BirchenallHowden

information | communication | technology

CRS328 as a Layer 2 Switch

UK MUM 2018

Oct 2018 © Jono Thompson
BirchenallHowden Ltd

Jono Thompson

- Networking background started as a Cisco Engineer
- Started using ROS June 2010
- MikroTik Consultant Since Dec 2014
- MikroTik Trainer since March 2017
  - MTCNA
  - MTCRE
  - MTCWE
  - MTCTCE
  - MTCINE

BirchenallHowden Ltd

- Established in 2006
- 29 staff
- Based in Sheffield, UK and working throughout the UK and Europe
- Currently providing IT support for over 75 companies and 2800 users
- Currently have 2 MikroTik consultants

BirchenallHowden Ltd

- Services Provided
  - Wired and wireless network design and installation,
  - Desktop and server installation, support and maintenance
  - ISP Services, leased lines, connectivity
  - Telephony
  - Wireless installs
  - MikroTik Consultancy
  - MikroTik Training

- Visit www.birchenallhowden.co.uk

Presentation Objectives

- Since 6.41 there has been some major changes to the Bridge
- Look at some of new features on the CRS3xx Series

- VLAN configuration on the CRS3xxx Switch
- Common Layer 2 misconfigurations
- Some of the other new features since 6.41 in bridge and on CRS3xx switch

Switch vs Router - which is most powerful?

CCR1072-1G-8S+

- 72 Core 1GHz Tile chipset
- 16GB Ram

- RRP $3050

- Layer 2 Throughput 79,000 Mbps
- Layer 3 Throughput 79,000 Mbps

CRS317-1G-16S+RM

- 2 Core 800MHz Arm Chipset
- 1GB RAM

- RRP $399

- Layer 2 Throughput 159,000 Mbps
- Layer3 Throughput 3,000 Mbps

CCR1072 test results 1518byte packet Bridging no filters with fastpath - https://mikrotik.com/product/CCR1072-1G-8Splus#fndtn-testresults
CRS317 test results 1518byte packet switching non blocking layer2 throughput - https://mikrotik.com/product/crs317_1g_16s_rm#fndtn-testresults

Switch vs Router - which is most powerful?

CCR1072-1G-8S+

CRS317-1G-16S+RM

Depends on what you going to use it for!

CRS has almost double the throughput at Layer2
CRS is just over 10% of the cost

Choose the correct unit for the correct job!

BirchenallHowden

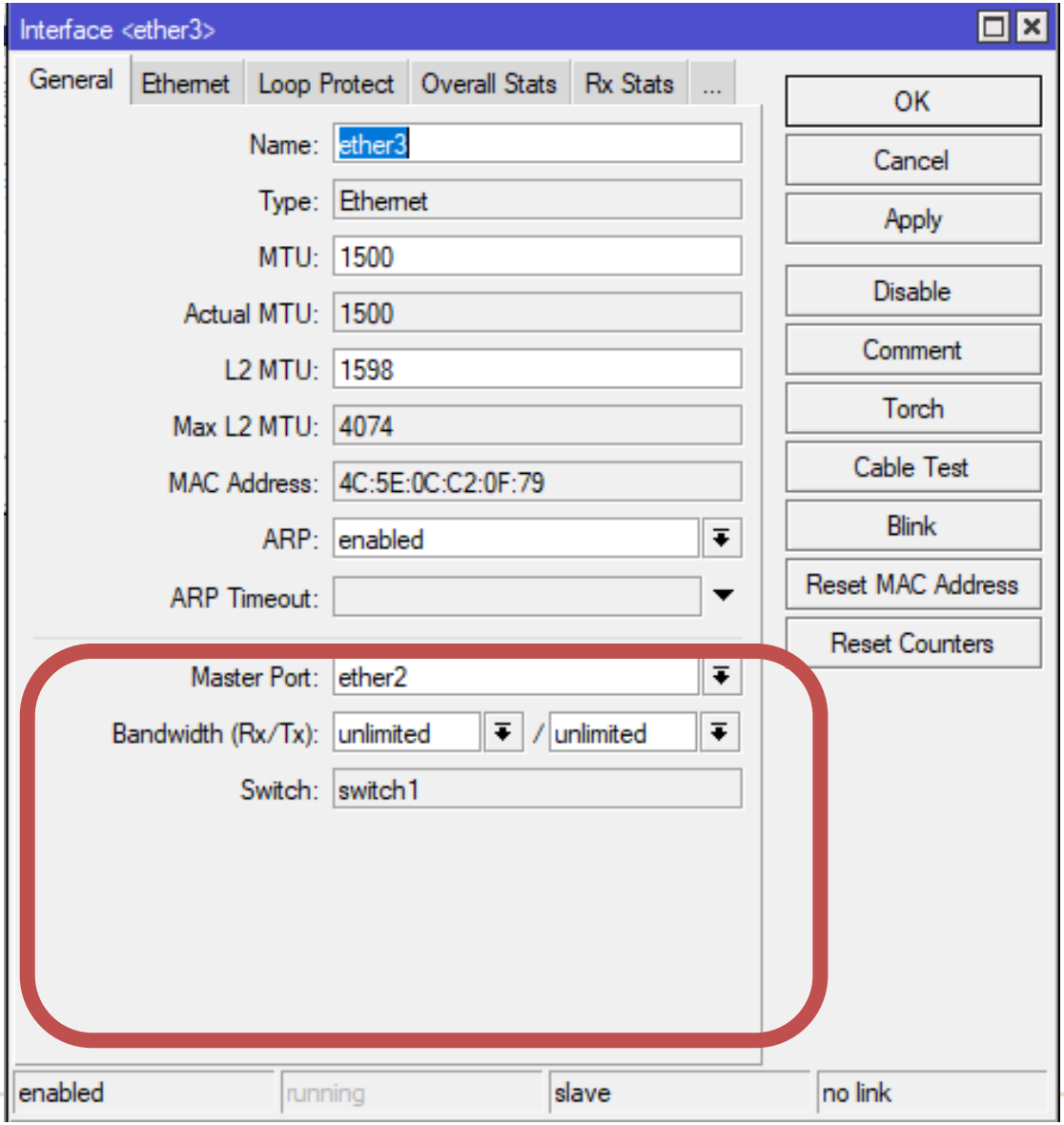
information | communication | technology

New Bridge Configuration

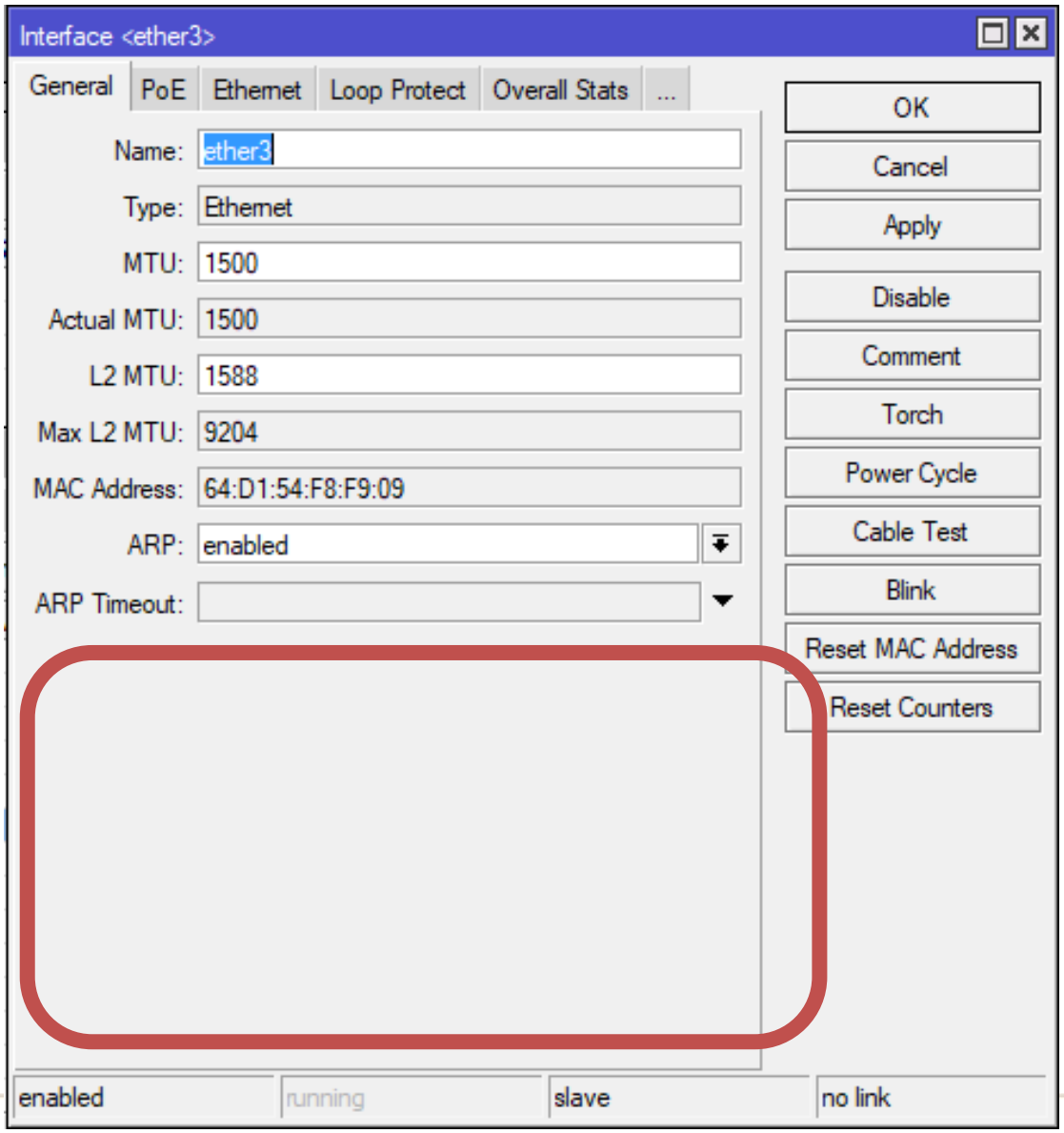
Bridge

- If you have started using stable versions and are not just using long-term versions you will have seen……
- Since 6.41 there has been some changes to the bridge and switch configuration
- No master/slave configuration on interface to pass packets through switch chip and not the CPU

Interfaces Pre 6.41

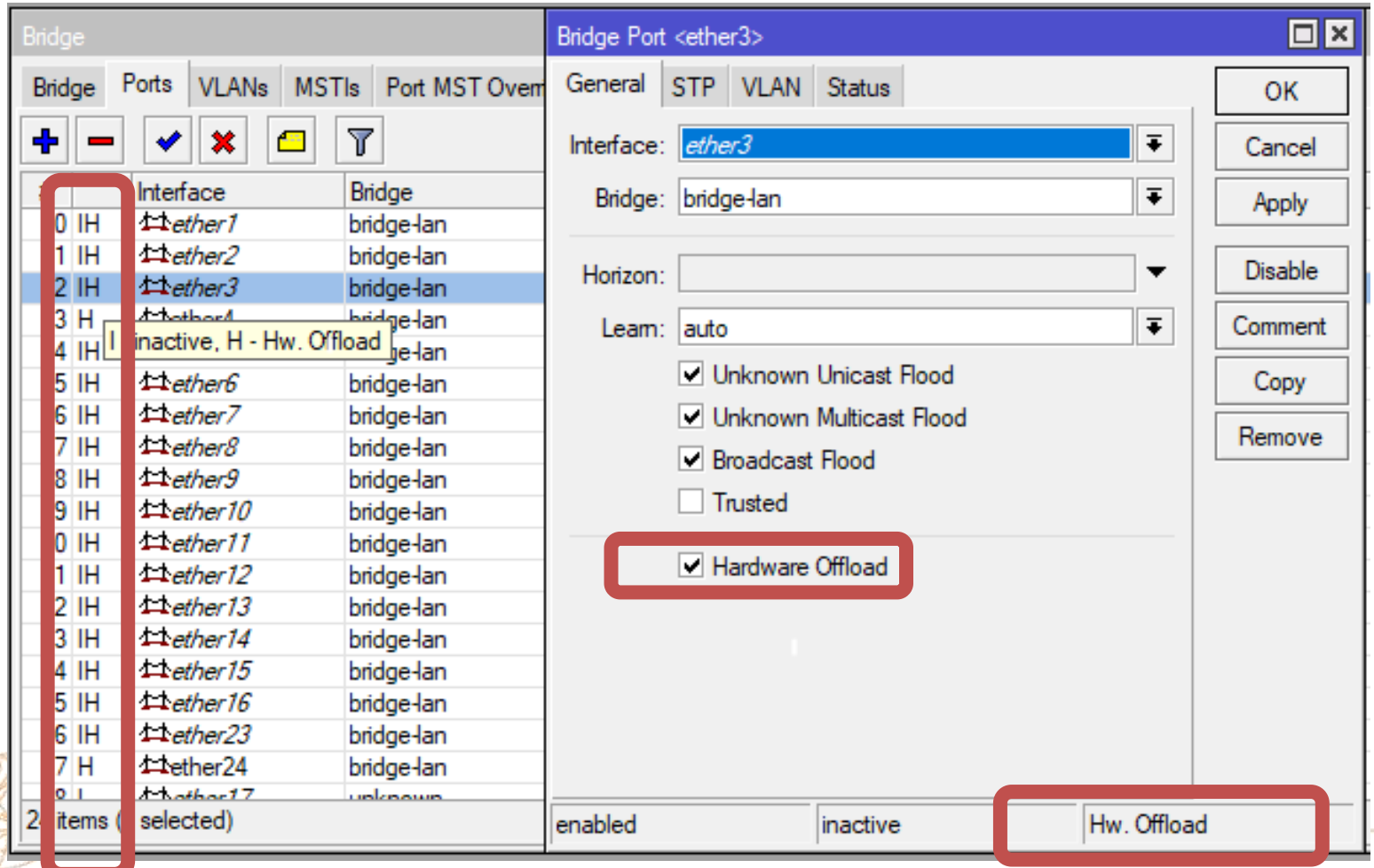


Interfaces 6.41 Onwards



Bridge hardware offloading

- Adding ports to the bridge will now automatically (if supported and enabled) use switch



Bridge – VLAN Filtering

- Since 6.41 bridge VLAN filtering has been supported
- This simplifies the VLAN setup on ROS
- This makes bridge operation more like a traditional Ethernet switch
- CRS326 makes an ideal LAN switch

- **TIP:**

  Create all VLANs before enabling VLAN filtering to prevent loosing access to the router during configuration!

Bridge – HW offloading

- Since ROS 6.41 Bridges handle all Layer2 forwarding and the use of the switch chip
- HW offloading is turned on if appropriate conditions are met

- Enabling some bridge features disables hw offloading eg:-
  - Spanning Tree
  - Rapid Spanning Tree
  - Multiple Spanning Tree
  - IGMP Snooping
  - DHCP Snooping
  - VLAN Filtering
  - Bonding

Bridge – HW offloading

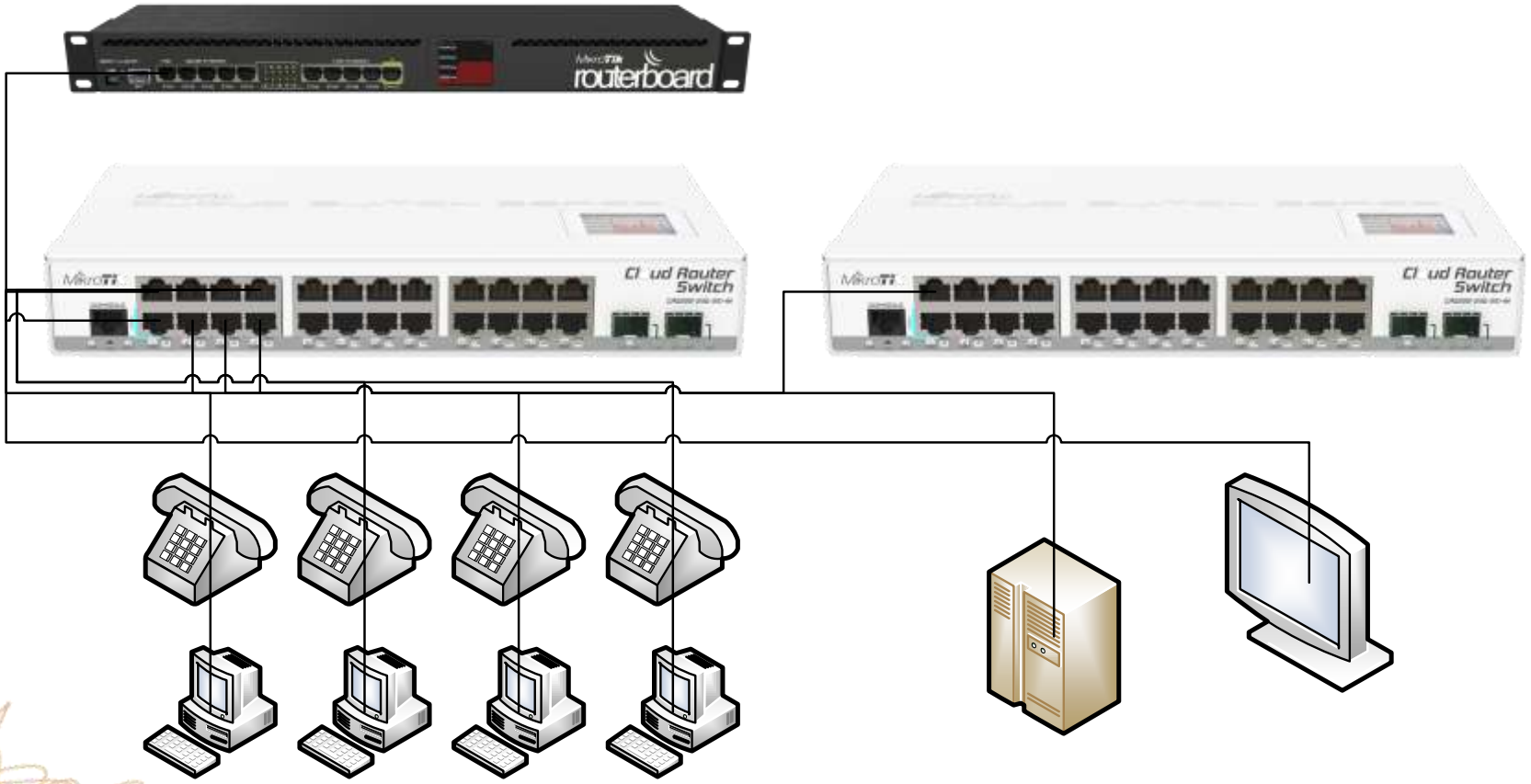
- Depending on the model or the switch chip, different features will disable bridge HW offloading

Model	STP/RSTP	MSTP	DHCP Snooping	VLAN Filtering	Bonding
CRS3xx	✓	✓	✓	✓	✓
CRS1xx/2xx	✓	×	×	×	×

Switch Chip	STP/RSTP	MSTP	DHCP Snooping	VLAN Filtering	Bonding
QCA8337	✓	×	×	×	×
AR8327	✓	×	×	×	×
AR8227	✓	×	×	×	×
AR8316	✓	×	×	×	×
AR7240	✓	×	×	×	×
RTL8367	×	×	×	×	×
ICPlus175D	×	×	×	×	×

Complete list https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features#Bridge_Hardware_Offloading

Bridge – VLAN Setup



Bridge – VLAN Setup

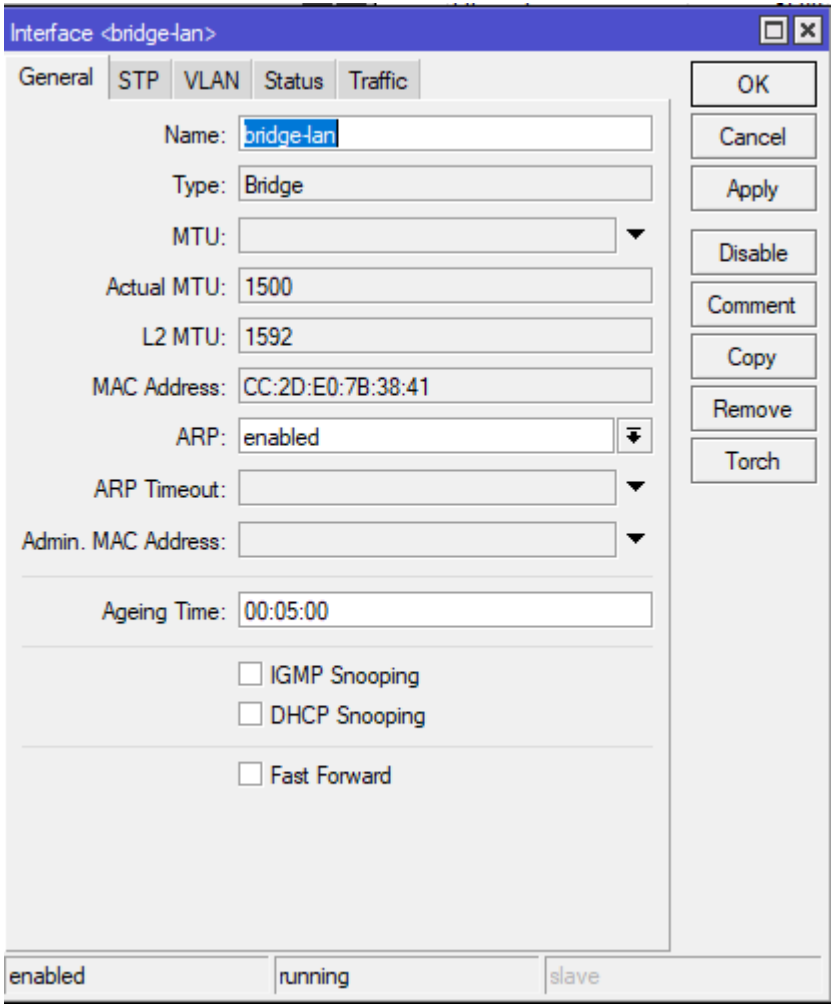
- For this configuration as we are unable to alter the phone configs we will need a mixture of

- **Trunk Ports** for link to other switches and router
  Port 1 – Link to router
  Port 2 – Link to next switch

- **Access ports** for the servers, PCs and phones
  Ports 3-6 – PCs and Phones
  Port 7 – Untagged in VLAN11 for a server
  Port 8 – Untagged in VLAN201 for public device

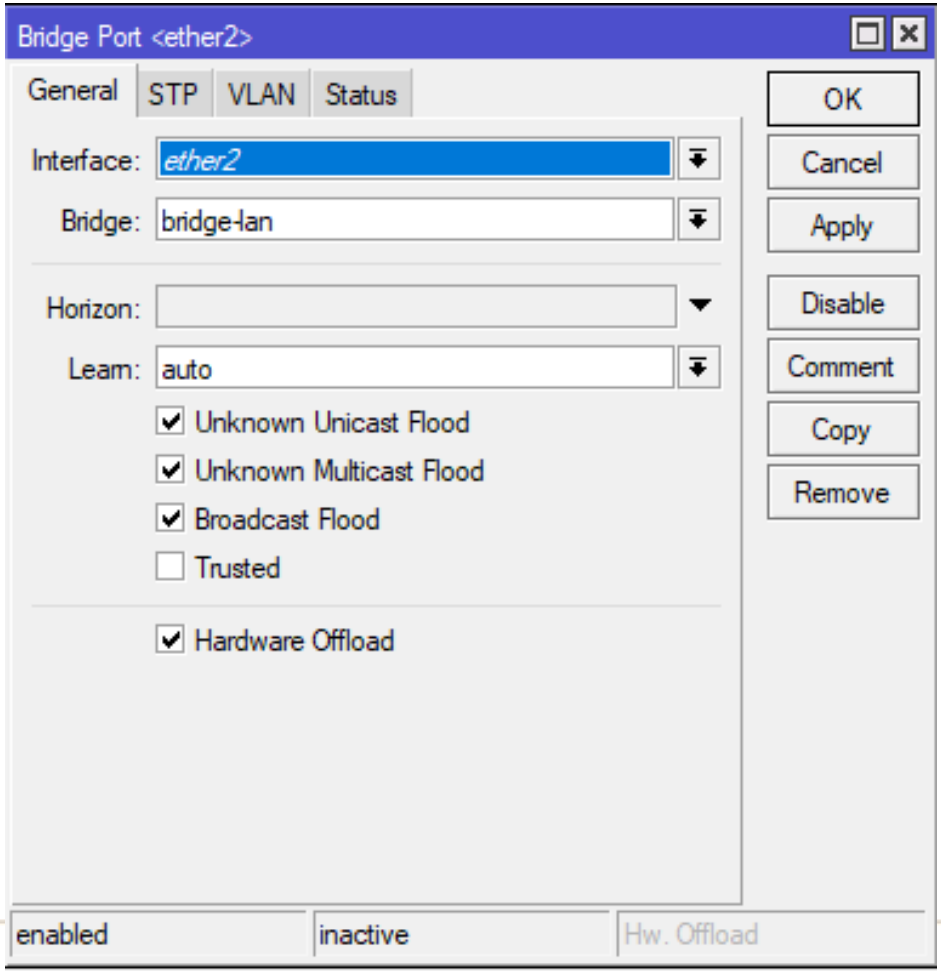
VLAN Configuration

- Create a bridge



VLAN Configuration

- Add all Switch Ports to the Bridge
- Default is hardware offloaded



VLAN Configuration

- Configure VLANs on bridge and assign ports to them

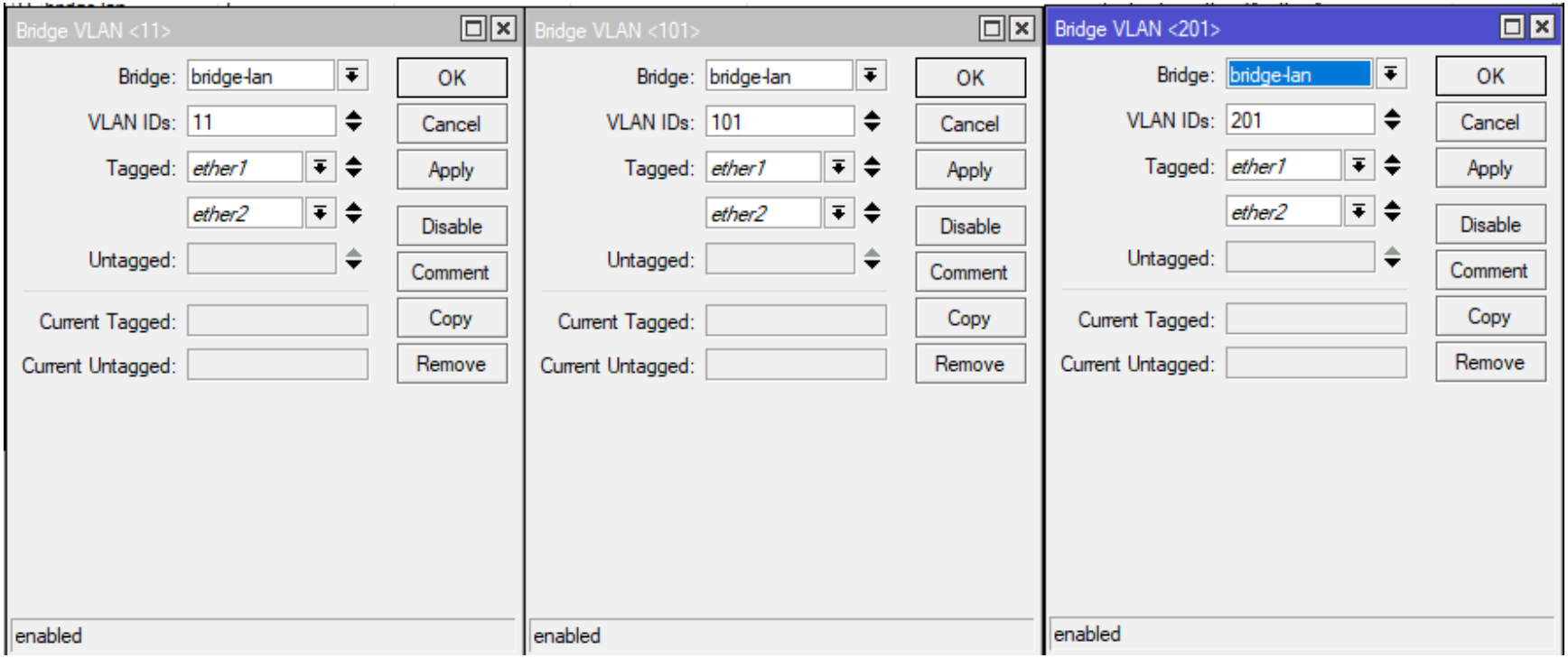
- For this example we have these VLANs

- VLAN 11 – Data
- VLAN 101 – Phones
- VLAN 201 – Public

- We going to Start with the Trunk Ports 1 & 2

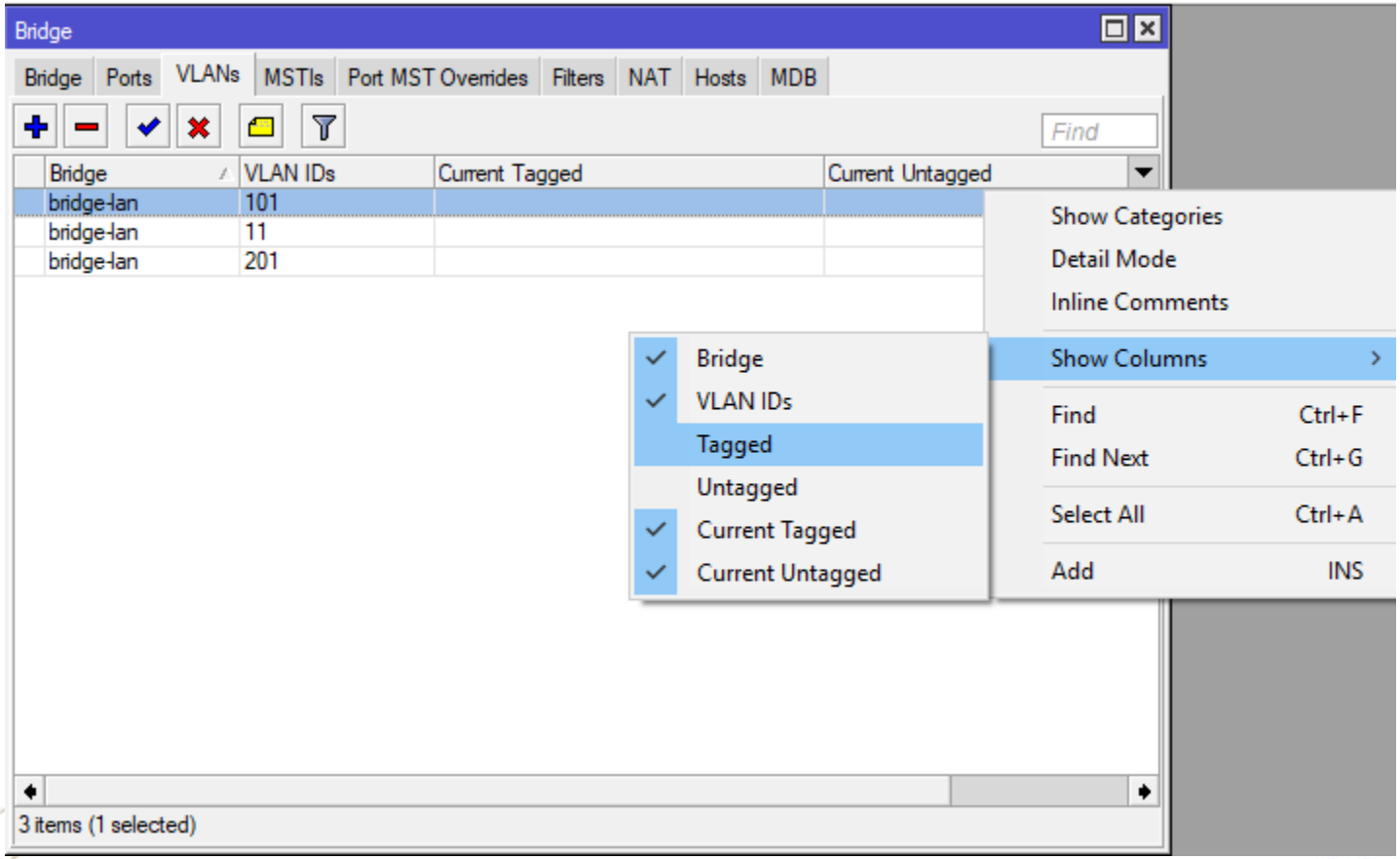
VLAN Configuration

- Create VLANs and add ether1 and ether2 as tagged



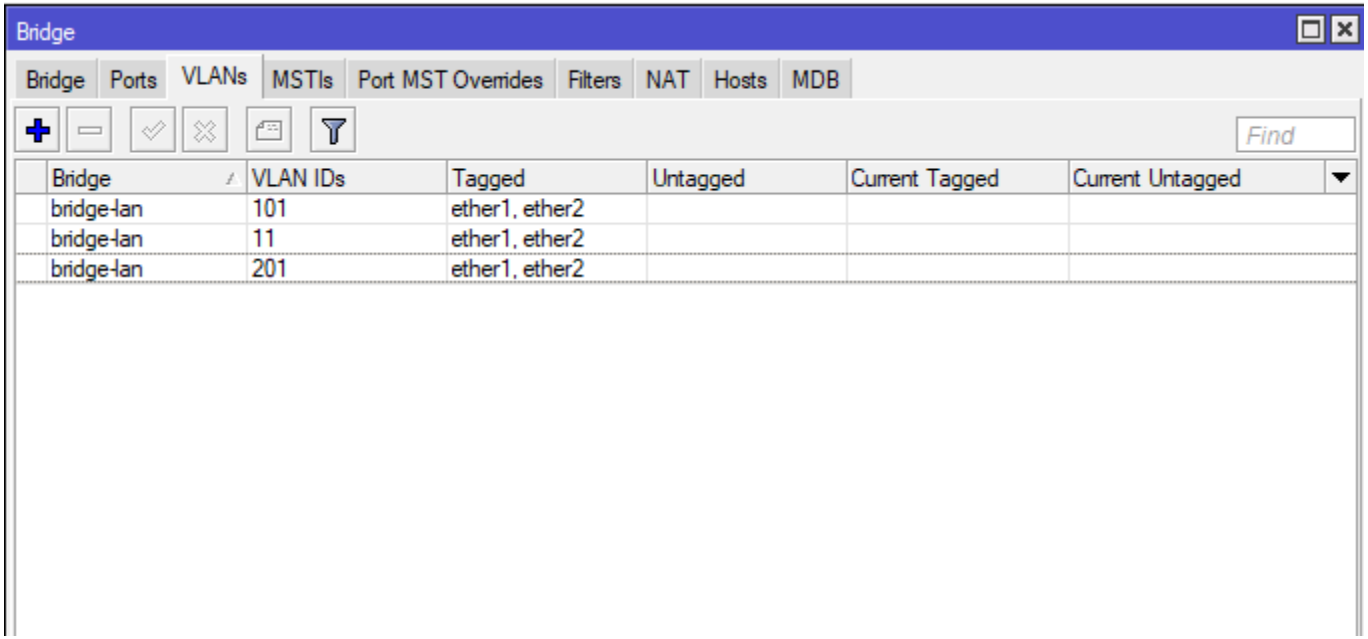
VLAN Configuration

- TIP – Add extra columns to WinBox! This will make it easier to see the config



VLAN Configuration

- Now you can see both the configured and current settings
- Current column populated when devices connected up



Untagged Ports

- Next we will configure ports 3-6
- These ports are for PCs and Phones
- PCs need to be in VLAN 11 and Phones in VLAN101.
- We will use a MAC based VLAN rule to put the phones in VLAN 101

MAC based VLAN

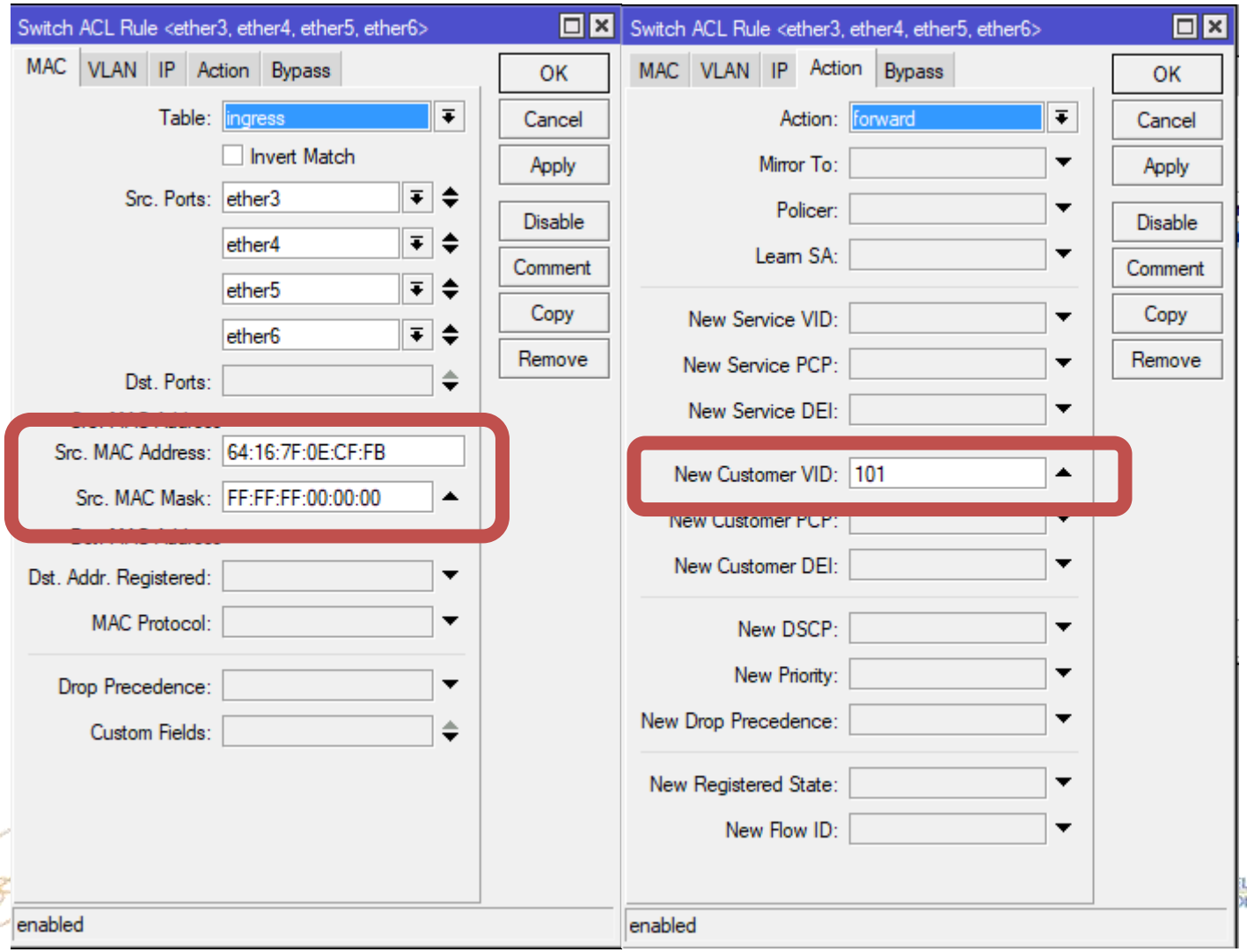
- We can use switch rules to create a MAC based VLAN. We will use this for our phones.

- We can use a MAC address mask to catch all phones with the same OUI based MAC

- We will set up these ports so we can also use the PC port in the phone without reconfiguring the phones.

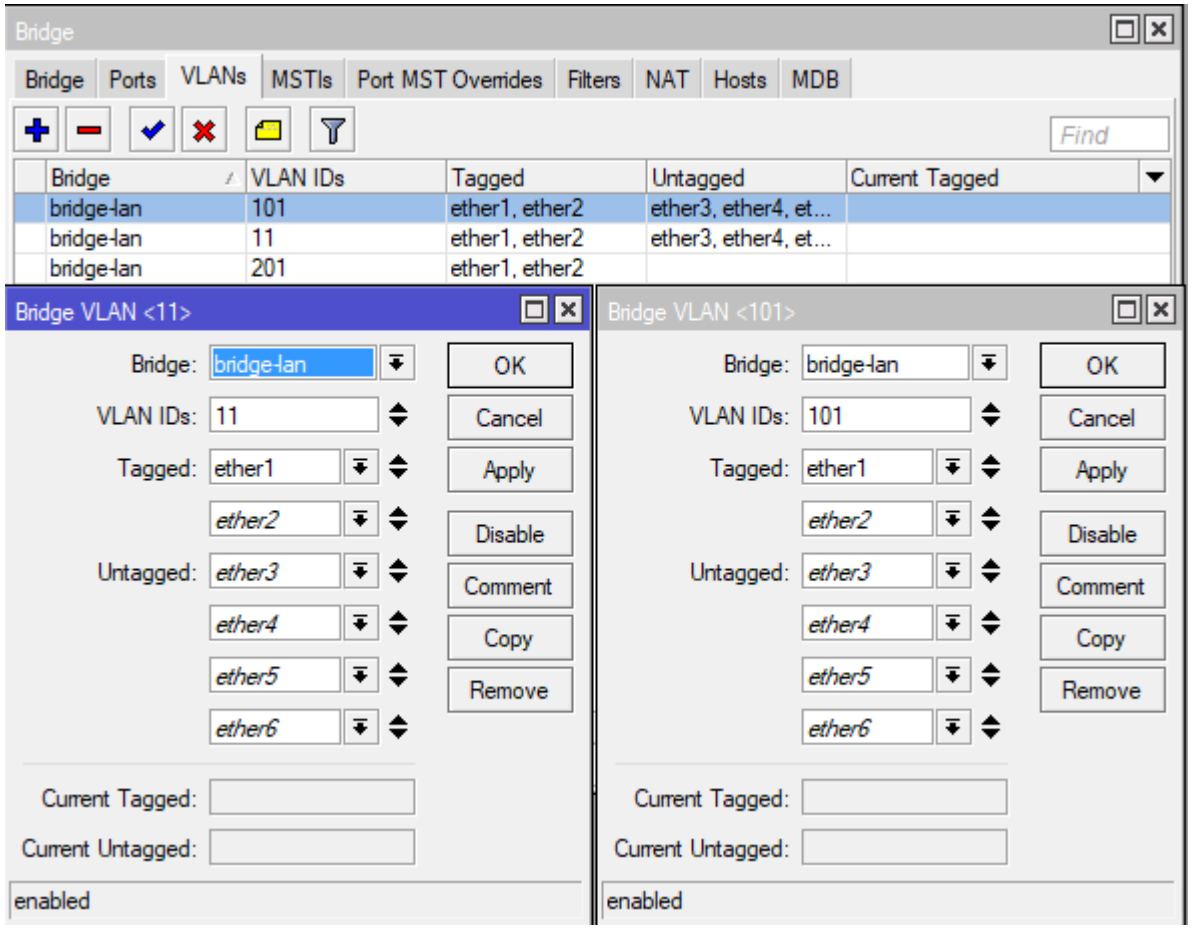
MAC based VLAN

- Create a Switch ACL rule to change VID based on MAC address



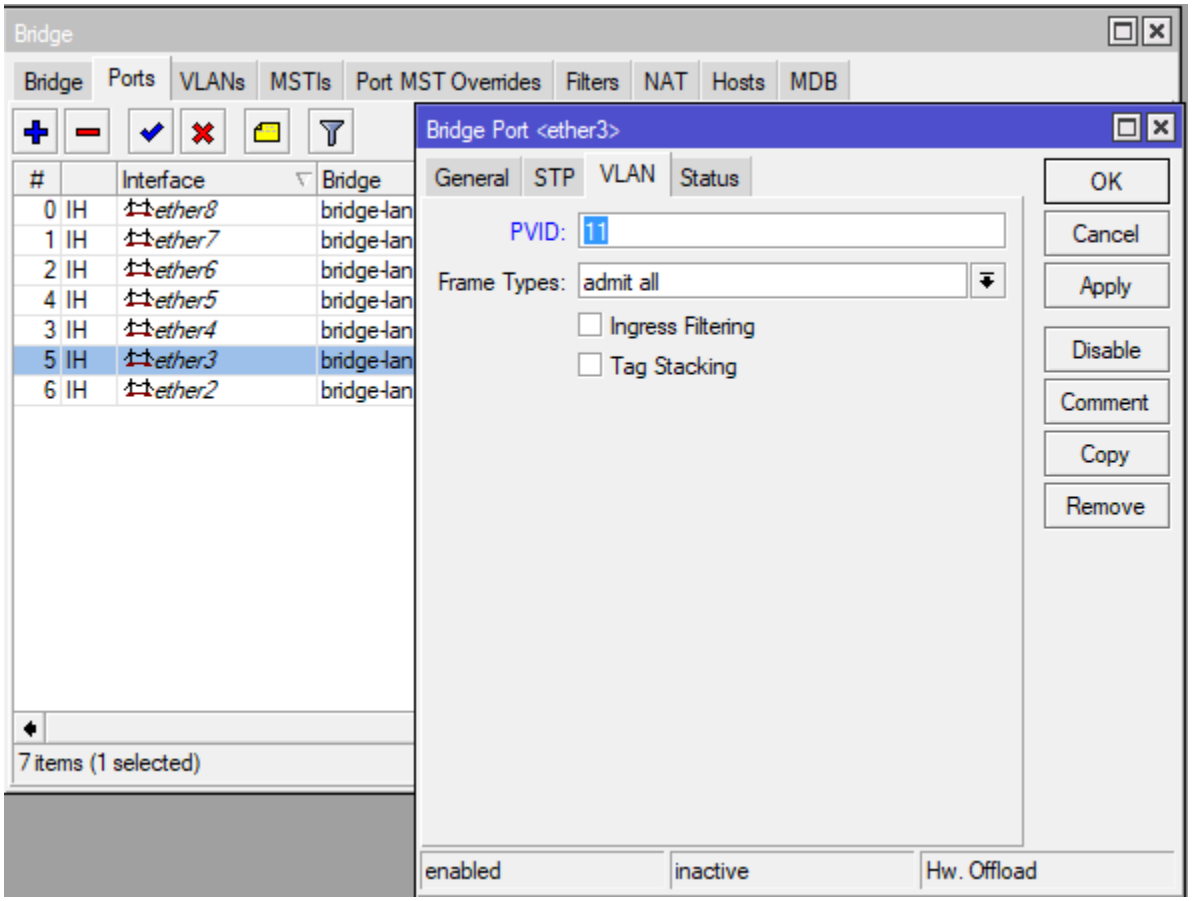
Untagged Ports

- We will now create some Untagged ports for our PCs and phones



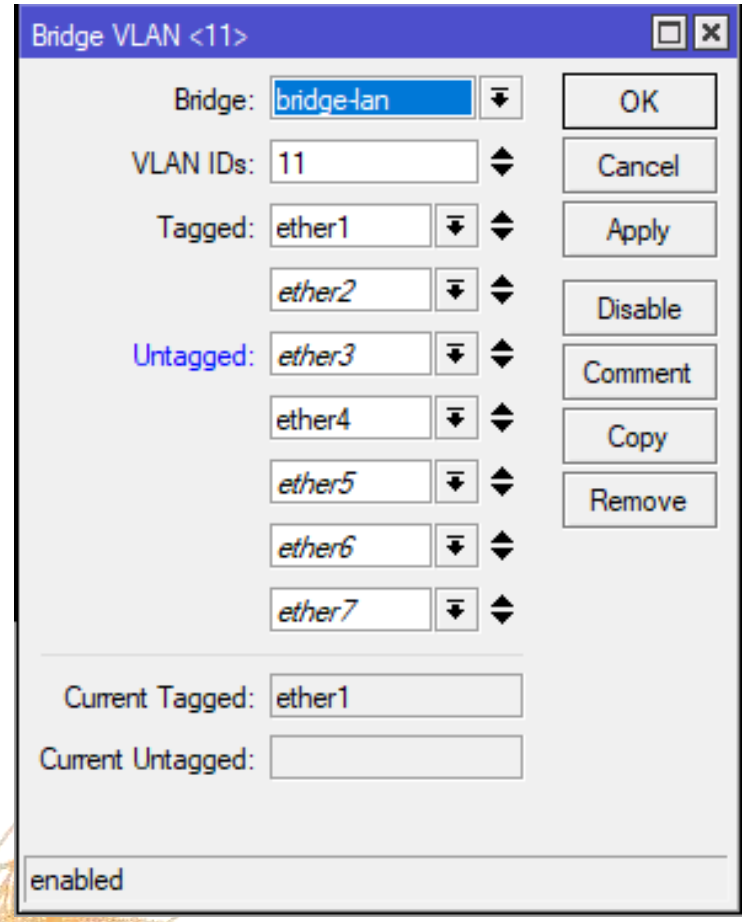
Untagged Ports

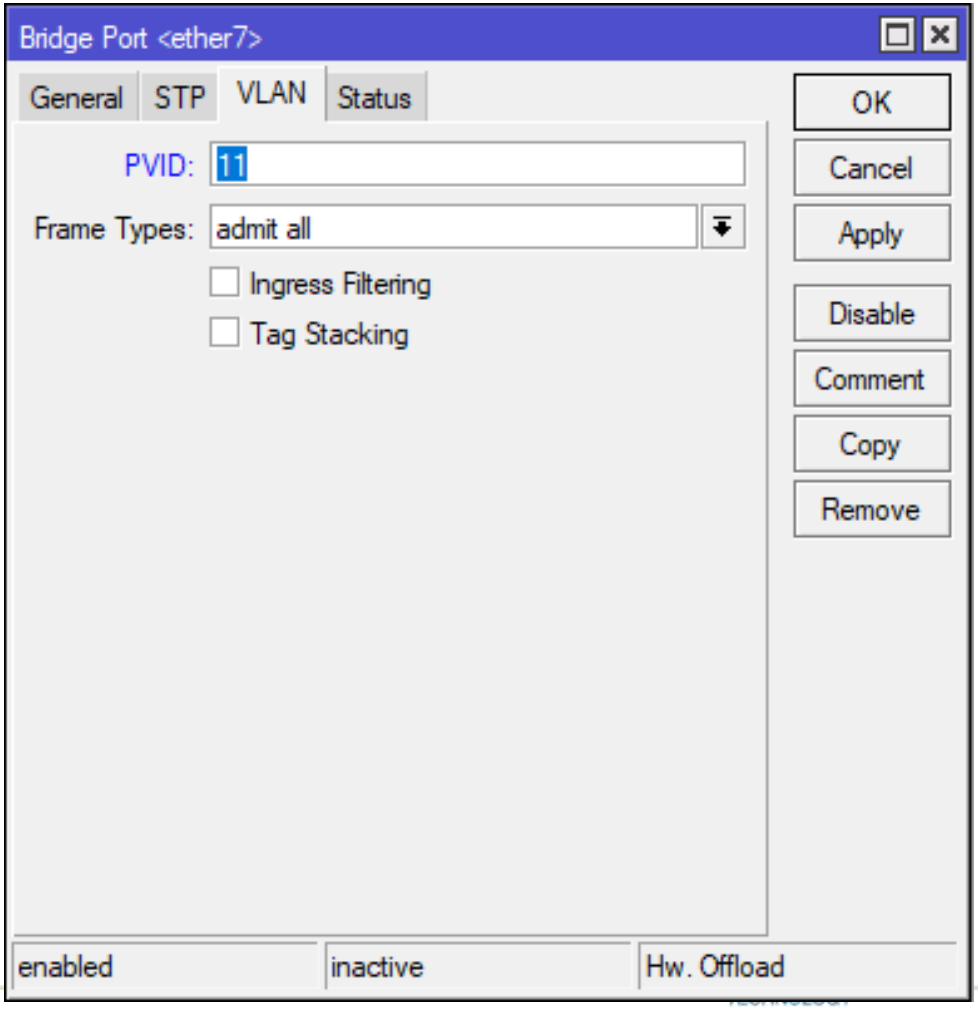
- Set the Ports to Add PVID to untagged traffic to put PC in data VLAN. Phones will be tagged in phone VLAN using the switch rule



Untagged Ports

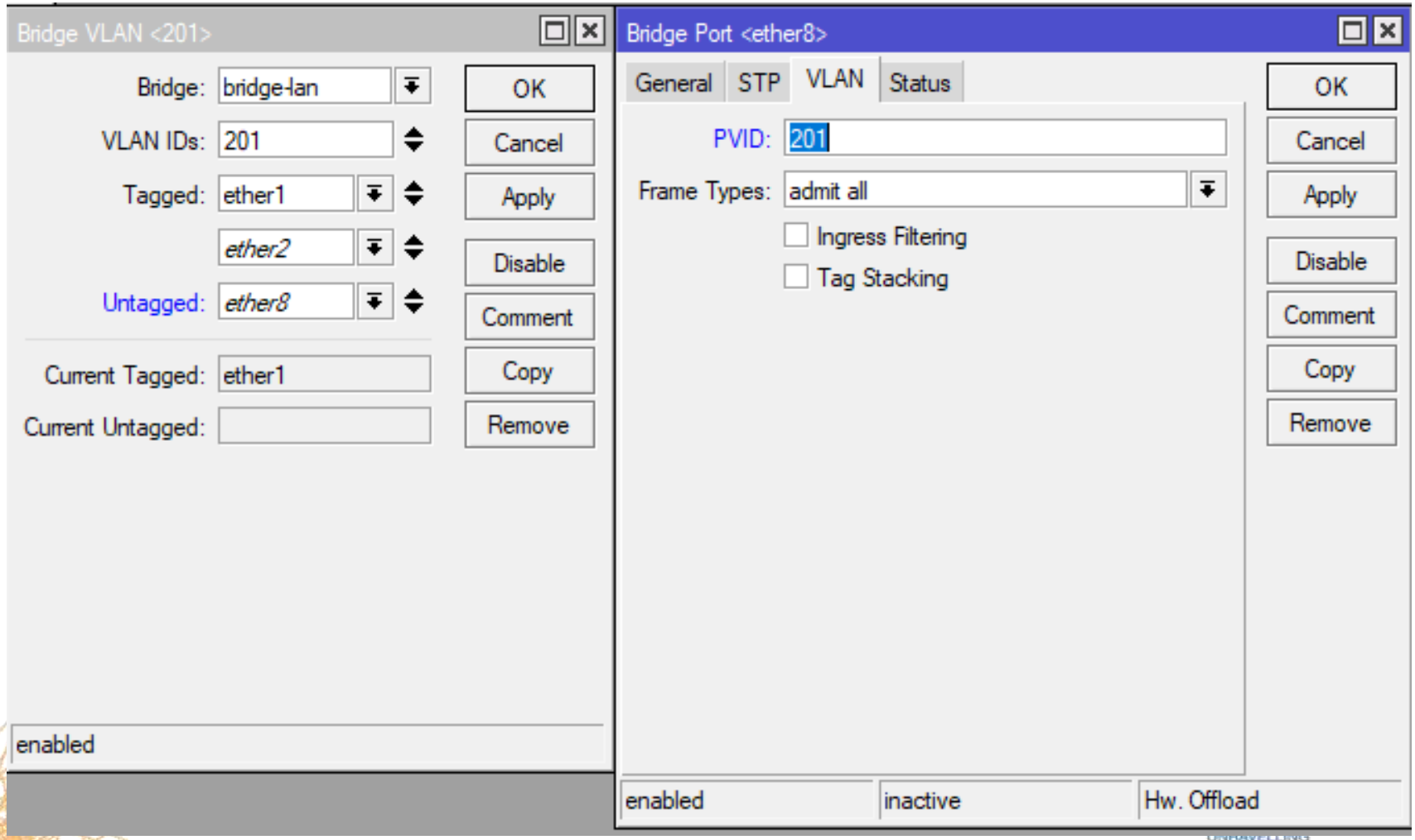
- Next we will configure Port 7 as a Data VLAN port and set the PVID on port 7





Untagged Ports

- And Port8 untagged in VLAN201 and PVID on port 8



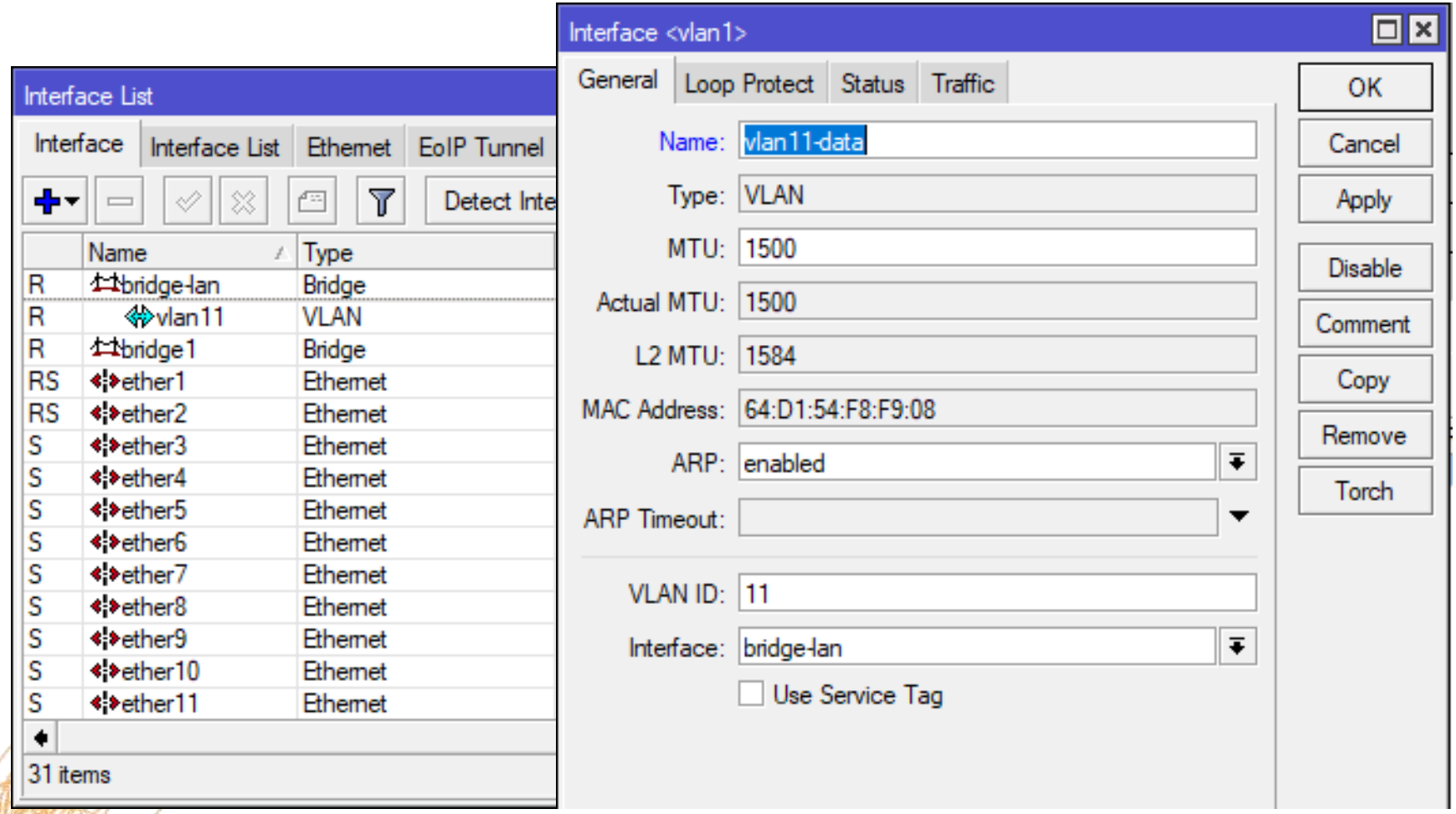
Management Interface

- We need an IP Address on the switch so we can manage it

- For this example we will manage the switch from the Data VLAN (VLAN 11)

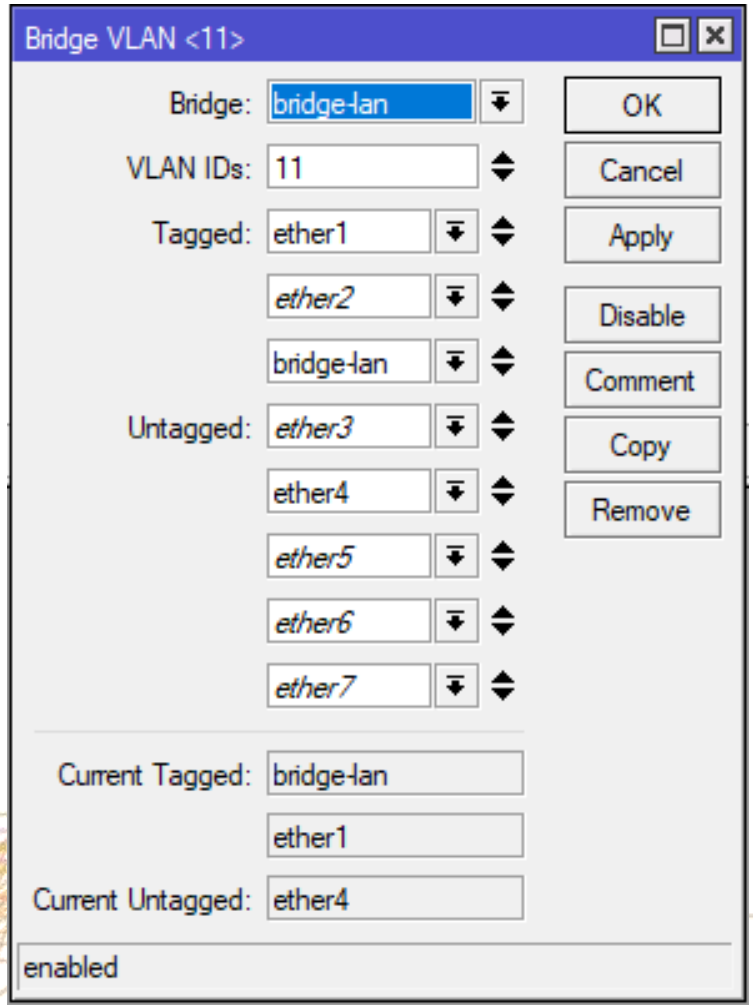
Management Interface

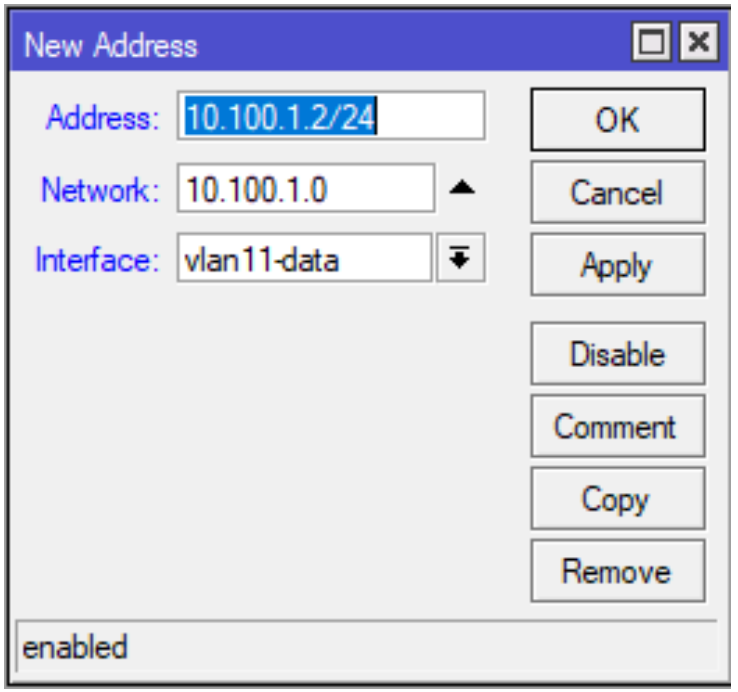
- Create a VLAN interface on the bridge interface



Management Interface

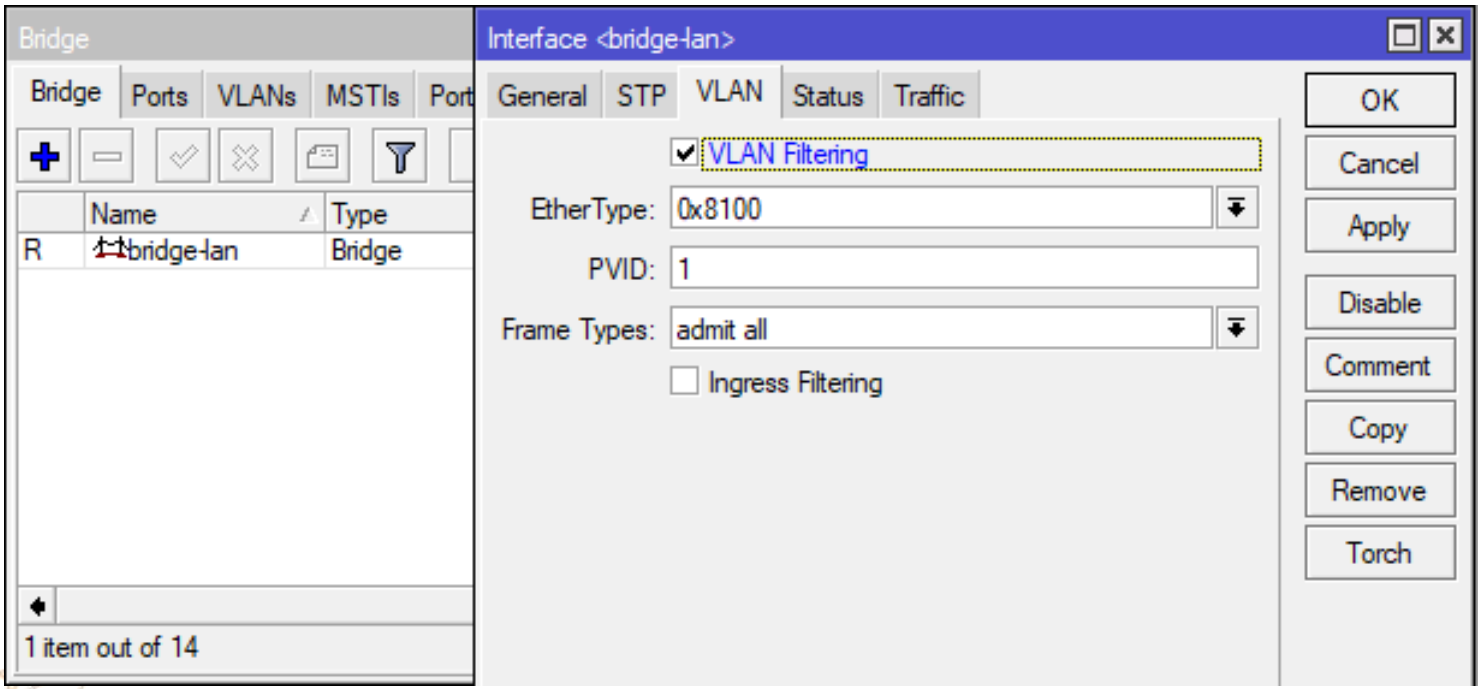
- Add bridge as a Tagged Port on the VLAN11 – IMPORTANT
- Add an IP Address to the VLAN interface





Enable VLAN filtering

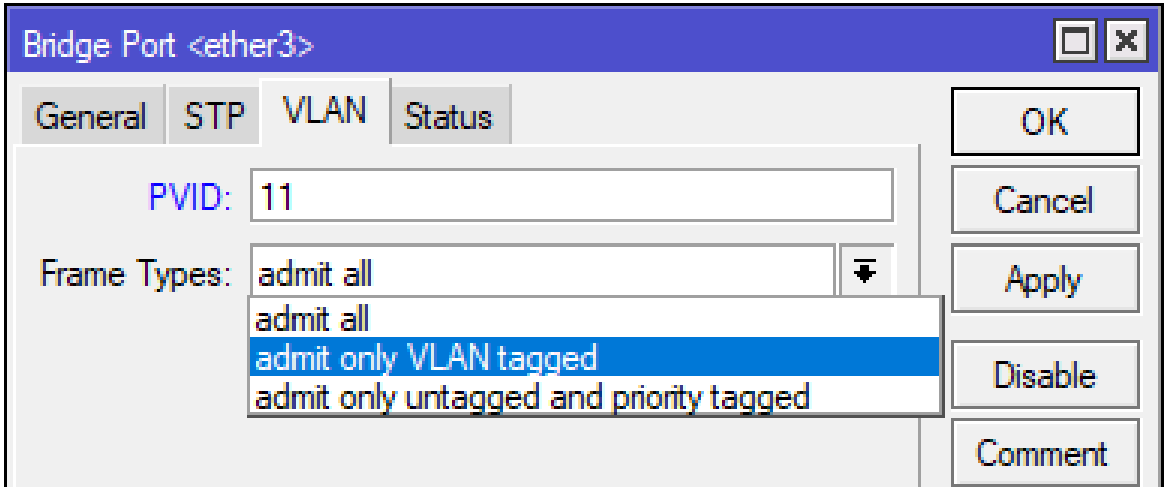
- Now we have finished the VLAN setup we can Enable VLAN Filtering
- We can also enable Ingress Filtering. This will only allow VLANs we have configured into the bridge



Ingress Filtering

- Checks Ingress Port and VLAN ID in bridge VLAN table.

- Specify what frames types to permit
  - Admit all (default)
  - Admit only untagged and priority tagged
  - Admit only VLAN tagged



BirchenallHowden

information | communication | technology

Layer 2 Misconfigurations

Layer 2 Misconfigurations

- Here are a few common incorrect Layer 2 configurations and then the correct way to do it.

- The following slides show the **INCORRECT** setup follow by the **correct** setup

- Do not follow the incorrect setup!

Layer 2 Misconfigurations
Multiple Bridges

Scenario:-

- You are using a CRS3xx series switch
- You need to isolate certain ports from each other.
- You decide to create 2 bridges.
- As each bridge is a separate Layer 2 domain you have isolated the ports from each other

Symptoms

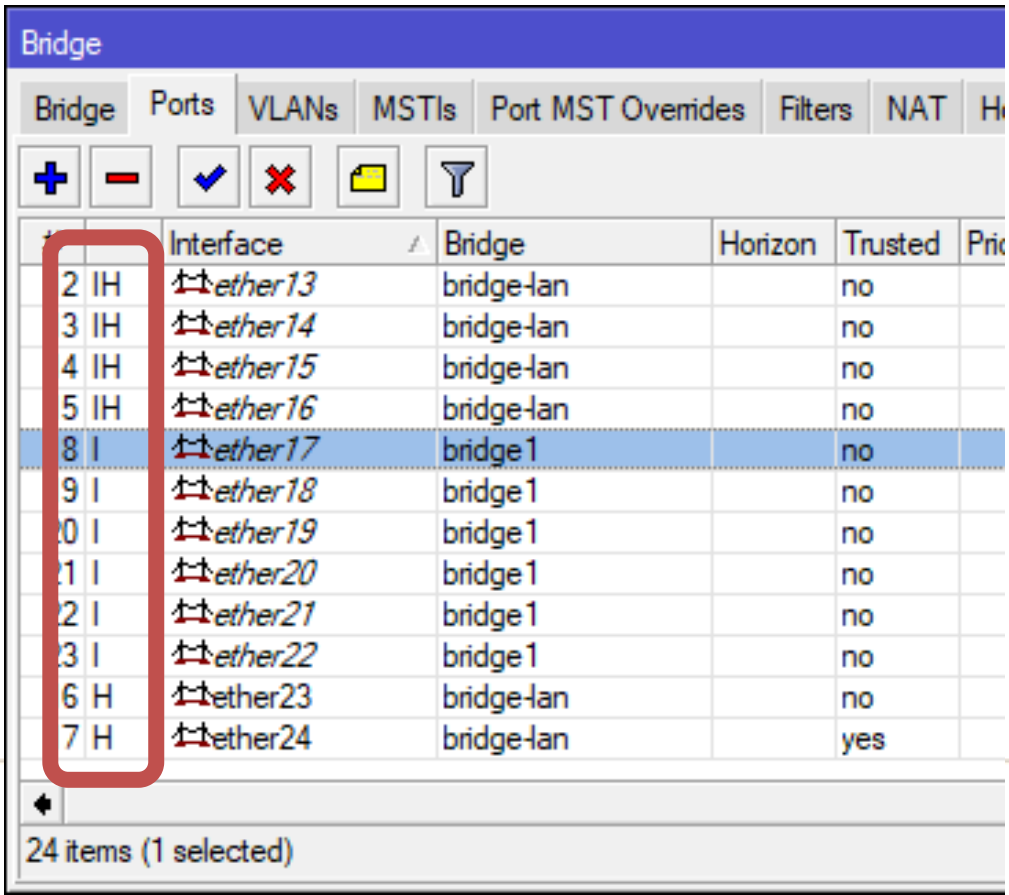
- You start to use your switch and notice that one set of ports work at wire speed and give full throughput. However the other set of ports do not.

Layer 2 Misconfigurations
Multiple Bridges

What has happened?

- You test further and notice that the CPU is very high when traffic flows slowly though one of the bridges.

- You look at your configuration
- See how the H flag is not set for ports in bridge1



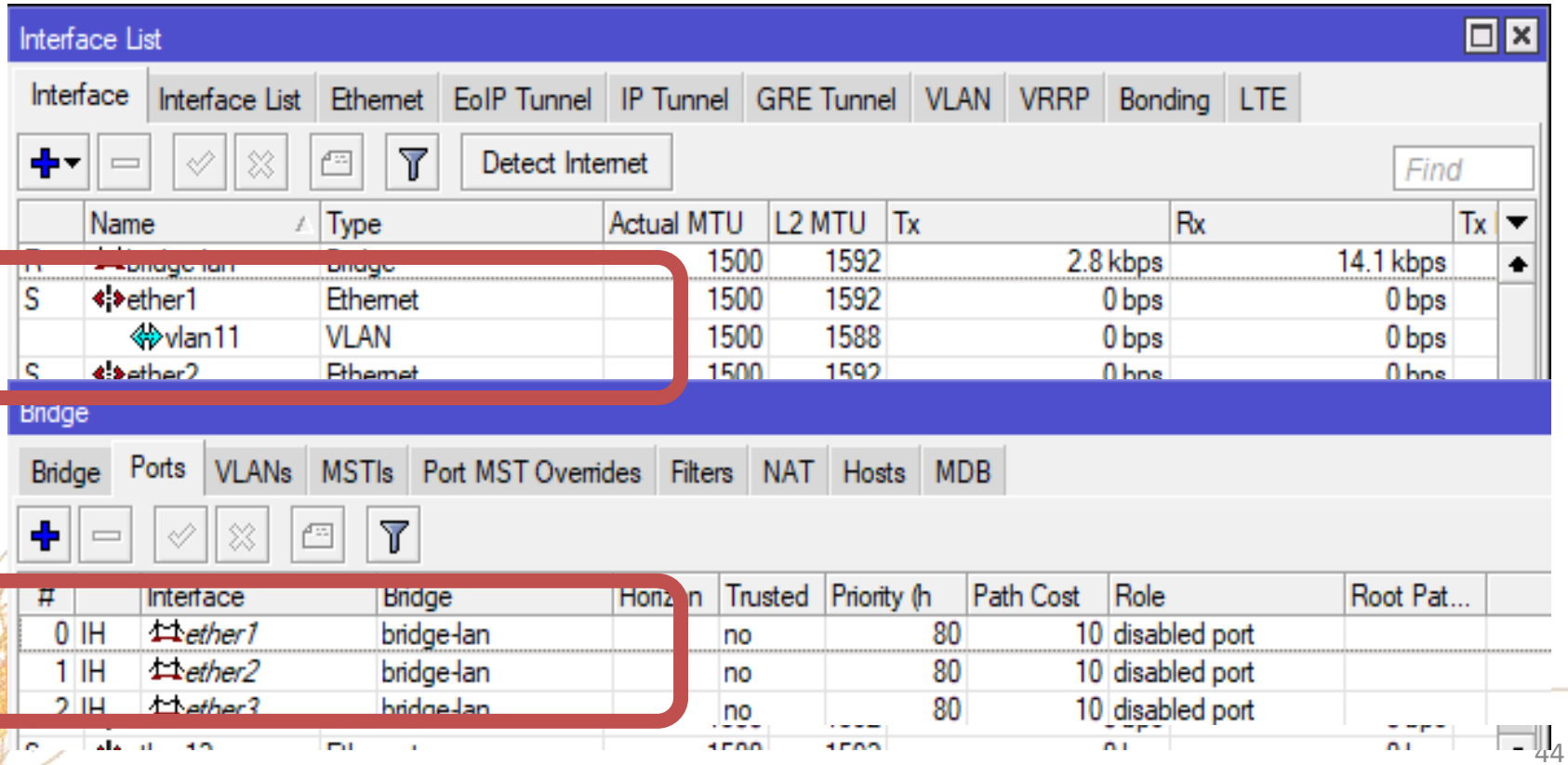
Layer 2 Misconfigurations
Multiple Bridges

- Only some devices support more than 1 hardware offloaded bridge
- CRS1xx\2xx series switch support up to 7 bridges using hardware offloading
- Consider reconfiguration of your network to use VLANs and VLAN filtering and port isolation.

Layer 2 Misconfigurations
VLAN – on slave interface

Scenario

- You want a DHCP server to give out IP addresses only to a certain tagged port



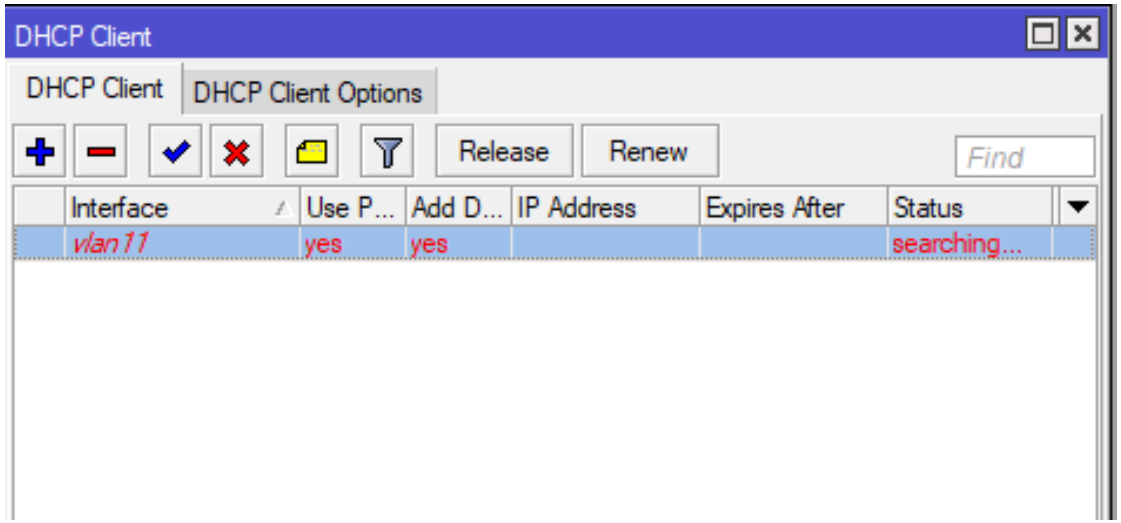
Layer 2 Misconfigurations
VLAN – on slave interface

Problem

- VLAN interface will never capture any traffic at all since it is immediately forwarded to the master interface before any packet processing is done.

Symptoms

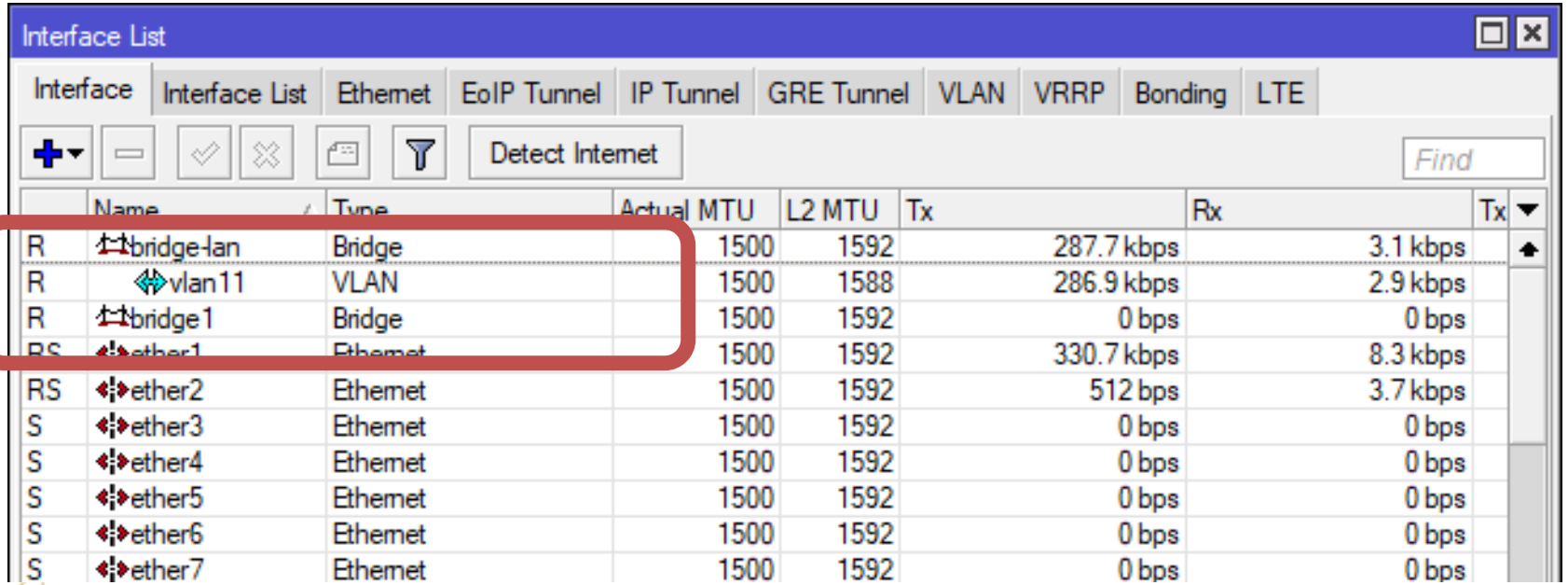
- DHCP Client / Server not working properly
- Device unreachable



Layer 2 Misconfigurations
VLAN – on slave interface

Solution

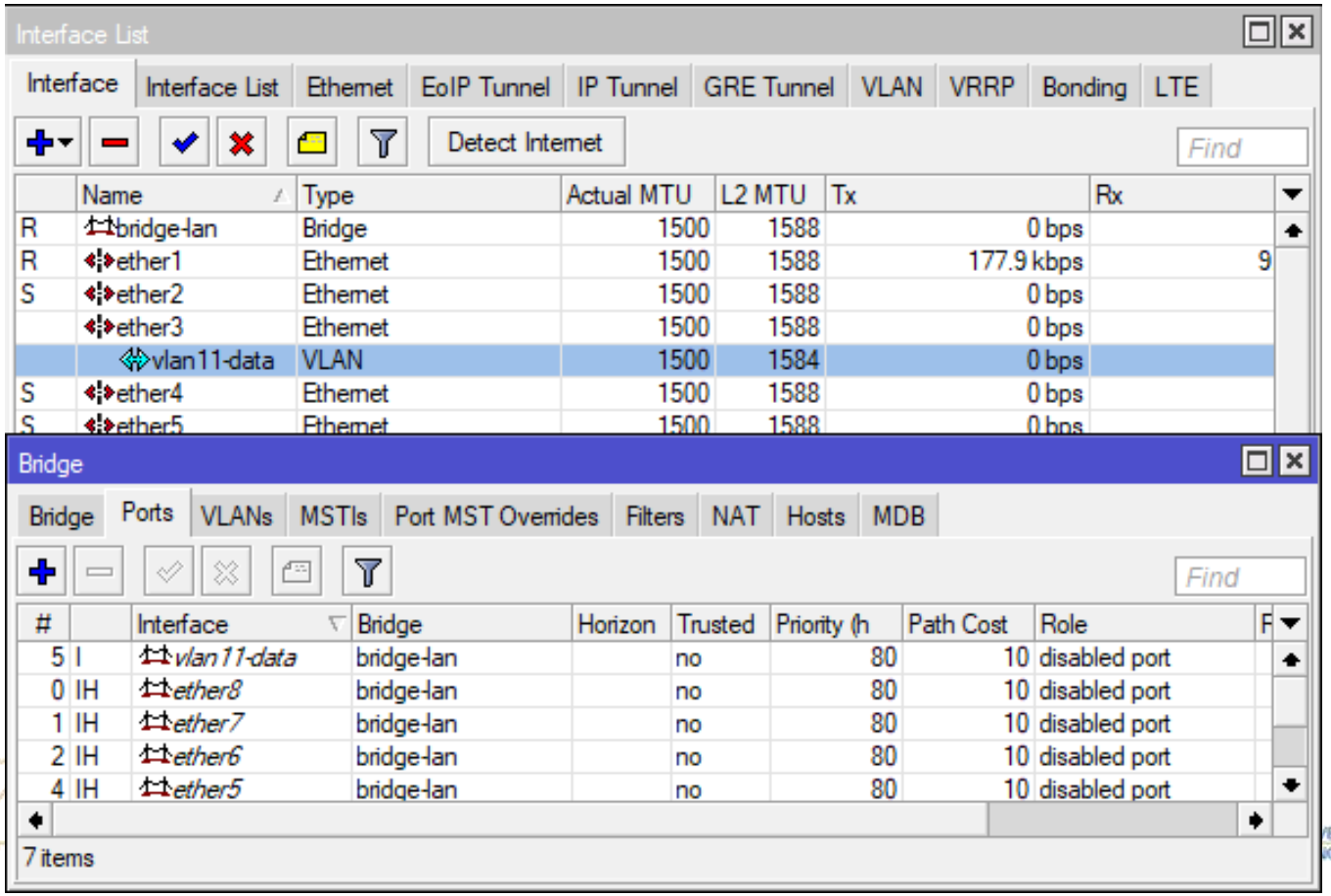
- Change the VLAN to the bridge



Layer 2 Misconfigurations
VLAN in a Bridge with Physical Interface

Scenario

- You want to send tagged traffic out of a physical port



Layer 2 Misconfigurations
VLAN in a Bridge with Physical Interface

Problem

- This will work in most cases
- It will cause problems if also using STP/RSTP with other vendor's switches because BPDUs are tagged
- Not all switches can understand tagged BPDUs

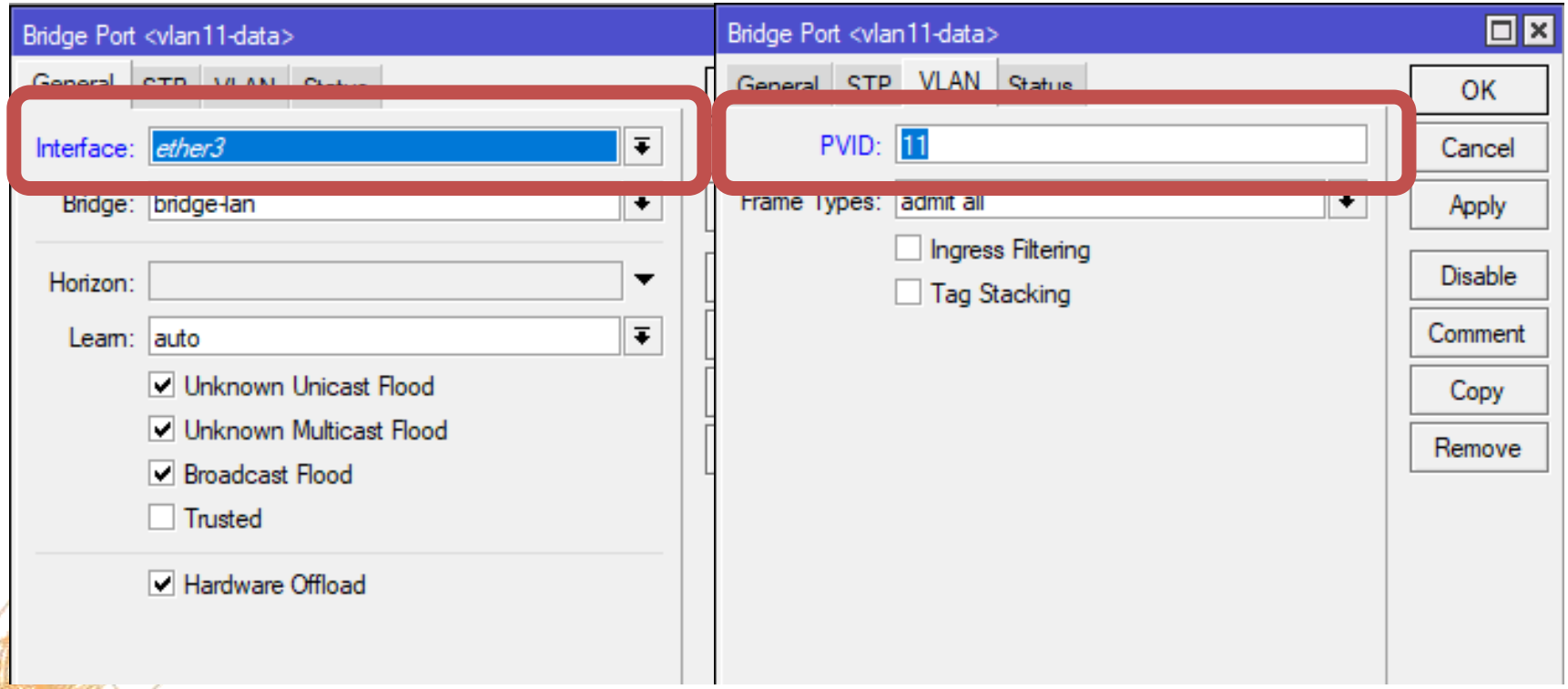
Symptoms

- Port blocking by RSTP
- Port flapping
- Network loops

Layer 2 Misconfigurations
VLAN in a Bridge with Physical Interface

Solution

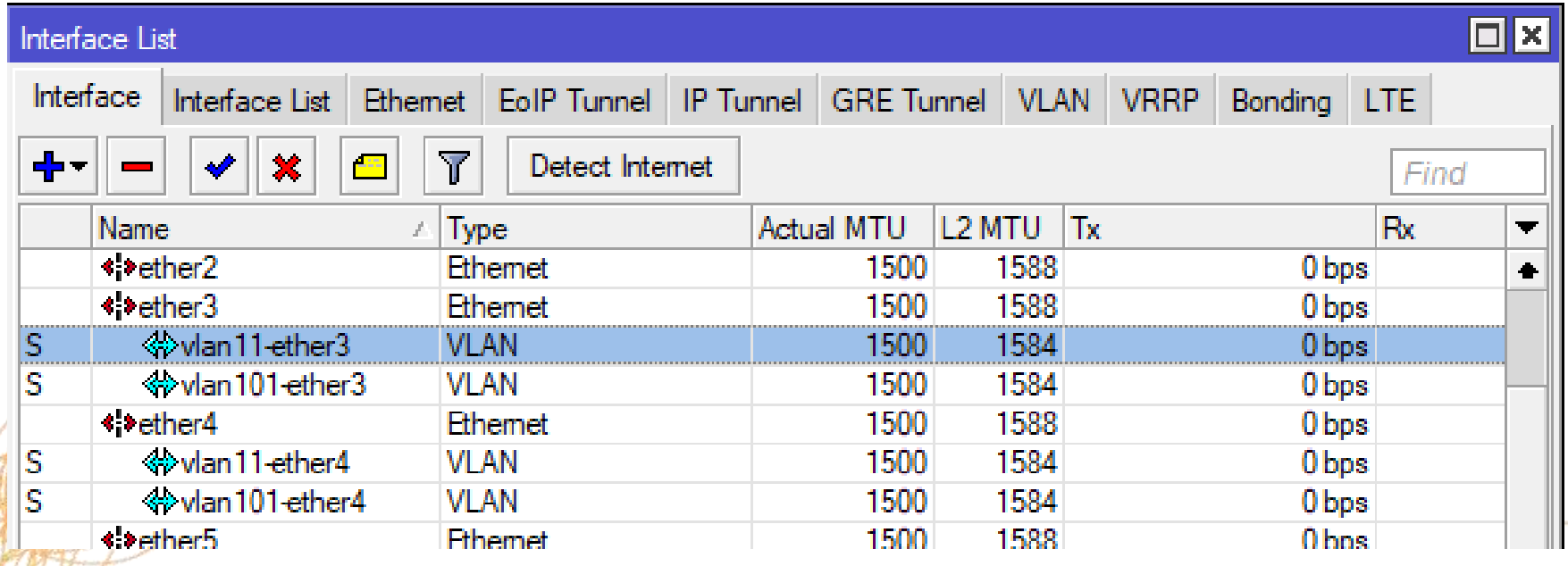
- Use VLAN filtering as we have just looked at



Layer 2 Misconfigurations
Bridged VLANs

Scenario

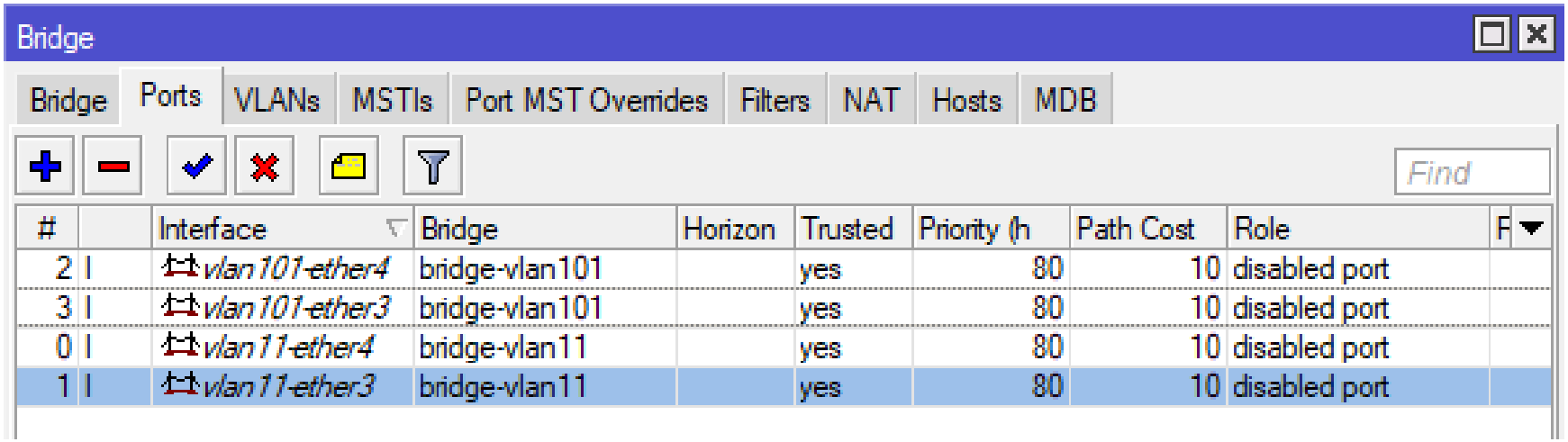
- You are using VLANs to isolate Layer 2 domains connected to your switch
- You create VLAN interfaces on each physical interface



Layer 2 Misconfigurations
Bridged VLANs

Scenario (cont..)

- Put VLAN interface into a separate bridge for each VLAN



Layer 2 Misconfigurations
Bridged VLANs

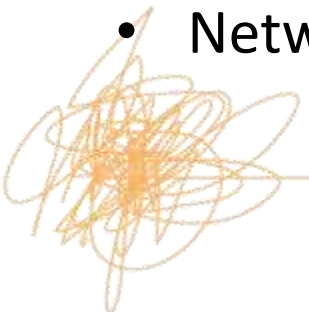
Problem

- You notice parts of the network are unreachable
- You notice links keep flapping.

- This is due to sending out tagged BPDU packets

Symptoms

- Port blocking by (R)STP
- Port flapping
- Network inaccessible



Layer 2 Misconfigurations
VLAN in a bridge with Physical interface

Solution

a) Easiest solution is to disable (R)STP on the bridge

Or Even still use recommend to rewrite your config and

b) Use VLAN filtering as we have just looked at

BirchenallHowden

information | communication | technology

New Features in 6.43

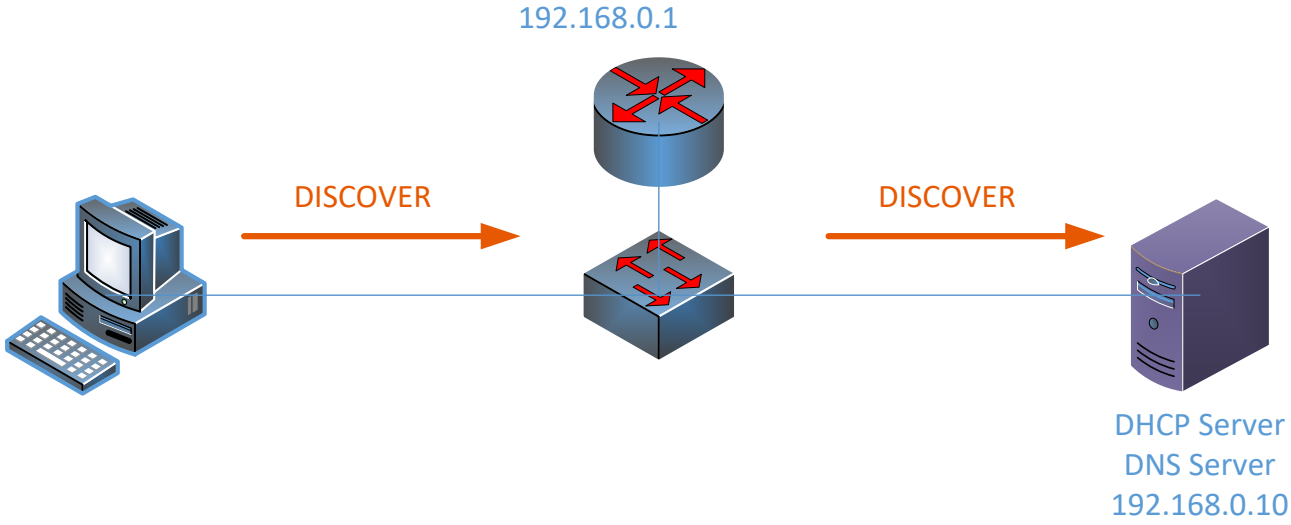
DHCP Snooping

- Since 6.43rc56, bridge supports DHCP Snooping
- DHCP Snooping is a Layer 2 Security feature
- This limits the ports on which DHCP Offer packets are received

Rogue DHCP Server

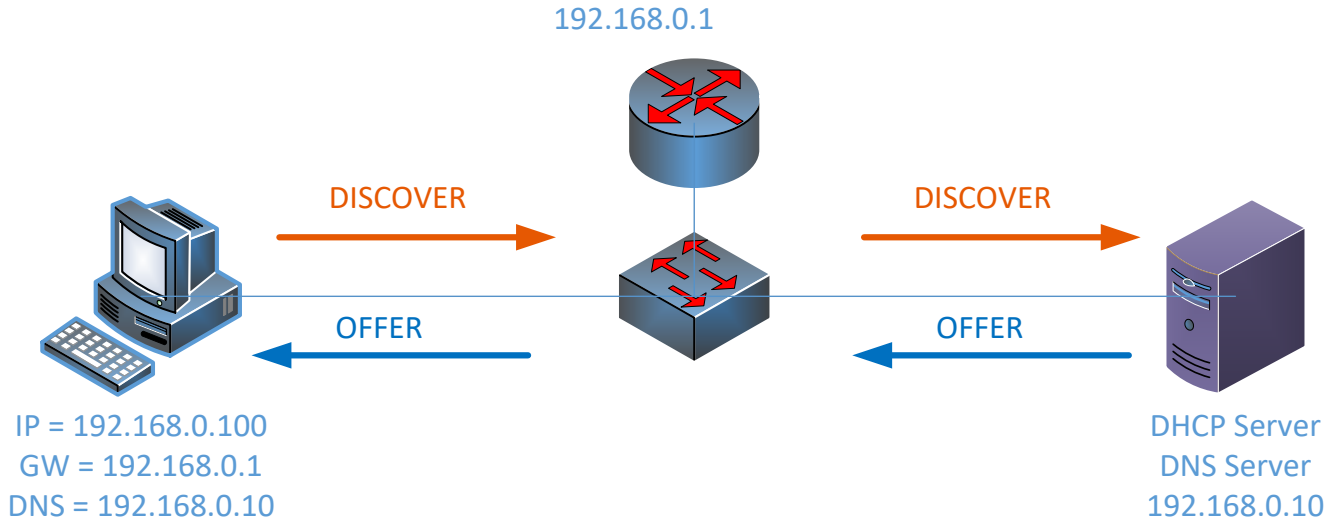
- Rogue DHCP Server could provide legitimate clients with bogus TCP/IP Information
- This could prevent them communicating on the network as their address is incorrect
- This could change their gateway address to a rogue gateway
- They could obtain rogue DNS server settings

DHCP Server Spoofing



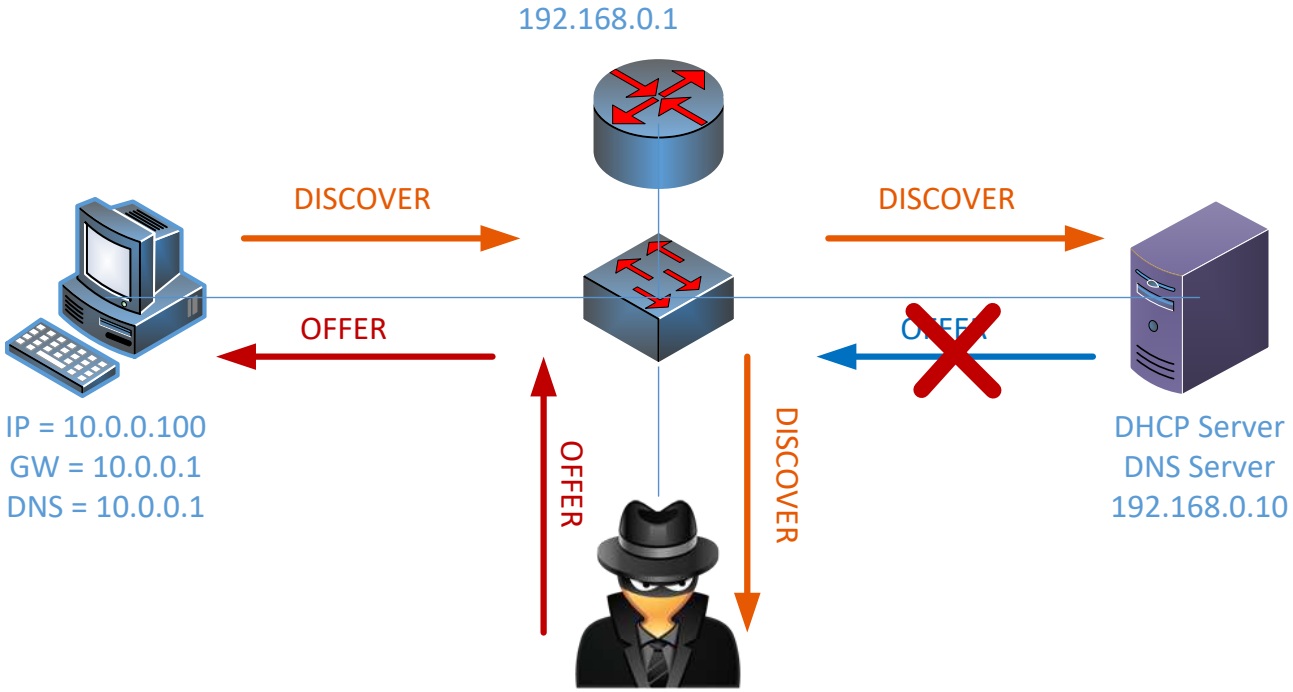
1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.

DHCP Server Spoofing



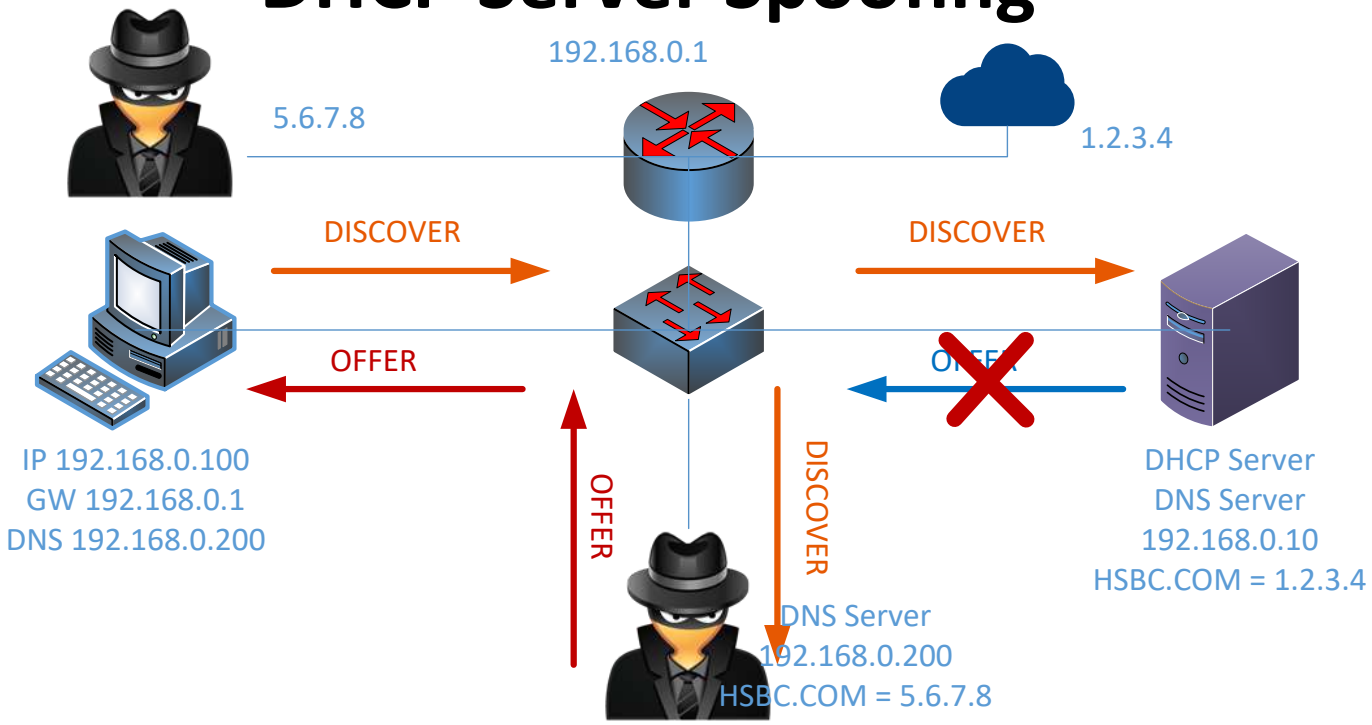
1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.
2. Server sends a DHCP Reply.

DHCP Server Spoofing



1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.
2. Server sends a DHCP Reply.
3. Fake DHCP server can also receive the DHCP DISCOVERY packet and send a DHCP Reply.
4. Attacker could give out incorrect IP addresses.

DHCP Server Spoofing



1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.
2. Server sends a DHCP Reply.
3. Fake DHCP server can also receive the DHCP DISCOVERY packet and send a DHCP Reply.
4. Attacker could give out incorrect IP addresses.
5. Attacker could give out incorrect DNS Server.

DHCP Snooping – HW offloading

- Depending on the model or the switch chip, using DHCP Snooping will disable bridge HW offloading

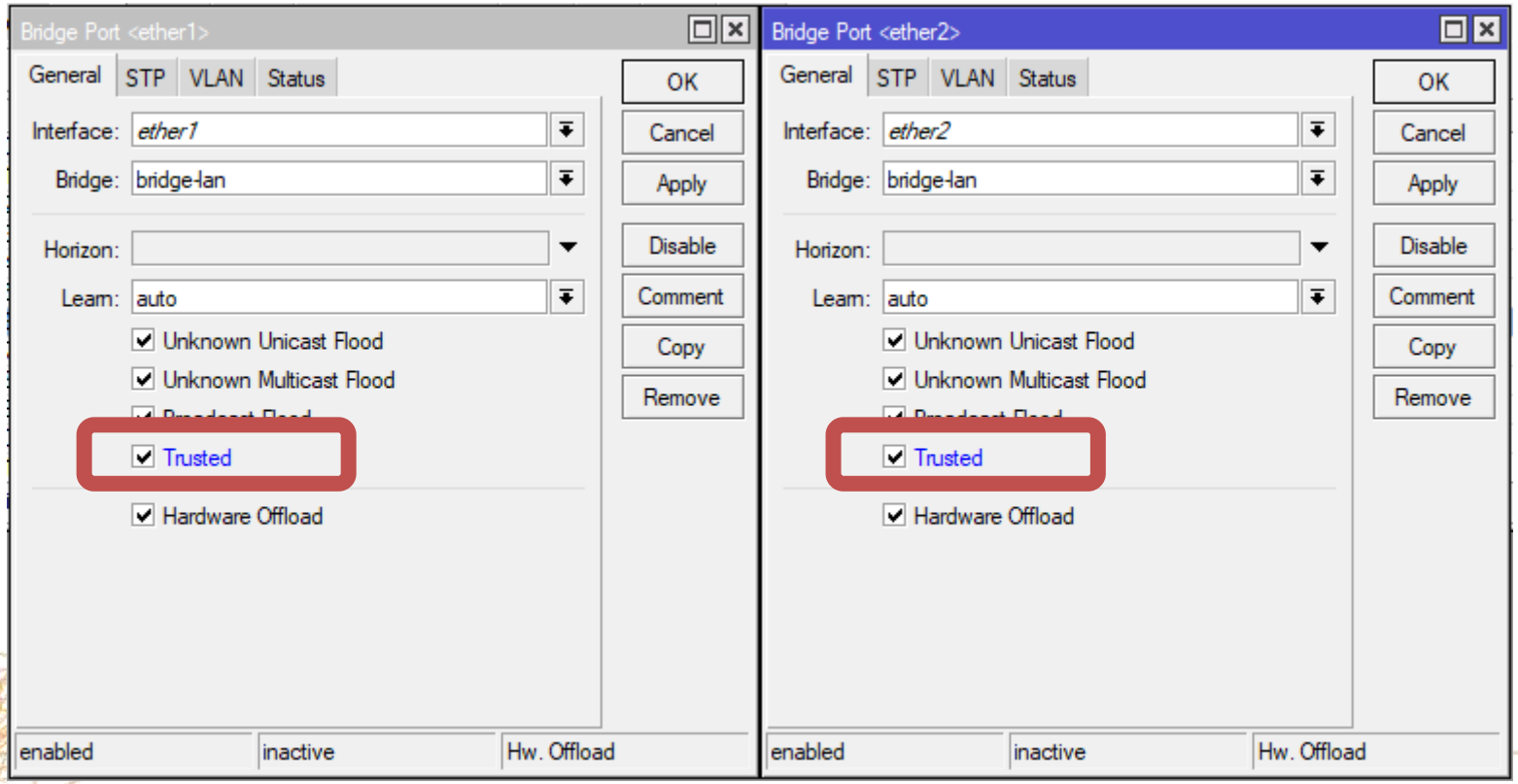
RouterBOARD model	HW offloading
CRS3xx series	✓
CRS1xx/CRS2xx series	×

Switch Chip model	
QCA8337	×
AR8327	×
AR8227	×
AR8316	×
AR7240	×
RTL8367	×
ICPlus175D	×

https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features#Bridge_Hardware_Offloading

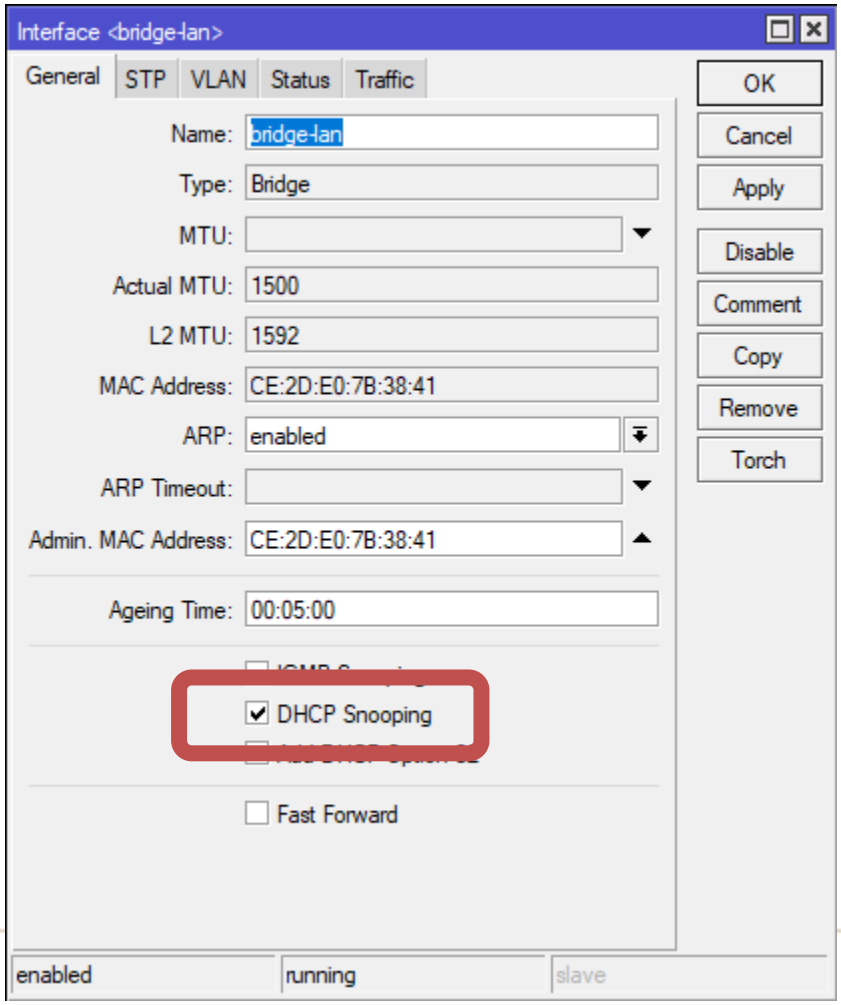
Bridge DHCP Snooping

- Create Trusted Port for port(s) which you want to allow DHCP ACK messages on
- This is normally ports with DHCP server connected and ports with other switches on. In this setup its Ether1 and Ether2



Bridge DHCP Snooping

- Once ports are configured
- Turn on DHCP Snooping on the bridge



Thank you for Listening

References

- Visio Templates – Mikrotik Forum user FernandoSuperGG
  https://forum.mikrotik.com/viewtopic.php?f=2&t=120957

- MikroTik Manual
  https://wiki.mikrotik.com/wiki/Manual:CRS_Router#CRS3xx_series_switches
  https://wiki.mikrotik.com/wiki/Manual:CRS3xx_series_switches
  https://wiki.mikrotik.com/wiki/Manual:Layer2_misconfiguration
  https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge
  https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features#Bridge_Hardware_Offloading