WiFi security appliance for authentication solution during conferences and seminars

Riccardo Veraldi

INFN - CNAF

HEPiX Spring 2009

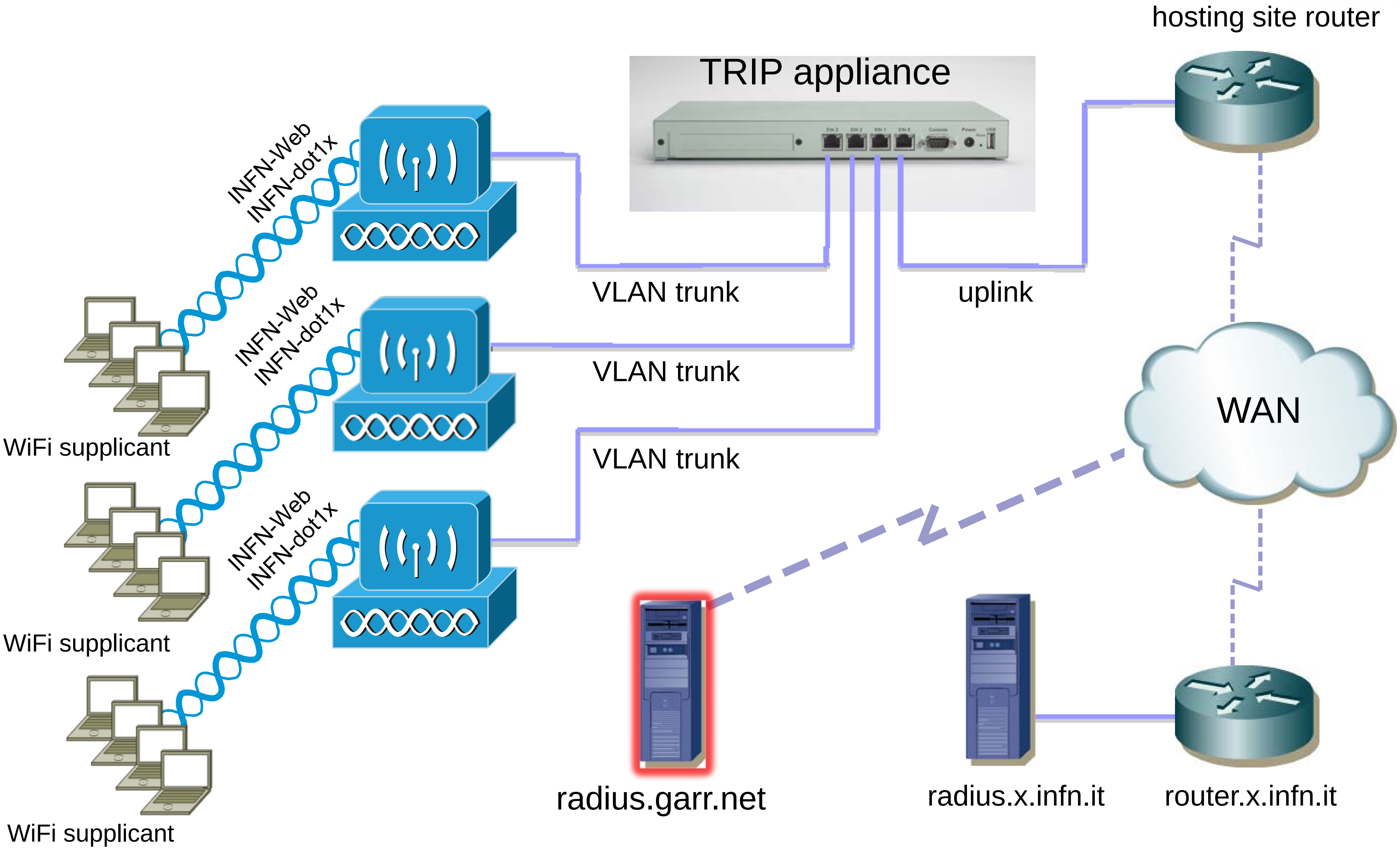
What is TRIP ?

- A distributed INFN-wide WiFi authentication architecture
- Based on proxy radius authentication for INFN staff people (INFN-dot1x SSID)
  - 802.1x EAP-TTLS phase 2 PAP
- Customized captive portal (INFN-Web SSID) for guests
  - Open SSID
  - Supports X509 authentication for non 802.1x compliant supplicants
  - Login/Password for non INFN guests

TRIP appliance

- Possibility to have the TRIP infrastructure avaliable everywhere during seminars and workshops outside INFN sites
- A portable, robust and secure system which manages INFN WiFi SSIDs everwhere: INFN-dot1x and INFN-Web
  - OpenBSD based
  - Strong hardware no HDD
- Nothing to install, only need to plug a CF card
- Users find the same WiFi environment they have in their own office at work

TRIP authentication schema



Soekris net5501

- CPU Geode AMD 586-class 500MHz
- 512 Mbyte DDR-SDRAM, soldered on board
- 4 Mbit BIOS/BOOT Flash
- CompactFLASH Type I/II socket
- UltraDMA-100 interface with 44 pins connector for 2.5" Hard Drive
- Serial ATA 1.0 interface for Hard Drive, with +5V and +12V power header
- 4 VIA VT6105M 10/100 Mbit Auto MDIX Ethernet ports, RJ-45, protected to 700W/40A Surge
- 2 Serial ports, DB9 and 10 pins internal header
- USB 2.0 interface, one internal, one external port
- Mini-PCI type III socket. (for t.ex. hardware encryption or wireless controller)
- PCI Slot, right angle 3.3V signaling only, dual PCI slot option
- Temperature and voltage monitor
- ower using external power supply is 6-25V DC, max 20 Watt,

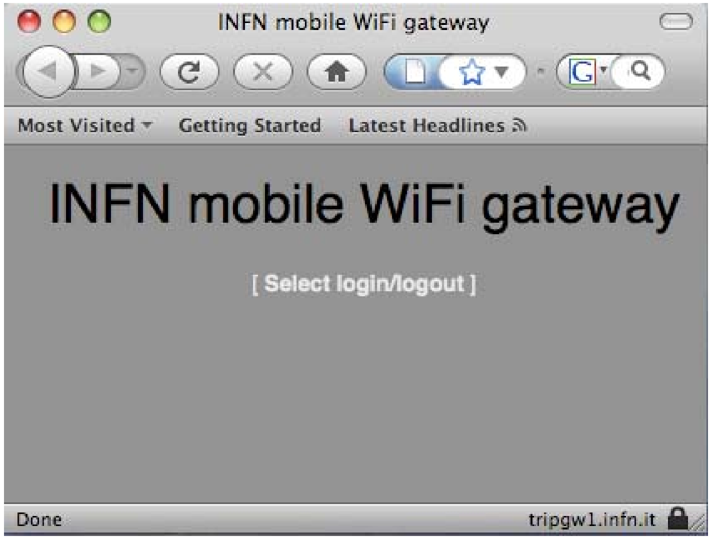
tripgw

- Soekris net5501
- Sw distribution derived from Flashdist (OpenBSD 4.5 based): 64MB CF
- Final distribution for TRIP: 256 MB
  - Flashdist 20090227 OpenBSD 4.5 kernel
  - Freeradius 1.1.6 distribution
  - OpenBSD Apache 1.3.29
  - TINO INFN 12032009 customized Captive Portal (support for X509 auth added)
  - ISC dhcpd v3.1.1
  - OpenBSD pf nat/firewall + ALTQ
  - Perl 5.10.0
    - RadiusPerl-0.13
    - Data-HexDump-0.02
- Standard unix userland added: less, sudo, bash…etc.
- Several configuration files required for TRIP to work

How TINO works (captive portal)

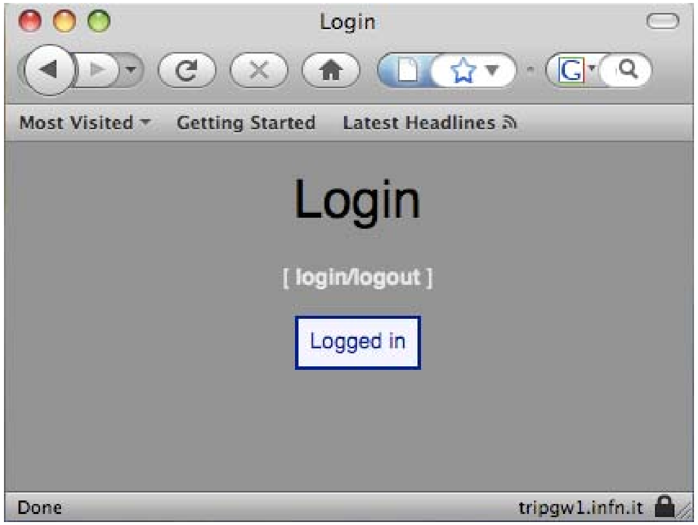
- Captive portal developed by Hannu Teulahti as a component of Palosaari Campus Wireless Network
- Added INFN customization and patches to enable PKI authentication
- Everything managed by a few perl cgi scripts
- Clients are assigned an IP address by DHCP after INFN-Web association
- Upon first TCP connection they are redirected to port 80 TCP and then to TINO https first login page
- Logon is based on X509 or login/password
- Credentials are checked against radius users file or local UN*X account or proxied to external radius
- A dynamic firewall open rule is created through firewall.sh triggered by TINO login page
  - firewall.sh is executed through sudo
- Firewall close rule is issued on user logoff or when user session goes into timeout
- Session timeout is managed with dhcpd leases file and users session log directory /var/spool/tino
- Everything is logged on static file or syslog

TINO login page



INFN mobile WiFi gateway

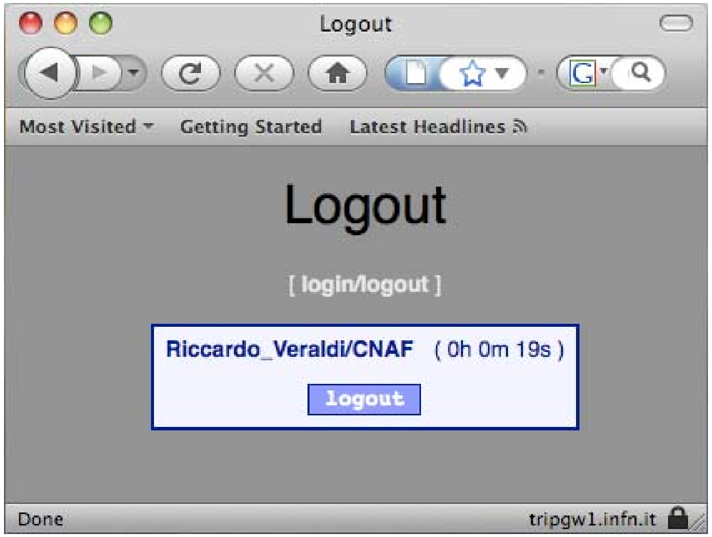
[Select login/logout]



Login

[login/logout]

Logged in

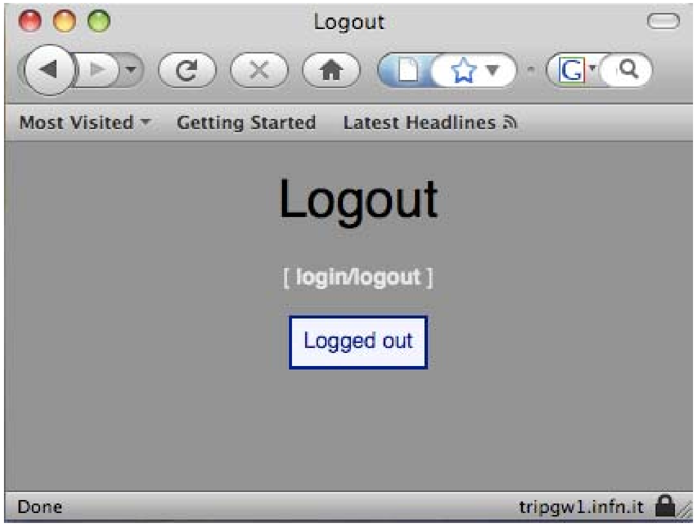


Logout

[login/logout]

Riccardo_Veraldi/CNAF (0h 0m 19s)

logout



Logout

[login/logout]

Logged out

Build appliance

- Installation of OpenBSD 4.5 snapshot 20090227 on a PC or virtual machine
- Build of TRIP mandatory software compiled from sources and statically linked if possible: httpd, radiusd, dhcpd, sudo, perl… etc.
- Copy back of all additional software over the base Flashdist image distribution
- Configuration of all the TRIP mandatory software and OpenBSD startup and system scripts. Copy back on the flashdist distribution:

  /etc/rc, radiusd.conf, pf.conf, firewall.sh… many other scripts
- Copy of the main system image and expansion over CF
- Soekris net5501 boot from CF

Boot appliance

- Boot configuration all inside /etc/rc script
  - mount /dev into memory 1MB
  - mount /tmp into memory 32MB
  - Symbolic link of /var into /tmp/var
    - The log partition /var/log is on volatile RAM
  - Creation of TINO Captive Portal environment and configuration, all files copyed to /tmp partition
  - SSH DSA e RSA keys creation
  - Hostname setting
  - VLAN and IP interfaces creation
  - VLAN forwarding on three physical interfaces
  - ntpdate, startup firewall, syslog startup
  - dhcpd startup over VLAN interfaces
  - sshd, apache, freeradius, cron startup

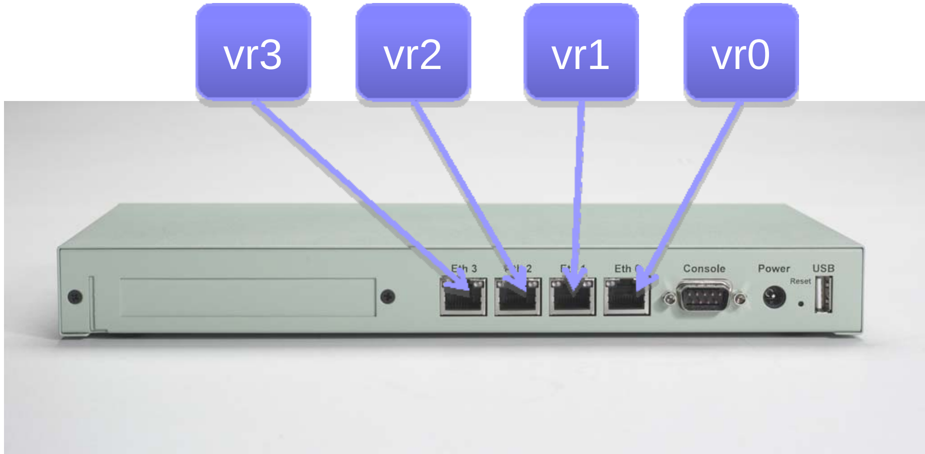
OpenBSD boot on soekris

```
>> OpenBSD/i386 BOOT 3.02
booting hd0a:/bsd: 2109736+393112 [52+124800+116772]=0x29e20c
entry point at 0x200120

[ using 241996 bytes of bsd ELF symbol table ]
Copyright (c) 1982, 1986, 1989, 1991, 1993
        The Regents of the University of California.  All rights reserved.
Copyright (c) 1995-2009 OpenBSD. All rights reserved.  http://www.OpenBSD.org

OpenBSD 4.5 (GEODE) #8: Fri Feb 27 09:31:52 PST 2009
    chris@tundra.nmedia.net:/usr/src/sys/arch/i386/compile/GEODE
cpu0: Geode(TM) Integrated Processor by AMD PCS ("AuthenticAMD" 586-class) 500 MHz
cpu0: FPU,DE,PSE,TSC,MSR,CX8,SEP,PGE,CMOV,CFLUSH,MMX
real mem  = 536440832 (511MB)
avail mem = 515358720 (491MB)
…
…
OpenBSD/i386 (tripgw1.infn.it) (tty00)

login:
```

VLAN list

- Default untagged
  - Network 172.16.1.0/24
  - Radius IP 172.16.1.254
- VLAN100 INFN-dot1x
  - Network 172.16.100.0/24
  - 802.1x gw 172.16.100.254
- VLAN101 INFN-Web
  - Network 172.16.101.0/24
  - TINO gw 172.16.101.254

AP1: 172.16.1.253
AP2: 172.16.1.252
AP3: 172.16.1.251



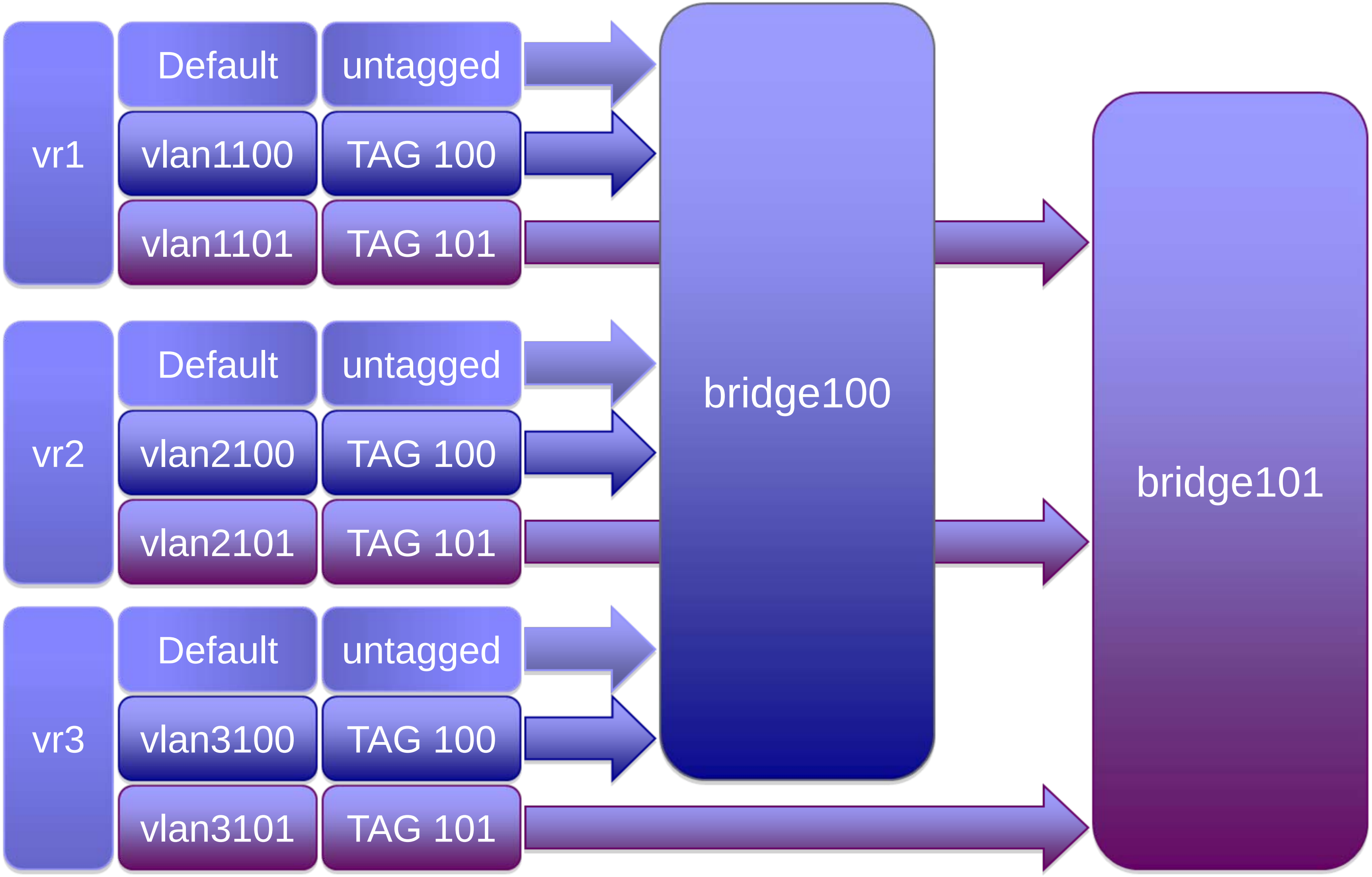
VLANs forwarded on vr1 vr2 vr3
vr0 UPLINK interface

VLAN configuration

One VLAN on each NIC for each TAG = 6 VLAN + Default Untagged

```
ifconfig vr1 172.16.1.254 netmask 255.255.255.0
ifconfig vr2 up
ifconfig vr3 up
ifconfig vr0 <uplink_ip> netmask 255.255.255.0
ifconfig vlan1100 vlan 100 vlandev vr1
ifconfig vlan2100 vlan 100 vlandev vr2
ifconfig vlan3100 vlan 100 vlandev vr3
ifconfig bridge100 create
brconfig bridge100 add vlan1100 add vlan2100 add vlan3100 add vr1 add vr2
   add vr3 up
ifconfig vlan1100 inet 172.16.100.254 netmask 255.255.255.0 up
ifconfig vlan1101 vlan 101 vlandev vr1
ifconfig vlan2101 vlan 101 vlandev vr2
ifconfig vlan3101 vlan 101 vlandev vr3
ifconfig bridge101 create
brconfig bridge101 add vlan1101 add vlan2101 add vlan3101 up
ifconfig vlan1101 inet 172.16.101.254 netmask 255.255.255.0
```

Multiport VLAN bridge



Radius configuration

- Freeradius 1.1.6 /usr/local/etc/raddb
- Radius authentication with proxying + radius local authentication for Captive Portal
- Need to configure proxy.conf with INFN remote peer radius server, eg:

```
realm DEFAULT {
        type            = radius
        authhost        = radius.x.infn.it:1812
        accthost        = radius.x.infn.it:1813
        secret          = *********
        nostrip
}
```

- Need to add APs IP addresses and peer radius server in clients.conf
- Localhost must also be added for local radius authentication interface with Captive Portal
  - □ Authentication bound to radius users file
  - □ Authentication with UN*X account

Firewall

- OpenBSD PF configuration pf.conf
  - Packet filter
    - vlan1101 (TAG 101) filtered by default (INFN-Web)
      - Only UDP 53 and TCP 80 and 443 to Captive Portal is allowed
    - vlan1100 (TAG 100) open by default (INFN-dot1x)
    - Dynamic PF table created by firewall.sh TINO script
  - Nat
    - Nat for both vlan1100 (INFN-dot1x) and vlan1101 (INFN-Web)
    - Redirection rules allowing APs configuration from outside
    - Redirection rules for Captive Portal

Traffic Shaping: ALTQ

- Mandatory for slow speed uplink

```
altq on vr0 priq bandwidth 330Kb queue { std_out, smtp_imaps_out, dns_out, tcp_ack_out }
queue std_out     priq(default)
queue dns_out     priority 4 priq(red)
queue smtp_imaps_out  priority 5 priq(red)
queue tcp_ack_out priority 6
pass  out on fxp0 inet proto tcp from (fxp0) to any flags S/SA \
      keep state queue(std_out, tcp_ack_out)
pass  out on fxp0 inet proto { tcp udp } from (fxp0) to any port domain \
      keep state queue dns_out
pass  out on fxp0 inet proto tcp from (fxp0) to any port { 22, 25, 587, 465, 993 } \
      flags S/SA keep state queue(smtp_imaps_out,  tcp_ack_out)
```

How to use it

- Read-only pre-configured CF
- If we need to change configuration (add users, add APs… etc)
  - Use { ro, rw } commands to modify CF access mode
  - UN*X shell, OpenBSD environment
    - adduser, vi, tcpdump… etc.
    - Users can be added with adduser or directly into freeradisu users file
  - Mandatory to use ro command after any modification to CF to preserve CF life
- Use the system in rw mode only when necessary
- Up to three access points can be attached to NICs (vr1, vr2, vr3)
- Mandatory to register vr0 IP address on the parent radius server configuration and on the logserver
- X509 host cert is pre-installed hostname tripgw1.infn.it

Where to use it

- Conferences and seminars outside INFN sites where TRIP INFN wide WiFi authentication architecture is required
- Conferences and seminars without TRIP
  - CF customized with Captive Portal only
- TRIP appliance for small INFN sites
- Anyone who need a WiFi authentication appliance with Captive Portal and 802.1x
- Eduroam ready
- Easy integration in any WiFi environment in any place to offer enterprise level WPA authentication and Captive Portal as well

TODO

- Add bind chrooted cache-only local nameserver
- Friendly user interface
  - Web user interface for setup
  - Console text only user interface for setup

Questions or Comments ?