

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

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!



Birchena**ll**Howden

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

Interface <ether3>

General Ethernet Loop Protect Overall Stats Rx Stats ...

Name: ether3

Type: Ethernet

MTU: 1500

Actual MTU: 1500

L2 MTU: 1598

Max L2 MTU: 4074

MAC Address: 4C:5E:0C:C2:0F:79

ARP: enabled

ARP Timeout:

Master Port: ether2

Bandwidth (Rx/Tx): unlimited / unlimited

Switch: switch1

OK

Cancel

Apply

Disable

Comment

Torch

Cable Test

Blink

Reset MAC Address

Reset Counters

enabled running slave no link

Interfaces 6.41 Onwards

Interface <ether3>

General PoE Ethernet Loop Protect Overall Stats ...

Name: ether3

Type: Ethernet

MTU: 1500

Actual MTU: 1500

L2 MTU: 1588

Max L2 MTU: 9204

MAC Address: 64:D1:54:F8:F9:09

ARP: enabled

ARP Timeout:

OK

Cancel

Apply

Disable

Comment

Torch

Power Cycle

Cable Test

Blink

Reset MAC Address

Reset Counters

enabled running slave no link

Bridge hardware offloading

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

The screenshot displays two windows from a network configuration tool. The left window, titled 'Bridge', shows a table of bridge ports. The right window, titled 'Bridge Port <ether3>', shows the configuration for a specific port.

Index	Type	Interface	Bridge
0	IH	ether1	bridge-lan
1	IH	ether2	bridge-lan
2	IH	ether3	bridge-lan
3	H	ether4	bridge-lan
4	IH	Inactive, H - Hw. Offload	bridge-lan
5	IH	ether6	bridge-lan
6	IH	ether7	bridge-lan
7	IH	ether8	bridge-lan
8	IH	ether9	bridge-lan
9	IH	ether10	bridge-lan
0	IH	ether11	bridge-lan
1	IH	ether12	bridge-lan
2	IH	ether13	bridge-lan
3	IH	ether14	bridge-lan
4	IH	ether15	bridge-lan
5	IH	ether16	bridge-lan
6	IH	ether23	bridge-lan
7	H	ether24	bridge-lan
8	I	ether17	unknown

The right window, 'Bridge Port <ether3>', has the following settings:

- Interface: ether3
- Bridge: bridge-lan
- Horizon: (empty)
- Learn: auto
- Unknown Unicast Flood
- Unknown Multicast Flood
- Broadcast Flood
- Trusted
- Hardware Offload

At the bottom of the right window, there are three status indicators: 'enabled', 'inactive', and 'Hw. Offload' (which is highlighted with a red box).

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 losing 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

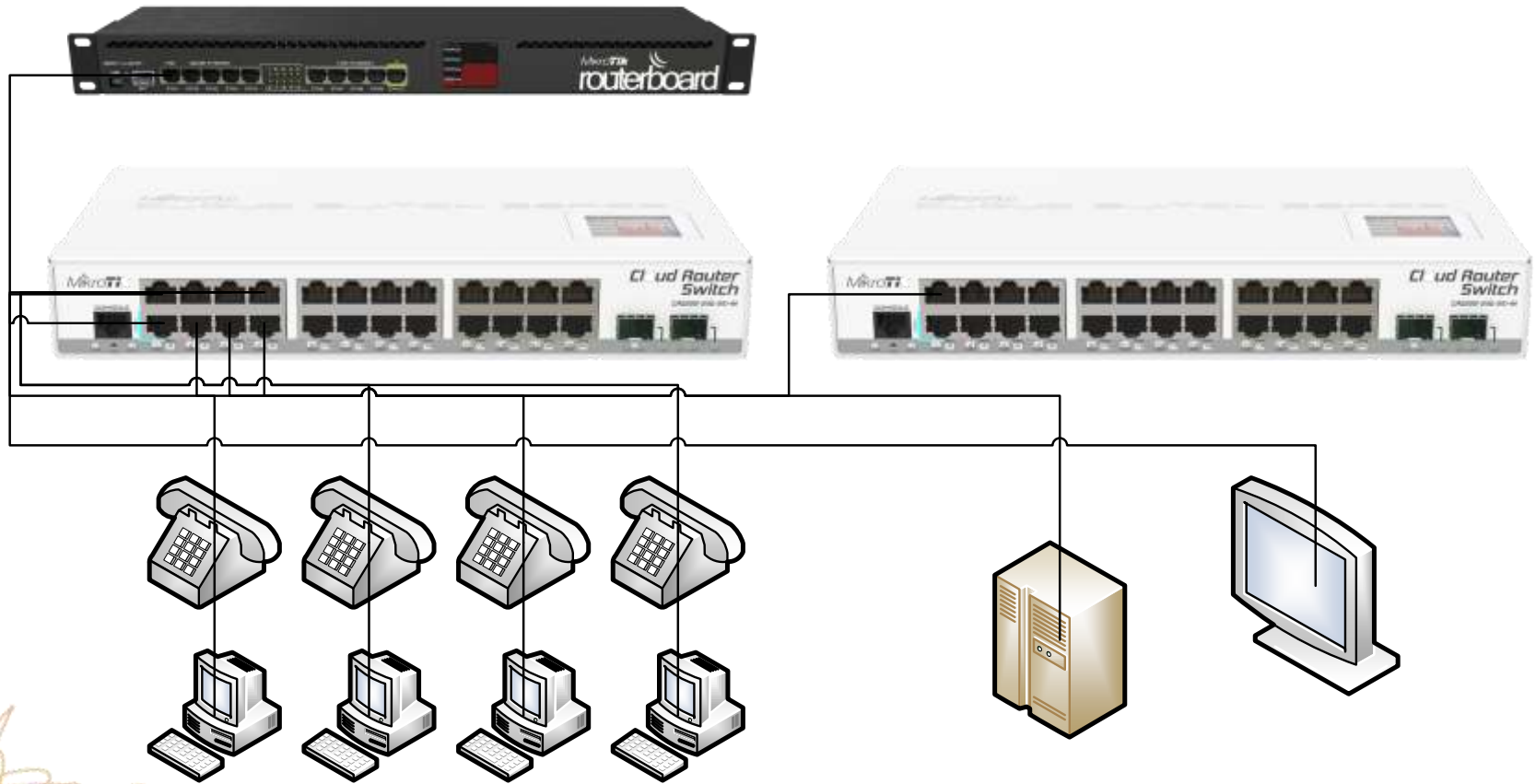
- Depending on the model or the switch chip, different features will disable bridge HW offloading

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



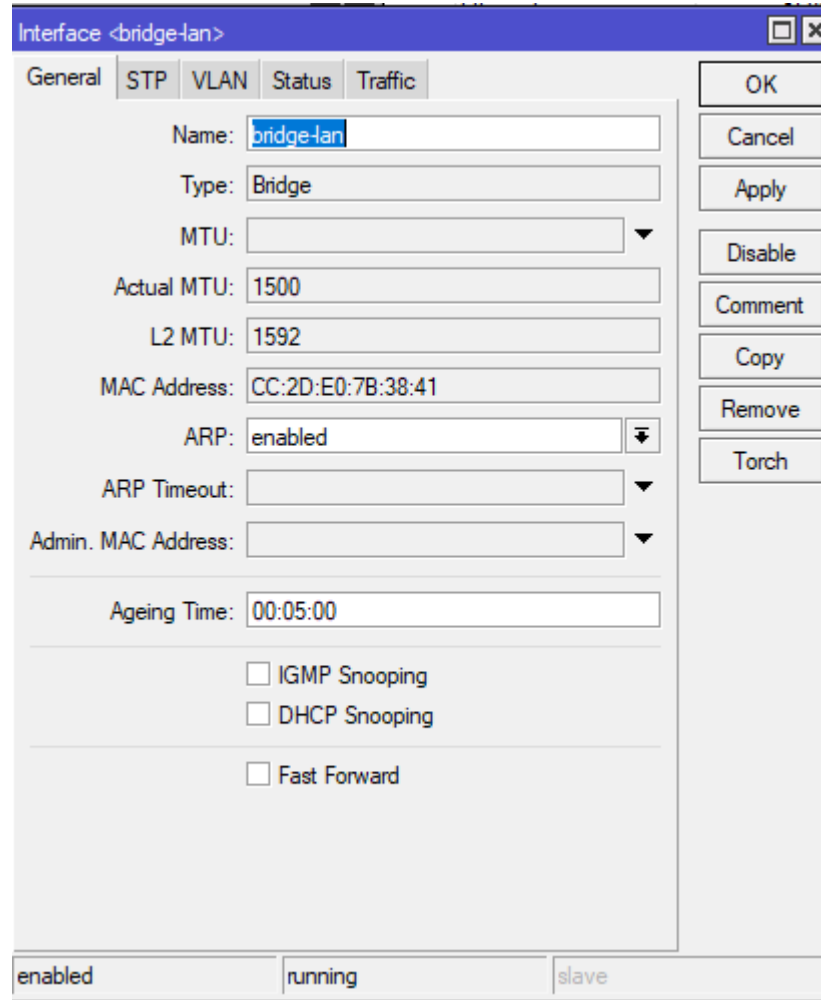
Bridge – VLAN Setup

- 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

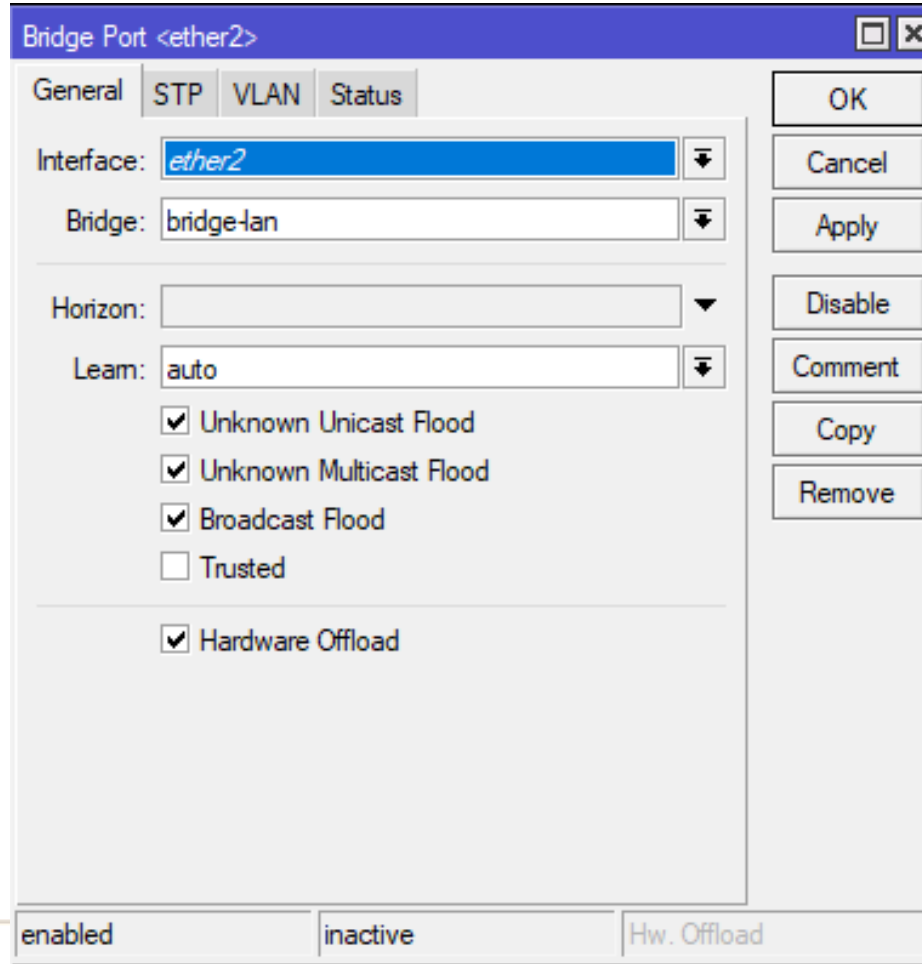
- Create a bridge



The screenshot shows a configuration window titled "Interface <bridge-lan>". It has tabs for "General", "STP", "VLAN", "Status", and "Traffic", with "General" selected. The "Name" field is "bridge-lan", "Type" is "Bridge", "MTU" is empty, "Actual MTU" is "1500", "L2 MTU" is "1592", "MAC Address" is "CC:2D:E0:7B:38:41", "ARP" is "enabled", "ARP Timeout" is empty, "Admin. MAC Address" is empty, and "Ageing Time" is "00:05:00". There are checkboxes for "IGMP Snooping", "DHCP Snooping", and "Fast Forward", all of which are unchecked. On the right side, there are buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", and "Torch". At the bottom, there are three status indicators: "enabled", "running", and "slave".

VLAN Configuration

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



Bridge Port <ether2>

General STP VLAN Status

Interface: ether2

Bridge: bridge-lan

Horizon:

Learn: auto

Unknown Unicast Flood

Unknown Multicast Flood

Broadcast Flood

Trusted

Hardware Offload

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled inactive Hw. Offload

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

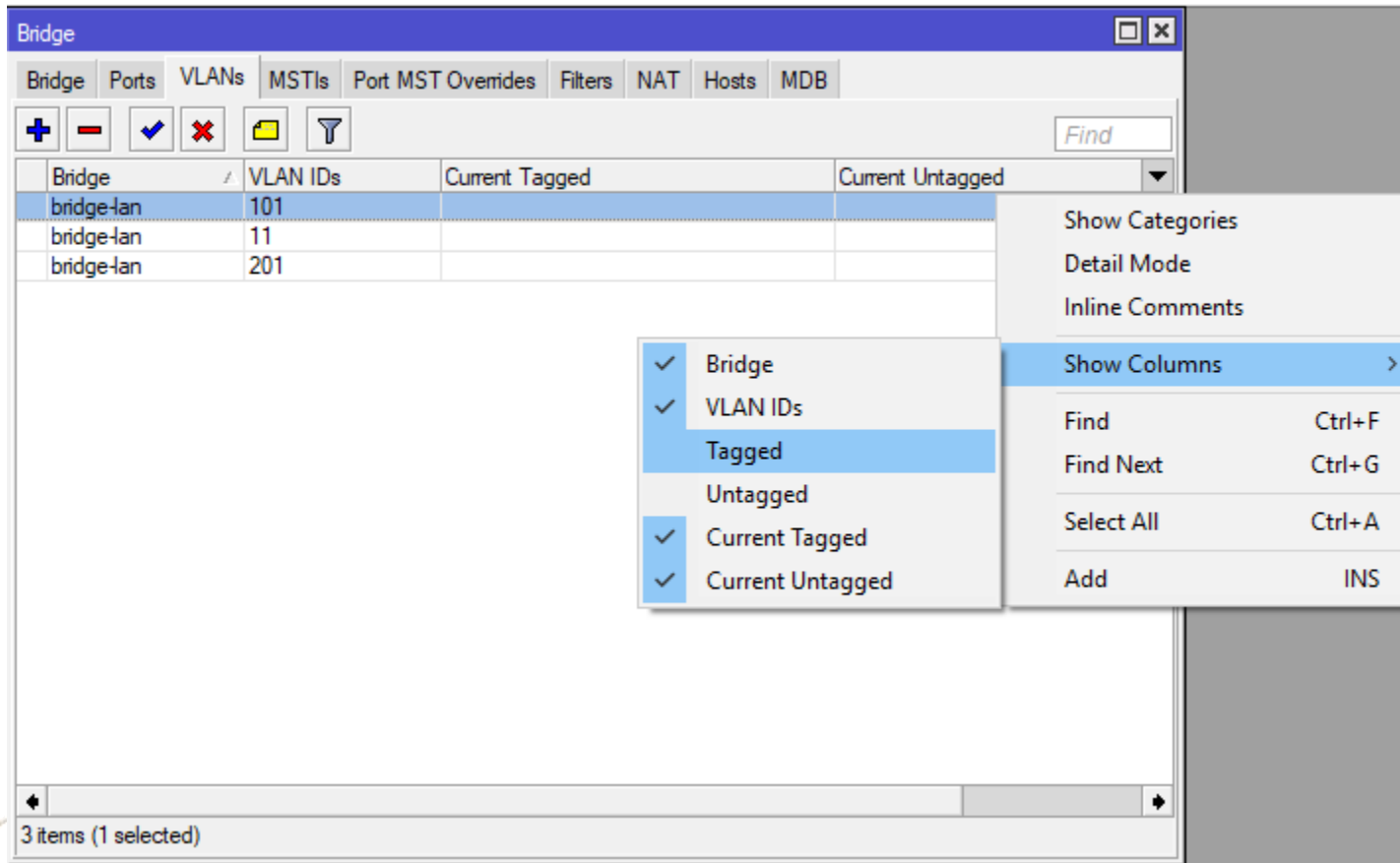
- Create VLANs and add ether1 and ether2 as tagged

The image displays three sequential screenshots of a network configuration interface for creating VLANs. Each window is titled 'Bridge VLAN <ID>' and contains the following fields and controls:

- Bridge:** A dropdown menu set to 'bridge-lan'.
- VLAN IDs:** A text input field containing the VLAN ID (11, 101, or 201).
- Tagged:** Two dropdown menus, both set to 'ether1' and 'ether2'.
- Untagged:** An empty text input field.
- Buttons:** 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.
- Status:** A label at the bottom of each window indicating the state as 'enabled'.

VLAN Configuration

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



The screenshot shows the WinBox Bridge configuration window. The 'VLANs' tab is active, displaying a table with the following data:

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge-lan	101		
bridge-lan	11		
bridge-lan	201		

A context menu is open over the table, showing the following options:

- ✓ Bridge
- ✓ VLAN IDs
- Tagged
- Untagged
- ✓ Current Tagged
- ✓ Current Untagged

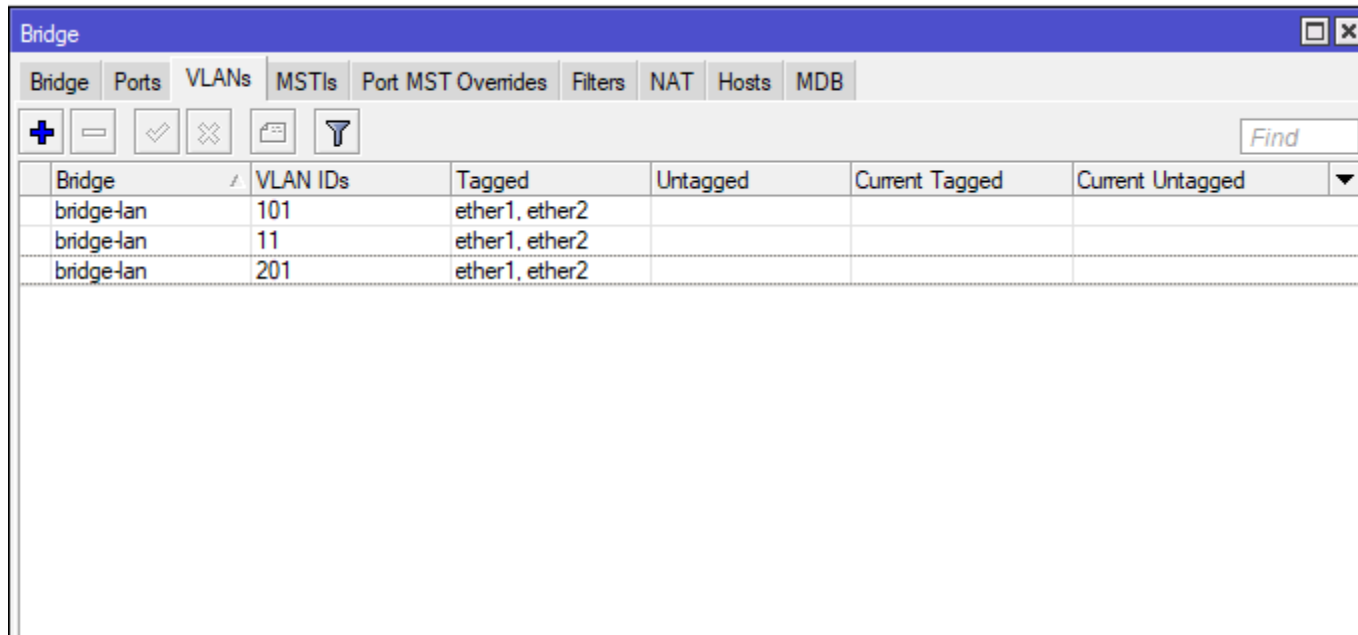
The 'Show Columns' option is highlighted, and a submenu is open showing the following options:

- Show Categories
- Detail Mode
- Inline Comments
- Show Columns >
- Find Ctrl+F
- Find Next Ctrl+G
- Select All Ctrl+A
- Add INS

The status bar at the bottom indicates '3 items (1 selected)'. There is a large orange scribble in the bottom left corner of the image.

VLAN Configuration

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



Bridge	VLAN IDs	Tagged	Untagged	Current Tagged	Current Untagged
bridge-lan	101	ether1, ether2			
bridge-lan	11	ether1, ether2			
bridge-lan	201	ether1, ether2			

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



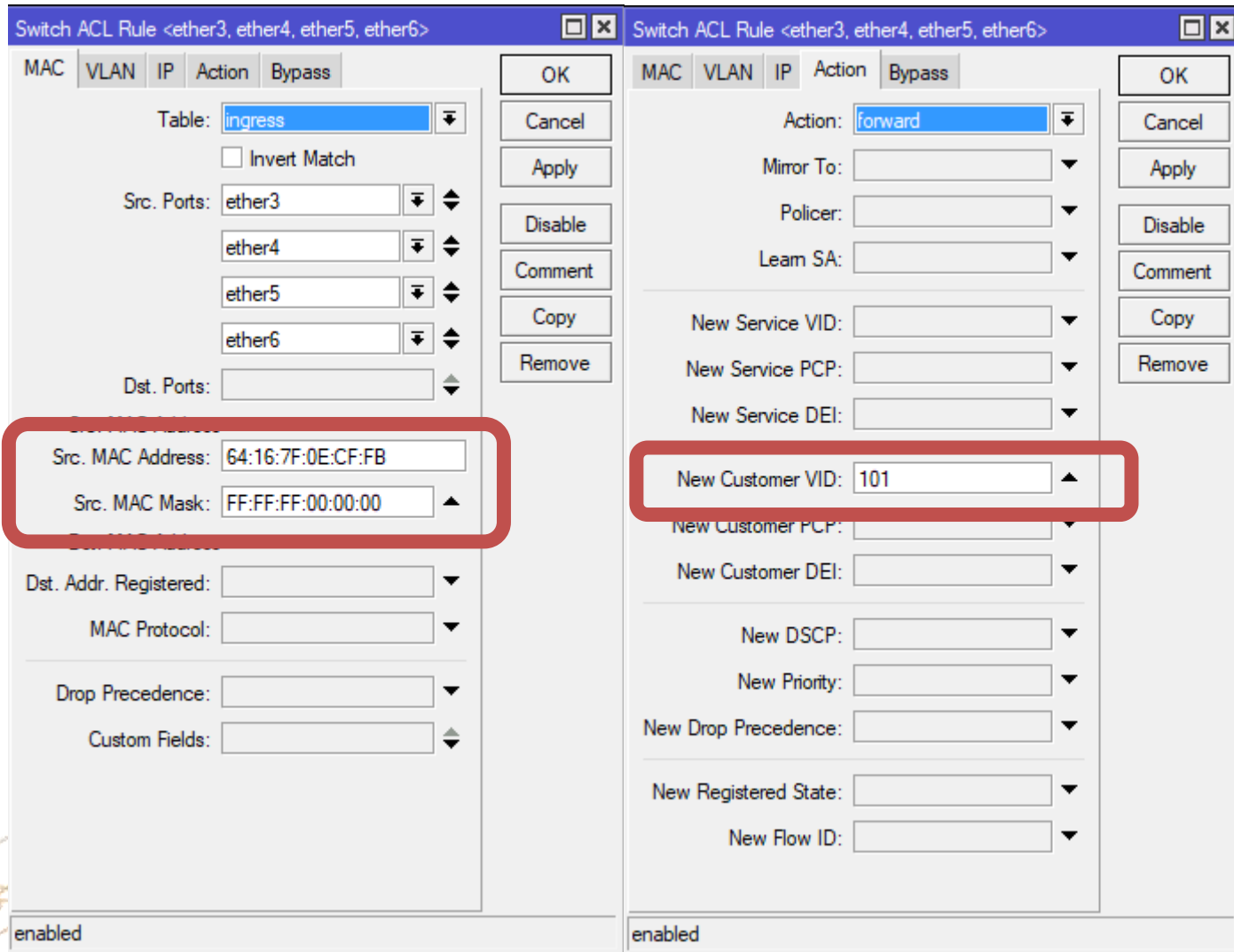
MAC based VLAN

- 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



The image displays two side-by-side screenshots of a network configuration interface for creating a Switch ACL rule. Both windows are titled "Switch ACL Rule <ether3, ether4, ether5, ether6>".

Left Screenshot (MAC Tab):

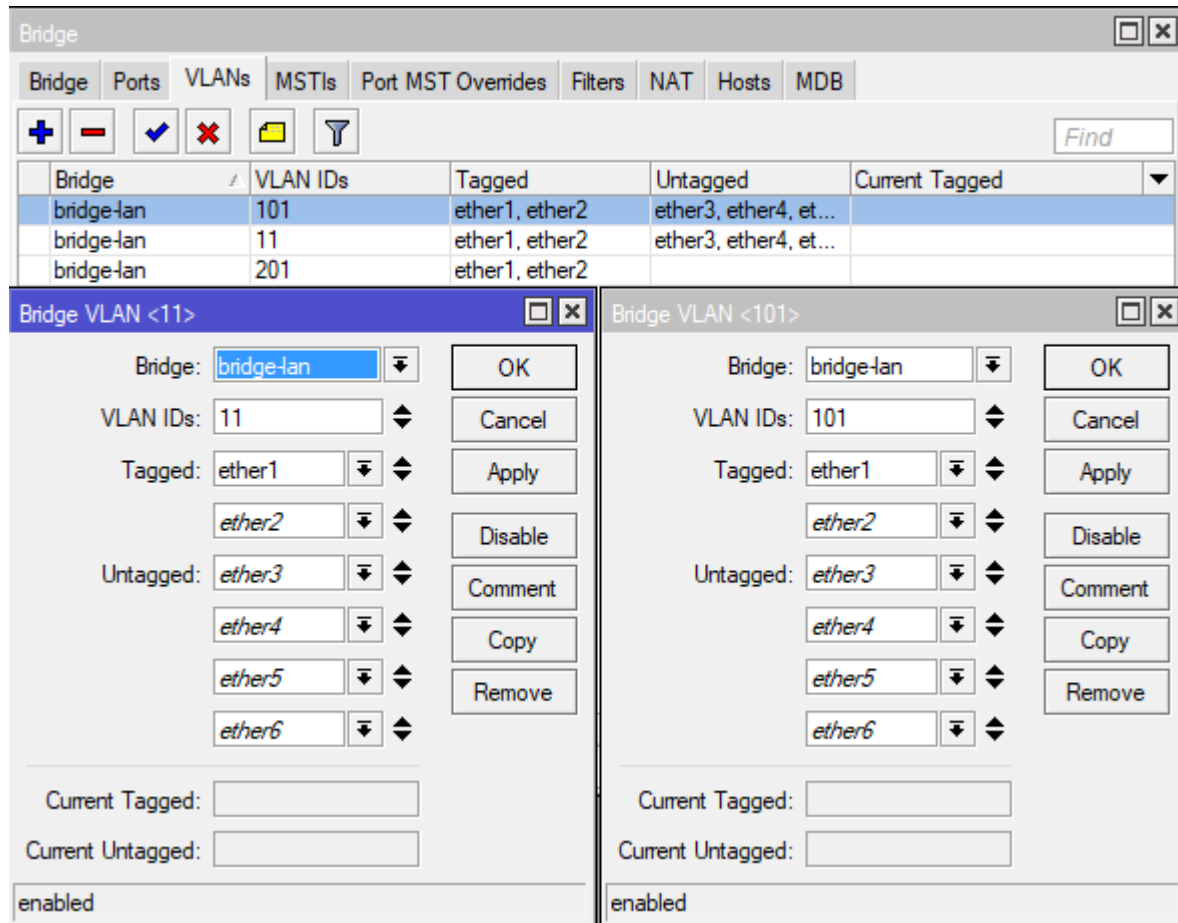
- Table: ingress
- Invert Match:
- Src. Ports: ether3, ether4, ether5, ether6
- Dst. Ports: (empty)
- Src. MAC Address: 64:16:7F:0E:CF:FB** (highlighted in red)
- Src. MAC Mask: FF:FF:FF:00:00:00** (highlighted in red)
- Dst. Addr. Registered: (empty)
- MAC Protocol: (empty)
- Drop Precedence: (empty)
- Custom Fields: (empty)
- Status: enabled

Right Screenshot (Action Tab):

- Action: forward
- Mirror To: (empty)
- Policer: (empty)
- Learn SA: (empty)
- New Service VID: (empty)
- New Service PCP: (empty)
- New Service DEI: (empty)
- New Customer VID: 101** (highlighted in red)
- New Customer PCP: (empty)
- New Customer DEI: (empty)
- New DSCP: (empty)
- New Priority: (empty)
- New Drop Precedence: (empty)
- New Registered State: (empty)
- New Flow ID: (empty)
- Status: enabled

Untagged Ports

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



The screenshot shows a network configuration interface with a table of bridge VLANs and two configuration dialog boxes.

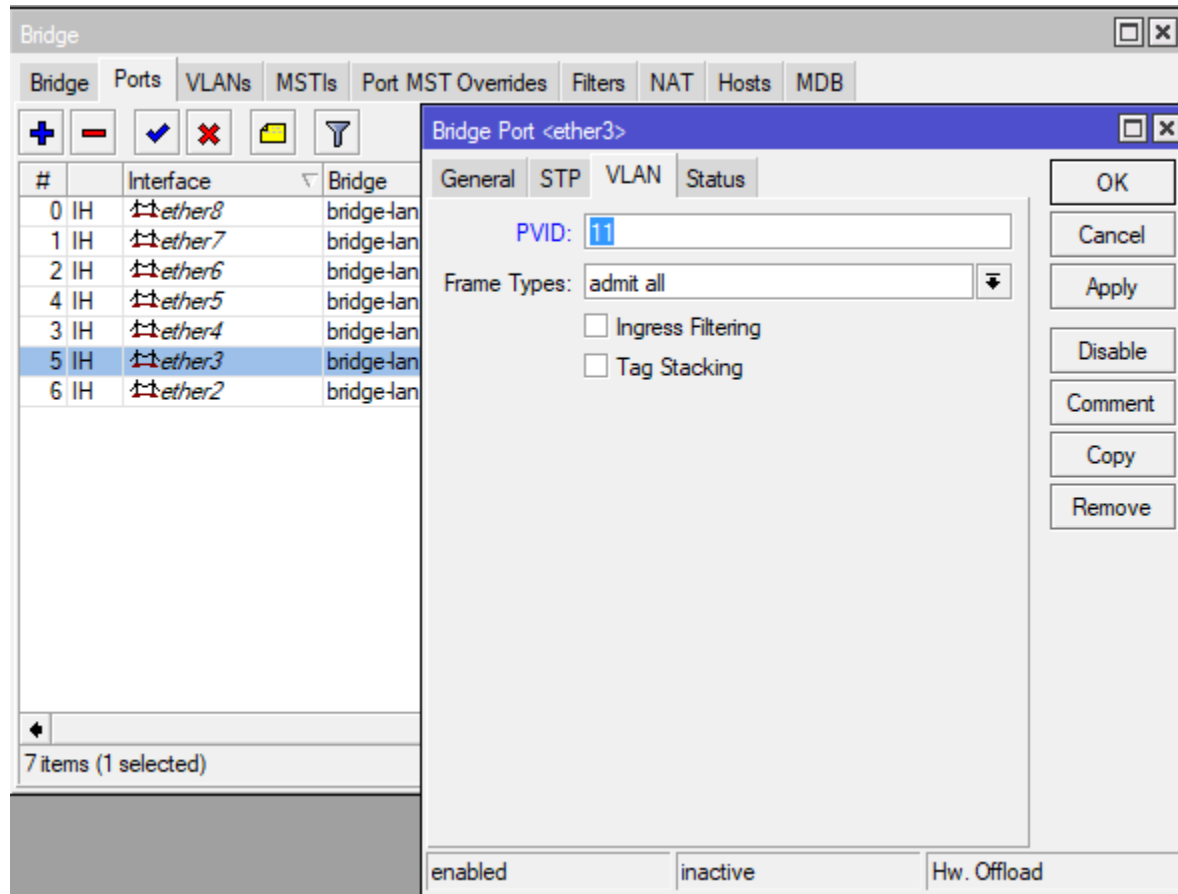
Bridge	VLAN IDs	Tagged	Untagged	Current Tagged
bridge-lan	101	ether1, ether2	ether3, ether4, et...	
bridge-lan	11	ether1, ether2	ether3, ether4, et...	
bridge-lan	201	ether1, ether2		

The dialog boxes show configuration options for Bridge VLAN <11> and Bridge VLAN <101>. The left dialog box is for Bridge VLAN <11> and the right dialog box is for Bridge VLAN <101>. Both dialog boxes have the following fields:

- Bridge: bridge-lan
- VLAN IDs: 11 (left) / 101 (right)
- Tagged: ether1, ether2
- Untagged: ether3, ether4, ether5, ether6
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Current Tagged: (empty)
- Current Untagged: (empty)
- enabled

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



The screenshot shows a network configuration window titled "Bridge" with a sub-window for "Bridge Port <ether3>". The sub-window has tabs for "General", "STP", "VLAN", and "Status". The "VLAN" tab is active, showing the "PVID" field set to "11". Below this, there is a "Frame Types" dropdown menu set to "admit all", and two checkboxes: "Ingress Filtering" and "Tag Stacking", both of which are unchecked. On the right side of the sub-window, there are buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove". At the bottom of the sub-window, there are three status indicators: "enabled", "inactive", and "Hw. Offload".

#	Interface	Bridge
0	IH ether8	bridge-lan
1	IH ether7	bridge-lan
2	IH ether6	bridge-lan
4	IH ether5	bridge-lan
3	IH ether4	bridge-lan
5	IH ether3	bridge-lan
6	IH ether2	bridge-lan



Untagged Ports

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

Bridge VLAN <11>

Bridge: **bridge-lan**

VLAN IDs: 11

Tagged: ether1

ether2

Untagged: ether3

ether4

ether5

ether6

ether7

Current Tagged: ether1

Current Untagged:

enabled

Bridge Port <ether7>

General STP VLAN Status

PVID: 11

Frame Types: admit all

Ingress Filtering

Tag Stacking

enabled inactive Hw. Offload

Untagged Ports

- And Port8 untagged in VLAN201 and PVID on port 8

The image displays two network configuration windows side-by-side. The left window, titled "Bridge VLAN <201>", shows the configuration for VLAN 201. It lists several ports: "ether1" and "ether2" are tagged, while "ether8" is untagged. The "Current Tagged" field shows "ether1" and "Current Untagged" is empty. The right window, titled "Bridge Port <ether8>", shows the configuration for port ether8. The "PVID" is set to "201", and "Frame Types" is set to "admit all". There are checkboxes for "Ingress Filtering" and "Tag Stacking", both of which are unchecked. Both windows have "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", and "Remove" buttons. The status bar at the bottom of the left window shows "enabled", and the status bar of the right window shows "enabled", "inactive", and "Hw. Offload".

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

Interface List							
Interface	Interface List	Ethernet	EoIP Tunnel				
							Detect Inte
	Name	Type					
R	↕↕bridge-lan	Bridge					
R	↔↔vlan11	VLAN					
R	↕↕bridge1	Bridge					
RS	↔↔ether1	Ethernet					
RS	↔↔ether2	Ethernet					
S	↔↔ether3	Ethernet					
S	↔↔ether4	Ethernet					
S	↔↔ether5	Ethernet					
S	↔↔ether6	Ethernet					
S	↔↔ether7	Ethernet					
S	↔↔ether8	Ethernet					
S	↔↔ether9	Ethernet					
S	↔↔ether10	Ethernet					
S	↔↔ether11	Ethernet					

31 items

Interface <vlan1>

General | Loop Protect | Status | Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP: ▾

ARP Timeout: ▾

VLAN ID:

Interface: ▾

Use Service Tag

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Management Interface

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

Bridge VLAN <11>

Bridge:

VLAN IDs:

Tagged:

Untagged:

Current Tagged:

Current Untagged:

enabled

New Address

Address:

Network:

Interface:

enabled

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

The screenshot displays a network configuration window for a bridge interface. The left pane shows a table of bridge components:

	Name	Type
R	bridge-lan	Bridge

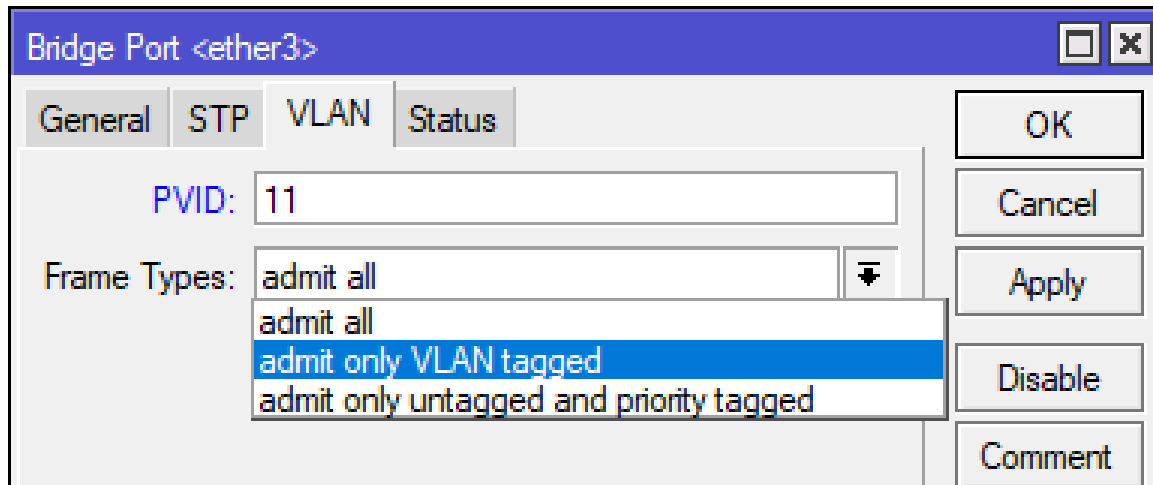
The right pane shows the configuration for the selected interface, with the 'VLAN' tab active. The 'VLAN Filtering' checkbox is checked and highlighted with a dashed yellow border. Other settings include:

- EtherType: 0x8100
- PVID: 1
- Frame Types: admit all
- Ingress Filtering: unchecked

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch. A status bar at the bottom left indicates '1 item out of 14'.

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



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

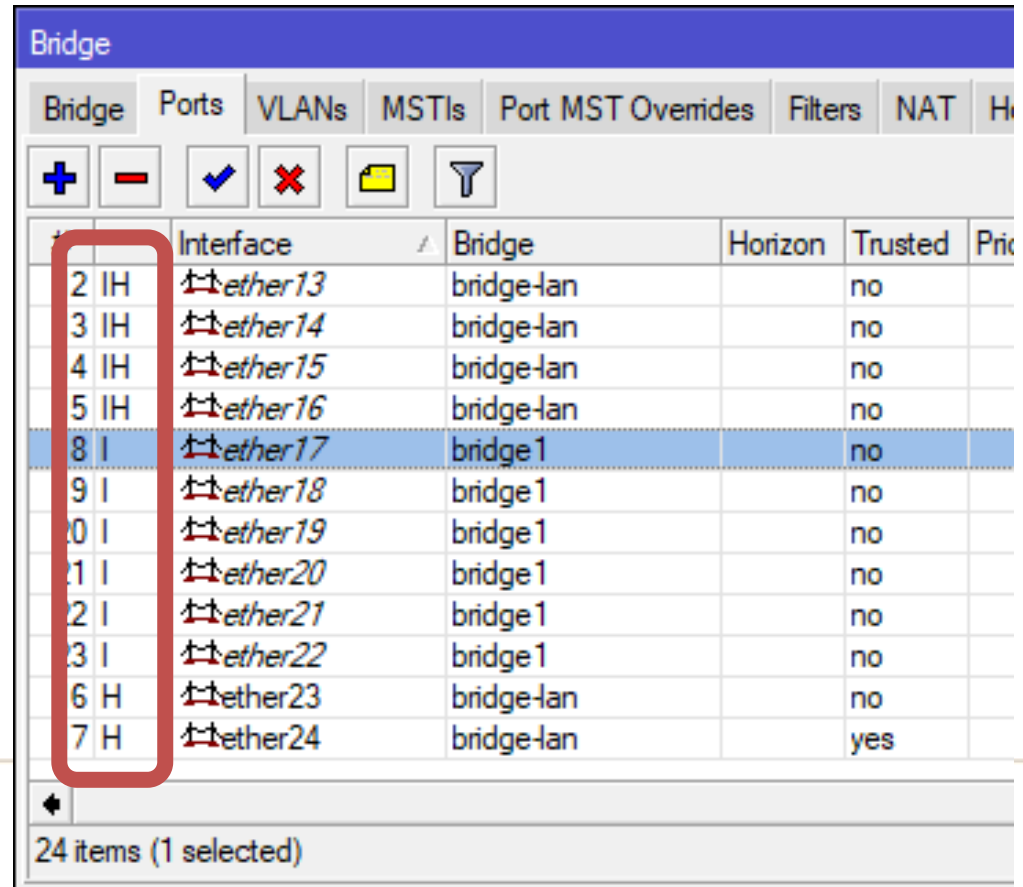
- You start to use your switch and notice that one set of ports work at wire speed and give full throughput. However the other set of ports do not.

Layer 2 Misconfigurations

Multiple Bridges

What has happened?

- You test further and notice that the CPU is very high when traffic flows slowly through one of the bridges.
- You look at your configuration
- See how the H flag is not set for ports in bridge1



		Interface	Bridge	Horizon	Trusted	Prio
2	IH	ether13	bridge-lan		no	
3	IH	ether14	bridge-lan		no	
4	IH	ether15	bridge-lan		no	
5	IH	ether16	bridge-lan		no	
8	I	ether17	bridge 1		no	
9	I	ether18	bridge 1		no	
10	I	ether19	bridge 1		no	
11	I	ether20	bridge 1		no	
12	I	ether21	bridge 1		no	
13	I	ether22	bridge 1		no	
16	HI	ether23	bridge-lan		no	
17	HI	ether24	bridge-lan		yes	

24 items (1 selected)



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

The screenshot displays two configuration windows in Mikrotik WinBox. The top window, titled 'Interface List', shows a table of network interfaces. The bottom window, titled 'Bridge', shows a table of bridge ports.

Interface List Table:

Name	Type	Actual MTU	L2 MTU	Tx	Rx
bridge-lan	Bridge	1500	1592	2.8 kbps	14.1 kbps
ether1	Ethernet	1500	1592	0 bps	0 bps
vlan11	VLAN	1500	1588	0 bps	0 bps
ether2	Ethernet	1500	1592	0 bps	0 bps

Bridge Table:

#	Interface	Bridge	Horizontal	Trusted	Priority (h)	Path Cost	Role	Root Pat...
0	ether1	bridge-lan		no	80	10	disabled port	
1	ether2	bridge-lan		no	80	10	disabled port	
2	ether3	bridge-lan		no	80	10	disabled port	

Layer 2 Misconfigurations

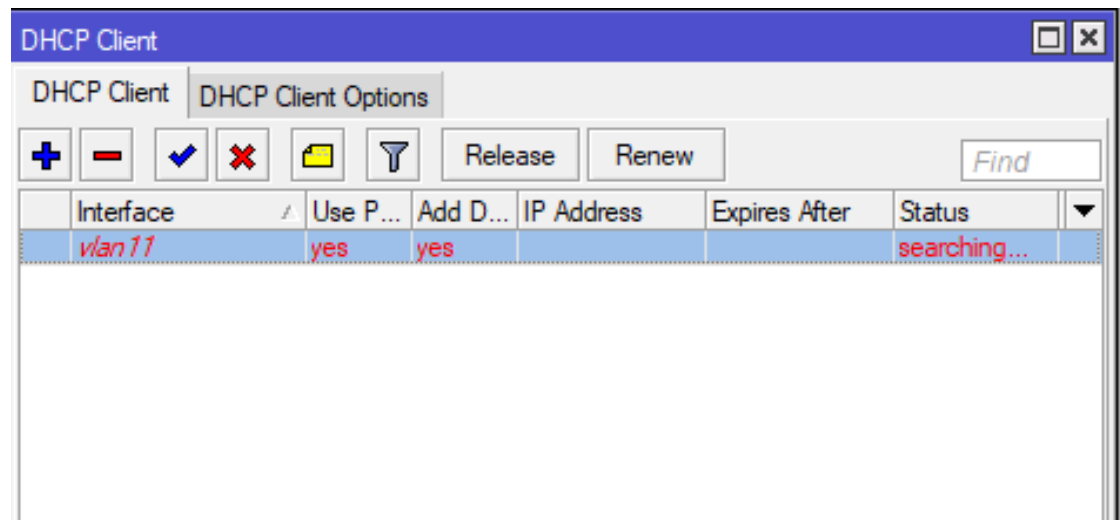
VLAN – on slave interface

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

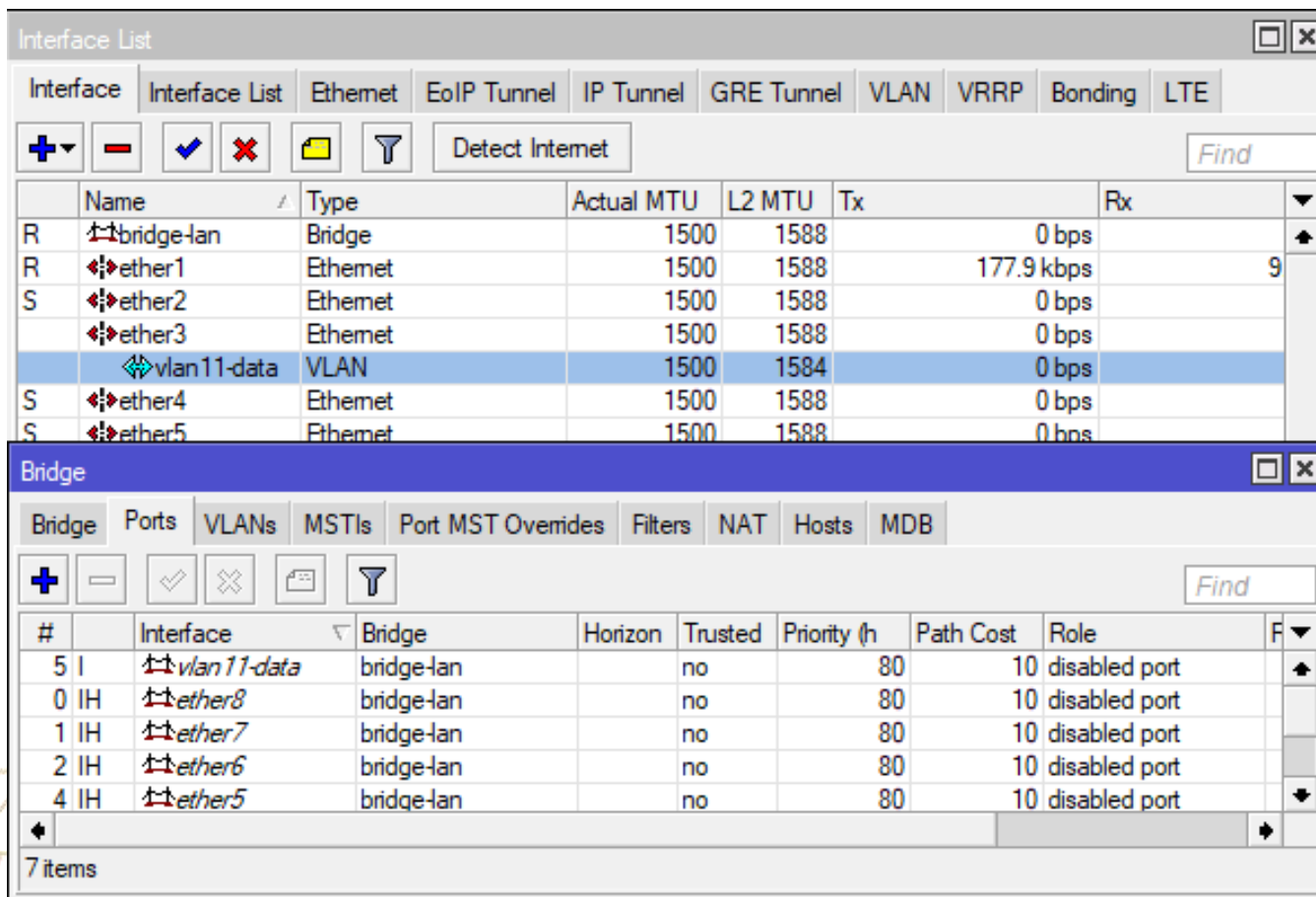
	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx
R	bridge-lan	Bridge	1500	1592	287.7 kbps	3.1 kbps	
R	vlan11	VLAN	1500	1588	286.9 kbps	2.9 kbps	
R	bridge1	Bridge	1500	1592	0 bps	0 bps	
RS	ether1	Ethernet	1500	1592	330.7 kbps	8.3 kbps	
RS	ether2	Ethernet	1500	1592	512 bps	3.7 kbps	
S	ether3	Ethernet	1500	1592	0 bps	0 bps	
S	ether4	Ethernet	1500	1592	0 bps	0 bps	
S	ether5	Ethernet	1500	1592	0 bps	0 bps	
S	ether6	Ethernet	1500	1592	0 bps	0 bps	
S	ether7	Ethernet	1500	1592	0 bps	0 bps	

Layer 2 Misconfigurations

VLAN in a Bridge with Physical Interface

Scenario

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



The screenshot displays two windows from a network configuration tool. The top window, titled "Interface List", shows a table of network interfaces. The bottom window, titled "Bridge", shows a table of bridge ports.

Interface List

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	bridge-lan	Bridge	1500	1588	0 bps	
R	ether1	Ethernet	1500	1588	177.9 kbps	9
S	ether2	Ethernet	1500	1588	0 bps	
	ether3	Ethernet	1500	1588	0 bps	
	vlan11-data	VLAN	1500	1584	0 bps	
S	ether4	Ethernet	1500	1588	0 bps	
S	ether5	Ethernet	1500	1588	0 bps	

Bridge

#	Interface	Bridge	Horizon	Trusted	Priority (h)	Path Cost	Role
5 I	vlan11-data	bridge-lan		no	80	10	disabled port
0 IH	ether8	bridge-lan		no	80	10	disabled port
1 IH	ether7	bridge-lan		no	80	10	disabled port
2 IH	ether6	bridge-lan		no	80	10	disabled port
4 IH	ether5	bridge-lan		no	80	10	disabled port

7 items

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

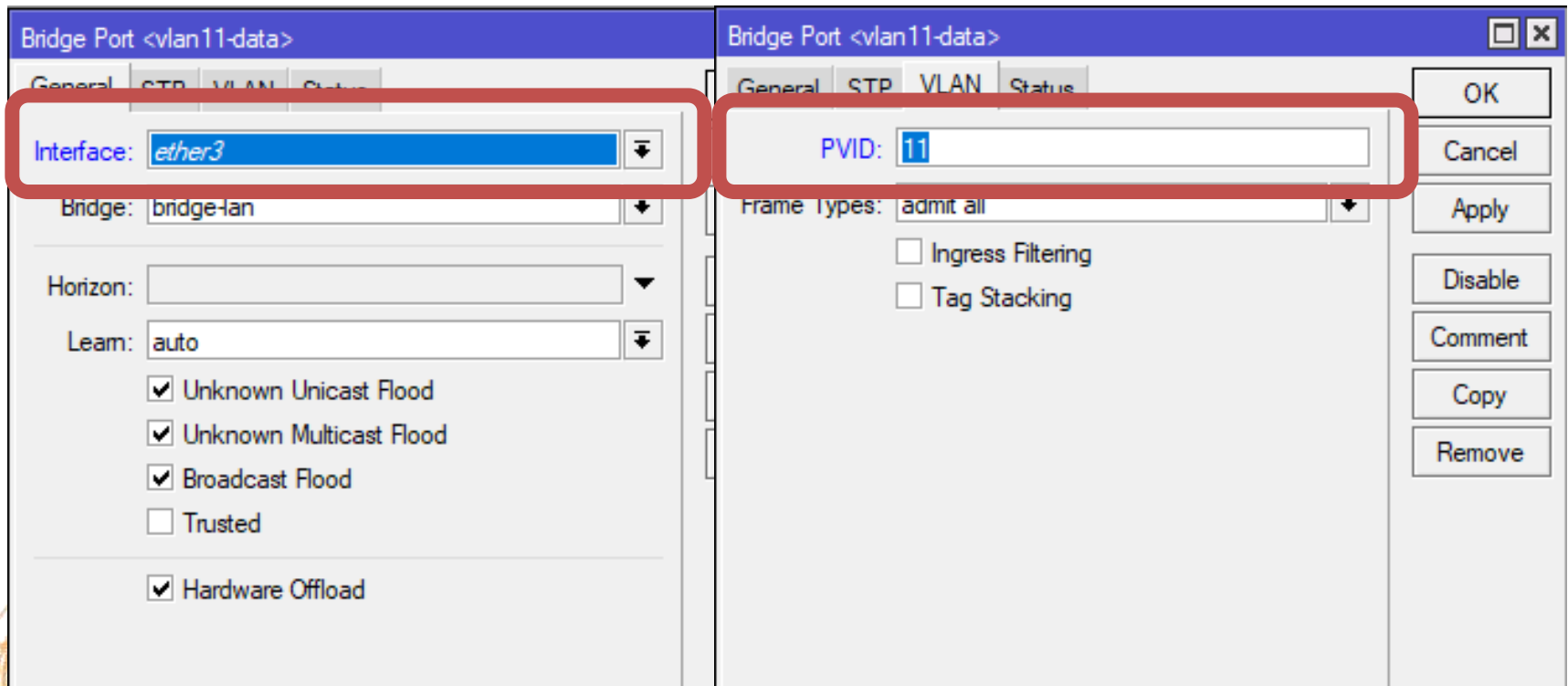
- Port blocking by RSTP
- Port flapping
- Network loops

Layer 2 Misconfigurations

VLAN in a Bridge with Physical Interface

Solution

- Use VLAN filtering as we have just looked at

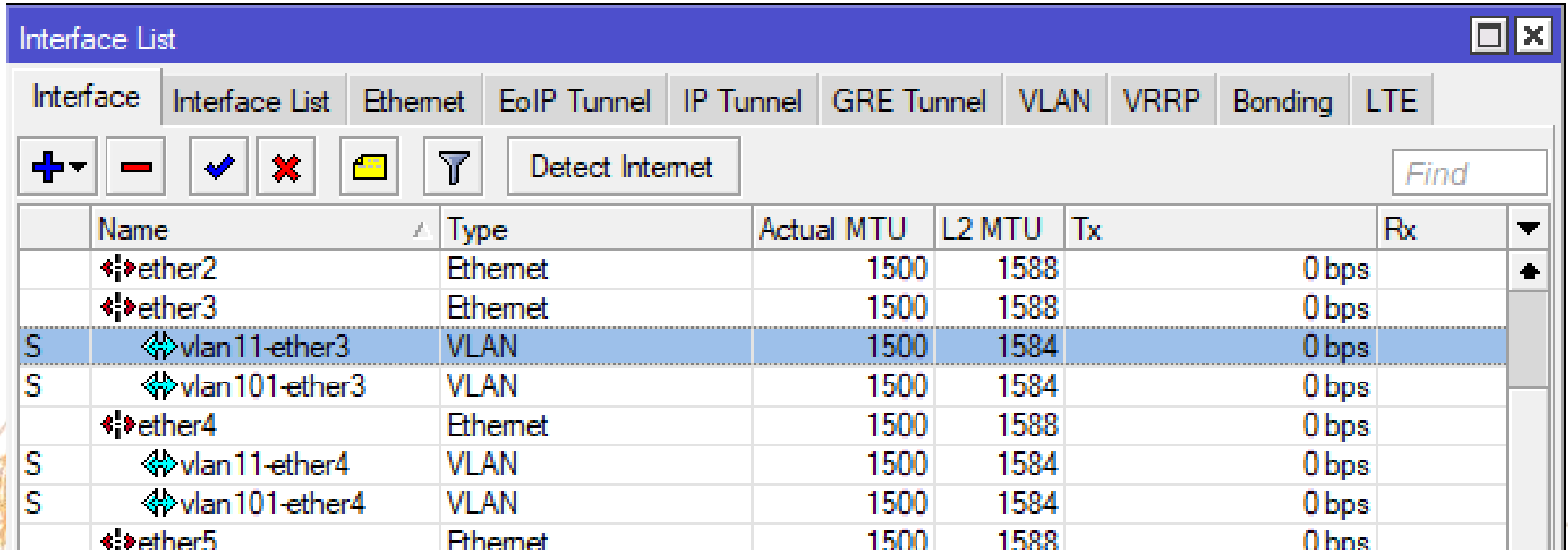


Layer 2 Misconfigurations

Bridged VLANs

Scenario

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



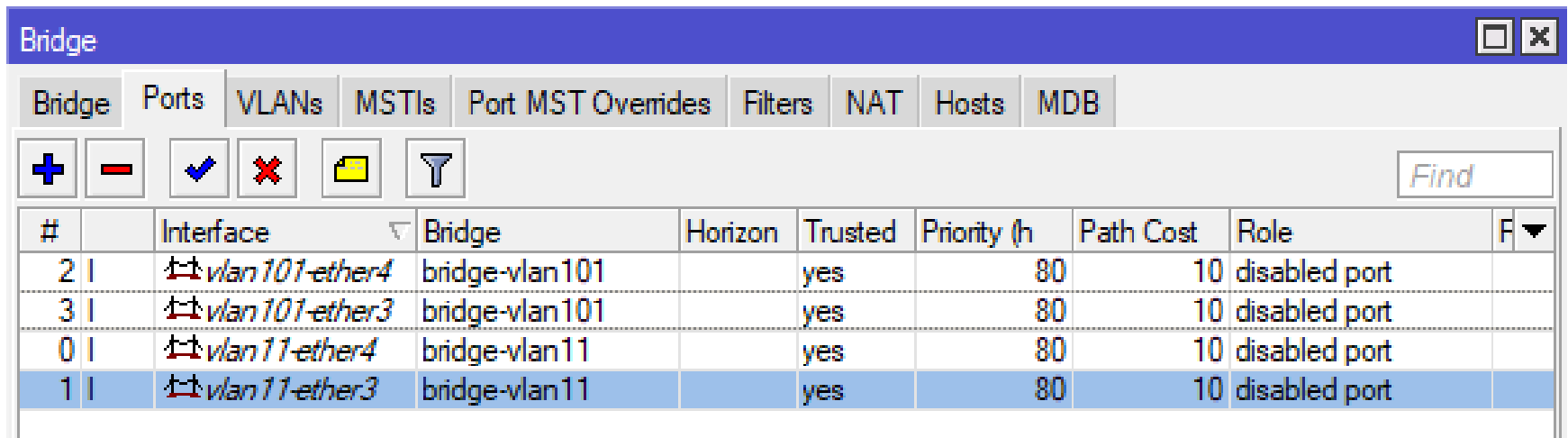
	Name	Type	Actual MTU	L2 MTU	Tx	Rx
	ether2	Ethernet	1500	1588		0 bps
	ether3	Ethernet	1500	1588		0 bps
S	vlan11-ether3	VLAN	1500	1584		0 bps
S	vlan101-ether3	VLAN	1500	1584		0 bps
	ether4	Ethernet	1500	1588		0 bps
S	vlan11-ether4	VLAN	1500	1584		0 bps
S	vlan101-ether4	VLAN	1500	1584		0 bps
	ether5	Fiber Ethernet	1500	1588		0 bps

Layer 2 Misconfigurations

Bridged VLANs

Scenario (cont..)

- Put VLAN interface into a separate bridge for each VLAN



The screenshot shows a network configuration window titled "Bridge". It has several tabs: "Bridge", "Ports", "VLANs", "MSTIs", "Port MST Overrides", "Filters", "NAT", "Hosts", and "MDB". The "VLANs" tab is selected. Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a red X, a folder, and a funnel. To the right of these icons is a "Find" search box. Below the icons is a table with the following columns: "#", "Interface", "Bridge", "Horizon", "Trusted", "Priority (h)", "Path Cost", "Role", and "F". The table contains four rows of data:

#	Interface	Bridge	Horizon	Trusted	Priority (h)	Path Cost	Role	F
2	vlan101-ether4	bridge-vlan101		yes	80	10	disabled port	
3	vlan101-ether3	bridge-vlan101		yes	80	10	disabled port	
0	vlan11-ether4	bridge-vlan11		yes	80	10	disabled port	
1	vlan11-ether3	bridge-vlan11		yes	80	10	disabled port	

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



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

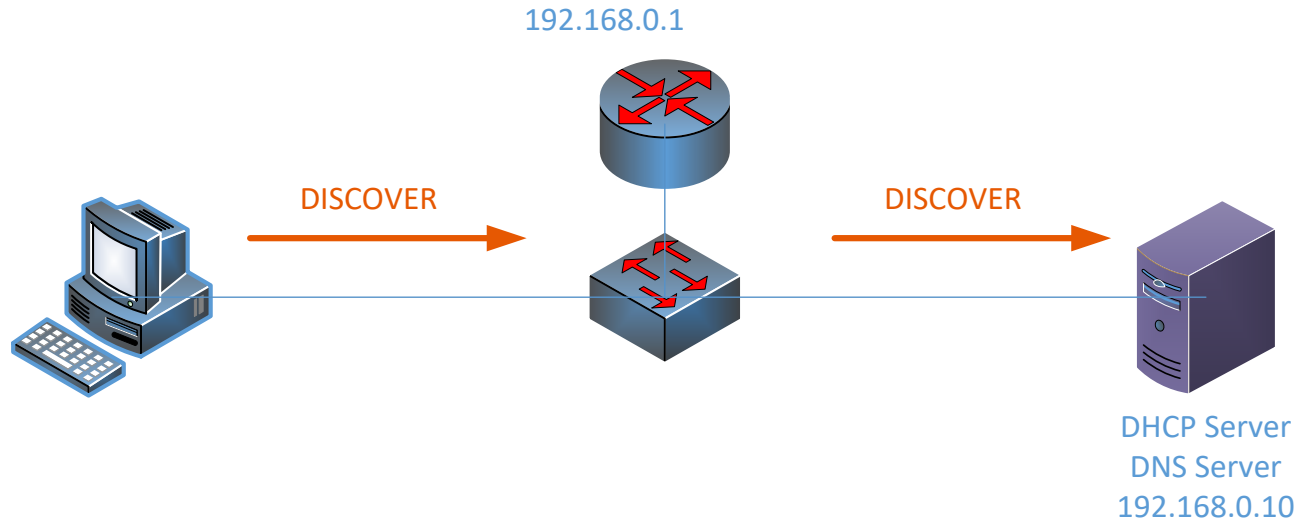


Rogue DHCP Server

- 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

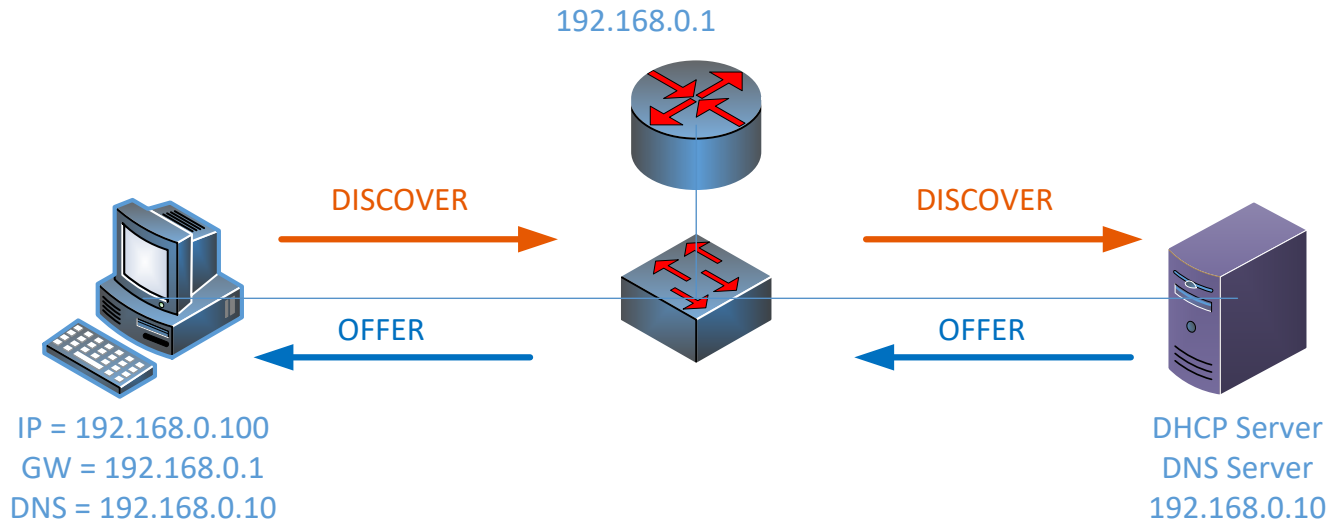


DHCP Server Spoofing



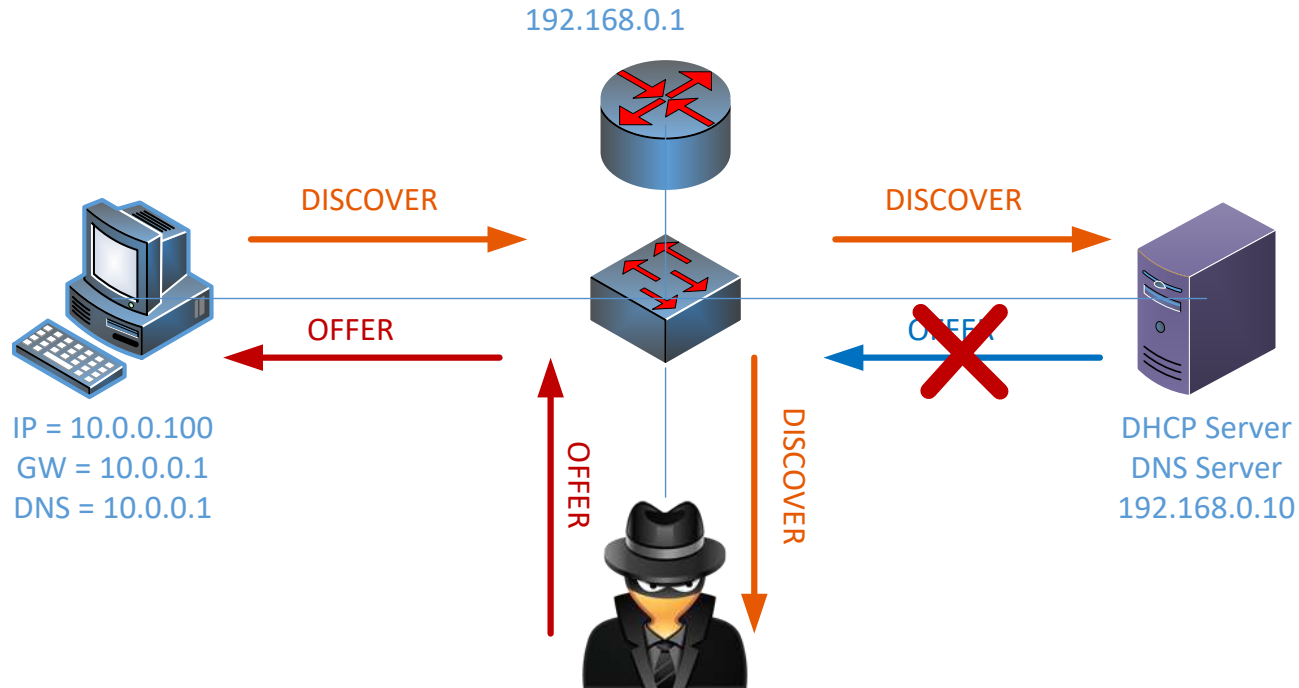
1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.

DHCP Server Spoofing



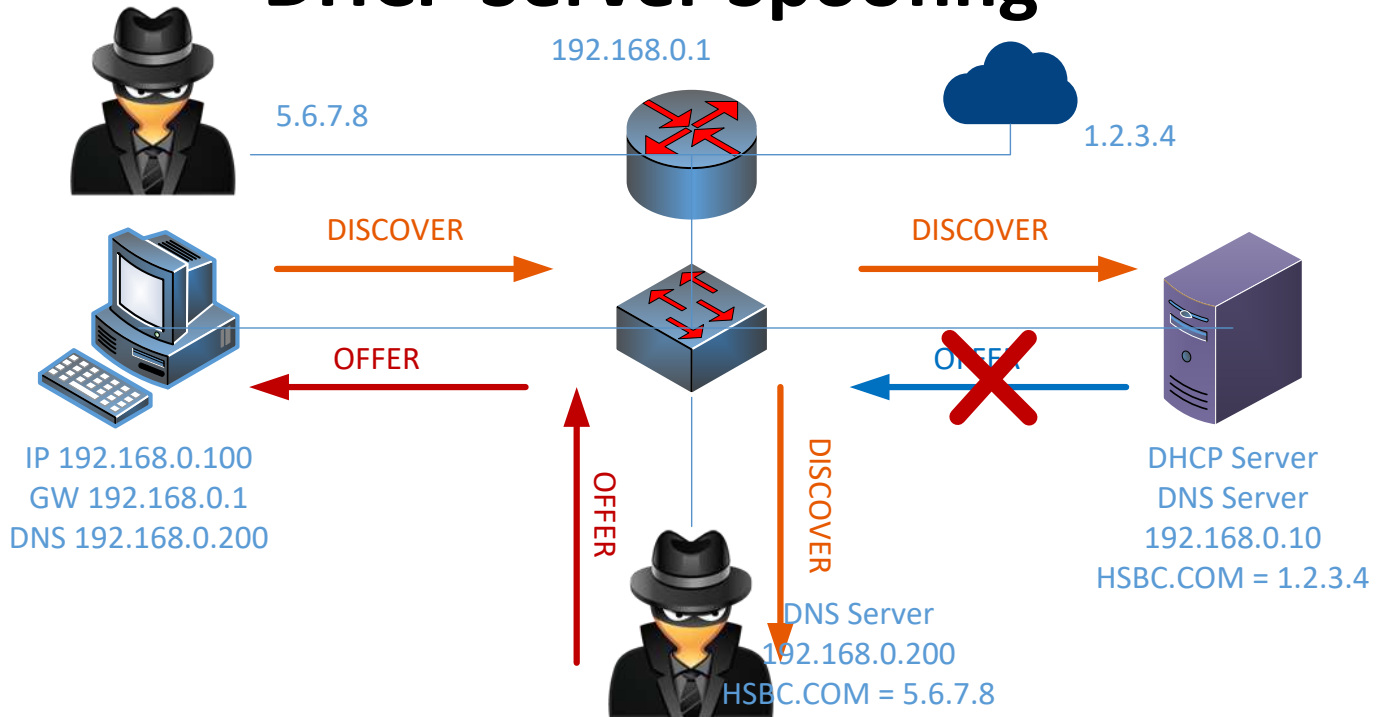
1. Client sends DHCP DISCOVERY broadcast packet. Because it is a broadcast packet, switch sends it out of every switch port.
2. Server sends a DHCP Reply.

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

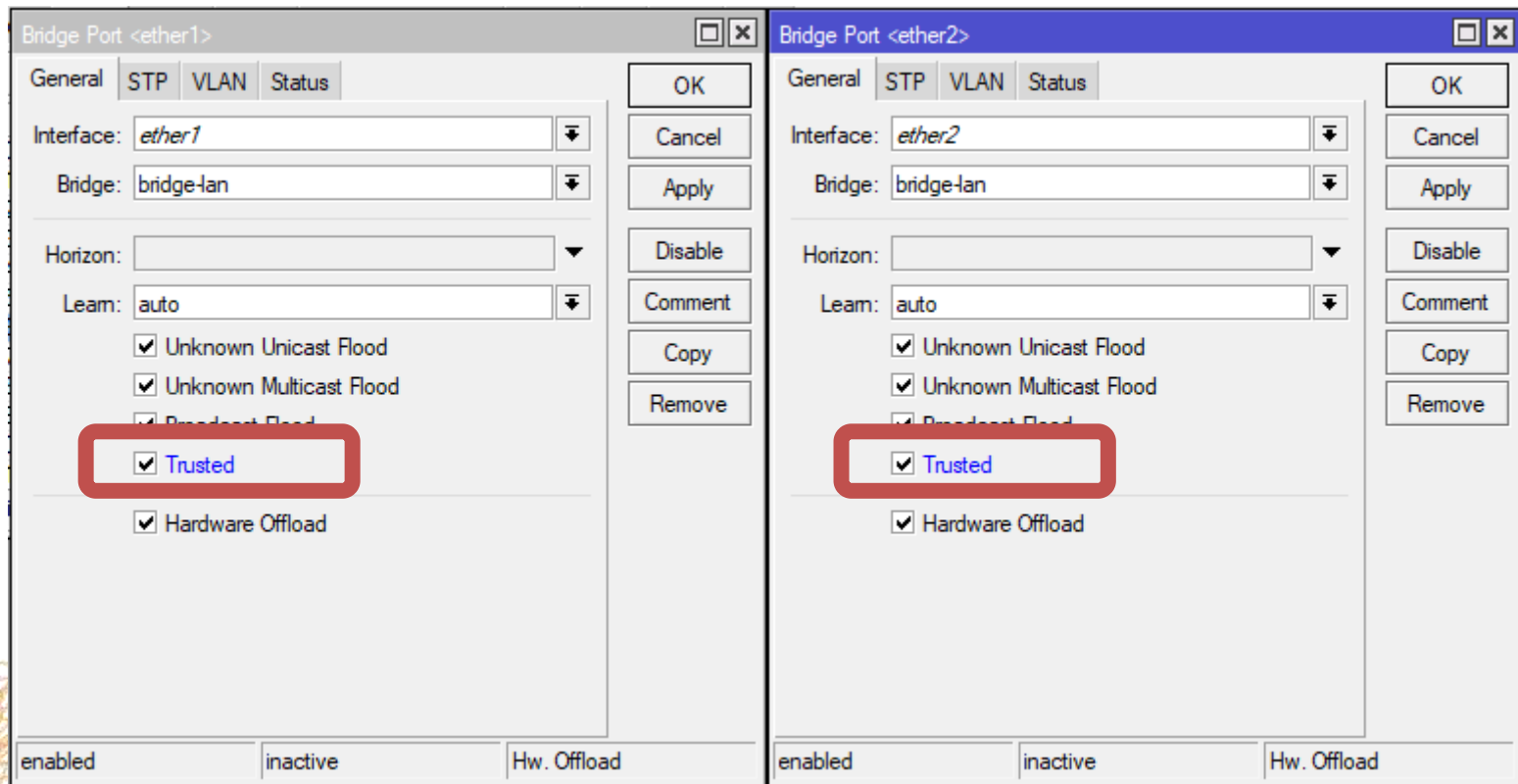
- Depending on the model or the switch chip, using DHCP Snooping will disable bridge HW offloading

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

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

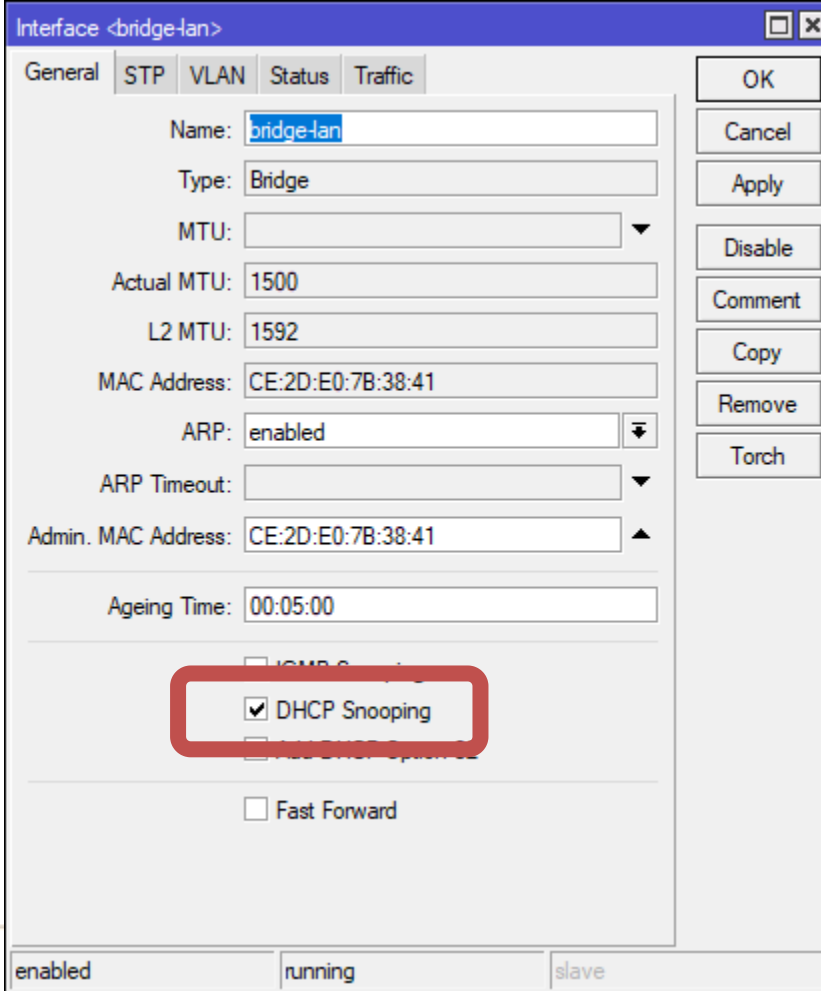
Bridge DHCP Snooping

- 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



Interface <bridge-lan>

General | STP | VLAN | Status | Traffic

Name: bridge-lan

Type: Bridge

MTU: []

Actual MTU: 1500

L2 MTU: 1592

MAC Address: CE:2D:E0:7B:38:41

ARP: enabled

ARP Timeout: []

Admin. MAC Address: CE:2D:E0:7B:38:41

Ageing Time: 00:05:00

DHCP Snooping

Fast Forward

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled | running | slave

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

