

RMLL 2009

Network virtualisation using Netkit and Dynamips

Cedric Foll
07.08.09

Cedric Foll

cedric.foll@laposte.net|education.gouv.fr

- Network and security architect and Chef Security Officer (CSO) of French Ministry of Education
- Teacher at INSA Rouen (French Engineer School)

Web: <http://cedric.foll.name>

Twitter: <http://twitter.com/follc>

Blog: <http://blog.foll.name>



Netkit

Linux network emulation

Netkit's Features

Created by the italian university Roma 3

- GPL code
- Run on Linux
- Based on UML (User Mode Linux)
- Just need to download and unzip three (big) files
- Don't need to have "root" privileges to install or use it
- Permit to simulate complex networks
- Can access to guest/outside using TAP interfaces.



DEMO

<http://www.youtube.com/watch?v=zrYoQ-hNyNw>

Is netkit (ie linux) suitable to play with/to teach networks?

- Yes!
 - Support of IPv4/IPv6 for routing and firewalling.
 - Many dynamic routing protocols (BGP, OSPF, RIP, IS-IS) thanks to Quagga.
 - Supports many network protocols (GRE, 802.1Q, IPSec, STP, ...) and even MPLS!
 - Netkit images integrate most of tools usefull for networkers (tcpdump, dsniiff, snort, nmap, ...)
 - Netkit images are based on debian unstable and it's possible to add packages with an "apt-get".

Limitations?

I want my f!!cking Cisco CLI

- Quagga isn't a real Cisco CLI
- Doesn't support proprietary protocols like EIGRP.
- Doesn't support weird layer 2 protocols like ATM
- Doesn't support the whole Spanning Tree family
- Lack of many network features (L2TPv3, VTP, full support of MPLS, ...)

“Need to buy cisco appliances just to play at home???”

It's expensive!
And it's very loud!!!

Dynamips/Dynagen/GNS3

By Christophe Fillot, Université de Technologie Compiègne

- Dynamips is a Cisco emulator
 - Like Gameboy, Super NES, ...
 - You provide the firmware, Dynamips emulate the hardware.
 - Works with 1700, 2600, 3600, 3700, and 7200.
 - Doesn't support Catalyst (ie switch) but supports NM-16ESW cards (ie switch cards).
 - Can access to guest host using TAP interfaces.
- Dynagen
 - Text based front end for Dynamips
- GNS3
 - A graphical front end for Dynagen

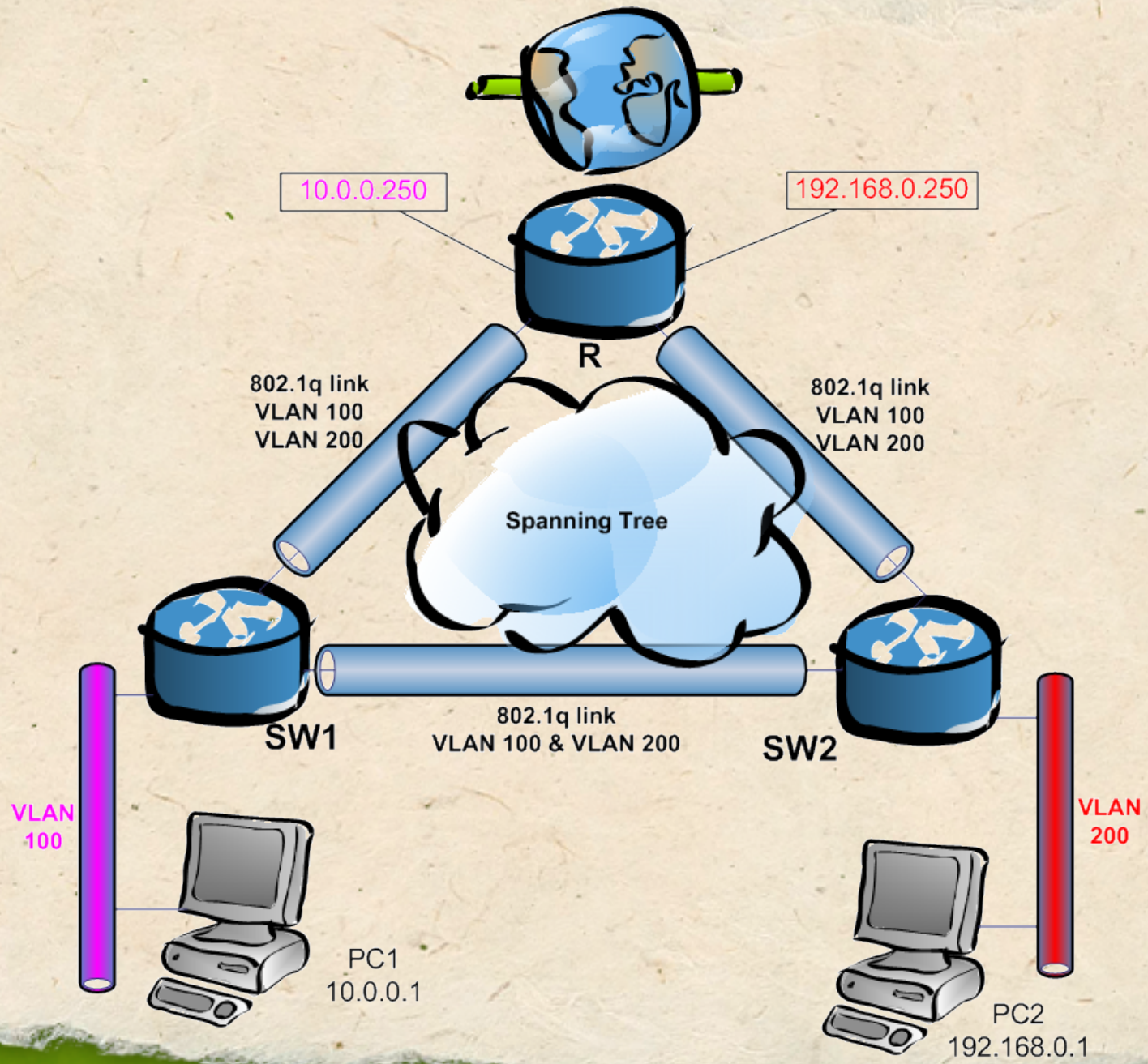


DEMO

<http://www.youtube.com/watch?v=tgXFJAjf-Bo>

Using Netkit & GNS3 together?

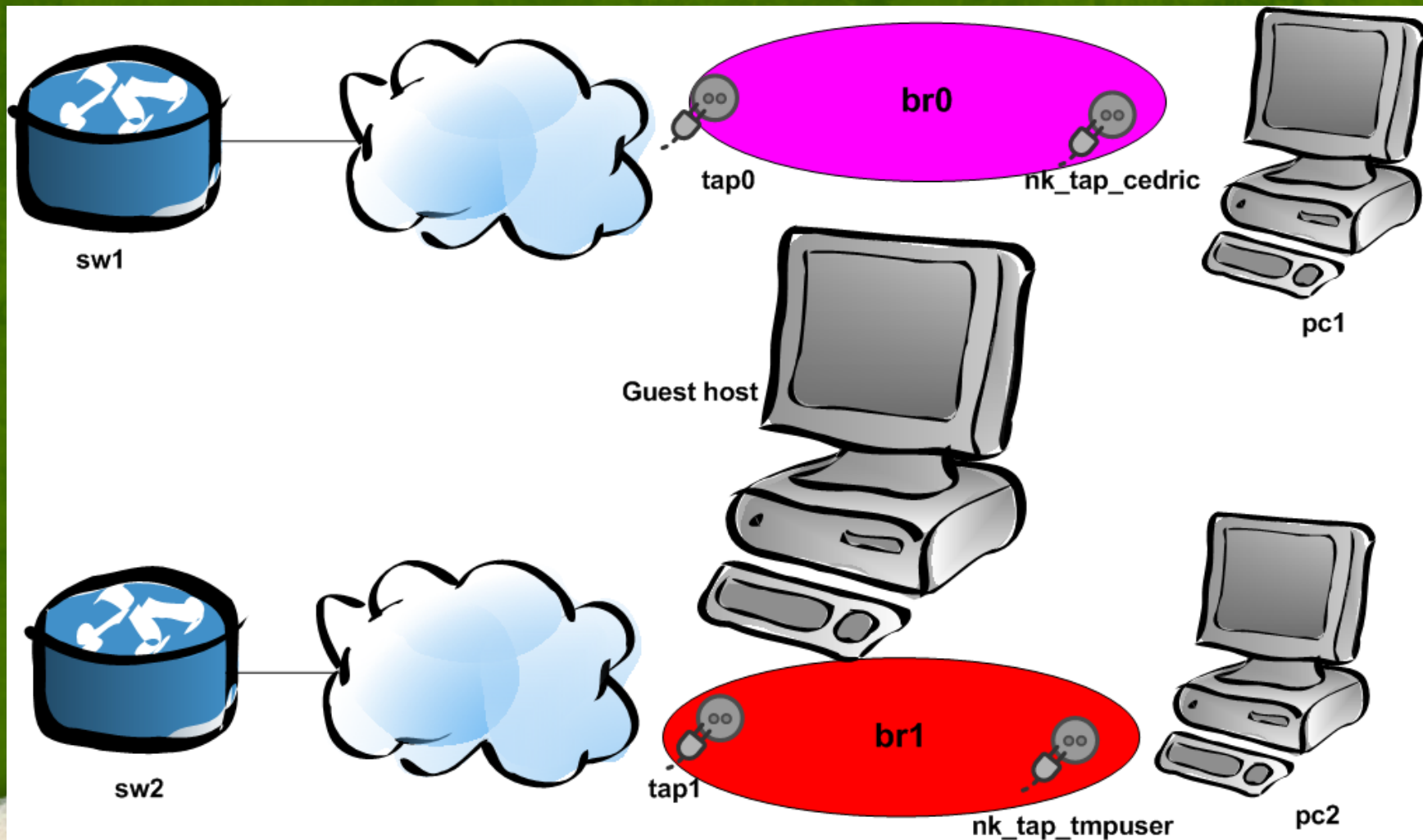
On the same guest host?



GNS3 and netkit together?

On the same guest

- It's possible by bridging TAP interfaces



OK, netkit and Dynamips are nice tools to learn networks but what else?

- Few examples?

- You want to try the Kaminsky's DNS flaw in various scenarios (patched/unpatched system, recursive/forwarding cache, timing issue, ...)
 - netkit is your friend!
- You've hacked a router during a pentest (the good old cisco/cisco default password :))
 - You can reproduce the exact configuration on your laptop ("show run" and then "copy/paste") in order to make tests before breaking everything.
- And what about using a Dynamips machine to play with the cisco router you've just hacked?

Kaminsky's DNS flaw

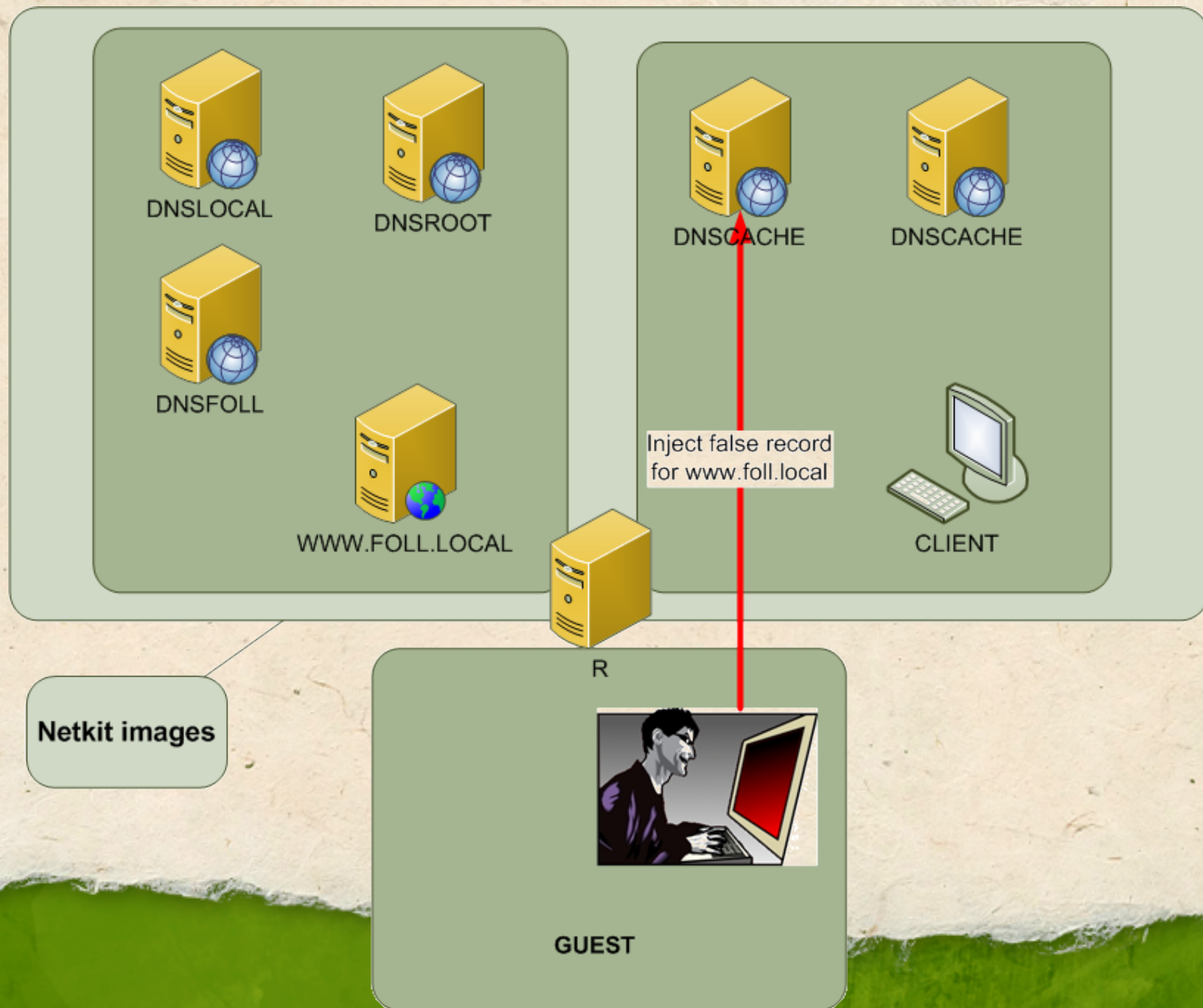
What is it?

- If a cache DNS server doesn't randomize its source port request, you can inject false records on it
 - You can tell to "ns.orange.fr" that gmail.com has the address 1.3.3.7 (or anything else).
 - Very nice in order to run "man in the middle" attacks.
- How does it work?
 - You ask to the cache server "what is azerty123.foll.local".
 - Before he gets answer from authoritative DNS server of foll.local, you send fake answer with additional record saying that www.foll.local has 1.3.3.7 as IP address.
 - You just have to guess the "query ID" (16bits) and answer before the real server does.

Netkit lab

Kaminsky's DNS flaw

- Two networks
 - First with authoritative DNS servers (root, master of "local.", master of "foll.local.") and the web server "www.foll.local".
 - Second with a client and two cache dns:
 - cachedns isn't patched and all its request are from the source port 12345.
 - cachedns2 is patched and each request is sent by a random source port.
- The router R has access to these networks and has a third interface on TAP in order to access to the guest.
- We attack the client from the guest with metasploit.



Demo

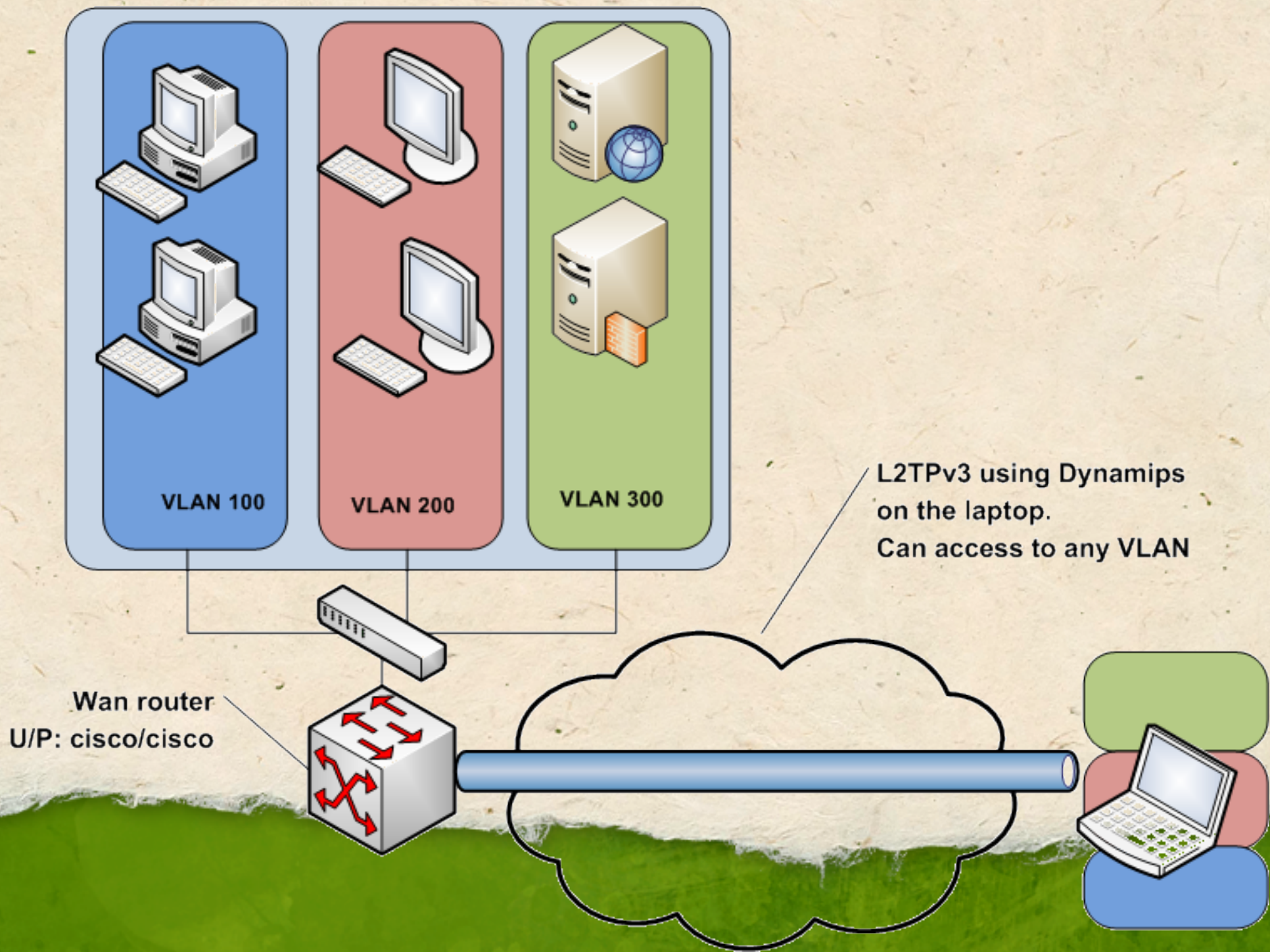
<http://www.youtube.com/watch?v=wxBSfEanumg>

The lab is available on <http://blog.foll.name>

Using Dynamips as a pentester?

How?

- Few attacks on a router/switch
 - Use of DTP to force the port to which you're connected to become a trunk.
 - Use STP to become the root of the tree.
 - Play with dynamic routing protocol to do re-draw network topology
 - Mount tunnel between your host and a hacked router
- Why use Dynamips?
 - You can use TAP to access to outside.
 - No need to collect a bunch of tools to emulate proprietary protocols (like yersinia for DTP)
 - Some protocols aren't supported at all on linux (EIGRP, L2TPv3, ...) and may be very useful for a hacker.



Thanks!