

&lt;

Search...

 Search

- Quick links
  - Unanswered topics
  - Active topics
  - Search
  - FAQ
  - The team
  - Active topics
- Active topics
- Forum
- Contact us
  - Community discussions

- Quick links
  - Unanswered topics
  - Active topics
  - Search
  - FAQ
  - The team
  - Active topics
- Active topics
- Forum
- Contact us

Search...

 Search

- Register
- Login
  - 
  - 
  - Remember me
  -

1. 

- Announcements
- RouterOS
- RouterOS v6 RC and v7 BETA
- RouterOS v7
- Beginner Basics
- General
- Forwarding Protocols
- Wireless Networking
- Scripting
- Virtualization
- Other topics
- The Dude
- RouterBOARD hardware
- The User Manager
- SwOS

- Training
- 2. Home
- 3. Forum index
- 4. RouterOS
- 5. General

## CRS VLAN multiple tagged/trunk ports case study

+ Post Reply



• Print view

Search this topic...

### CRS VLAN multiple tagged/trunk ports case study (#p447474)

- [Quote](#) ([./posting.php?mode=quote&f=2&p=447474&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#))
- [#1](#) ([#p447474](#))
- [\(javascript:void\(0\);.\)](#)

Tue Sep 16, 2014 8:30 pm

Hello everyone,

I have a CRS226-24G-2S+RM, and I've been struggling to setup a connection for some ESXi servers that have several virtual machines on them in different vlan's, and I've attempted numerous configurations without no luck...

The idea here is to setup a few interfaces as trunk so that most of the vlan's (yes most of them but not all of them, the idea is to have a management vlan with private addressing) of each ESXi server can be accessed from the outside (WAN/internet), ether1 will have a public IP address and it will be in a DMZ provided by another L3 switch so that it can be directly accessed from the outside via vpn for remote management (the IP on ether1 is for that purpose only).

Most of the virtual machines are running services with public IP addresses such as webservers, e-mail servers and so on.

Here some schematics about what I've been trying to achieve for several days now with no luck at all:

[Image](http://postimg.org/image/uqrumjxjp/) (<http://postimg.org/image/uqrumjxjp/>)

I've been able to test with access/untagged ports with computers and such and succeeded with non-aware vlan devices but, my struggle is how in the hell do I configure multiple tagged vlans/trunk in a mikrotik CRS for me to get access from the outside for services like webservers and such?

Before someone asks me if I read the information in these links:

[http://wiki.mikrotik.com/wiki/Manual:CRS\\_examples](http://wiki.mikrotik.com/wiki/Manual:CRS_examples)

([http://wiki.mikrotik.com/wiki/Manual:CRS\\_examples](http://wiki.mikrotik.com/wiki/Manual:CRS_examples))

[http://wiki.mikrotik.com/wiki/Manual:CRS\\_features](http://wiki.mikrotik.com/wiki/Manual:CRS_features) ([http://wiki.mikrotik.com/wiki/Manual:CRS\\_features](http://wiki.mikrotik.com/wiki/Manual:CRS_features))

Yes I have...I've followed those steps and the only thing I was able to put it to work was the first port based VLAN example...

Any enlightenment in this issue would be highly appreciated, or I'm about to put the CRS's on a shelf waiting for the VLAN configuration became a bit more comprehensive in future RouterOS versions...

Thanks in advance and best regards

Last edited by Gr0ove ([./memberlist.php?mode=viewprofile&u=69714&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#)) on Wed Sep 17, 2014

11:51 am, edited 1 time in total.

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447543)

- [Quote](#) ([./posting.php?mode=quote&f=2&p=447543&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#))
- [#2 \(#p447543\)](#)
- [\(javascript:void\(0\);\)](#)

Wed Sep 17, 2014 8:39 am

The "tagged-ports" option in "egress-vlan-tag" table allows multiple values to support tagging on multiple ports.

Code: [Select all \(#\)](#)

```
/interface ethernet switch egress-vlan-tag
add tagged-ports=ether2,ether7,ether8 vlan-id=200
add tagged-ports=ether2,ether6,ether8 vlan-id=300
add tagged-ports=ether2,ether6,ether7 vlan-id=400
```

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447650)

- [Quote](#) ([./posting.php?mode=quote&f=2&p=447650&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#))
- [#3 \(#p447650\)](#)
- [\(javascript:void\(0\);\)](#)

Wed Sep 17, 2014 5:26 pm

Well...unfortunately the tagging isn't working for some reason, done everything has the examples and has **becs** said and I'm still haven't been able to have a port with no tagging + vlan500 (for example)

only been able to setup access ports, the rest nothing...

CRS's are crap dealing with vlan traffic...

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447797)

- [Quote](#) ([./posting.php?mode=quote&f=2&p=447797&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#))
- [#4 \(#p447797\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 1:01 pm

For example, I want **ether10** in a no-vlan network (vlan 0) so it would be untagged for vlan 0, and I want it to be tagged in vlan 500.

**Trunk port** where all vlan's traffic will go thru will be **ether1**.

Please correct me if I'm wrong:

Code: [Select all \(#\)](#)

```
/interface ethernet
```

```
set ether10 master-port=ether1
```

untagged:

Code: [Select all \(#\)](#)

```
/interface ethernet switch ingress-vlan-translation
```

```
add ports=ether1,ether10 customer-vid=0 new-customer-vid=0 sa-learning=yes
```

tagged:

Code: [Select all \(#\)](#)

```
/interface ethernet switch egress-vlan-tag
```

```
add tagged-ports=ether1,ether10 vlan-id=500
```

vlan membership:

Code: [Select all \(#\)](#)

```
/interface ethernet switch vlan
```

```
add ports=ether1,ether10 vlan-id=0 learn=yes
```

```
add ports=ether1,ether10 vlan-id=500 learn=yes
```

disable unknown vlan's:

Code: [Select all \(#\)](#)

```
/interface ethernet switch
```

```
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10
```

Afterwards I connect a PC to the ether10 and I get an IP via DHCP server of the correct vlan 0 network, "BUT" after 3 seconds it loses connectivity to the network and the IPv4 connectivity of the PC network adapter goes from having internet from not having and I can't ping other devices in the same network...

Not getting why it's doing this, strange... 😕

Last edited by Gr0ove ([./memberlist.php?mode=viewprofile&u=69714&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#)) on Thu Sep 18, 2014

4:48 pm, edited 1 time in total.

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447826)

- [Quote \(\[./posting.php?mode=quote&f=2&p=447826&sid=a8236cde195e02be4ab41bdcc0c6ed5f\]\(#\)\)](#)
- [#5 \(#p447826\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 3:49 pm

The current configuration does both tagging and untagging on both ports at the same time which seems to cause the problem.

Trunk ports typically do not need ingress VLAN translation rules.

And the ingress VLAN translation rule makes untagged traffic to be a member of VLAN500, therefore VLAN0 is not necessary.

This should be correct configuration:

untagged:

Code: [Select all \(#\)](#)

```
/interface ethernet switch ingress-vlan-translation
```

```
add ports=ether10 customer-vid=0 new-customer-vid=500 sa-learning=yes
```

tagged:

Code: [Select all \(#\)](#)

```
/interface ethernet switch egress-vlan-tag
```

```
add tagged-ports=ether1 vlan-id=500
```

vlan membership:

Code: [Select all \(#\)](#)

```
/interface ethernet switch vlan
add ports=ether1,ether10 vlan-id=500 learn=yes
```

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447840)

- [Quote \(./posting.php?mode=quote&f=2&p=447840&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#6 \(#p447840\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 4:58 pm

First of all thanks for the help 😊

But with the configuration that you told me I've just put ether10 only in access mode/untagged for vlan 500, so every vlan non-aware device will connect to vlan 500 network and it's not what I'm looking for.

The goal here is to configure ether10 to have an untagged vlan (normal network without any tagging) and a tagged vlan 500, so that when I connect for example a ESXi vmware server the physical NIC stays in the untagged network and a virtual machine in vlan 500 (the virtual machine is already in vlan 500 in its network configuration).

I can do that very easily with another standard L2 manageable switch and it works fine, I'm having trouble only with mikrotik tagging and untagging logic and procedures.

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447847)

- [Quote \(./posting.php?mode=quote&f=2&p=447847&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#7 \(#p447847\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 5:27 pm

I got it now. 😊 Such configuration should already work with default settings or simply with a group of switched ports because all VLANs are allowed by default.

You do not need to do tagging or untagging on the CRS, just configure VLAN filtering to allow certain VLANs and block others.

Code: [Select all \(#\)](#)

```
/interface ethernet
set ether10 master-port=ether1
```

```
/interface ethernet switch vlan
add ports=ether1,ether10 vlan-id=0 learn=yes
add ports=ether1,ether10 vlan-id=500 learn=yes
/interface ethernet switch
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10
```

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447853)

- [Quote \(./posting.php?mode=quote&f=2&p=447853&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)

- [#8 \(#p447853\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 6:29 pm

Hi again and thanks for all your help so far 😊

But CRS still isn't isolating things right, so I connected the ESXi server to ether10 and the virtual machine in vlan 500 communicates fine but for the network of the physical NIC in default vlan that isn't the case unfortunately...it loses packets all around, try to ping the NIC and in 50 pings it only responds to 15 and randomly

Something is missing in the configuration or there's bugs in RouterOS in terms of vlan functions 😞

This is becoming annoying...Mikrotik should arrange a more simple and effective method of working with vlans has other manufacturers do 🤦

[Top](#)

## Re: CRS VLAN multiple tagged/trunk ports case study (#p447872)

- [Quote \(./posting.php?mode=quote&f=2&p=447872&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#9 \(#p447872\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 18, 2014 8:41 pm

I think I discovered what the problem was...looks like the CRS doesn't like too much default vlan (or vlan 0) 😊 so just because, I tested the next setup:

In ether10 I've configured for another vlan to be untagged other then vlan 0, for example, I've configured vlan 99 to be untagged and afterwards just added ether1 and ether10 to vlan 99 membership and now my ESXi server physical NIC connects to vlan 99 and the virtual machine connects to vlan 500 without the need of tagging in the CRS of some sort which I'm not used to see or think 😕 oh well at least I discovered why I wasn't succeeding by trying to configure default vlan in the physical NIC...

Such has this basic schematics:



My configuration:

create group of switched ports:

Code: [Select all \(#\)](#)

**/interface ethernet**

**set ether10 master-port=ether1**

untagged:

Code: [Select all \(#\)](#)

**/interface ethernet switch ingress-vlan-translation**

**add ports=ether10 customer-vid=0 new-customer-vid=99 sa-learning=yes**

vlan membership:

Code: [Select all \(#\)](#)

**/interface ethernet switch vlan**

**add ports=ether1,ether10 vlan-id=99 learn=yes**

**add ports=ether1,ether10 vlan-id=500 learn=yes**

disable unknown vlans:

Code: [Select all \(#\)](#)

```
/interface ethernet switch
```

```
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10
```

I know that at first sight it looks simple and it really is but the default vlan situation was giving me a headache so this was the only way I've discovered to do what I've needed...but I still think the way mikrotik switches deal with vlans it's weird...

Top

## Re: CRS VLAN multiple tagged/trunk ports case study (#p448914)

- [Quote \(./posting.php?mode=quote&f=2&p=448914&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#10 \(#p448914\)](#)
- [\(javascript:void\(0\);\)](#)

Thu Sep 25, 2014 6:34 pm

Hi again,

Looks like the procedure I last described wasn't exactly what it was intended...

Is there any way of doing the schematics in the picture below without any routing at all? Or I'm obligated to do routing?



I'm running out of ideas... 😞

Thanks in advance

Top

## Re: CRS VLAN multiple tagged/trunk ports case study (#p449010)

- [Quote \(./posting.php?mode=quote&f=2&p=449010&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#11 \(#p449010\)](#)
- [\(javascript:void\(0\);\)](#)

Fri Sep 26, 2014 10:21 am

Try the following configuration, it should work wire-speed and without routing.

Code: [Select all \(#\)](#)

```
/interface ethernet
```

```
set ether10 master-port=ether1
```

```
set ether11 master-port=ether1
```

```
/interface ethernet switch vlan
```

```
add ports=ether10,ether11,switch1-cpu vlan-id=99 learn=yes
```

```
add ports=ether1,ether10,ether11 vlan-id=500 learn=yes
```

```
/interface ethernet switch
```

```
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10,et1
```

*#CRS226 management configuration*

```
/interface vlan
```

```
add name=vlan99 vlan-id=99 interface=ether1
```

```
/ip address
```

```
add address=192.168.88.1/24 interface=vlan99 network=192.168.88.0
```

I would like to know details about what is not working if it is not working.

[Top](#)**Re: CRS VLAN multiple tagged/trunk ports case study (#p449027)**

- [Quote](#) ([./posting.php?mode=quote&f=2&p=449027&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#)).
- [#12](#) ([#p449027](#)).
- [\(javascript:void\(0\);\)](#).

Fri Sep 26, 2014 1:08 pm

Hi there, thanks for the reply

My question here is, internet comes in without any vlan or tagging of some sort because it comes from another switch of the ISP that provides direct internet connection, so will it be possible for virtual machines in vlan500 to pass directly to the internet and maintain isolation from management vlan99? Wouldn't be needed some kind of tagging for the incoming traffic that comes through ETHER1 for it to distinguish what goes to where?

The goal I'm looking for is isolate both vlan's from each other (as obvious) with only vlan500 accessing directly to the internet. Vlan99 as I mentioned in the schematics it would be only for local management or remote management through VPN connection to the mikrotik.

Thanks

[Top](#)**Re: CRS VLAN multiple tagged/trunk ports case study (#p449036)**

- [Quote](#) ([./posting.php?mode=quote&f=2&p=449036&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#)).
- [#13](#) ([#p449036](#)).
- [\(javascript:void\(0\);\)](#).

Fri Sep 26, 2014 2:48 pm

The previous configuration would work if the Internet comes in with tagged VLAN500.

When you have to start dealing with tagging and untagging in CRS switch-chip, both Ingress VLAN translation and Egress VLAN Tag tables have to be configured for particular VLAN, in this case VLAN500.

Code: [Select all](#) (#).

```
/interface ethernet switch egress-vlan-tag
add tagged-ports=ether10,ether11 vlan-id=500
```

```
/interface ethernet switch ingress-vlan-translation
```

```
add customer-vid=0 new-customer-vid=500 ports=ether1 sa-learning=yes
```

Note this configuration will do your required forwarding except CRS will not be accessible from the Internet (CRS won't be accessible from ether1 port).

[Top](#)**Re: CRS VLAN multiple tagged/trunk ports case study (#p449054)**

- [Quote](#) ([./posting.php?mode=quote&f=2&p=449054&sid=a8236cde195e02be4ab41bdcc0c6ed5f](#)).
- [#14](#) ([#p449054](#)).
- [\(javascript:void\(0\);\)](#).

Fri Sep 26, 2014 4:19 pm

Thanks again for the quick reply,

I've tested both scenarios that you've suggested and for the configuration:

Code: [Select all \(#\)](#)

```
/interface ethernet
set ether10 master-port=ether1
set ether11 master-port=ether1

/interface ethernet switch vlan
add ports=ether10,ether11,switch1-cpu vlan-id=99 learn=yes
add ports=ether1,ether10,ether11 vlan-id=500 learn=yes
/interface ethernet switch
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10,ether11
```

#### *#CRS226 management configuration*

```
/interface vlan
add name=vlan99 vlan-id=99 interface=ether1
/ip address
add address=192.168.88.1/24 interface=vlan99 network=192.168.88.0
```

I lose connection to ether1 from outside and can't get to the virtual machines on the other side either when inserting command:

```
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10,ether11
```

In the second configuration method that you suggested, if remote access can't be implemented it would be useless for my situation 😞

Maybe it can't be done with Mikrotik CRS only in layer 2, I don't know...maybe I'll be obligated to use routing

Top

#### **Re: CRS VLAN multiple tagged/trunk ports case study (#p449546)**

- [Quote \(./posting.php?mode=quote&f=2&p=449546&sid=a8236cde195e02be4ab41bdcc0c6ed5f\)](#)
- [#15 \(#p449546\)](#)
- [\(javascript:void\(0\);\)](#)

Tue Sep 30, 2014 10:59 am

I modified configuration to allow remote access to CRS226 from ether1 port too.

Also I set VLAN filtering in the last place in configuration, probably, access is lost to the CRS before all necessary configuration is applied.

P.S. IP addresses are just for an example.

Code: [Select all \(#\)](#)

```
#Group of switched ports
/interface ethernet
set ether10 master-port=ether1
set ether11 master-port=ether1
```

#### *#CRS226 internal management*

```
/interface vlan
add name=vlan99 vlan-id=99 interface=ether1
/ip address
add address=10.0.0.1/24 interface=vlan99 network=10.0.0.0
```

#### *#CRS226 external management*

```

/interface vlan
add name=vlan500 vlan-id=500 interface=ether1
/ip address
add address=20.0.0.1/24 interface=vlan500 network=20.0.0.0
/ip route
add gateway=20.0.0.254

#VLAN trunk ports
/interface ethernet switch egress-vlan-tag
add tagged-ports=ether10,ether11,switch1-cpu vlan-id=99
add tagged-ports=ether10,ether11,switch1-cpu vlan-id=500

#VLAN access port
/interface ethernet switch ingress-vlan-translation
add customer-vid=0 new-customer-vid=500 ports=ether1 sa-learning=yes

#VLAN filtering
/interface ethernet switch vlan
add ports=ether10,ether11,switch1-cpu vlan-id=99 learn=yes
add ports=ether1,ether10,ether11,switch1-cpu vlan-id=500 learn=yes
/interface ethernet switch
set drop-if-invalid-or-src-port-not-member-of-vlan-on-ports=ether1,ether10,ether11

```

Top

## Re: CRS VLAN multiple tagged/trunk ports case study (#p450105)

- [Quote \(./posting.php?mode=quote&f=2&p=450105&sid=a8236cde195e02be4ab41bdcc0c6ed5f\).](#)
- [#16 \(#p450105\).](#)
- [\(javascript:void\(0\);\).](#)

Fri Oct 03, 2014 7:02 pm

Hi there, thanks again for the reply

I have a question (maybe a stupid one but I want to learn and understand this), so if the internet traffic comes without any tagging at all, how will the virtual machines communicate directly to the internet only through Layer 2?

The traffic from the internet comes untagged right, and will it be tagged to vlan500 when it enters CRS and will be untagged when exiting? Don't know if I've made my self cleared 😊

And just another thing, in the "/ip route add gateway=20.0.0.254" don't I have to define the destination address also? Like 0.0.0.0?

Thank you

Top

## Re: CRS VLAN multiple tagged/trunk ports case study (#p450803)

- [Quote \(./posting.php?mode=quote&f=2&p=450803&sid=a8236cde195e02be4ab41bdcc0c6ed5f\).](#)
- [#17 \(#p450803\).](#)
- [\(javascript:void\(0\);\).](#)

Wed Oct 08, 2014 12:44 pm

I have a question (maybe a stupid one but I want to learn and understand this), so if the internet traffic comes without any tagging at all, how will the virtual machines communicate directly to the internet only through Layer 2?

The traffic from the internet comes untagged right, and will it be tagged to vlan500 when it enters CRS and will be untagged when exiting? Don't know if I've made my self cleared 😊

The traffic in CRS from ether1 to ether10 & ether11 will be tagged with vlan500 and traffic from ether10 & ether11 to ether1 in CRS will be untagged. The Internet will not know anything about vlan500.

And just another thing, in the "/ip route add gateway=20.0.0.254" don't I have to define the destination address also? Like 0.0.0.0?

"/ip route add gateway=20.0.0.254" is the short version of command, because "dst-address" parameter already has default value - "0.0.0.0/0"

Top

### **Re: CRS VLAN multiple tagged/trunk ports case study (#p451806)**

- [Quote](#) (. ./posting.php?mode=quote&f=2&p=451806&sid=a8236cde195e02be4ab41bdcc0c6ed5f).
- [#18 \(#p451806\)](#).
- [\(javascript:void\(0\);\)](#).

Tue Oct 14, 2014 7:49 pm

Hi becs,

Sorry for the late reply, just to say it worked like a charmed 😊 fully tested and doing what it was intended, thanks for all your great help 😊

Best regards

Top

Display posts from previous: [All posts](#) ▼ [All posts](#) Sort by [Post time](#) ▼ [Post time](#)  
[Ascending](#) ▼ [Ascending](#) ➔

+ Post Reply



• [Print view](#)

### **Who is online**

Users browsing this forum: No registered users and 59 guests

1.

- Announcements
- RouterOS
- RouterOS v6 RC and v7 BETA
- RouterOS v7
- Beginner Basics
- General
- Forwarding Protocols
- Wireless Networking
- Scripting
- Virtualization
- Other topics

- The Dude
  - RouterBOARD hardware
  - The User Manager
  - SwOS
  - Training
2. Home
3. Forum index
4. RouterOS
5. General
- × Delete all board cookies
  - The team
  - Contact us
  - × Delete all board cookies
  - The team
  - Contact us



Powered by phpBB® Forum Software © phpBB Limited  
Design by SlickThemes

X  
^ v