Linux Bridging

Teaching an Old Dog New Tricks

Stephen Hemminger
shemminger@vyatta.com
Topics

- Background
- Tunneling
- Security
- Status
Bridge Forwarding

- Multicast?
  - IGMP table
- Destination?
  - Forwarding Table
  - Flood
  - Output
Spanning Tree Protocol

Root

Leaf

BPDU

Disabled

Edge
BILLIONS AND BILLIONS OF VLANS
Cloud Tunneling Protocols

- VxLan
  - Arista, Broadcom, Cisco, VMware, Red Hat
- NVGRE
  - Microsoft, Intel, Dell, Broadcom, Emulex
- STT
  - Niciria
API flavor’s

- loctl
  - Compatibility
  - non-extensible
- Sysfs
  - Text based
- Netlink
  - Notifications
  - TLV format
Hw offload

- Common netlink API
  - Forwarding table
  - Monitoring
Security

- BPDU guard
- BPDU filter
- Root port protect
- Port locking
STP Security Issues

Bridge (core)

Bridge (edge)

Guest VM
BPDU Filter

Core Bridge

BPDU blocked
Not sent or received

Untrusted Host
BPDU Guard

Core Bridge

Untrusted Host/Bridge

Rogue BPDU!
Link disabled

BPDU Guard
Root Port Protect

Core Bridge

Semi-trusted Host/Bridge

BPDU Allowed if Priority < Root
Port lock

Core Bridge

Source Address Must match

Untrusted Guest
Spanning Tree

- **Current**
  - Kernel – 802.1d 1998
  - Userspace – RSTP daemon

- **Goal**
  - Kernel – 802.1d/802.1s
  - Userspace – SPB or TRILL?
Status

- VXLAN – 3.7
- Security – 3.8?
- STP update – 3.9??
Bridge vs Openvswitch

Ethernet Bridge
- Plug and Play
- Firewall rules
- Integrated

Openvswitch
- Table driven
- Flexible
- Management agent
Thank you