



ROMON VS MANAGEMENT VLAN

WISPCASTS.COM

MANAGING ROUTERS



How do We do it

ROUTER MANAGEMENT

- ▶ Only via Management Port (really?)
- ▶ via Data Port
- ▶ Most of the time Discovery is not disabled on L2 Networks
- ▶ Mac-Winbox can be a life saver !

“IF YOU WANT TOTAL SECURITY, GO TO PRISON. THERE YOU'RE FED, CLOTHED, GIVEN MEDICAL CARE AND SO ON. THE ONLY THING LACKING... IS FREEDOM.”

Dwight D. Eisenhower



WHAT IF NETWORK IS LARGER ?

MANAGEMENT IN LARGE SCALE

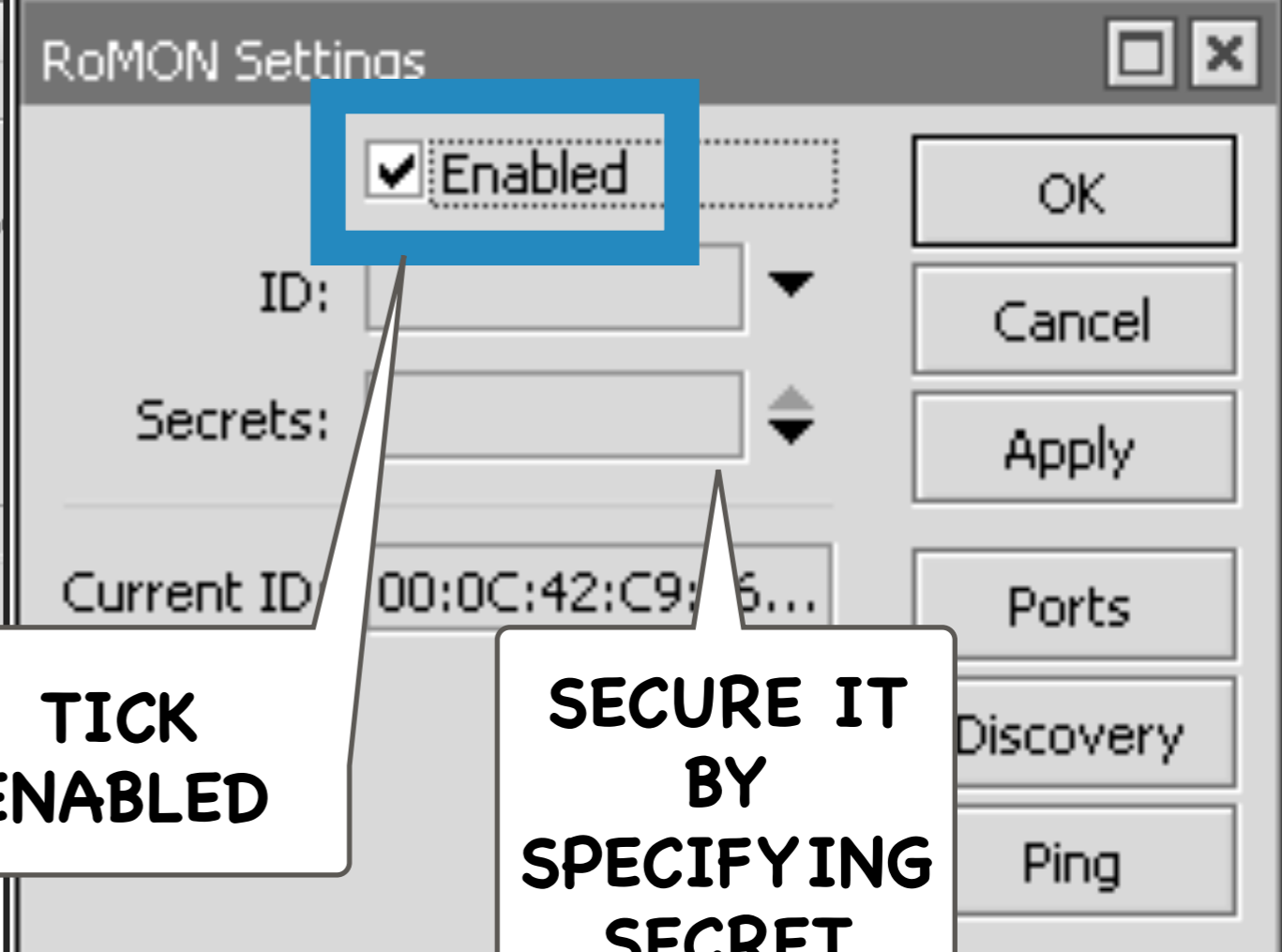
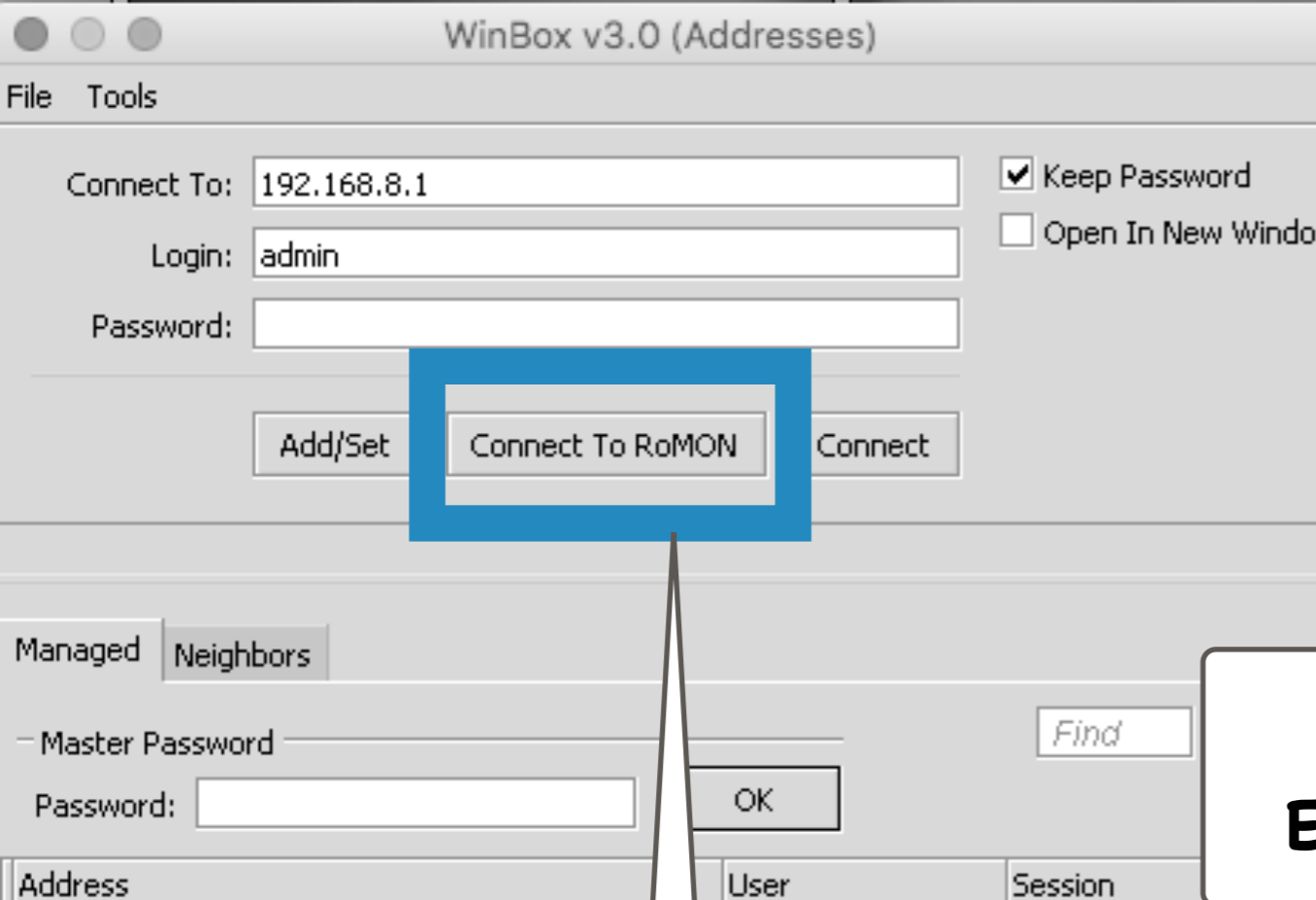


ROMON

**ONE EXTRA
LAYER ?**

LAYER 2 ACCESS ACROSS LAYER3 NETWORK

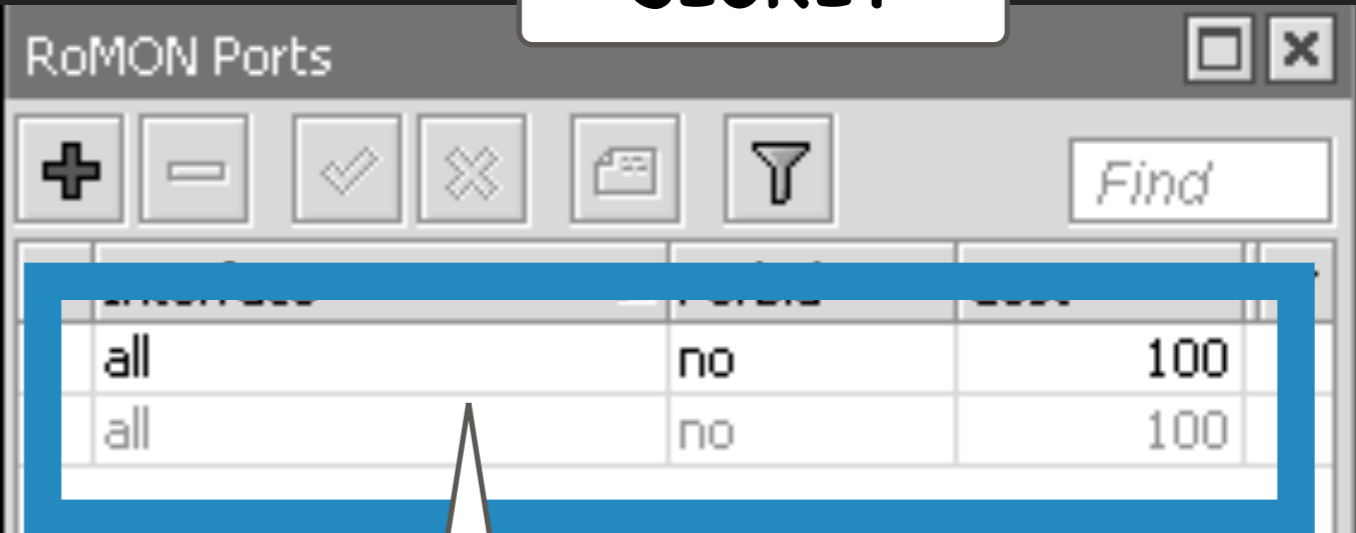
- ▶ Allow Discovery and Management
- ▶ Works across multiple hops
- ▶ Dead easy to configure
- ▶ Dead easy to use with latest Winbox (3.x) version



**TICK
ENABLED**

**SECURE IT
BY
SPECIFYING
SECRET**

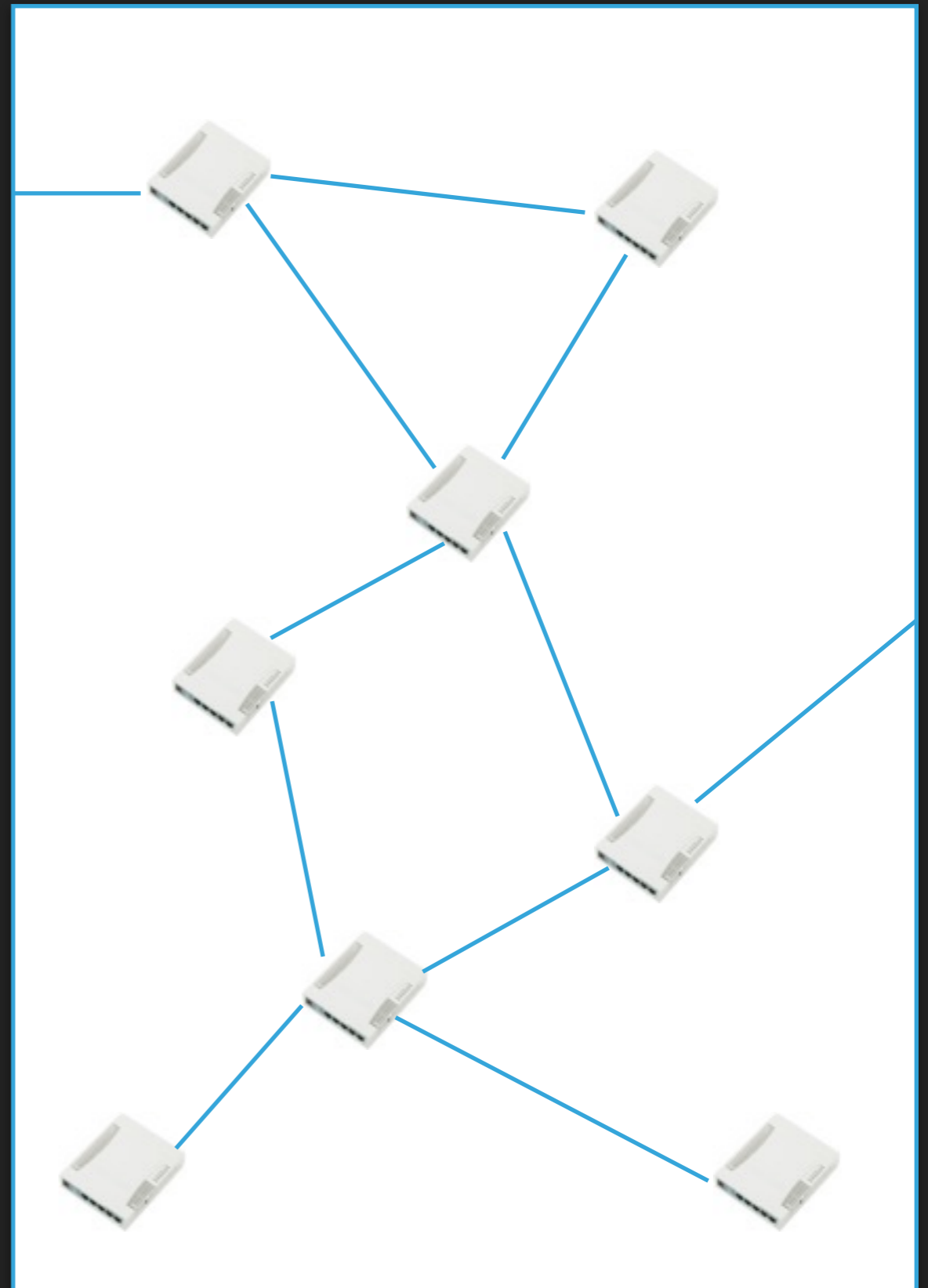
**ROMON IS IMPLEMENTED IN
WINBOX CLIENT AND IS
SUPER EASY TO USE**



**SECURE IT MORE
EXCLUDING CUSTOMER
FACING INTERFACES**

WITH ROMON YOU CAN:

- ▶ Discover devices many hops away
- ▶ Have a emergency access if your OSPF (or you) will fail
- ▶ No need for big layer two network !



THERE IS ONLY ONE "BUT"

UNFORTUNATELY ROMON IS A PROPRIETARY PROTOCOL

Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.
Open source is good for me. Proprietary is evil.



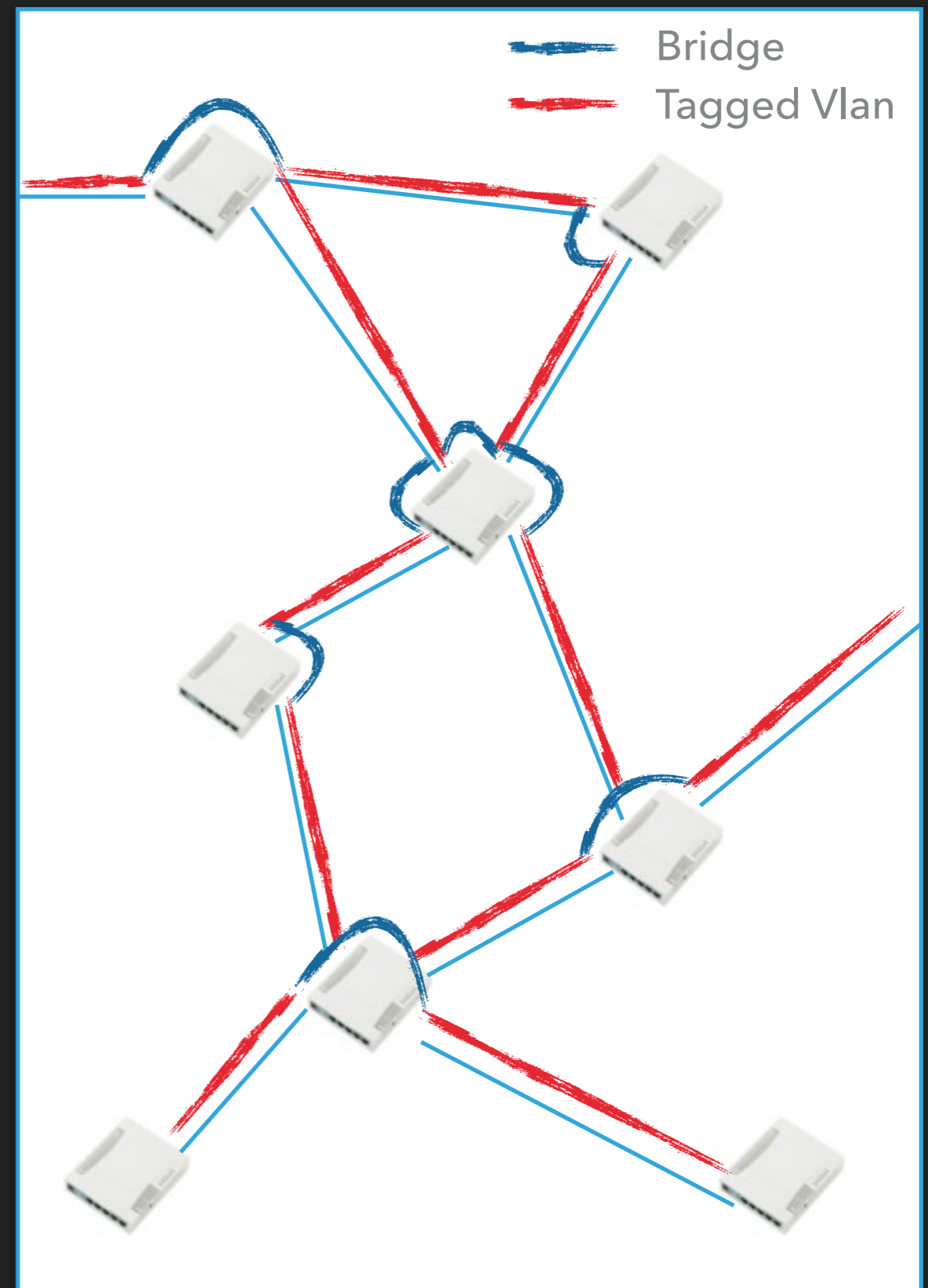
**“HOWEVER, THERE IS
SOMETHING WE CAN DO ABOUT
THAT !”**

Jeremy Clarkson, BBC


WHAT IF WE BRIDGE ALL TOGETHER AGAIN ?

MANAGEMENT VLAN

- ▶ Management layer can be a totally bridged topology
- ▶ Why use vlans ?
- ▶ One Vlan-ID can be used across entire network



BENEFITS OF MANAGEMENT VLAN

- ▶ Separation of Data (customer) and Management Traffic (better security)
- ▶ VLAN technology is standardised and widely implemented - vendor independent
- ▶ Easy to configure **EXCEPT CRS SERIES ;)**
- ▶ Ability to access third party devices on L2

New Bridge Port

General Status

Interface: **vlan67_ether1_managment**

Bridge: **managment_bridge**

Priority: 80 hex

Path Cost: 10

Horizontal

Edge

Point To Point

External Flooding

Auto Isolate

enabled inactive

OK Cancel Apply Disable Comment Copy

AND BRIDGE ALL THEM TOGETHER

New Interface

General Status Traffic

Name: **vlan67_ether2_managment**

Type: VLAN

MTU: 1500

L2 MTU:

MAC Address:

ARP: **enabled**

VLAN ID: **67**

Interface: **ether2**

OK Cancel Apply Disable Comment Copy Remove Torch

CREATE VLANS ON CORE INTERFACE

Interface <managment_bridge>

General STP Status Traffic

Protocol Mode: none stp **rstp**

Priority: 8000 hex

Ma

Trans

OK Cancel Apply Disable Comment Copy

MAKE SURE IF (R)STP IS ENABLED

New Interface

General Status Traffic

Name: **vlan67_ether1_managment**

Type: VLAN

MTU: 1500

L2 MTU:

MAC Address:

ARP: **enabled**

VLAN ID: **67**

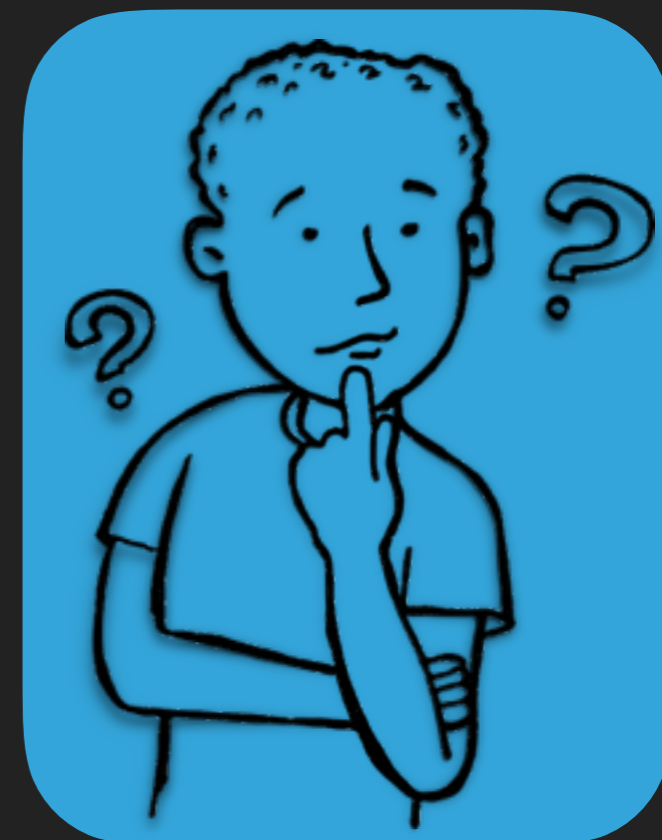
Interface: **ether1**

OK Cancel Apply Disable Comment Copy Remove Torch

MANAGEMENT VLAN – ONE BIG BRIDGE ?

HUH ? I'VE IMPLEMENTED OSPF AND NEED TO CREATE ONE BIG BRIDGE AGAIN ?

- ▶ Management Bridge „network“ is not used for carrying customer data
- ▶ Broadcast Storm is not that serious as only core devices exists in management „network“
- ▶ STP may lead to not optimized path, but that is ok for emergency management traffic



TEXT

RoMON

Managmement
Vlan

Can manage devices
behind NAT

YES

NO

Support other clients
then Winbox

NO

YES

Vendor Independent

NO

YES

Allow secure
connections

YES

NO

SO SHOULD WE SWAP RoMON TO VLANS?

- ▶ RoMON is great protocol and never let me down
- ▶ Both methods can be used at same time
- ▶ I personally use both methods in networks I manage.

WANT TO LEARN MORE ?

- ▶ Visit wispcasts.com - place where you can improve your skills

SITE IS STILL UNDER PRODUCTION BUT VIDEO CONTENT IS ALREADY AVAILABLE, AND PUBLISHED FREQUENTLY

**TWO VIDEO SERIES AVAILABLE:
MIKROTIK INTRODUCTION
MIKROTIK VPN**

AND MANY MORE UNDERWAY

