
: × Ð	PROXY-ARP	SNAT	10.0.0.10	Any	20.20.20.10		0	Enabled	🌒 Success 😋 🖂

Figure 12 - Source NAT Rule configured on the Tier-1 gateway.

The following output demonstrates that Proxy ARP has been automatically enabled on the uplink interface of the active Tier-0 SR facing the 20.20.20.0/24 subnet.

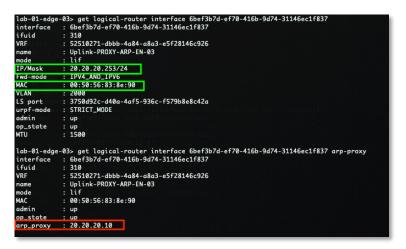


Figure 13 - Active Tier-O Interfaces CLI output after NAT rule configuration.

The standby Tier-O SR has also the "ARP_Proxy" field defined but it will not answer to any ARP request for that IP address while running in standby mode.

lab-01-edge	:-04> get logical-router interface a4280164-4633-4e1e-8f43-7a0e04044699
interface	: a4280164-4633-4e1e-8f43-7a0e04044699
ifuid	: 502
VRF	: 11f72fa5-3d06-49bd-8f9d-0b09d81849d6
name	: Uplink-PROXY-ARP-EN-04
mode	: lif
IP/Mask	: 20.20.254/24
Fwd-mode	: IPV4_AND_IPV6
MAC	: 00:50:56:83:50:42
VLAN	: 2000
LS port	: 93d9f3b1-d8db-49b4-9df1-c126a0e1b9e0
urpf-mode	: STRICT_MODE
admin	: up
op_state	: up
MTU	: 1500
Jab 01 adaa	:-04> get logical-router interface a4280164-4633-4e1e-8f43-7a0e04044699 arp-proxy
interface	: a4280164-4633-4e1e-8f43-7a0e04044699
ifuid	: 44280104-4655-4616-8745-740604044699 : 502
VRF	: 302 : 11f72fa5-3d06-49bd-8f9d-0b09d81849d6
name mode	: Uplink-PROXY-ARP-EN-04 : lif
MAC	: 00:50:56:83:50:42
admin	: up
op_state	
arp_proxy	: 20.20.20.10

Figure 14 - Standby Tier-O Interfaces CLI output after NAT rule configuration.

Server 02 on the VLAN segment has the following ARP table:



C:\Users∖admin>ar⊏ -a	
Interface: 20.20.20.20 0x3	
Internet Address Physical Addr	ress Type
20.20.20.253 00-50-56-83-8	8e-90 dynamic
20.20.20.254 00-50-56-83-5	50-42 dynamic
20.20.20.255 ff-ff-ff-ff-f	f-ff static
224.0.0.22 01-00-5e-00-0	00-16 static
224.0.0.251 01-00-5e-00-0	00-fb static
224.0.0.252 01-00-5e-00-0	00-fc static
239.255.255.250 01-00-5e-7f-f	f-fa static

Figure 15 - Server 02 - ARP entries before any traffic is initiated

The Active Tier-0 SR interface IP address of 20.20.20.253 corresponds to the mac address "00:50:56:83:8E:90".

The Standby Tier-0 SR interface IP address of 20.20.20.254 corresponds to the mac address "00:50:56:83:50:42".

The previous output demonstrates that the Server 02 has already the knowledge of both Tier-O Uplink interfaces. The virtual machine 01 on the overlay segment initiate some network traffic to the destination of Server 02 on the VLAN segment. At first, the traffic is sent to the Tier-01 DR on the transport node and then sent to the Tier-01 SR on an edge node. The IP traffic will match the SNAT rule previously configured on the Tier-01 SR. All the IP packets sourced by the virtual machine 01 are sent to the Tier-0 DR/SR with a source IP address of 20.20.20.10.

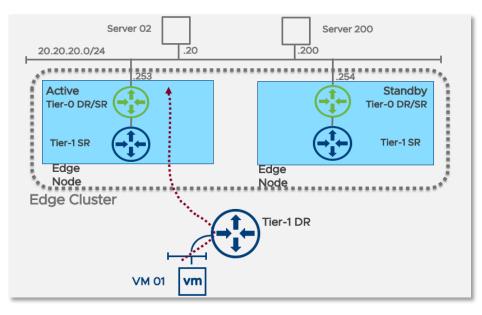


Figure 16 - Traffic initiated by virtual mach 01 and traversing the NSX fabric.

The active Tier-O DR sends the traffic to the active Tier-O SR. When the traffic reaches the Tier-O SR, the MAC address for Server 02 is unknown from a Tier-O point of view.

The following network trace will demonstrate how the ARP request/replies and the ICMP packets are exchanged between the Tier-0 and Server 02.

Packet #'1 – Broadcast: it shows the ARP request sent by the active Tier-0 SR needed in order to map the MAC address of Server 02.

Packet #2 – Unicast: shows the ARP reply sent by Server 02 to the active Tier-0 SR with its own MAC Address embedded.

Packet #3 – Unicast: ICMP Echo request type 8 code 0 – Sent by the Active Tier-0 SR.

Packet #4 – Broadcast: it shows the ARP request sent by Server 02 needed in order to map the MAC address of 20.20.20.10.²

Packet #5 – Unicast: shows the ARP reply sent by the active Tier-O SR showing that the Proxy ARP feature is enabled and effective.

Time Source Destination Protocol Length Info 1 0.000000 VMware.83:86:90 Broadcast ARP 60 Who has 20.20.20.20:21 Ell 20.20.20.253 2 0.000007 VMware.83:96:100 Broadcast ARP 60 Who has 20.20.20.20:21 Ell 20.20.20.253 3 0.001154 20.20.20.10 20.20.20.20 ICMP 98 Echo (ping) request id+0x5e09, seq-1/256, ttl=62 (reply in 6) 4 0.001375 VMware_83:96:1b0 Broadcast ARP 42 Who has 20.20.20.107 Tell 20.20.20.20 5 0.007539 VMware_83:96:1b0 Broadcast ARP 60 20.20.20.20.107 Tell 20.20.20.20	_		🗙 🔄 🍳 🗢 🗢 😫	· · · ·	~ Ⅲ	
1 0.000000 VHware_83:8e:90 Broadcast ARP 60 Who has 20.20.20.20 Tell 20.20.20.253 2 0.000057 VHware_83:90 bb VHware_83:90 bb VHware_83:90 bb ARP 42 20.20.20 is at 00:50:56:83:90 bb 3 0.001154 20.20.20.10 20.20.20.20 ICNP 98 Echo (ping) request id=0x5609, seq=1/256, ttl=62 (reply in 6) 4 0.001375 VHware_83:90 bb Broadcast ARP 42 Who has 20.20.20.10 Tell 20.20.20.20 5 0.007539 VHware_83:90 bb ARP 42 Who has 20.20.20.10 Tell 20.20.20.20 Cmpl and an an an and an	App	ply a display filter <	Ctrl-/>			
2 0.000057 VHware_83:9b:bb VHware_83:8b:b0 ARP 42 20.20.20.20 is at 00:50:56:83:9b:bb 3 0.00154 20.20.20.10 20.20.20.20 ICMP 98 Echo [ring] request id=0x5e09, seq=1/256, ttl=62 (reply in 6) 4 0.001375 VHware_83:9b:bb Broadcast AP 42 Uho has 20.20.20.20.20 is at 00:50:56:83:9b:bb 5 0.007539 VHware_83:9b:bb Broadcast AP 42 Huho has 20.20.20.20.20.20.20.20.20.20.20.20.20.2	о.	Time	Source	Destination	Protocol	Length Info
3 0.001154 20.20.20.10 20.20.20.20 ICMP 98 Echo (ng) request id=0x5609, seq=1/256, ttl=62 (reply in 6) 4 0.001375 VHware_83:96:bb Broadcast ARP 42 Who has 20.20.20.20.20.20.20.20.20.20.20.20.20.2		1 0.000000	VMware_83:8e:90	Broadcast	ARP	60 Who has 20.20.20.20? Tell 20.20.20.253
4 0.001375 VHware_83:9b:bb Broadcast ARP 42 Who has 20.20.20.10? Tell 20.20.20.20 5 0.007539 VHware_83:8e:90 VHware_83:9b:bb ARP 60 20.20.20.10 is at 00:50:56:83:8e:90		2 0.000057	VMware_83:9b:bb	VMware_83:8e:90	ARP	42 20.20.20.20 is at 00:50:56:83:9b:bb
5 0.007539 VMware_83:8e:90 VMware_83:9b:bb ARP 60 20.20.20.10 is at 00:50:56:83:8e:90		3 0.001154	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x5e09, seq=1/256, ttl=62 (reply in 6)
		4 0.001375	VMware_83:9b:bb	Broadcast	ARP	42 Who has 20.20.20.10? Tell 20.20.20.20
6 0.007588 20.20.20.20 20.20.10 ICMP 98 Echo (ping) reply id=0x5e09, seq=1/256, ttl=128 (request in		5 0.007539	VMware_83:8e:90	VMware_83:9b:bb	ARP	60 20.20.20.10 is at 00:50:56:83:8e:90
		6 0.007588	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x5e09, seq=1/256, ttl=128 (request in 3

Packet #6 – Unicast: ICMP Echo reply type 0 code 0 – Sent by Server 02.

Figure 17 – ICMP trace on host 02 – Traffic initiated by host 01

The following ARP table output will demonstrate that the MAC Address mapped to the respective IP Addresses of 20.20.20.10 and 20.20.20.253 are identical.

C:\Users∖admin>arp -a		
Interface: 20.20.20.2	0 0x3	
Internet Address	Physical Address	Туре
20.20.20.10	00-50-56-83-8e-90	dynamic
20.20.20.253	00-50-56-83-8e-90	dynamic
20.20.20.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Figure 18 – ARP table Host 02

² ARP caching behavior has been changed in Windows Vista. The TCP/IP stack implementations in Windows Vista (and later versions) comply with RFC4861 (Neighbor Discovery protocol for IP version 6 [lpv6]) for both the IPv4 and the IPv6 Neighbor Discovery process. : Source https://support.microsoft.com/enus/help/949589/description-of-address-resolution-protocol-arp-caching-behavior-inwin.



As a reminder, it is crucial to note that in our case, the traffic is initiated by the virtual machine 01 which is connected to the overlay segment on the Tier-01. If the initial traffic was initiated by a server on the VLAN segment, a Destination NAT rule would have been required on the Tier-1/Tier-0 since the initial traffic would not match the SNAT rule that has been configured previously.

If the edge nodes hosting the Tier-O gateways experience an outage, a failover will be triggered, the newly active Tier-O gateway will send a gratuitous ARP to announce the new MAC address to be used by the hosts on the VLAN segment in order to reach virtual machine O1. It is critical to fathom that the newly active Tier-O will send a Gratuitous ARP for each IP address that are configured for Proxy ARP.

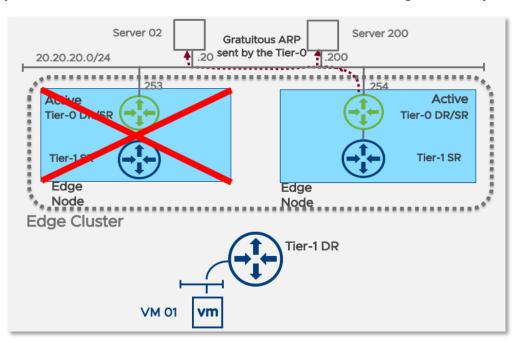


Figure 19 - Edge node failover - Gratuitous ARP sent by the Tier-0.

The following capture shows a single gratuitous ARP sent by the newly active Tier-0 for the IP address 20.20.20.10.

A I A	pply a display filter <					•
b.	Time	Source	Destination	Protocol	Length Info	
	132 63.225404	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=76/19456, ttl=128 (request in 131)	
	133 64.227374	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=77/19712, ttl=62 (reply in 134)	
	134 64.227523	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=77/19712, ttl=128 (request in 133)	
	135 65.229723	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=78/19968, ttl=62 (reply in 136)	
	136 65.229861	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=78/19968, ttl=128 (request in 135)	
	137 69.544828	VMware_83:50:42	Broadcast	ARP	60 Gratuitous ARP for 20.20.20.10 (Reply) (duplicate use of 20.20.20.10 detected!)	
	138 70.371671	VMware_83:50:42	Broadcast	ARP	60 Who has 20.20.20.20? Tell 20.20.254	
	139 70.371722	VMware_83:9b:bb	VMware_83:50:42	ARP	42 20.20.20 is at 00:50:56:83:9b:bb	
	140 70.372209	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=83/21248, ttl=62 (reply in 141)	
	141 70.372367	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=83/21248, ttl=128 (request in 140)	
	142 71.331515	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=84/21504, ttl=62 (reply in 143)	
	143 71.331680	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=84/21504, ttl=128 (request in 142)	
	144 72.332893	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=85/21760, ttl=62 (reply in 145)	
	145 72.333028	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=85/21760, ttl=128 (request in 144)	
	146 73.335168	20.20.20.10	20.20.20.20	ICMP	98 Echo (ping) request id=0x95c7, seq=86/22016, ttl=62 (reply in 147)	
	147 73.335289	20.20.20.20	20.20.20.10	ICMP	98 Echo (ping) reply id=0x95c7, seq=86/22016, ttl=128 (request in 146)	

Figure 20 - Edge node failover - GARP sent by the newly active Tier-0 Gateway.

After announcing the new MAC address to use, Server 02 updates (and all other hosts on the VLAN segment with an entry for 20.20.20.10) its ARP table entry for 20.20.20.10 and traffic will be sent to the newly active Tier-0 SR.

C:\Users\admin>arp -a				
Interface: 20.20.20.20) 0x3			
Internet Address	Physical Address	Туре		
20.20.20.10	00-50-56-83-50-42	dynamic		
20.20.20.253	00-50-56-83-8e-90	dynamic		
20.20.20.254	00-50-56-83-50-42	dynamic		
20.20.20.255	ff-ff-ff-ff-ff-ff	static		
224.0.0.22	01-00-5e-00-00-16	static		
224.0.0.251	01-00-5e-00-00-fb	static		
224.0.0.252	01-00-5e-00-00-fc	static		
239.255.255.250	01-00-5e-7f-ff-fa	static		

Figure 21 - ARP Table Server 02 - After Tier-O failover.

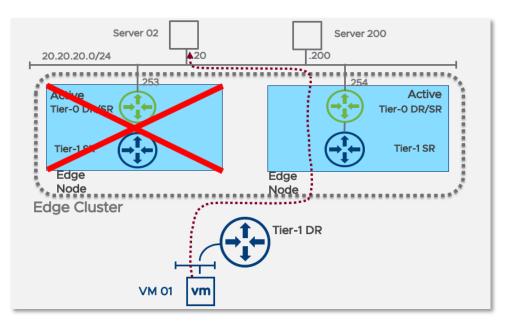


Figure 22 - Edge node failover - Traffic initiated by Host 01.

Proxy ARP implementation in NSX-T Data Center – Active Active architecture

In an Active/Active mode, IP traffic uses all the equal cost and available paths to reach the physical fabric through the Tier-O gateway. In this mode, stateful NAT is not supported because of asymmetrical path might cause issues. It is possible to configure reflexive NAT. The stateless NAT rule will rewrite the source IP address field of the IP packets sent by VM 01.

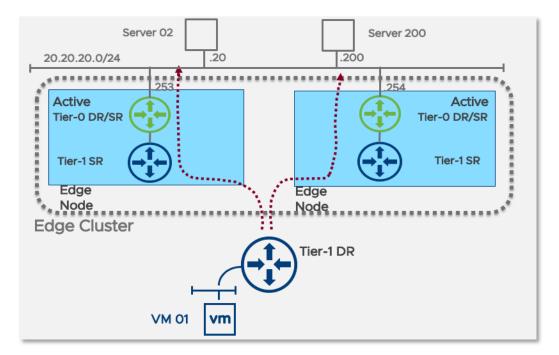


Figure 23 - Active/Active Tier-0 - Traffic initiated by VM 01

In contrast with our previous example, none of the Tier-O SR will respond to the ARP Requests sent by the servers on the VLAN segments for the IP 20.20.20.10.

31.000000 Whomer_83:90:bb Broadcast ARP 42 Who has 20:00.20.010 FTLl 20. 41.22970 28.78.78.110 20.20.20.20.20 ICIMP 95 Echo (ping) request id=dxbdbb 52.247642 20.20.20.10 20.20.20.20 ICIMP 95 Echo (ping) request id=dxbdbb 52.247642 20.20.20.10 20.20.20.20 ICIMP 95 Echo (ping) request id=dxbdbb 52.247642 20.20.20.10 Broadcast ARP 42 Who has 20.20.20.20.10 FTLl 20. 72.299944 Whare 35:90:bb Broadcast ARP 42 Who has 20.20.20.20.10 FTLl 20. 8 3.271675 20.20.20.10 20.20.20.20 ICIMP 95 Echo (ping) request id=dxbdbb 94.000100 Whare 63:90:bb Broadcast ARP 42 Who has 20.20.20.20.10 FTLl 20. 8 3.271675 20.20.20.20 ICIMP 98 Echo (ping) request id=dxbdbb 98 Echo (ping) request id=dxbdbbb 94.000100 Whare 63:90:bb Broadcast ARP 42 Who has 20.20.20.20.10 FTLl 20.	b84, seq=13/3328, ttl=62 (no response foundi) 0.20.20.20 b84, seq=14/3584, ttl=62 (no response foundi) b84, seq=15/3849, ttl=62 (no response foundi)
2 0.199129 22.28.28.18 20.28.29.29 ICMP 98 Echo (ping) request id=dxdxbb 3 1.000000 Whare 83:90:bb Broadcast ARP 42 Akho has 20:20:20.107 Tell 20:1 4 1.223072 282:28:20:20 101P 98 Echo (ping) request id=dxdxbb 5 2.427642 282:28:20:10 20:20:28:20 ICMP 98 Echo (ping) request id=dxdxbb 7 2.999946 Whare 83:90:bb Broadcast ARP 42 Akho has 20:20:20:107 Tell 20:1 8 3.21678 20:20:20:20 ICMP 98 Echo (ping) request id=dxdxbb 7 2.999946 Whare 83:90:bb Broadcast ARP 42 Akho has 20:20:20:107 Tell 20:1 8 3.21678 20:20:20:107 98 Echo (ping) request id=dxdxbb 94 40 Whare 83:90:bb Broadcast ARP 42 Akho has 20:20:20:107 Tell 20:108 8 3.21678 20:20:20:107 98 Echo (ping) request id=dxdxbb Akho has 20:20:20:	0.20.20.20 b84, seq=14/3584, ttl=62 (no response found!) b84, seq=15/3840, ttl=62 (no response found!)
B Le000000 Whaver (33:99:bb) Broadcast AP 42 Who has 20:20:20:10* 11:20:20 41.223972 28:28:20:10 20:20:20:20 ICMP 98 Echo (ping) request id=debdbB 52:247642 20:20:20:10 20:20:20 ICMP 98 Echo (ping) request id=debdbB 62:247643 Whaver @3:9b:bb Broadcast ABP 42 Who has 20:20:20:10* 12:20 72:299946 Whaver @3:9b:bb Broadcast ABP 42 Who has 20:20:20:10* 12:20:20 63:271678 20:20:20:10 20:20:20 ICMP 98 Echo (ping) request id=debdbB 64:400504 Whaver @3:9b:bb Broadcast ABP 42 Who has 20:20:20:10* 12:20:20 63:271678 20:20:20:10 20:20:20:20 ICMP 98 Echo (ping) request id=debdbB 64:400504 94:400504 98 Echo (ping) request id=debdbB 12:20:20:20 12:20:20	0.20.20.20 b84, seq=14/3584, ttl=62 (no response found!) b84, seq=15/3840, ttl=62 (no response found!)
4 1.223072 28.28.28.18 28.28.28.18 28.28.28.18 98 Echo (ping) request id=0xdb8 5 2.247642 28.28.28.18 28.28.29.28 ICMP 98 Echo (ping) request id=0xdb8 6 2.247642 28.28.28.18 28.28.29.28 ICMP 98 Echo (ping) request id=0xdb8 6 2.247643 MMare 83:99:bb Broadcast ARP 42 Who has 20.28.20.81.09 Tell 28.1 7 2.99946 Whore 83:99:bb Broadcast ARP 42 Who has 20.28.20.81.09 Tell 28.1 8 3.271678 28.20.20.10 20.20.20.20 ICMP 98 Echo (ping) request id=0xdb84 9 4.060181 Whore 83:99:bb Broadcast ARP 42 Who has 20.20.20.81.07 Tell 28.1	b84, seq=15/3840, ttl=62 (no response found!)
5 2.24742 20.20.20.10 20.20.20.20 ICMP 98 Echo (rung) request id-dxddb4 6 2.247843 Whare 8.3:90:bb Broadcast APP 42 Who has 20.20.20.1017 Fcll 20.20.20 7 2.99944 Whare 83:90:bb Broadcast APP 42 Who has 20.20.20.1017 Fcll 20.20.20.20 8 3.271678 20.20.20.10 20.20.20.20 ICMP 98 Echo (rung) request id-dxdb4 94.00010 Whare 8.3:90:bb Broadcast APP 42 Who has 20.20.20.1017 Fcll 20.20.20 8 3.271678 20.20.20.10 Broadcast APP 42 Who has 20.20.20.1017 Fcll 20.20.20	b84, seq=15/3840, ttl=62 (no response found!)
7 2.999946 Whare 83:99:bb Broadcast ABP 42 Who has 28.29.20.10? Tell 28.; 8 3.21076 20.28.20.20 ICIP 98 Echo (ping) request ind-word68 9 4.00010 Whare 63:99:bb Broadcast ABP 42 Who has 20.20.20.10? Tell 20.; 9 4.00010 Whare 63:99:bb Broadcast ABP 42 Who has 20.20.20.10? Tell 20.;	
8 3.271678 20.20.20.10 20.20.20.20 ICMP 98 Echo (ping) request id=0xdb8- 9 4.000101 VMware_83:9b:bb Broadcast ARP 42 Who has 20.20.20.10? Tell 20.3	0.20.20.20
9 4.000101 VMware_83:9b:bb Broadcast ARP 42 Who has 20.20.20.10? Tell 20.2	0.20.20.20
	b84, seq=16/4096, ttl=62 (no response found!)
	0.20.20.20
10 4.294972 20.20.20.10 20.20.20 ICMP 98 Echo (ping) request id=0xdb84	b84, seq=17/4352, ttl=62 (no response found!)
11 5.318978 20.20.20.10 20.20.20 ICMP 98 Echo (ping) request id=0xdb84	b84, seq=18/4608, ttl=62 (no response found!)
12 5.319197 VMware_83:9b:bb Broadcast ARP 42 Who has 20.20.20.10? Tell 20.2	0.20.20.20
13 6.000382 VMware 83:9b:bb Broadcast ARP 42 Who has 20.20.20.10? Tell 20.2	0.20.20.20
ame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_(1758C2CA-04FA nernet II, Src: Whware 33:90:bb (08:59:56:63:90:bb), Dst: Broadcast (ff:ff:ff:ff:ff:ff) dress Resolution Protocol (result)	#FA-42E4-BCAE-CECD5FAC7721}, id 0

Figure 24 - Active/Active Topology – Tier-O does not answer to ARP requests sent for 20.20.20.10

lab-01-edge)3> get logical-router interface 6bef3b7d-ef70-416b-9d74-31146ec1f837
interface	: 6bef3b7d-ef70-416b-9d74-31146ec1f837
ifuid	281
VRF	: 52510271-dbbb-4a84-a8a3-e5f28146c926
name	: Uplink-PROXY-ARP-EN-03
mode	lif
IP/Mask	20.20.20.253/24
Fwd-mode	IPV4_AND_IPV6
МАС	00:50:56:83:8e:90
VLAN	2000
LS port	: 3750d92c-d40a-4af5-936c-f579b8e8c42a
urpf-mode	STRICT_MODE
admin	: up
op_state	: up
MTU	: 1500
lab-01-edae)3> aet logical-router interface 6bef3b7d-ef70-416b-9d74-31146ec1f837 arp-proxy
interface	6bef3b7d-ef70-416b-9d74-31146ec1f837
ifuid	281
VRF	52510271-dbbb-4a84-a8a3-e5f28146c926
name	Uplink-PROXY-ARP-EN-03
mode	lif
MAC	00:50:56:83:8e:90
admin	: up
op_state	
arp_proxy	
1 - 1 - 3	

Figure 25 - Active Tier-O Interfaces CLI - Edge Node O3 - output after NAT rule configuration.

lab-01-edge	e-04> get logical-router interface eb12d624-2c32-4354-b8f3-39aea8d1455d
interface	: eb12d624-2c32-4354-b8f3-39aea8d1455d
ifuid	: 612
VRF	: b2acc729-b19f-4607-84db-ffe394883ac2
name	: Uplink-PROXY-ARP-EN-04
mode	<u>: lif</u>
IP/Mask	: 20.20.254/24
Fwd-mode	: IPV4_AND_IPV6
MAC	: 00:50:56:83:50:42
VLAN	: 2000
LS port	: 67040350-10fc-4f4e-b9d5-350b02abd057
urpf-mode	: STRICT_MODE
admin	: up
op_state	: up
MTU	: 1500
lab-01-edae	e-04> get logical-router interface eb12d624-2c32-4354-b8f3-39gea8d1455d _arp-proxy
interface	: eb12d624-2c32-4354-b8f3-39aea8d1455d
ifuid	: 612
VRF	: b2acc729-b19f-4607-84db-ffe394883ac2
name	: Uplink-PROXY-ARP-EN-04
mode	: lif
MAC	: 00:50:56:83:50:42
admin	: up
op_state	: up
arp_proxy	

Figure 26 - Standby Tier-O Interfaces CLI - Edge Node 03 - output after NAT rule configuration





VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com. Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-wp-temp-word 1/20