Fun with VLANs on Proxmox

About me

+ Ceph Connoisseur at croit GmbH (https://croit.io)

+ Coffee Connoisseur at home

+ Self-anointed Infrastructure specialist (https://kayg.org)

+ Love hosting free software as a service to the www / friends

A very important detail about me

that I missed

I suck at networking

a lot.

So I made sure you don't

What are VLANs?

+ Logical division of a network that can span multiple physical devices

+ Bridge, bond, NIC, you name it

+ Each VLAN is a separate broadcast domain

+ A broadcast domain is a logical division of a single computer network

What are VLANs?

+ Devices in a broadcast domain can talk to each other

+ Therefore, devices within a VLAN can talk to each other

+ Devices in one broadcast domain cannot talk to devices in another

+ Therefore, devices in one VLAN *should not be able to* talk to devices in another VLAN

Why VLANs?

+ Separate set of machines with intent

+ Route and shape traffic for a set of machines without affecting others

+ Don't let your smart fridge eat 300 gigs a month. Spend the data scrolling Instagram instead… maybe not.

+ Learn networking!

Proxmox…

+ Open-source hypervisor, with active development

+ Based on Debian, so familiar to most people

+ Mature, widely used with years of community support

+ Serves as a superb testbed for learning containers, networking, virtualization, orchestration… most things Linux

Enough tell

Please show

The two paths to VLANs

+ Transparent: make bridge vlan-aware, create vlans on the linux bridge, assign vlan tag to the vm network device

+ Traditional: connect a linux bridge to a vlan on the NIC (dynamically created/destroyed), assign bridge to the vm network device

Walking both paths

+ Ping within the VLAN
  - Transparent? ✅
  - Traditional? ✅

+ Ping another VLAN
  - Transparent? ❓
  - Traditional? ❓❓❓

WHY?

Because forwarding

How does that work?

+ Remember how the host is also on the VLAN?

+ Remember how the gateway for our vms is the VLAN?

+ Our host is forwarding the packets here because:
    o We have it configured as our gateway
    o AND the linux kernel is configured to forward packets

+ Our host acts as a router here to forward packets the same way your router forwards packets to your isp's router at home

How do we prevent it?

+ with a firewall – iptables!

+ Prevent forwarding by default
    o Allow communication between bridge and NIC, both ways
    o Allow communication between VLANs and bridge, both ways
    o Finally, allow communication within VLANs

+ Now we have completely configured VLANs!

Out of Scope / Later

+ Trunk ports

+ VLAN in VLAN (QinQ)

+ Bonds

+ ...

Thank you for your patience

until next time!