About Me

- Steve Discher, from College Station, Texas, USA
- MikroTik Certified Trainer since 2008 and teach RouterOS classes, LearnMikroTik.com and blog at SteveDischer.com
- Operate a wireless distribution company, ISP Supplies
- Author of RouterOS by Example

Congratulations!
28 New MTCNA Engineers


01:00

How to Properly Use the Switching Functions of the CRS Cloud Router Switches

Practice Quiz

This is a:

A. Switch

B. Router

C. All of the above

Practice Quiz

This is a:

A. Switch

B. Router

C. All of the above

CRS Features

Switching Features & Highlights

Features	Description
Forwarding	• Configurable ports for switching or routing • Full non-blocking wirespeed switching • Up to 16k MAC entries in Unicast FDB for Layer 2 unicast forwarding • Up to 1k MAC entries in Multicast FDB for multicast forwarding • Up to 256 MAC entries in Reserved FDB for control and management purposes • All Forwarding Databases support IVL and SVL • Configurable Port based MAC learning limit (max 1024 MACs per port) • Jumbo frame support (CRS1xx: 4064 Bytes; CRS2xx: 9204 Bytes)

Mirroring	• Various types of mirroring:
	  • Port based mirroring
	  • VLAN based mirroring
	  • MAC based mirroring
	• 2 independent mirroring analyzer ports

Wires speed switching and jumbo frame support

Port, VLAN and MAC based mirroring

CRS Features

Features	Description

VLAN	• Fully compatible with IEEE802.1Q and IEEE802.1ad VLAN
	• 4k active VLANs
	• Flexible VLAN assignment:
	  • Port based VLAN
	  • Protocol based VLAN
	  • MAC based VLAN
	• From any to any VLAN translation and swapping
	• 1:1 VLAN switching - VLAN to port mapping
	• VLAN filtering

Port Isolation and Leakage	• Applicable for Private VLAN implementation • 3 port profile types: Promiscuous, Isolated and Community • Up to 28 Community profiles • Leakage profiles allow bypassing egress VLAN filtering

802.1Q and Q in Q VLANs, up to 4000 VLANs

Port isolation and leakage

CRS Features

Features	Description
Trunking	• Supports static link aggregation groups • Up to 8 Port Trunk groups • Up to 8 member ports per Port Trunk group • Hardware automatic failover and load balancing

Quality of Service (QoS)	• Flexible QoS classification and assignment:
	  • Port based
	  • MAC based
	  • VLAN based
	  • Protocol based
	  • PCP/DEI based
	  • DSCP based
	  • ACL based
	• QoS remarking and remapping for QoS domain translation between service provider and client networks
	• Overriding of each QoS assignment according to the configured priority

Trunking including standards based LAG, Link Aggregation Groups

Layer 2 QOS based on port, MAC, VLAN and many other matchers

CRS Features

Features	Description
Shaping and Scheduling	• 8 queues on each physical port • Shaping per port, per queue, per queue group
Access Control List	• Ingress and Egress ACL tables • Up to 512 ACL rules • Classification based on ports, L2, L3, L4 protocol header fields • ACL actions include filtering, forwarding and modifying of the protocol header fields

Traffic shaping

Ingress and Egress ACL's

CRS

- Those are the switching features
- Don’t forget about RouterOS

Question

True or False: Steve knows how to use all the capabilities of the CRS?

Answer

False. Why? There are three to four features that most people need all the time, the rest are designed to address certain, less common scenarios.

Question

True or False: I can solve most if not all of the switching needs of the average WISP or integrator by learning 3 basic switching setups on the CRS.

Answer

True. We will look at three simple setups that will work for the majority of your applications.

Agenda

1. Why switch, why not just bridge?
2. Background knowledge
3. Examples of setups


BACK TO
SCHOOL

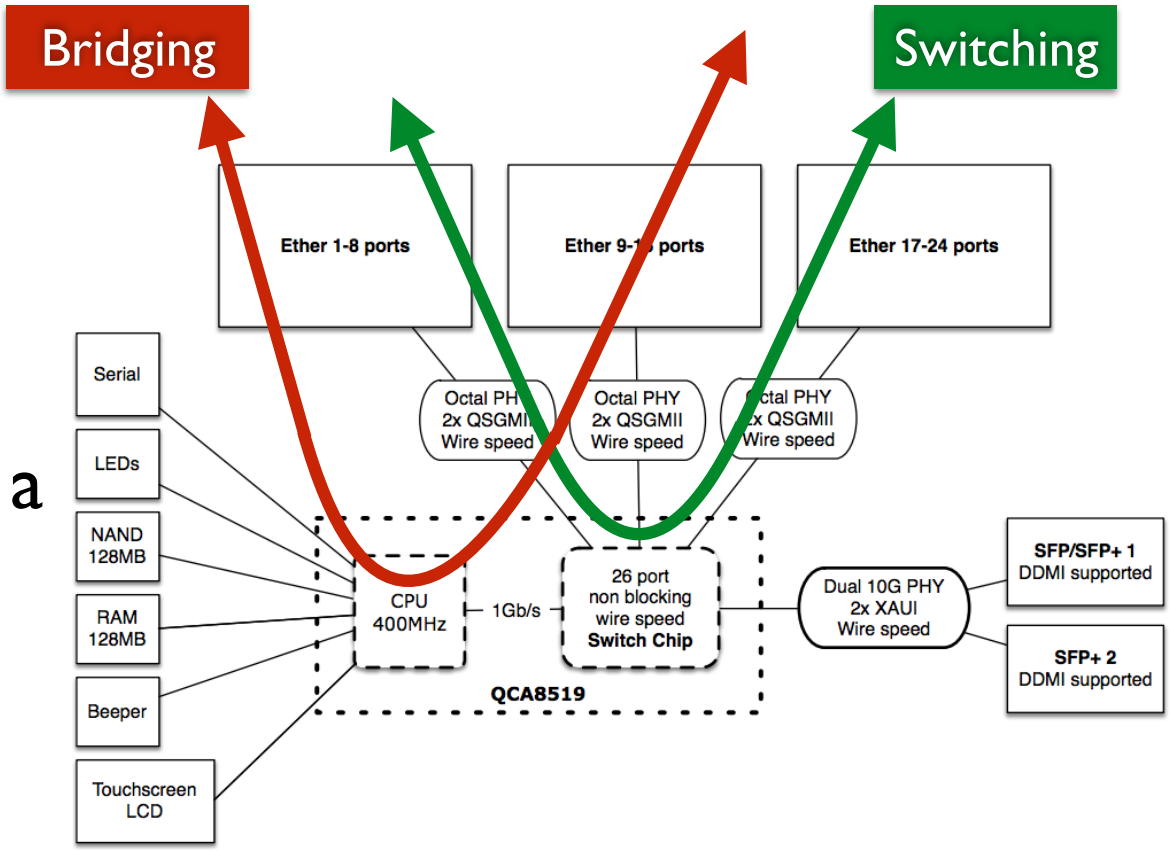
Why Use Switching Instead of Bridging?

- Bridges are easy, and perfect for joining ports that can not be joined any other way
  - Example: Wireless to Ethernet
- Bridges are done in software, resource hit
- Bridges could max out a CPU before the interfaces hit wire speed

How Are Switches Different Than Bridges?

How Are Switches Different Than Bridges?

- Although functionally they are the same, operationally they are very different
- Switching involves using a dedicated switch chip, separate and apart from the Router CPU and processes



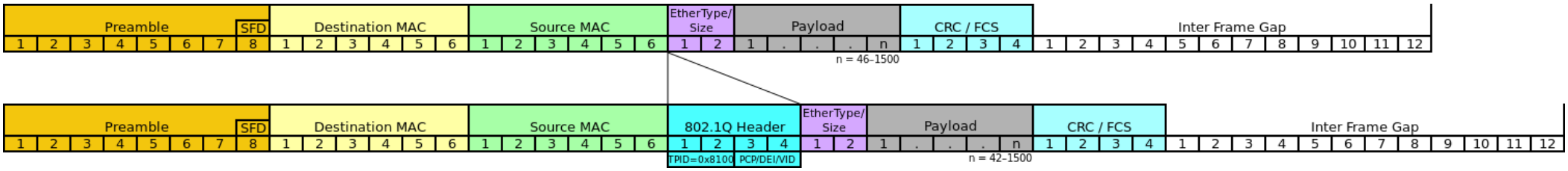
Dedicated hardware, not software

What are VLANs?

- A Virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). -*Wikipedia*
- It is like a virtual switch or switches inside a physical switch

How Are VLANs Done

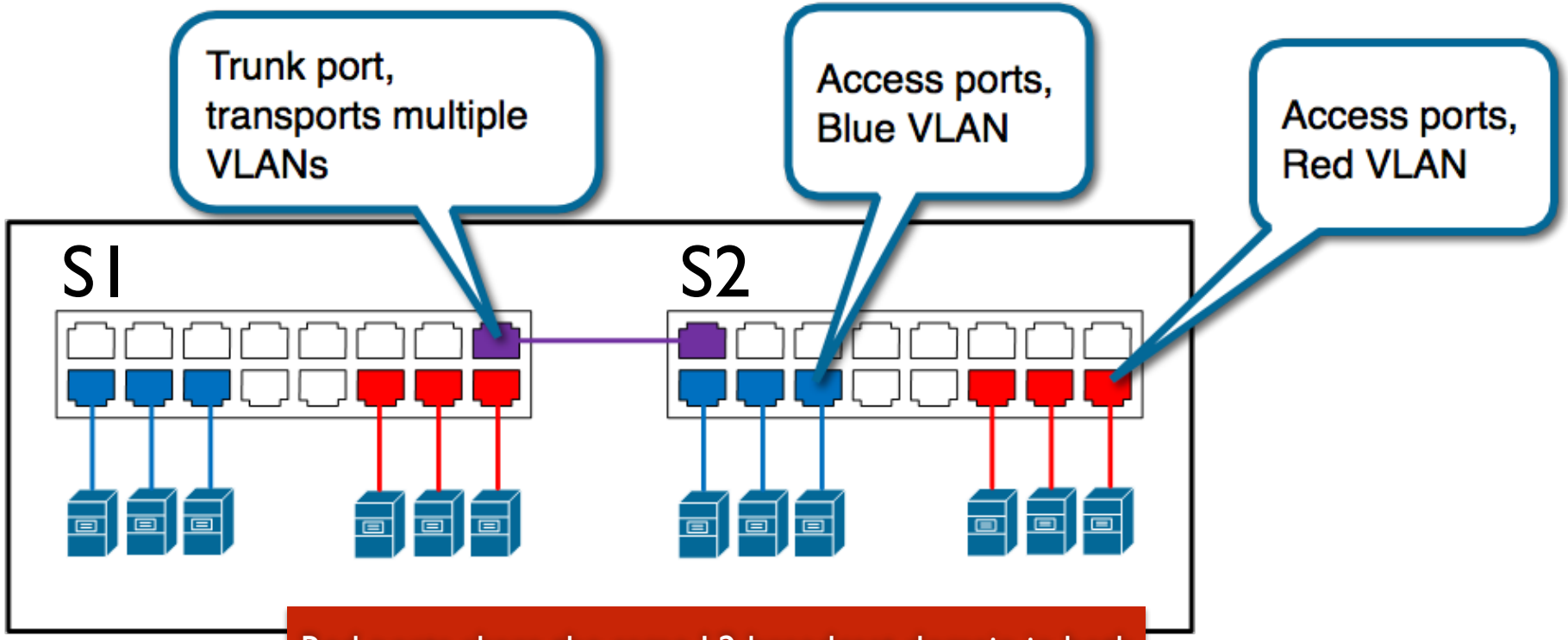
- "Encapsulation" is a misnomer
- 802.1Q does not "encapsulate" the original frame, per se, instead it adds a 32-bit field between the source MAC address and the "EtherType" field of the original frame



VLAN Terms

- **Tagging -** adding the VLAN tag to frames
- **Untagging -** Stripping the VLAN tag
- **Trunk Port - (not an aggregation group)** Allowing various, different frame tags to pass through a switch typically without change
- **Access port -** Receives only frames with a certain tag and strips them before the frames leave the port for non-VLAN aware devices
- **Hybrid port -** Passes some tags intact but strips others

VLANs in Action



Red ports share the same L2 broadcast domain in both the same and geographically different locations

Blue ports share the same L2 broadcast domain in both the same and geographically different locations

School's out!


Common
Setups

Application Examples

How can we use these features?

Example 1

- **Basic switch** - Set all or a group of ports to be switched together

Example 2

- **Inter VLAN Routing** - Trunk VLANs to a router port to be presented as VLAN sub-interfaces

Example 3

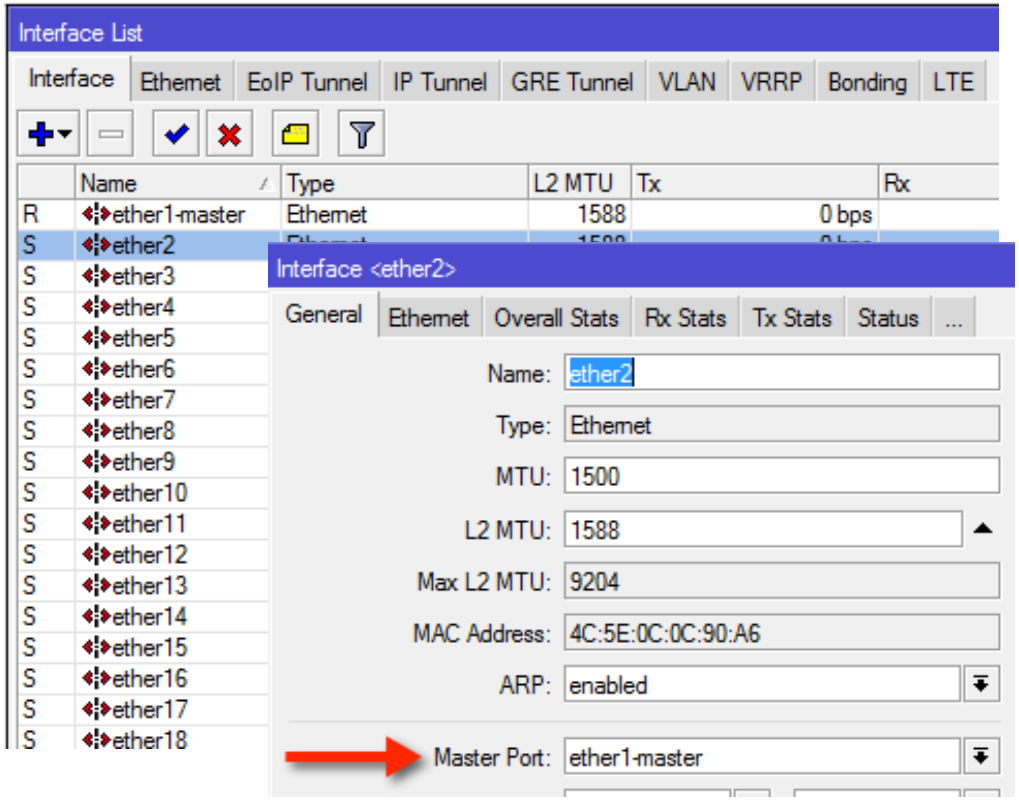
- **Port Isolation** - Prevent rogue DHCP servers on a switch

Example 1

Example 1

Configure a Basic Switch

- Using default configuration, all ports are switched with ether1 as the master

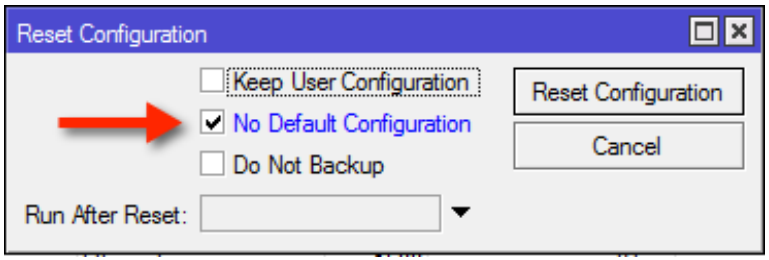


Interfaces

Example 1

Configure a Basic Switch

- Without default configuration, you will need to assign ports manually or by using a script
- "No Default Configuration" does just that

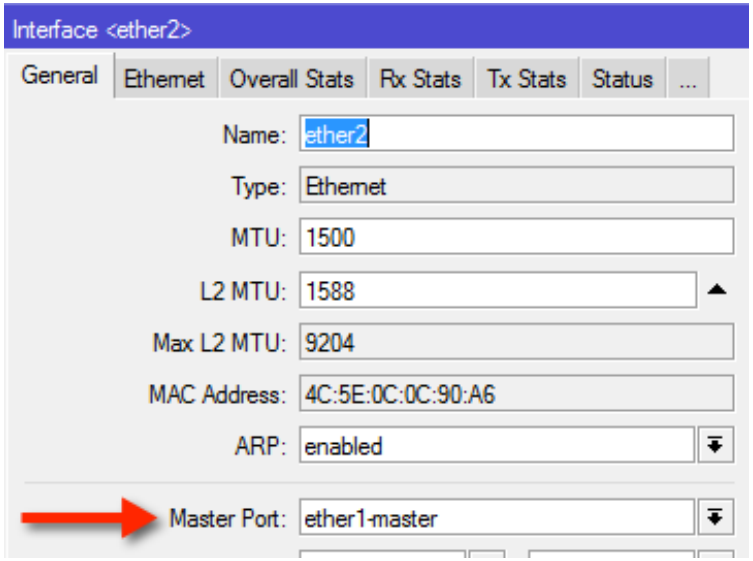


System → Reset Configuration

Example 1

Configure a Basic Switch

- After reset, we can assign interfaces manually or using a script
- Without scripting this can take a while!

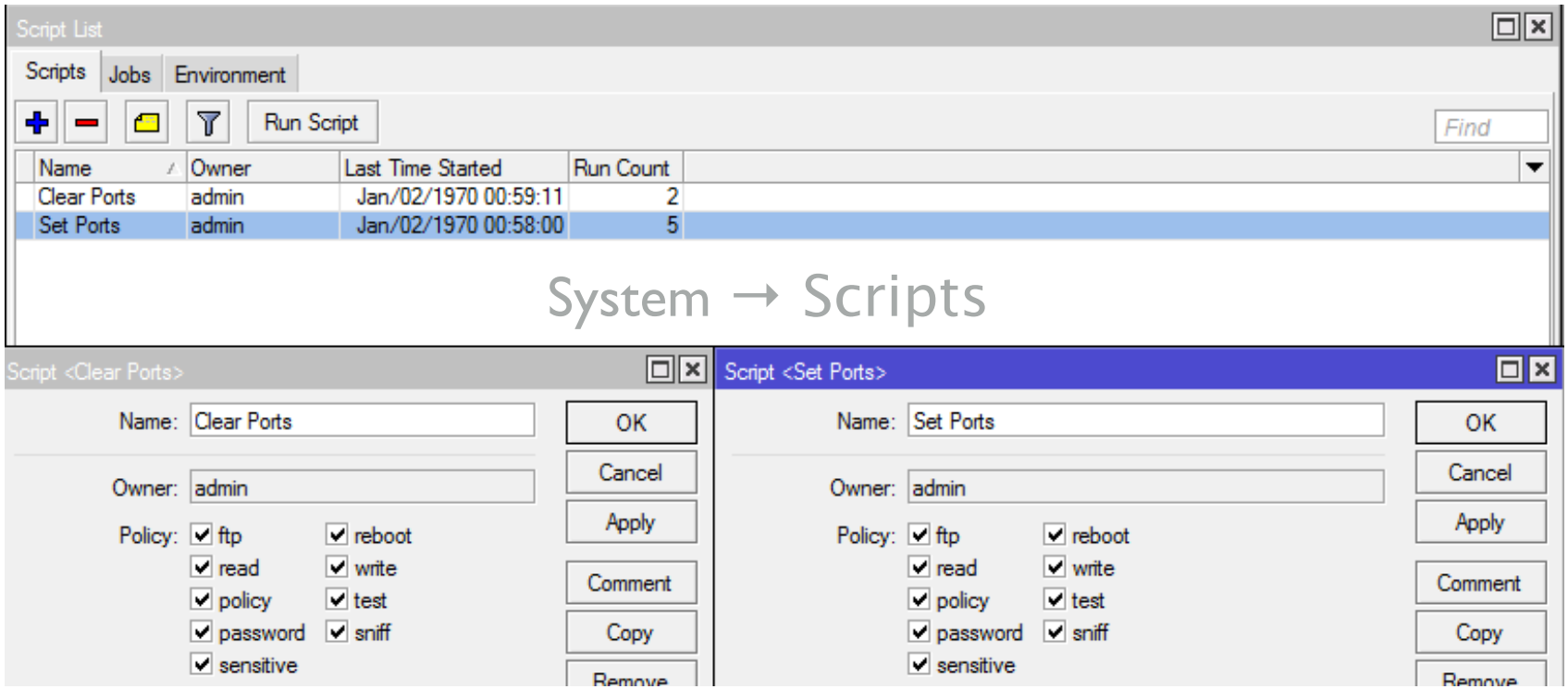


Interfaces

Example 1

Configure a Basic Switch

- Two scripts to greatly simply configuration



Example 1

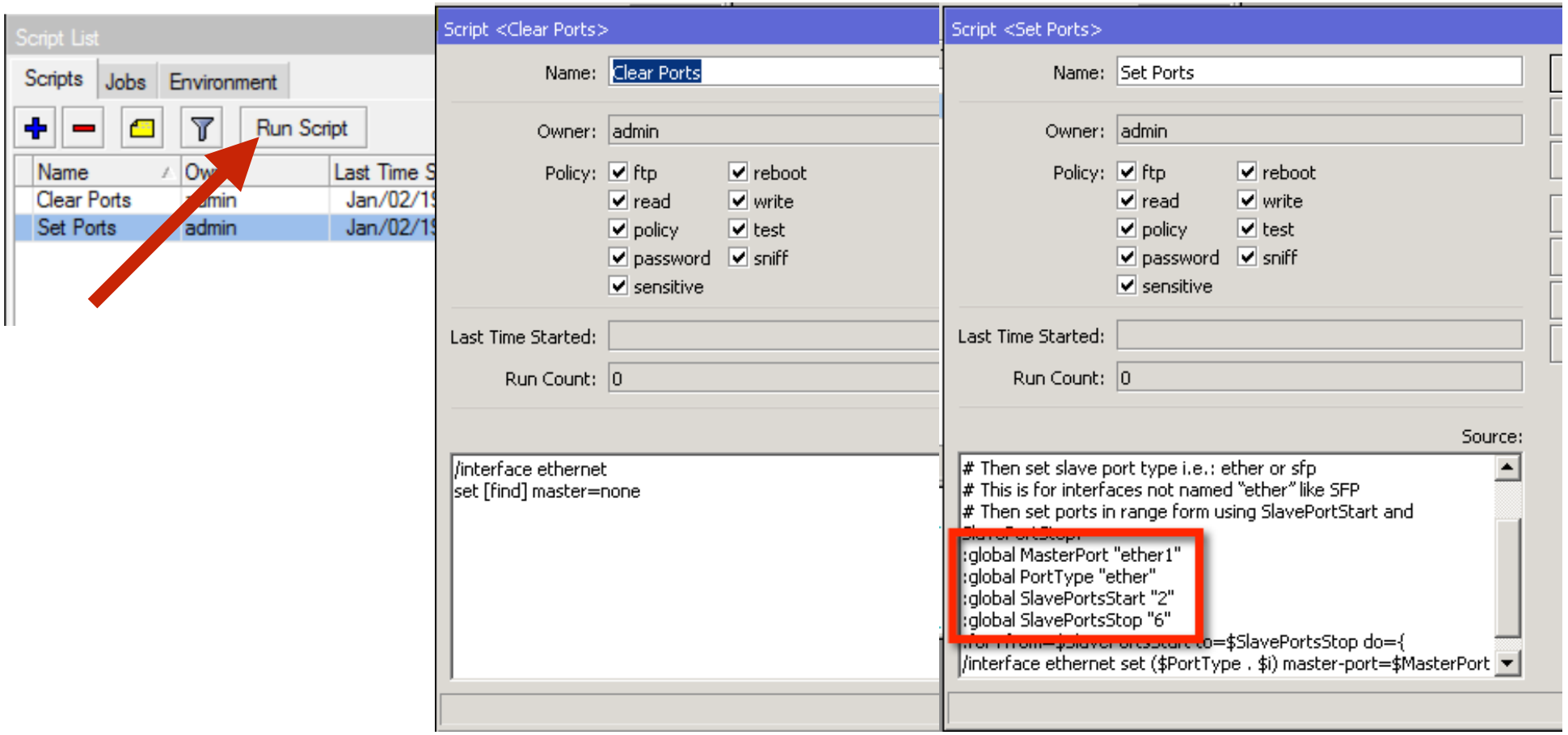
Configure a Basic Switch

```
/system script
add name="Set Ports" owner=admin policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
source="#\r\
    \n#\r\
    \n# Set master port\r\
    \n# Then set slave port type i.e.: ether or sfp \r\
    \n# This is for interfaces not named \93ether\94 like SFP\r\
    \n# Then set ports in range form using SlavePortStart and SlavePortStop.\r\
    \n:global MasterPort \"ether24\"\r\
    \n:global PortType \"ether\"\r\
    \n:global SlavePortsStart \"1\"\r\
    \n:global SlavePortsStop \"9\"\r\
    \n:for i from=\$SlavePortsStart to=\$SlavePortsStop do={\r\
    \n/interface ethernet set (\$PortType . \$i) master-port=\$MasterPort\r\
    \n}"
add name="Clear Ports" owner=admin policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive
source=\
    "/interface ethernet\r\
    \nset [find] master=none"
```

Download at http://wiki.ispsupplies.com
Search for "script"

Example 1

Helpful Scripts

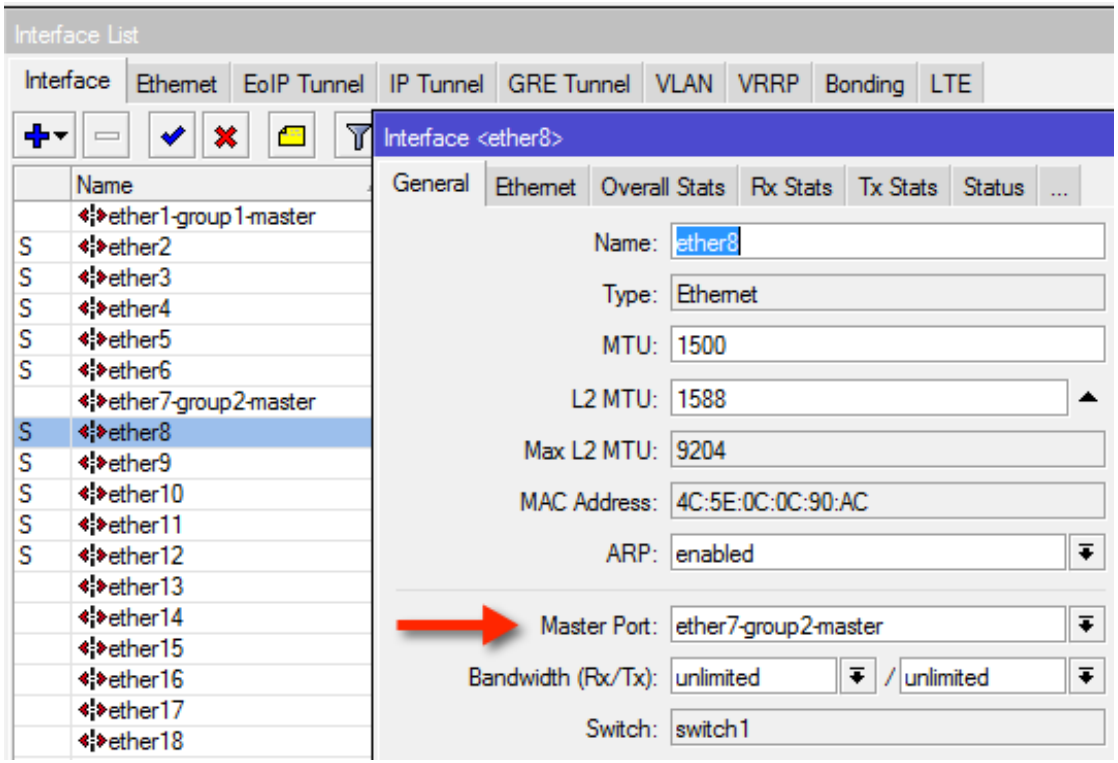


Example 1

Configure a Basic Switch

ether1
ether2
ether3
ether4
ether5
ether6

ether7
ether8
ether9
ether10
ether11
ether12



Result=2 x 6 port switches

That's it!

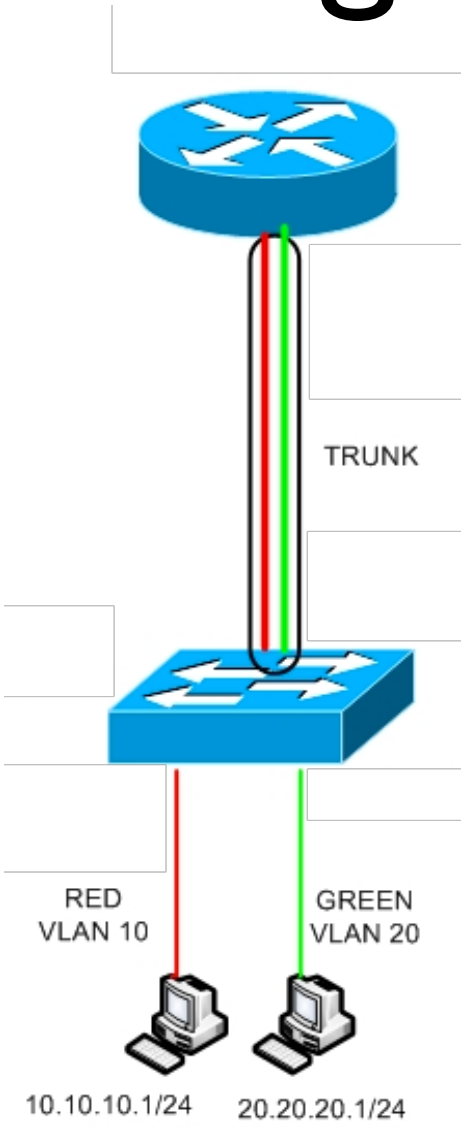
Interfaces

Example 2

Example 2

Inter VLAN Routing

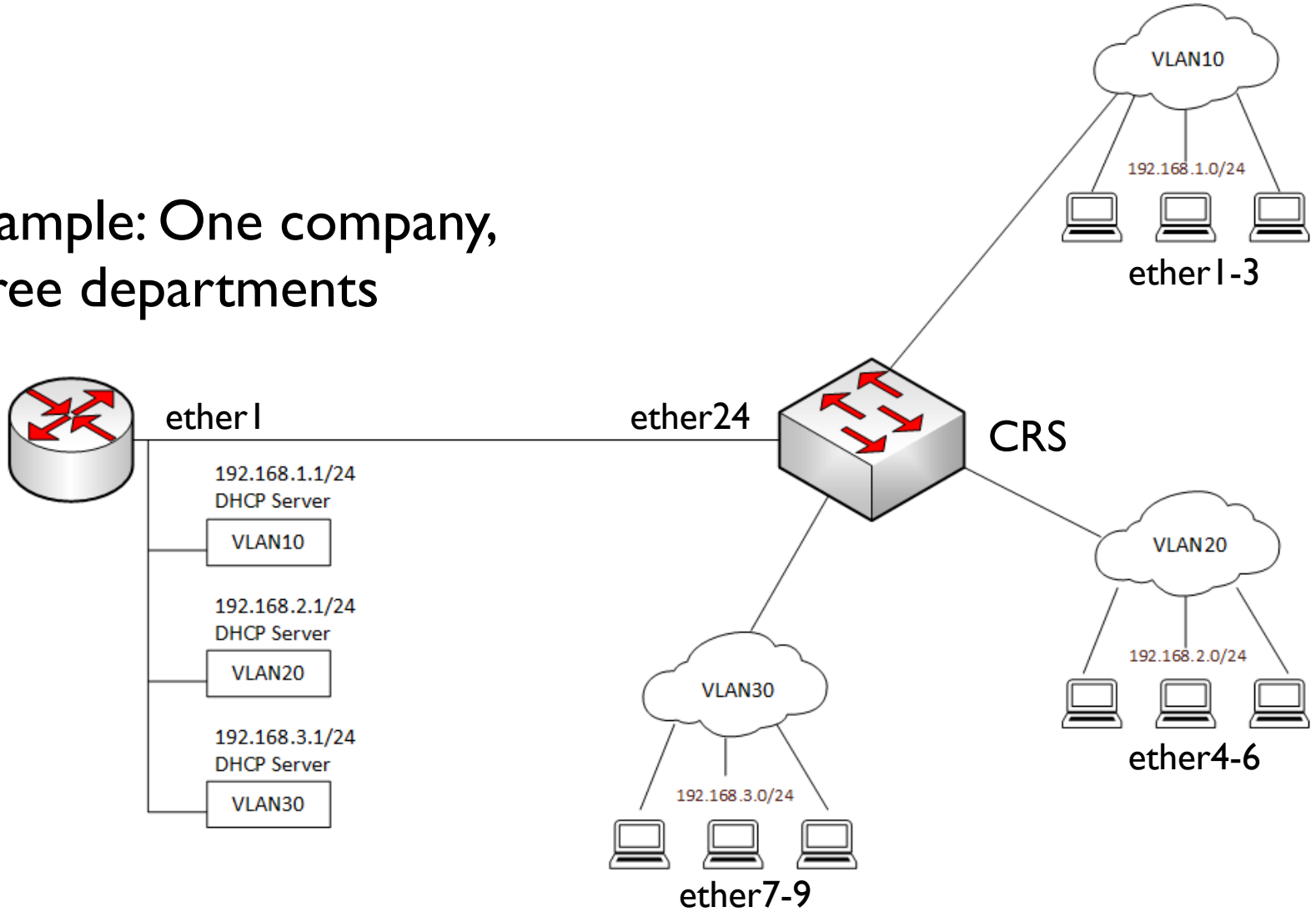
- Common configuration when a router needs many independent ports
- Each switch port appears as a separate virtual interface on the router



Example 2

Inter VLAN Routing

Example: One company, three departments



Example 2

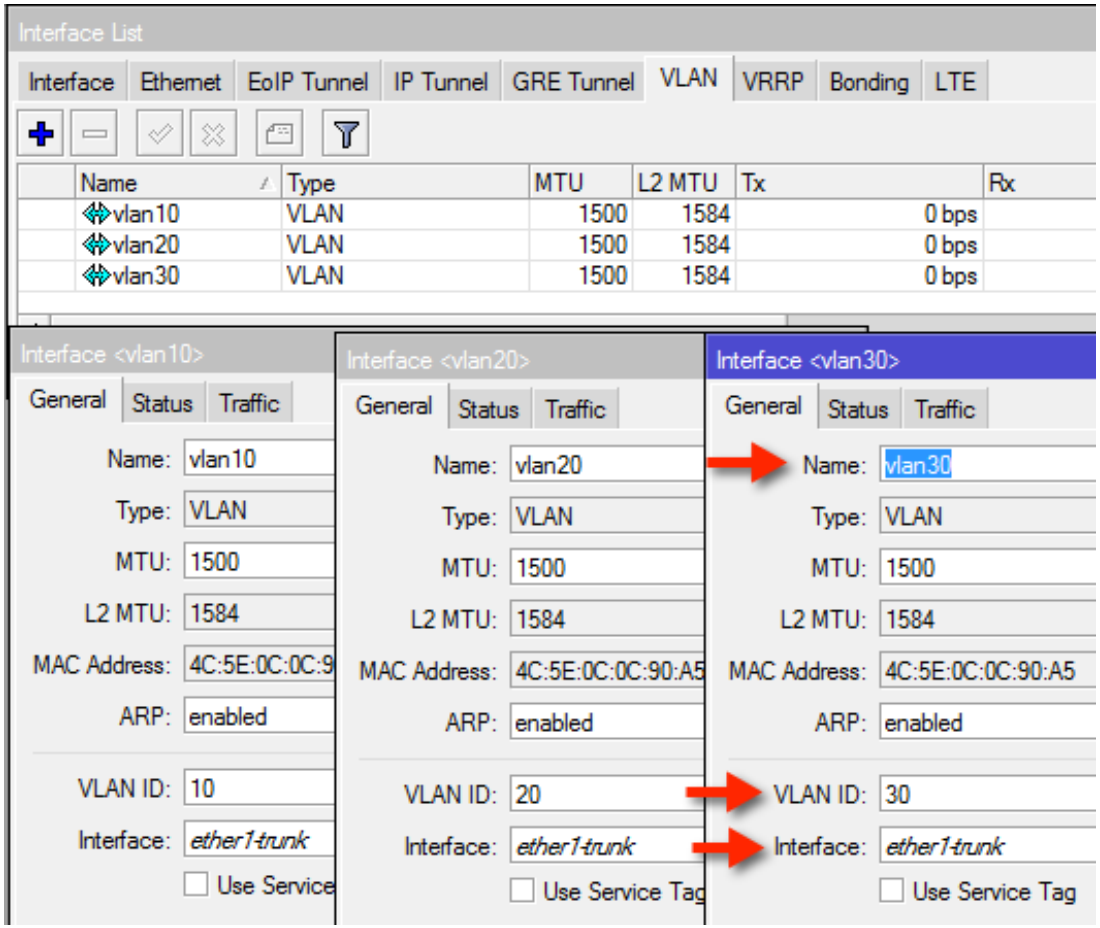
Inter VLAN Routing

Router Config

Step 1

- Separate routing device apart from CRS
- Router, create three VLAN interfaces subordinate to ether1

Interfaces → VLAN



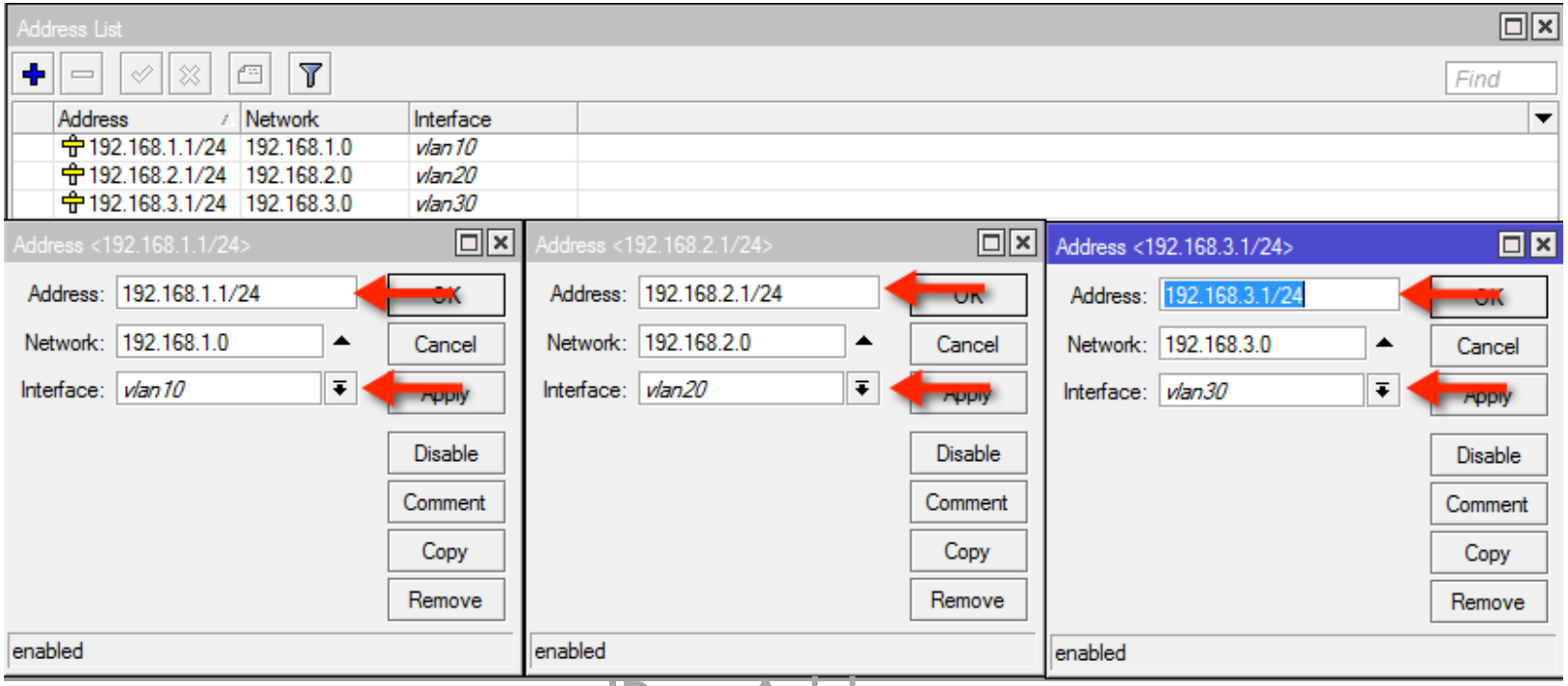
Example 2

Inter VLAN Routing

Router Config

Step 2

- Add IP Addresses to each VLAN interface



IP → Addresses

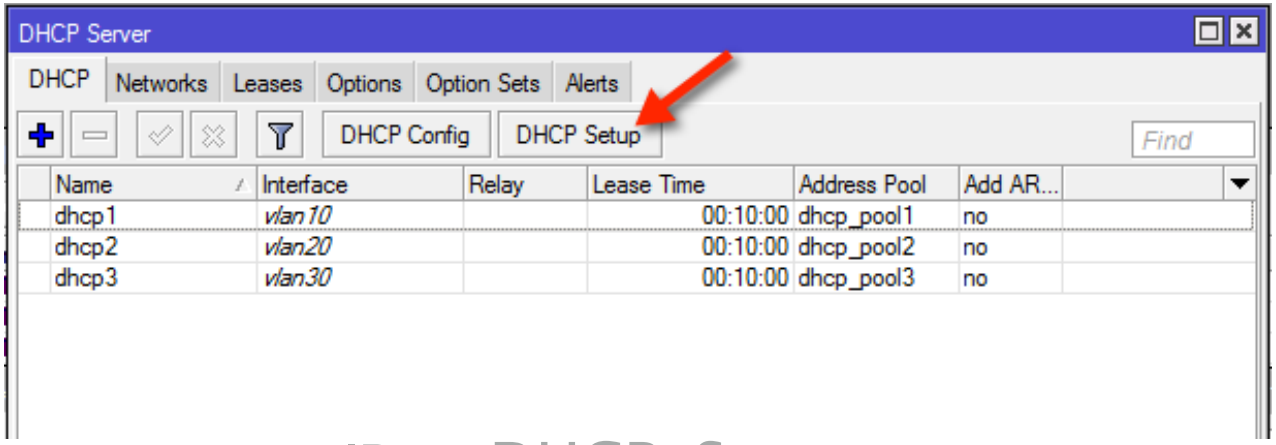
Example 2

Inter VLAN Routing

Router Config

Step 3

- And add DHCP Servers to each VLAN interface using the setup button and accept the defaults



IP → DHCP-Server

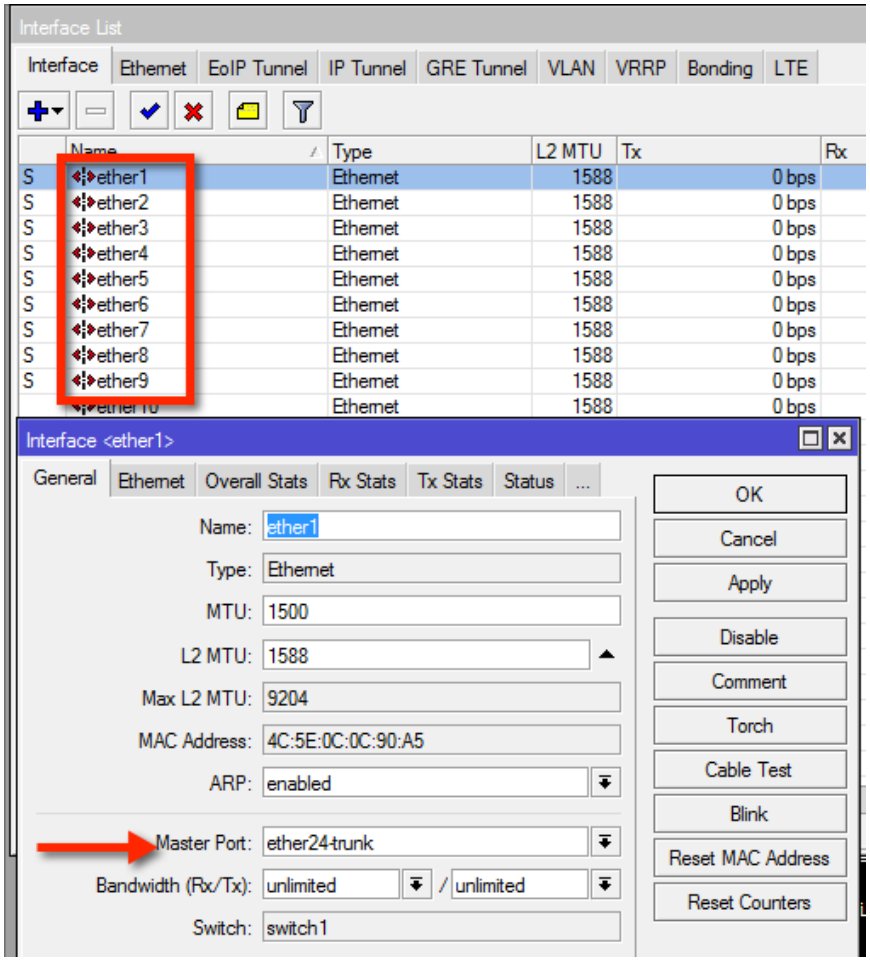
Example 2

Inter VLAN Routing

Switch Config

Step 1

- Create a switch port group, ether24 is master, ether1-ether9 are slaves to port 24 using our script "Set Ports"
- 1 switch port group



Interfaces

Example 2

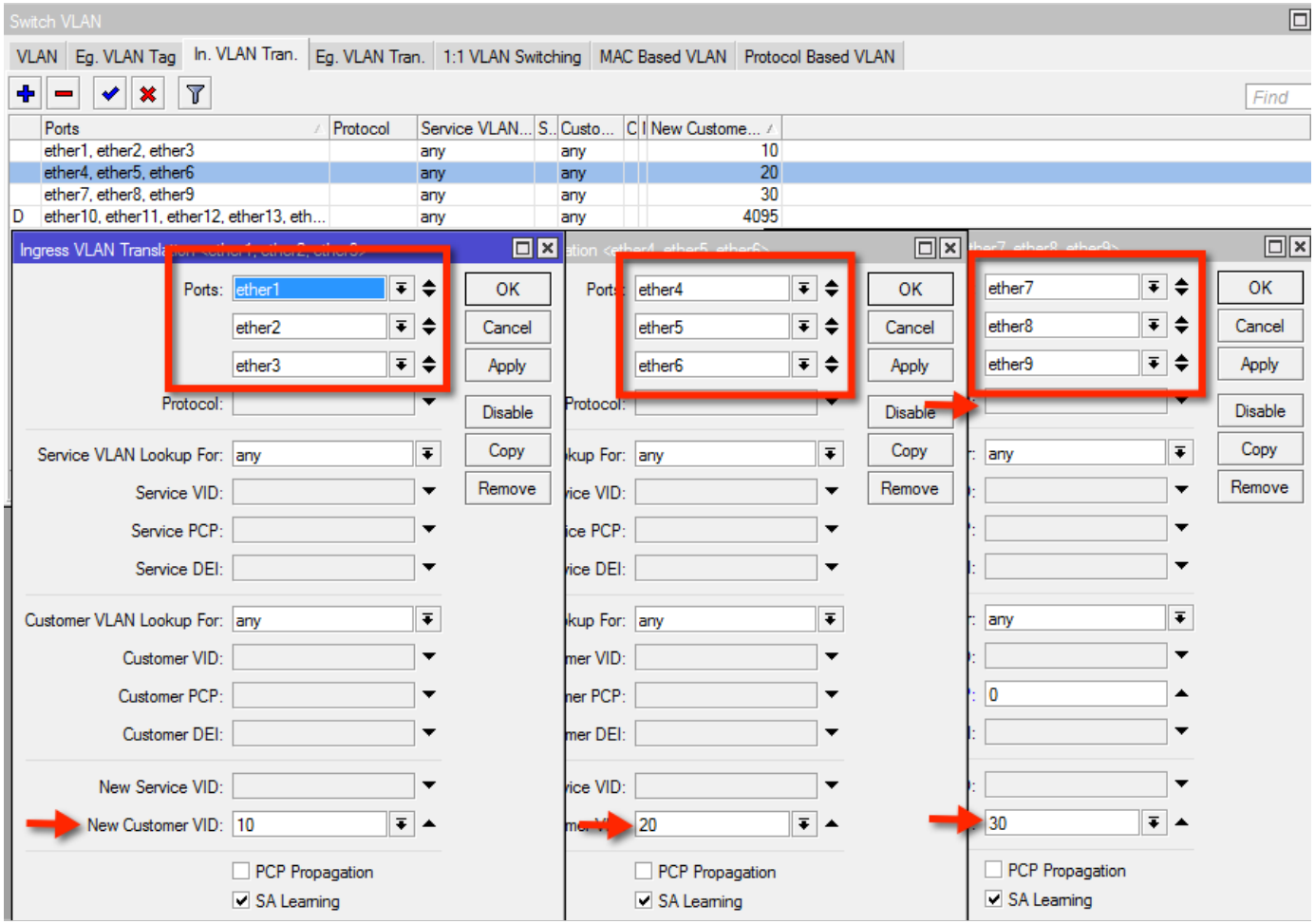
Inter VLAN Routing

Switch Config

Step 2

- Set access ports for each VLAN

Switch → VLAN → In-VLAN-Tran



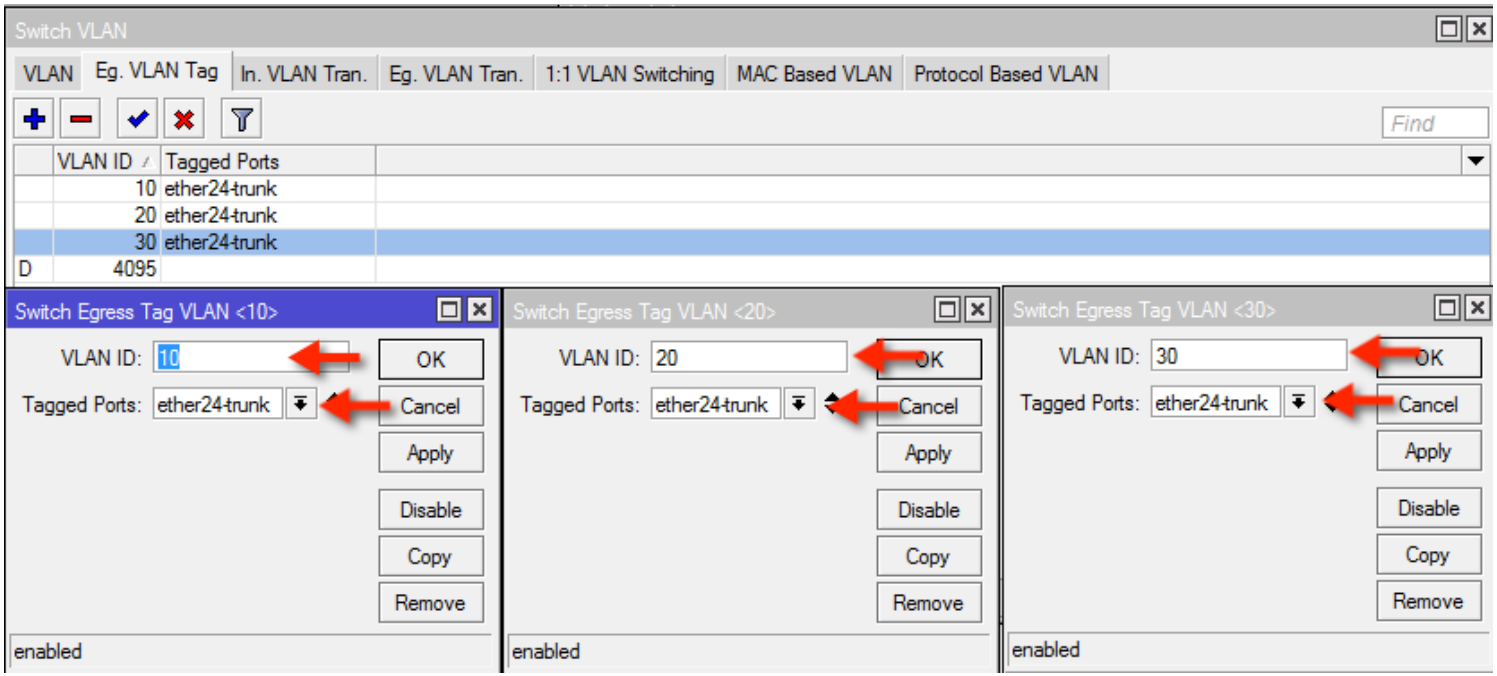
Example 2

Inter VLAN Routing

Switch Config

Step 3

- Set the trunk port, ether24



Switch → VLAN → Eg-VLAN-Tag

Example 2

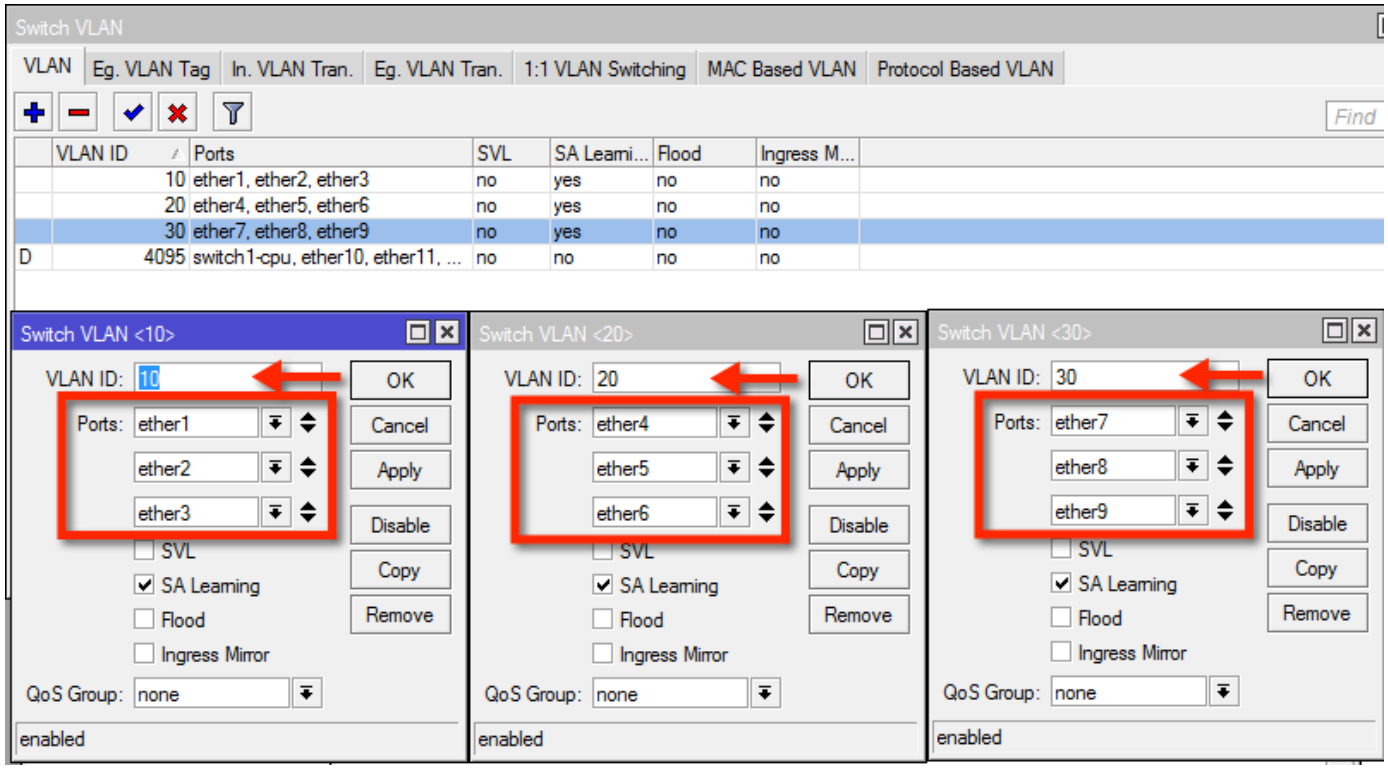
Inter VLAN Routing

Switch Config

Step 4

- Add VLAN membership definitions in the VLAN table

That's it!



Switch → VLAN → VLAN

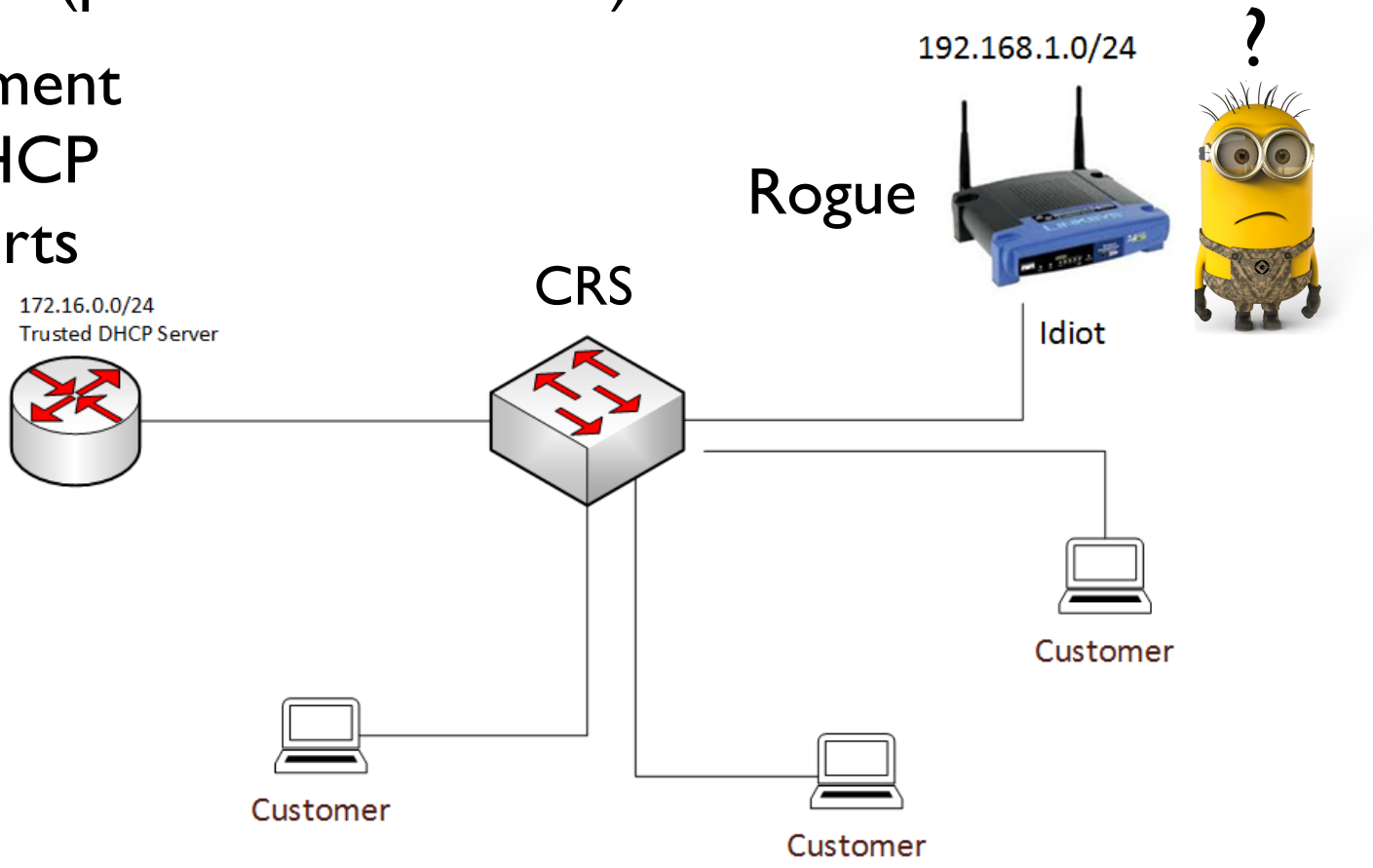
Example 3

Example 3

Configure Rogue DHCP Prevention

(port level isolation)

Example: MDU, apartment complex, etc., one DHCP server, 9 customer ports

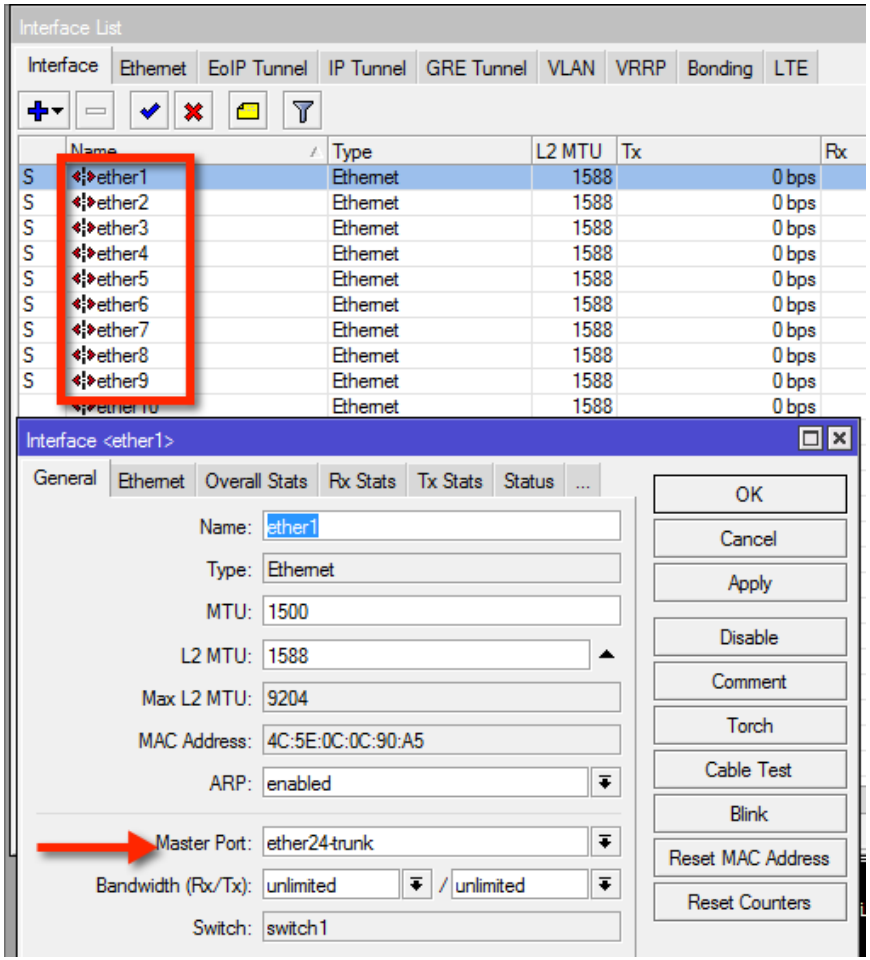


Example 3

Configure Rogue DHCP Prevention

Step 1

- Create a switch port group, ether24 is master, ether1-ether9 are slaves to port 24 using our script "Set Ports"



Interfaces

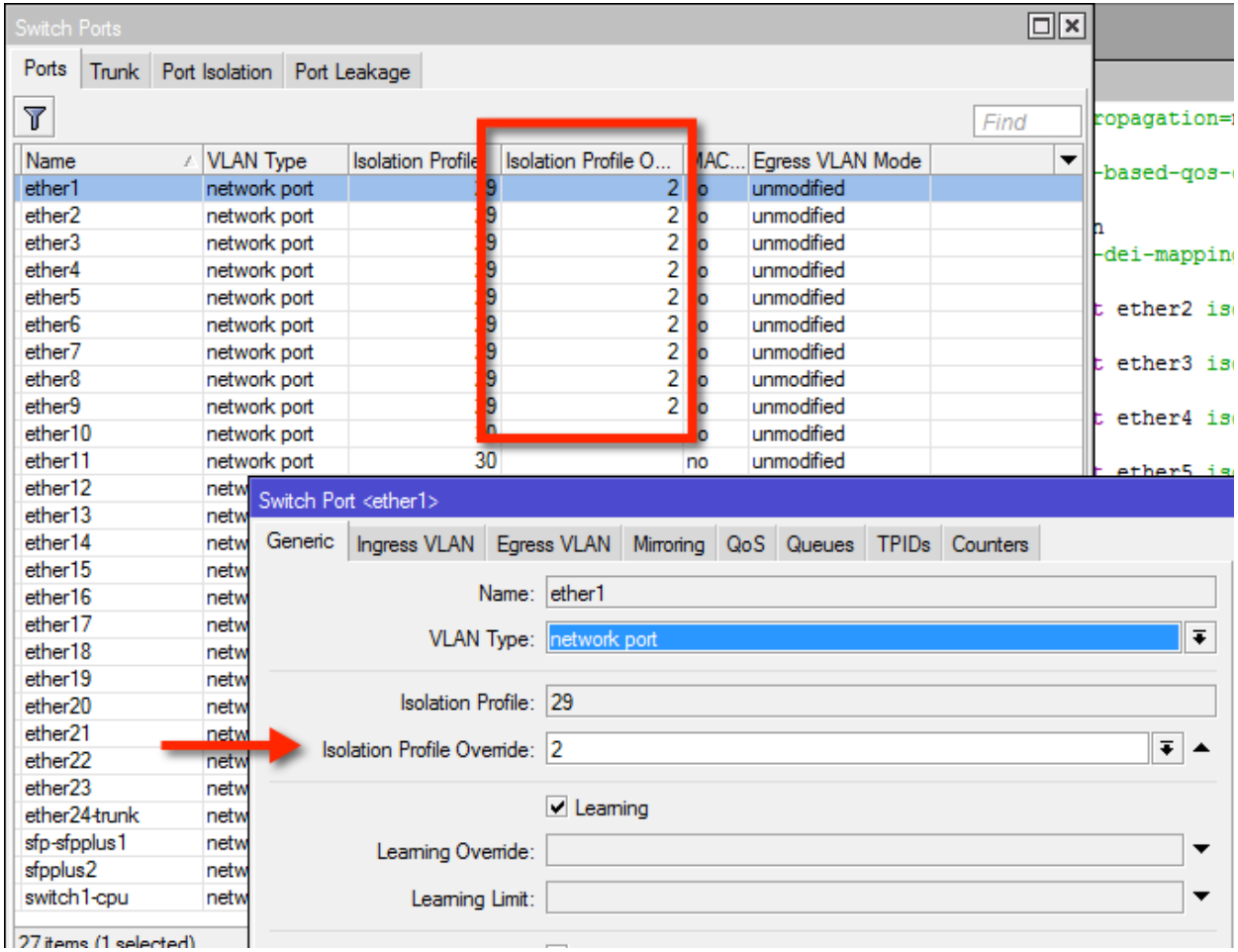
Example 3

Configure Rogue DHCP Prevention

Step 2

- Set the same Community port profile for all DHCP client ports. Community port profile numbers are from 2 to 30

Switch →Ports



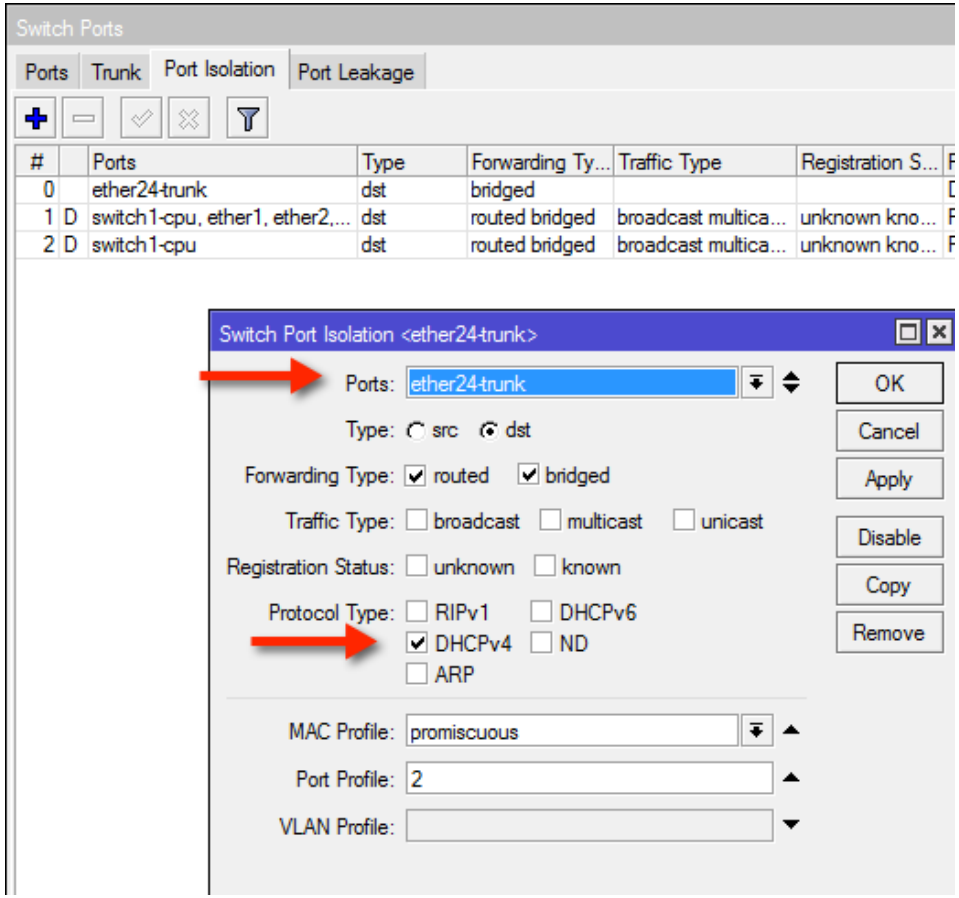
Example 3

Configure Rogue DHCP Prevention

Step 3

- Tell the switch which port is trusted for DHCP server
- Define your profile to match DHCP protocol traffic only, straight from the wiki.

Switch →Port Isolation



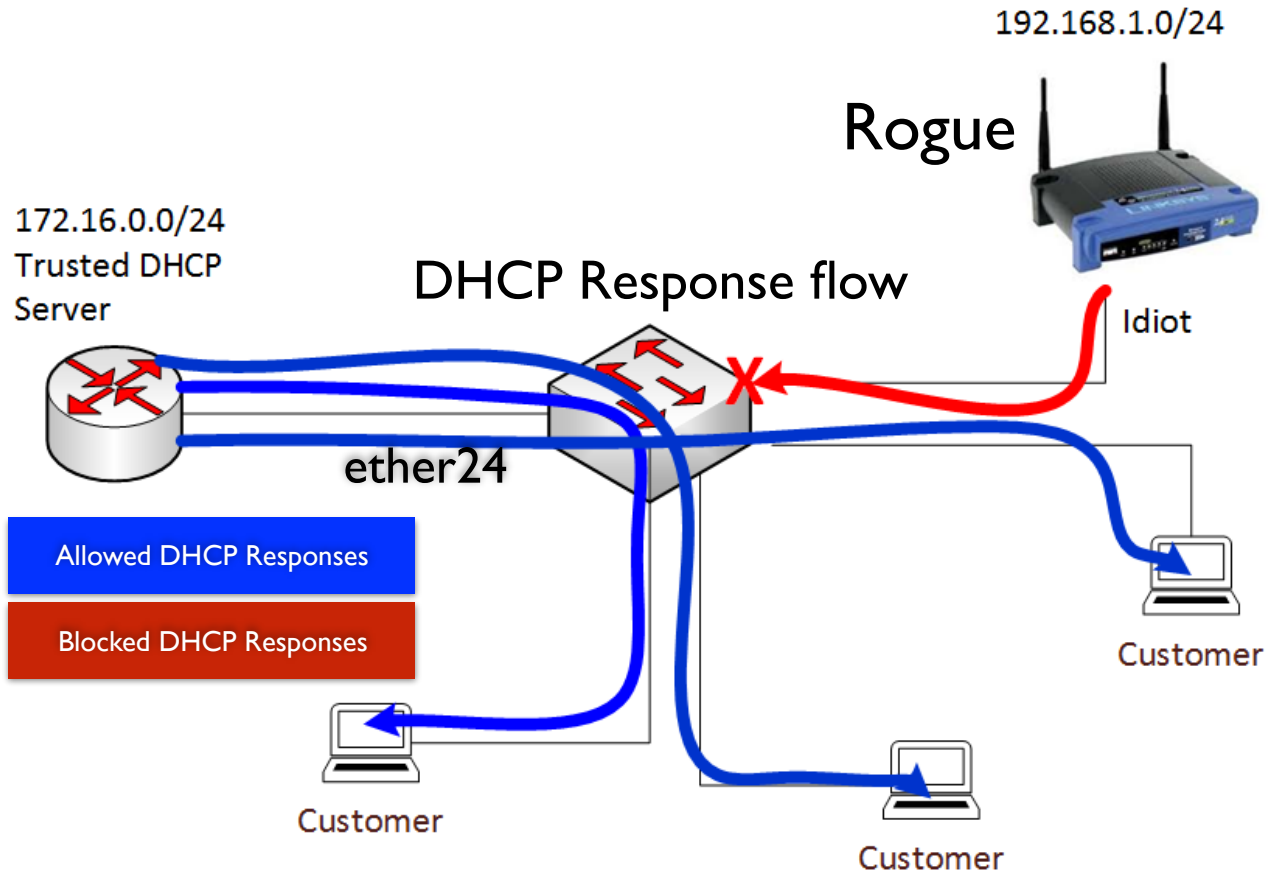
Example 3

Configure Rogue DHCP Prevention

Result: Customers will not see DHCP server responses unless they come from port 24.

All other traffic is allowed.

That's it!



Other Ideas With CRS

- **MAC based VLAN.** Tag packets as they enter a port based on MAC matcher

  Example: All Grandstream phones tag as VLAN100 based on MAC address pattern matcher

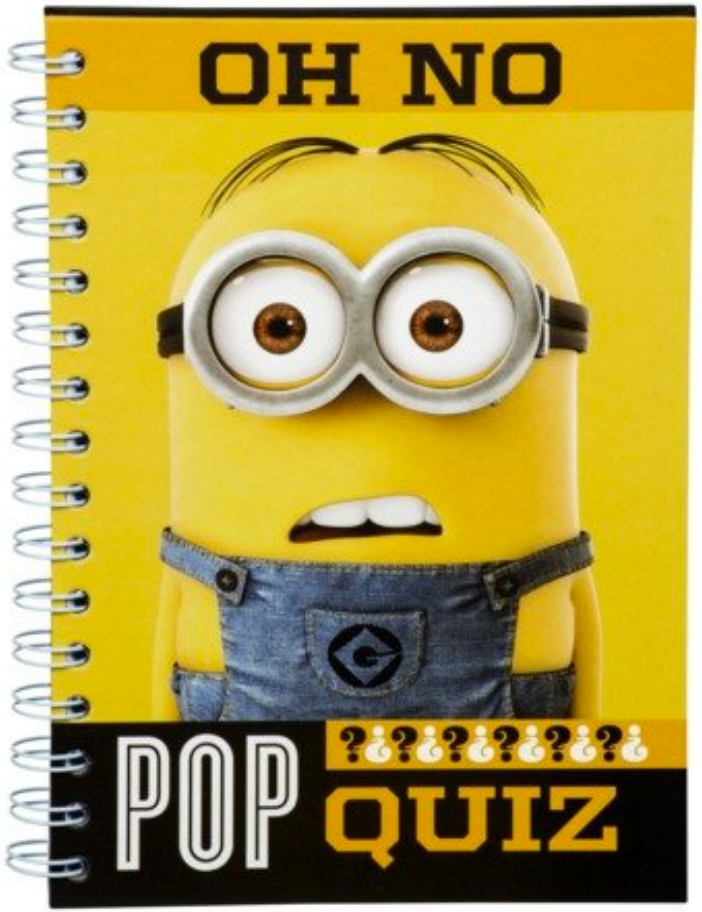
- **Port based bandwidth limiting**. Ensures virus infected hosts do not saturate uplinks.

- **Port based storm control.** Prevent disruptions on Layer 2 ports caused by broadcast, multicast or unicast traffic storms.

- Many other examples at http://wiki.mikrotik.com/wiki/Manual:CRS_examples

Summary

- Stop bridging when you have switching capabilities.
- Don't be overwhelmed by all the features, pick the two or three setups you actually need and learn them.
- Make your networks more efficient by utilizing VLANs and other advanced CRS features


OH NO
POP
QUIZ

Pop Quiz

- True or false - CRS supports various frame sizes up to but not including jumbo frames?
- What is the maximum number of VLANs supported by the CRS? 4000
- Which is done in software, switching or bridging? Bridging
- True or false - To configure port level isolation for rogue DHCP server control, we use the Port Isolation feature?
- True or false - To configure a basic switch on the CRS using the switch chip, create a bridge interface and add ports to it.

Questions?

MikroTik Maze Winners

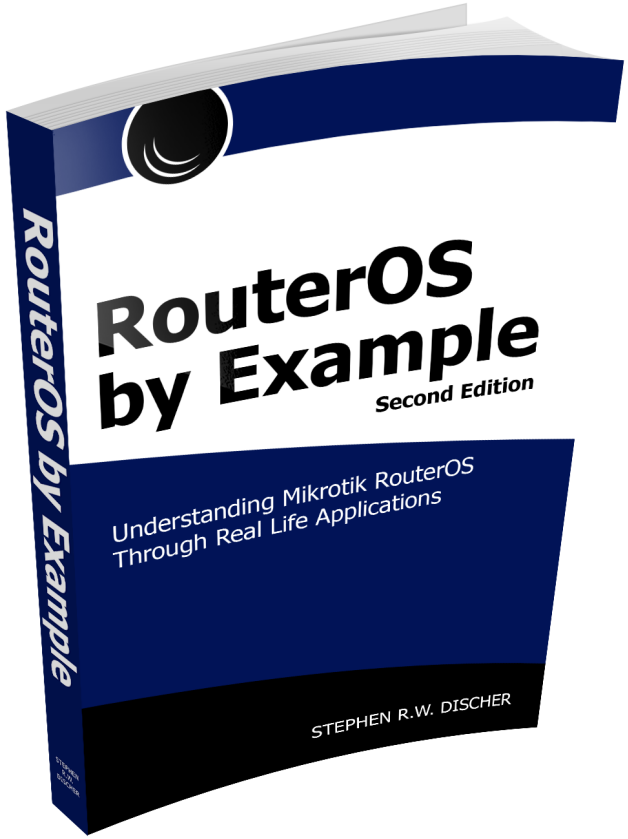
http://learnmikrotik.com/mazerunner/game.php

Top 5 Prizes

Come Get a Shirt!

Second Edition

- Updated everything to version 6
- Expanded the examples
- Added significant content for CRS switches
- Currently in edit, shipping beginning of summer 2016 Amazon and ISPSupplies.com



Thank you for playing!

- Try our MikroTik Maze at ISP Supplies table
- Training: MyWISPTraining.com & LearnMikroTik.com
- Store: ISPSupplies.com
- Blog: SteveDischer.com
- "RouterOS by Example" available from ISP Supplies, Amazon, 2nd Edition early summer
- Configurator: MikroTikConfig.com