

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Solving Duplicate IP Addressing Problems with Layer2 NAT

Subtitle goes here

Albert Mitchell, Technical Marketing Engineer, Industrial IoT Networking
Twitter: @asentient
BRKIOT-2013

cisco *Live!*

#CiscoLive

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

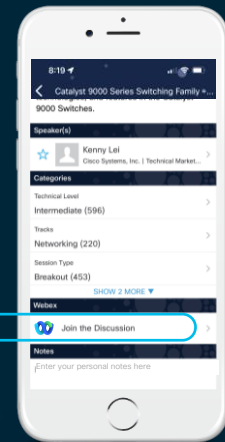
How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



#CiscoLive BRKIOT-2013



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2013>

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 3



Agenda

- L2NAT – What’s the problem to solve
- L2NAT fundamentals – how it works
- Deployment scenarios
- Troubleshooting
- Conclusion

What's the problem to solve with L2NAT

CISCO *Live!*

IP Addresses are duplicated on Purpose

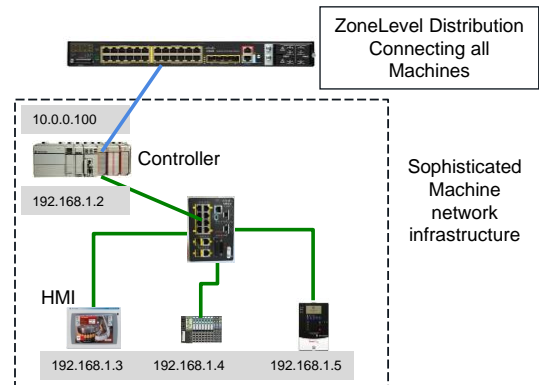
And they like it that way!

- Same SW for every machine
- Machine Components have same IP in each machine
- SW Duplication across machines means IP Addresses reused across machines
- SW in any 'packaged solution'



Machine Internal connectivity

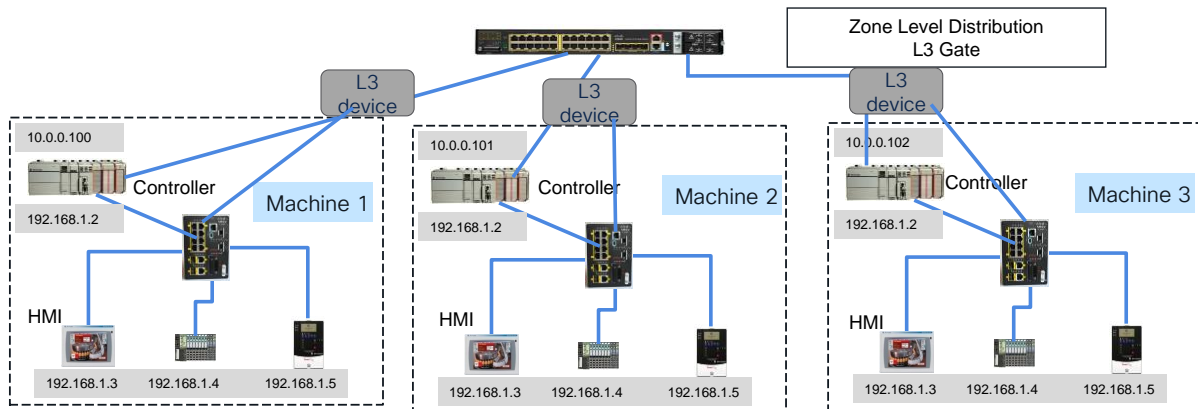
- Sophisticated machines have internal networks
- Main Controller with Dual NICs for inside and outside connectivity
- Outside Communication to controller only – No Problem



Internal 192.168.1.x subnet used for machine internal communication. Never designed machine components to communicate outside the machine. Only controller designed for communication outside the machine.

Current Solutions – additional L3 device

- L3 Device – Router or FW inserted for translation
- More devices to manage!



cisco *Live!*

#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

8

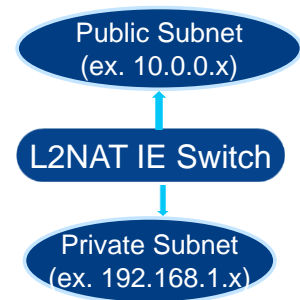
One way to solve today is by adding a L3 device. Either a L3 router, or firewall to do network translation. This is a multi box solution. Sometimes requiring a L3 device per machine.

L2NAT Fundamentals

CISCO *Live!*

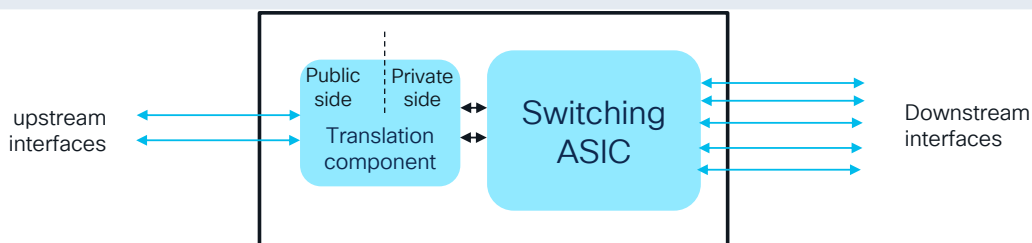
Solution: L2NAT on Industrial Ethernet (IE) Switches

- L2NAT Does 1:1 IPv4 Address Translation
 - It does NOT do 1:N translation. This is Port Address Translation (PAT)
- Translates at Line Rate (Gigabit speeds)
- Translates Bi-directionally
- Terms: Public IP is unique, Private is duplicate
- Works with ICMP and ARP (fixup the payload)
- Can be any IPv4 address
 - Not just 192.168.x.y, which are examples



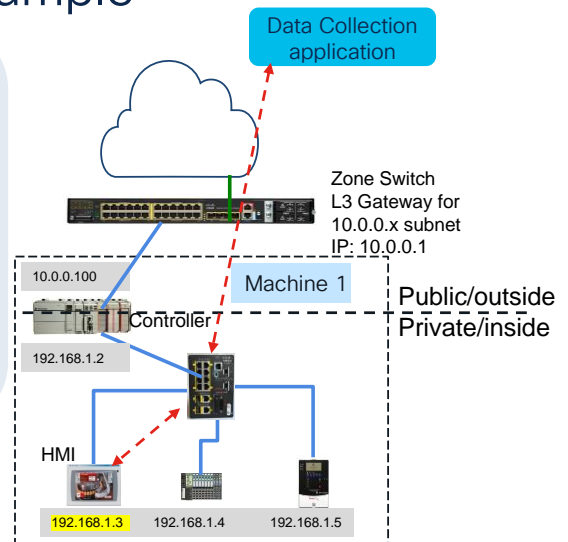
Internals of the IPv4 Translation

- The IPv4 header translation happens in outside of Switching ASIC.
- Translation and forwarding decision not related.
- Only specific interfaces have Translation capabilities
 - Different for different IE switching models



L2NAT: simple use case example

- Data Collection Application communicates with HMI over IP
- Network Admin Defines the translation of private IP to public IP
 - Inside from host 192.168.1.3 to 10.0.0.99
- Machine 1 HMI known as 10.0.0.99 in public network

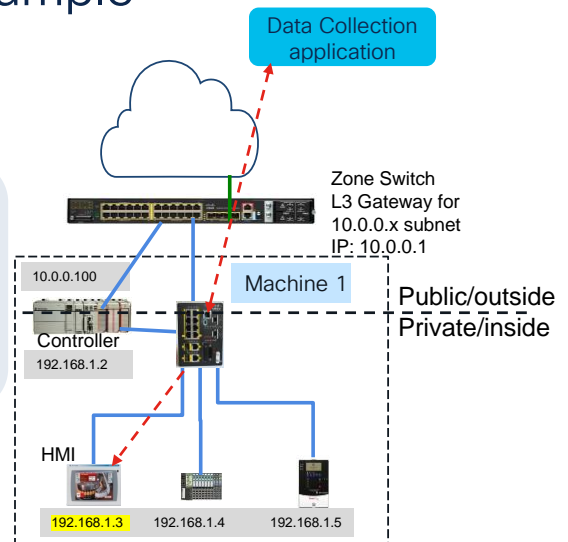


Simple example to show L2NAT at work. How to get HMI onto the public network with an IP address which is A) not routable outside the machine, and B) duplicated across the network in other machines?

L2NAT: simple use case example

- Network architecture change
- Add link from IE Switch to Zone SW
- Switch exists public and private

Inside from host 192.168.1.3 to 10.0.0.99



CISCO *Live!*

#CiscoLive

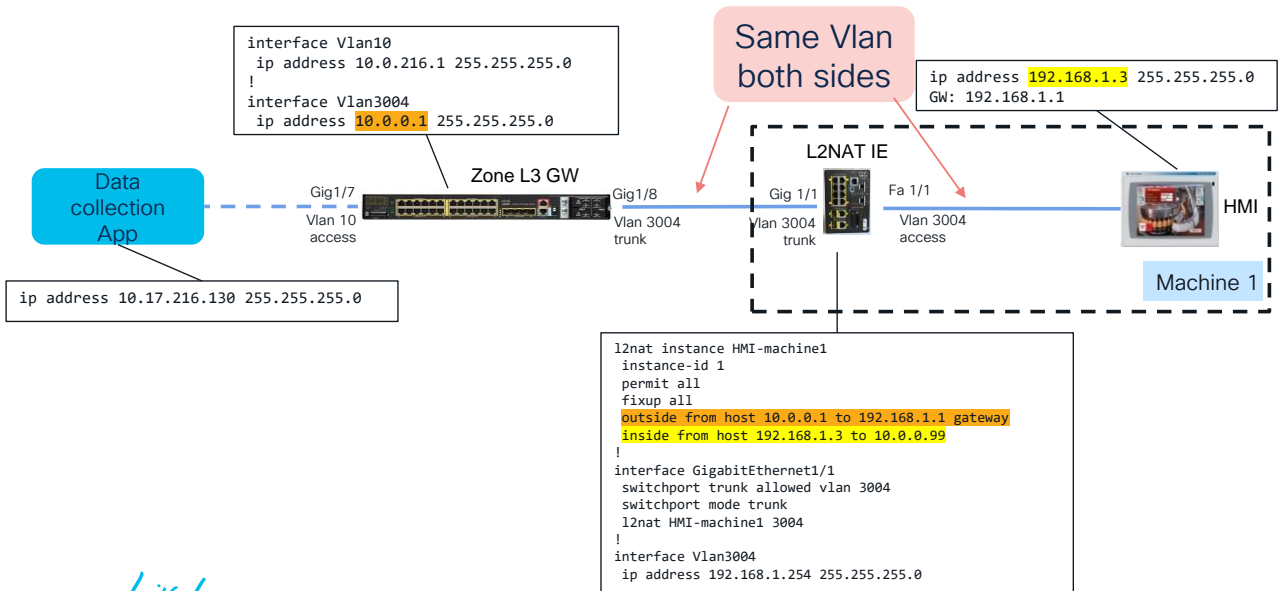
BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

13

Simple example to show L2NAT at work. How to get HMI onto the public network with an IP address which is A) not routable outside the machine, and B) duplicated across the network in other machines?

IE does L2NAT to L3 Zone Gateway



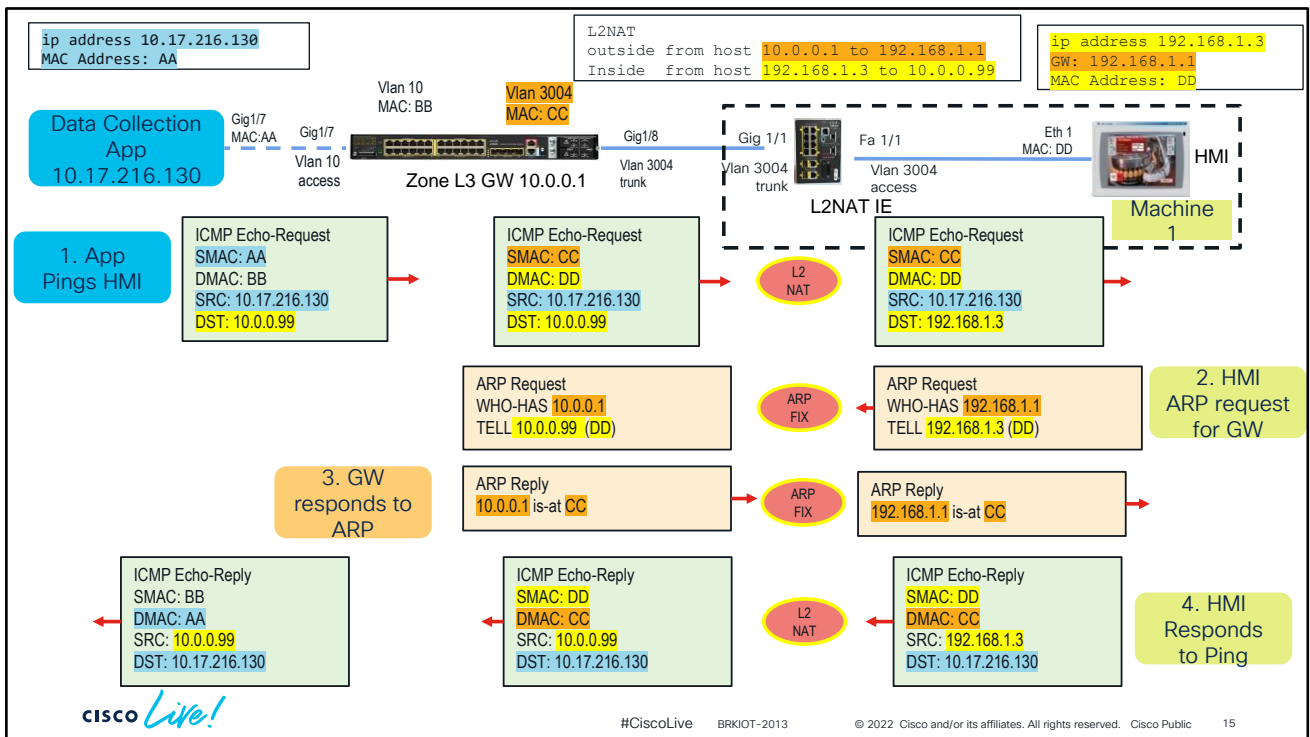
CISCO Live!

#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

14



Step 1, assume the GW has the MAC of the Private Host, but not other way around

In all L2NAT translations and Fixups – MAC Address does not change in pure Layer 2 switching.

Questions so far?

CISCO *Live!*

L2NAT 'permit' and 'fixup'

Details on 'permit' and 'fixup'

```
l2nat instance HMI-machine1
instance-id 1
permit all
fixup all
outside from host 10.0.0.1 to 192.168.1.1 gateway
inside from host 192.168.1.3 to 10.0.0.99
```



#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

17

ICMP and ARP are special because the IP address is carried in the payload as well as in L3 header.

ICMP and ARP would fail if they weren't fixed up.

In this case fixup means, go into the payload and translate the IP address there too.

Known other IP packets which are not fixed, and fail with L2NAT :

FTP active mode. Passive FTP works.

SNMP returns IP Addresses in payload, not fixed up.

Radius authentications

To name a few

L2NAT 'permit'

Permit – controls ingress / egress of packets – recommend 'all'

Blunt instrument which acts as ACL 'deny'

'all' is equivalent to 'permit any any'

```
IE_Switch(config-l2nat)# permit ?
all          Permit unmatched, multicast and IGMP packets - in, out
igmp         Permit IGMP packets - in, out using keywords, default is both
multicast    Permit multicast packets - in, out using keywords, default is both
unmatched    Permit packets that don't match any NAT entry - in, out using
              keywords, default is both
```

'multicast' – any mcast packet (CDP,LLDP, STP, VTP, ...)

'unmatched' – allows all packets on vlan to ingress/egress

cisco *Live!*

#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 18

In examples so far, 'permit all' has been used. And it will be so in future examples.

This slide gives the basics of for what permit does.

Like the name implies is essentially and ACL. Permit all – is just that. It's a permit any any.

When using L2NAT without 'permit all', there's implicit deny for packets not matching. They get dropped.

A Deep dive into strategic use of 'permit' is topic for another day.

L2NAT 'Fixup'

Fixup is for ICMP and ARP – recommend 'all'

```
IE_Switch(config-l2nat)# fixup ?  
all    Fixup ARP, ICMP  
arp    Fixup ARP  
icmp   Fixup ICMP
```



#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 19

ICMP and ARP are special because the IP address is carried in the payload as well as in L3 header.

ICMP and ARP would fail if they weren't fixed up.

In this case fixup means, go into the payload and translate the IP address there too.

Known other IP packets which are not fixed, and fail with L2NAT :

FTP active mode. Passive FTP works.

SNMP returns IP Addresses in payload, not fixed up.

Radius authentications

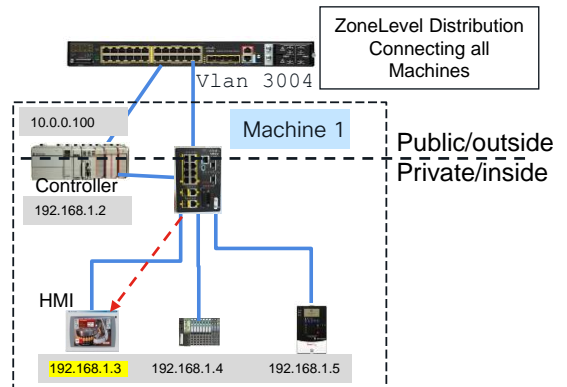
To name a few

A different way

CISCO *Live!*

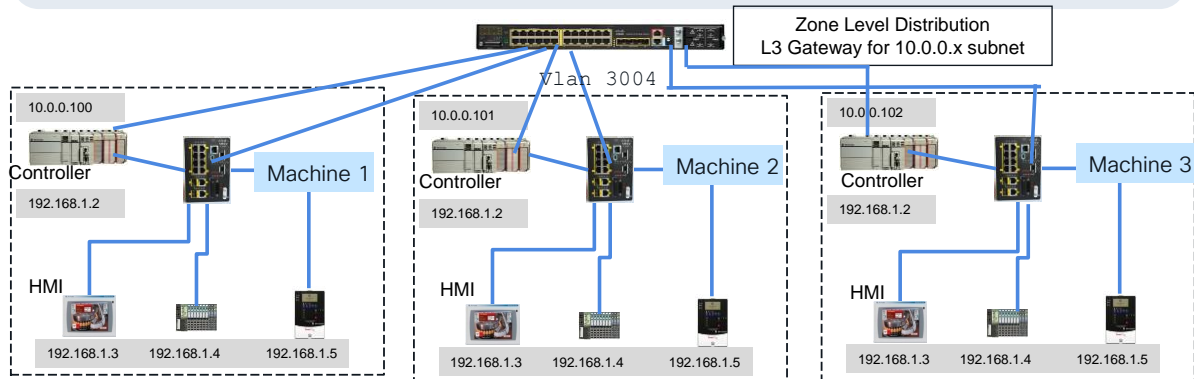
Issues with L2 only on IE

- Works for single machine subnet on 192.168.1.x and 1 vlan 3004
- Potential problems
- All Bcast traffic on vlan 3004 is FWD'd to GW not translated.
 - What about machine 2, 3, 4?
 - They all have same subnets but different vlans? Same vlans, same subnet?



Zone level view showing issues

- Same vlan all machines????
 - Broadcast domain creates duplicate IP Address issue!
 - Not for HMI, its L2NAT'd; for 192.168.1.4 and 1.5

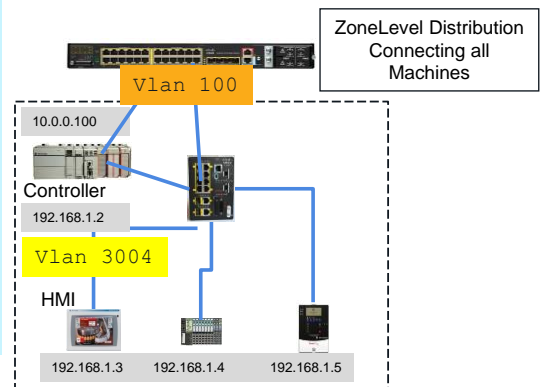


Another way

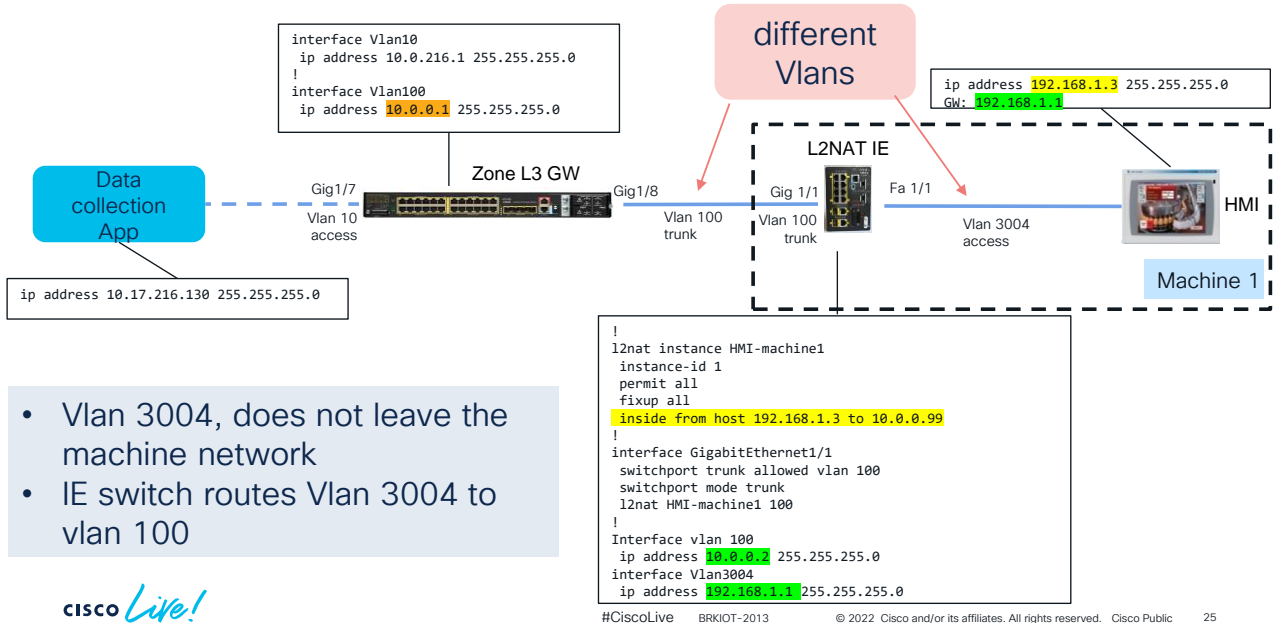
CISCO *Live!*

Different Vlans: public and private

- Eliminate machine to machine Broadcast:
 - different vlan 'private' from 'public'
 - Vlan 3004 inside machine
 - Vlan 100 outside machine
- IE switch 'routes' between vlans.
- IE switch is L3 GW for 192.168.1.x



IE switch as L3 Gateway for HMI (Routed Access)



This technique is referred to as 'Routed Access'

Making changes to previous example. Changed the vlan between IE and L3 Gateway.

IE now has L3 GW for machine 1 subnet 192.168.0.x

Now multiple machines with same IP can be connected to same L3 Gateway because IE is doing the routing, and the machine subnet (192.168.0.x) does not leave the machine

When going from private to public, the IE switch will first route the packet from vlan 3004 to vlan 100, then the packet is translated.

And when going from public to private, the packet is translated then the packet is routed. The L3 routing function sees the private IP addresses.

IE Switch ARP table

- IE ARP table and routed packets

```
IE_Switch# show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 10.0.0.1          95        0000.0133.3333 ARPA   Vlan100
Internet 10.0.0.2          -         18e7.2864.0245 ARPA   Vlan100
Internet 192.168.1.1       -         18e7.2864.0242 ARPA   Vlan3004
Internet 192.168.1.3      141       0001.01ab.cdef ARPA   Vlan3004

IE_Switch # show ip interface brief | exclude unassigned

Interface      IP-Address      OK? Method Status      Protocol
Vlan100        10.0.0.2        YES manual up          up
Vlan3004       192.168.1.1    YES manual up          up

IE_Switch# show mac address dynamic vlan 3004

Vlan    Mac Address      Type      Ports
----    -
3004    0001.01ab.cdef   DYNAMIC   Fa1/1
Total Mac Addresses for this criterion: 1
```



#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

26

the ARP, IP addresses and dynamic tables allow you to see how the devices are learned and how where packets will be forwarded.

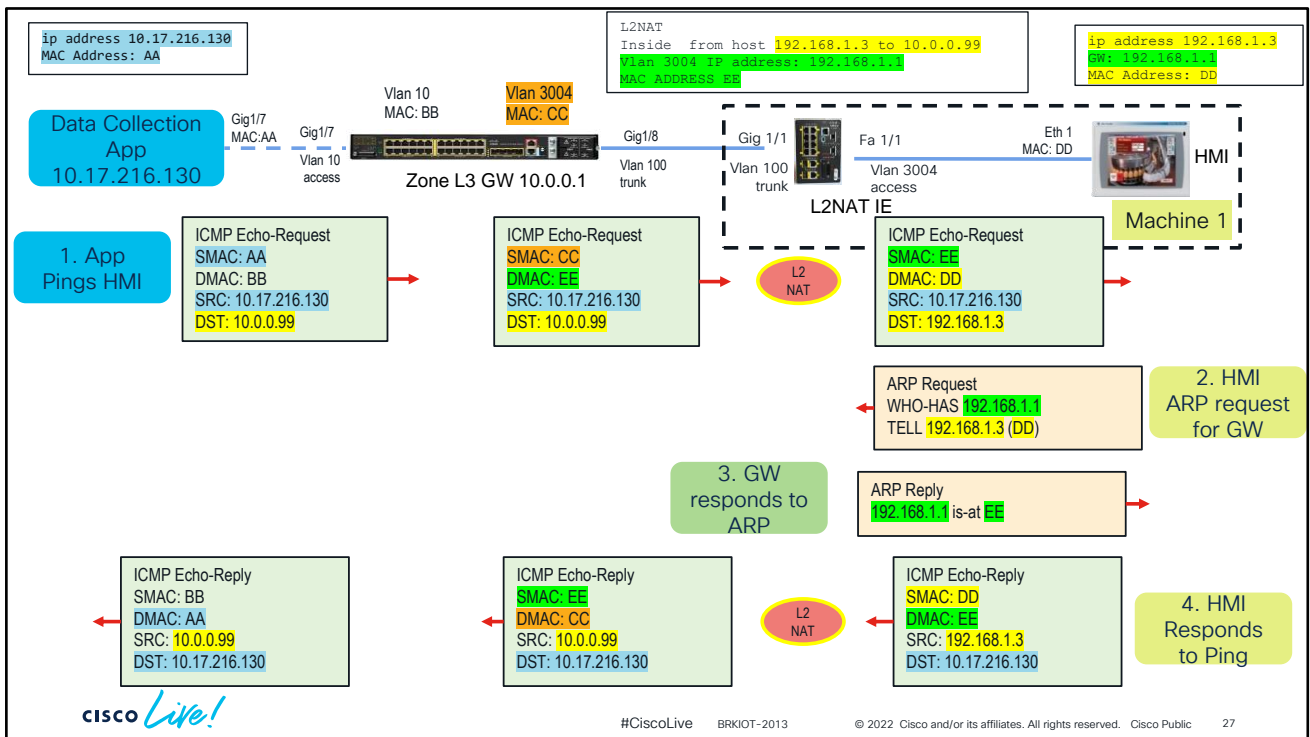
Again this is a simple example, and the CLI outputs shown have been edited to focus on relevant interfaces

The end device sends packets for '10.17.216.130' to the IE Switch's GW MAC Address on vlan 3004 '18e7.2864.0242'.

The ie3400 then routes this packet to destination on vlan 100 (Gig1/1).

The IE3400 changes source mac to its own MAC address for vlan 100 layer 3 interface which is same as vlan 3004 L3 interface. This is OK to have duplicate mac's they are on different vlans.

There's no ARP entry for 10.17.216.130 because device is not within the IE's L2 bcast domain.



Same scenario as before.

This time the MAC Addresses are different because the IE switch is doing the routing between vlan 100 and vlan 3004

The Layer3 header translation doesn't change.

No longer need to translation for GW 192.168.1.1 because its in same vlan as HMI. GW is the IE switch.

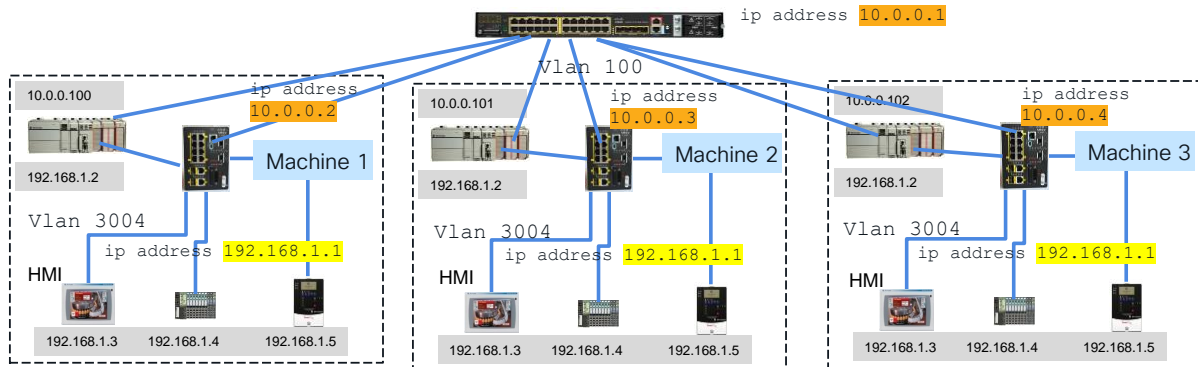
No ARP fixups needed. ARP does not go past the IE switch. No need to translate

Questions?

CISCO *Live!*

Zone level view showing solution

- Inside machine vlan 3004 (same for all machines, safe)
- 'public' vlan - All Machines use 100
- IE switches have unique IP on vlan 100; HMI have unique IP's too



CISCO Live!

#CiscoLive BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

29

Looking at the bigger picture with multiple machines.

The IE switch still has same GW IP Address for all machines 192.268.1.1

IE switch in each machine has unique IP on vlan 100 because it's the public IP.

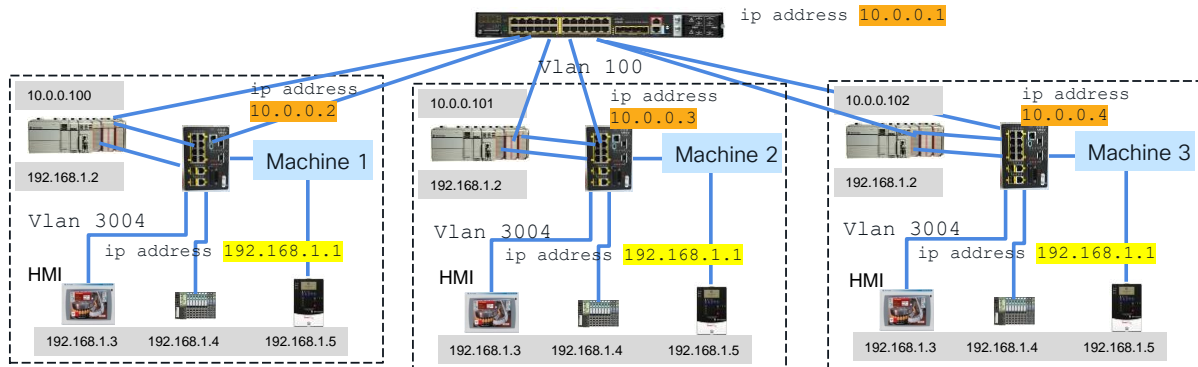
IE switch IP Address 192.168.1.1 is not translated.

IP Addresses of devices in machine do NOT change

The gateway for devices in machine does not change

While were at it – reduce cabling

- Save cabling.
- Move Vlan 100 cable from Zone switch to IE Switch



CISCO Live!

#CiscoLive BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 30

Has animation. There are not 3 cables from controller. Only 2.

Now that IE Switch is on same vlan as controller's public link, controller no longer needs link to Zone switch.

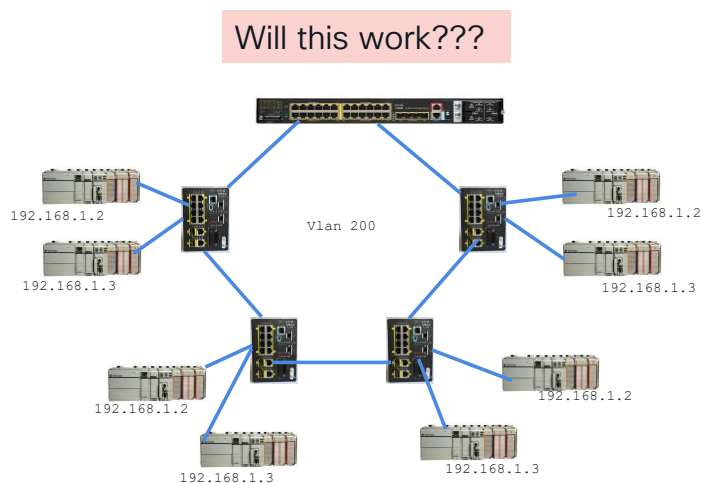
Connect controller vlan 100 link to IE switch.

Saves on cabling.

What about rings?

CISCO *Live!*

IE switches in a ring - L2NAT ??



cisco *Live!*

#CiscoLive

BRKIOT-2013

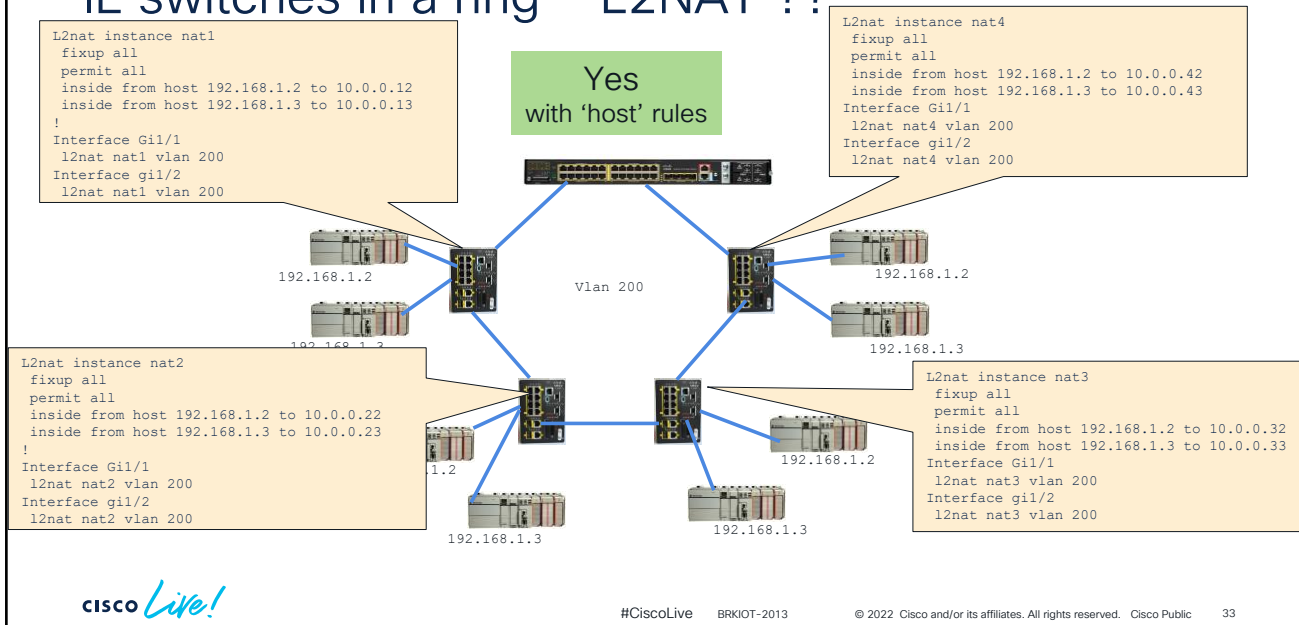
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

32

Forget about previous examples. New example: end devices connected to IE switches in a ring. IP address replicated all over the ring.

Is it possible to give all end devices unique IP addresses without conflicts?

IE switches in a ring – L2NAT ??



Yes it works with 'host' rules and apply L2NAT instance to each uplink on all IE switches.

L2NAT instance for each IE switch has unique public IP.

Could use same nat instance name for each IE. I used unique name (nat1, nat2, nat3, nat4) for ease of understanding.

L2 NAT in a Ring – a few details

- All host IP Addresses in ring must be translated.
 - no untranslated, Private IP addresses allowed in Ring
- STP and REP protocols will coexist with L2NAT

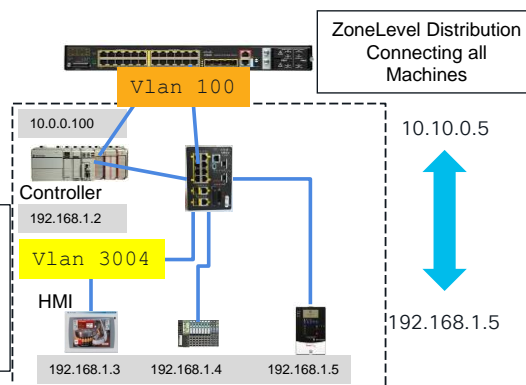
How about all the devices?

CISCO *Live!*

Scale the L2NAT translations with 'network'

- How to translate all the end devices, not just HMI?
- Use 'network' instead of 'host'
- 'mask' determines how many hosts
 - /28 = 0xF0 = 16 hosts
 - Last nibble of IP remains unchanged

```
L2nat instance network1
permit all
fixup all
inside from network 192.168.1.0 to 10.10.0.0 mask 255.255.255.240
!
Interface gi1/1
l2nat network1 100
```



/28 = 255.255.255.240

What about machines 2, 3 & 'network' ?

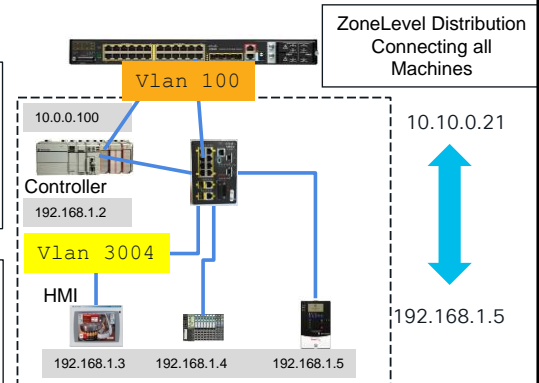
- To translate the other 2 machines to unique public IP address using 'network'

Machine 2

```
L2nat instance network1
permit all
fixup all
inside from network 192.168.1.0 to 10.10.0.16 mask 255.255.255.240
!
Interface gil/1
l2nat network1 100
```

Machine 3

```
L2nat instance network1
permit all
fixup all
inside from network 192.168.1.0 to 10.10.0.32 mask 255.255.255.240
!
Interface gil/1
l2nat network1 100
```



CISCO *Live!*

#CiscoLive BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 37

/28 = 255.255.255.240

Machine 2

192.168.1.5 translate to 10.10.0.21

And machine 3

192.168.1.5 translate to 10.10.0.37

Questions?

CISCO *Live!*

troubleshooting

CISCO *Live!*

Debugging L2NAT – Show L2NAT statistics

```
IE2K-2011# show l2nat statistics

STATS FOR INSTANCE: HMI-machine1 (IN PACKETS)

TRANSLATED STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  BYPASSED    DISCARDED    TRANSLATED    TOTAL PACKETS
Gi1/1      EGRESS    3004    0           0             6             6
Gi1/1      INGRESS    3004    0           0             6             6
-----

PROTOCOL FIXUP STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN  ARP        ICMP
Gi1/1      EGRESS    100    1           5
Gi1/1      INGRESS    100    1           5
-----

PER TRANSLATION STATS (IN PACKETS)
=====
TYPE      DIRECTION SA/DA ORIGINAL IP    TRANSLATED IP    COUNT    ACTIVE (90Sec)
INSIDE    EGRESS    SA    192.168.1.3    10.0.0.99        6         6
INSIDE    INGRESS    DA    10.0.0.99      192.168.1.3      6         6
=====
```

#CiscoLive BRKIOT-2013 © 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 40

When things are not working, this command is useful.

L2NAT Statistics for the interface, for fixups, and per rule with direction.

The above is truncated output to get the results to fit and be readable.

conclusion

CISCO *Live!*



CISCO *Live!*

- Duplicate IP addresses are done on purpose
 - Network has to adjust
- L2NAT is 1:1 IP translation
 - Its not 1:N (eg: NAT/PAT)
- Single box solution
- Works at line rate. 😊

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

42

Where to get More information

- L2NAT configuration Guide on Cisco.com
https://www.cisco.com/c/en/us/td/docs/switches/lan/industrial/software/configuration/guide/b_l2_nat_ie.html
- Cisco CPwE L2 Network Address Translation
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD/CPwE_NAT_Chap3.html
- Cisco IOT Networking youtube channel
<https://www.youtube.com/c/CiscoloTTMETV>
- Remember: L2NAT is not NAT/PAT on a router

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Connect, Automate, and Operate Anywhere

Introducing new wireless and remote operational capabilities from Cisco IoT

Learn how Cisco's newest industrial wireless and operation tools enable organizations to securely connect, automate and operate at scale.

Join us on June 21st for this 35-minute webinar where we will discuss:

- How to meet new requirements in wireless networking and security
- How operational networks can benefit from enterprise-grade capabilities
- The latest Cisco innovations in industrial wireless technology from Wi-Fi 6 to fiber-like wireless connectivity
- Improving IT and OT more efficiently through better visibility and enhanced tools to enable operations from anywhere



#CiscoLive BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 45

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



#CiscoLive


BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

46

Continue your education

- 1 Industrial Zero Trust: Opportunities and Realities ([BRKIOT-2012](#))
- 2 Leveraging Visibility to drive Zero Trust for Industrial Security ([BRKIOT-2353](#))
- 3 Securing Industrial Networks: Where do I start? ([BRKSEC-2077](#))
- 4 Extending Cisco Cyber Vision capabilities by using REST API ([DEVNET-1818](#))



Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public 48



The bridge to possible

Thank you

cisco *Live!*

#CiscoLive

CISCO *Live!*



#CiscoLive

More on “network” rule

- Use ‘network’ to scale hosts sharing same subnet
- Only consumes 1 L2NAT rule resource. Same as ‘host’ rule
- Unmasked ‘bits’ in original retained in translation.
 - Only masked value translated

Examples

Rule with mask	original IP	Translated IP
from network 192.168.1.0 to 10.10.0.0 mask 255.255.255.0	192.168.1.3 192.168.1.129	10.10.0.3 10.10.0.129
from network 192.168.1.0 to 10.10.0.0 mask 255.255.255.240	192.168.1.3 192.168.1.129	10.10.0.3 192.168.1.129
from network 192.168.1.0 to 10.10.0.128 mask 255.255.255.240	192.168.1.3 192.168.1.129	10.10.0.131 192.168.1.129
from network 192.168.1.0 to 10.10.128.128 mask 255.255.0.0	192.168.1.3 192.168.1.129	10.10.1.3 10.10.1.129

#CiscoLive

BRKIOT-2013

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

51