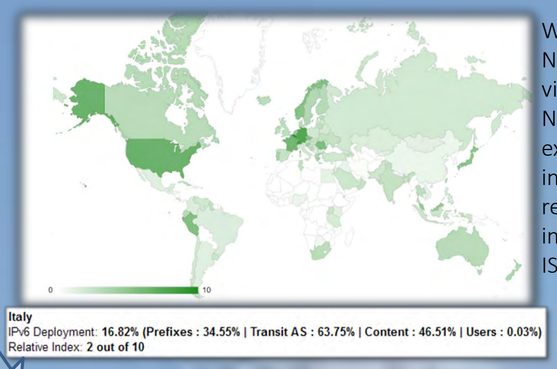
## IPv6




When the TCP/IP was first developed and the IPv4 protocol was born, nobody could imagine a such enormous usage of networks like nowadays. Networks were expected to be used by researchers and military forces, not certainly by 2 billion people around the world. From a design point of view, IPv4 isn't well suited anymore due to its "poor" amount of available addresses. In fact , on February the 3rd of 2011, the Internet Assigned Numbers Authority (IANA) declared the end of all stocks of IPv4 addresses possessed. Anyway, despite this, the current usage of IPv6 doesn't exceed the 3-4% of total. This can lead to several reasons: from the perspective of network stability, as often happens, any change may introduce periods that creates inefficiencies. Moreover, there are huge costs due to the redesign of the network (where needed), staff training, release update on devices and replacement of older equipment unable to evolve to IPv6. In this way, the companies do not see immediate gains in the use of the new system, thus extending the time of transition. However, the shortage of addresses will become unsustainable soon, forcing ISPs and istitutions to migrate to IPv6.

Continual Improvement

- Procedure
- Checklist
- Audit

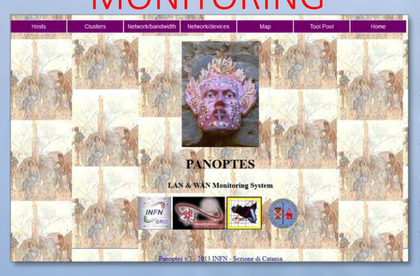
## SDN

OPEN NETWORKING FOUNDATION

OpenFlow

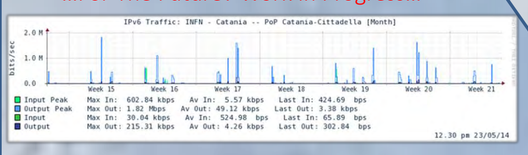
Software Defined Networking can be considered as a new and game-changing way of thinking about networks. The best way to introduce this technology is to quote the Open Networking Foundation, the organization dedicated to the promotion and adoption of SDN: "SDN is an emerging architecture that is dynamic, manageable, cost-effective and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to became directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow protocol is a foundational element for building SDN solutions."

## MONITORING




It was necessary to improve our monitoring system Panoptes and to configure new tools of Flows Analysis to control our network during the operations of migration to IPv6 protocol. During the year 2013 two videoconferences were organized with the experts of GARR to obtain new useful informations for our thesis students. All these items completed the planning phase (the first step of the cycle of Deming) of our training program.

## ...For The Future? Work In Progress...




Using the new configuration, DNS now resolves IPv6 names

```
> server alp4ct.ct.infn.it
Server predefinito:  alp4ct.ct.infn.it
Address:  192.84.150.104

> www.ct.infn.it
Server:  alp4ct.ct.infn.it
Address:  192.84.150.104

Nome:    webnew.ct.infn.it
Addresses:  2001:760:420c::f250
          192.167.0.254
Aliases:  www.ct.infn.it
```

The Website www.ct.infn.it now fully supports IPv6.



UNIVERSITÀ DEGLI STUDI DI CATANIA
Corso di Laurea in Ingegneria delle Telecomunicazioni
DIPARTIMENTO DI INGEGNERIA ELETTRICA, ELETTRONICA E INFORMATICA

GABRIELE GERBINO

IPv6 SECURITY VULNERABILITIES IN A DEPARTMENTAL RESEARCH NETWORK: EXPLORATION AND MITIGATION

Tesi di Laurea

Relatore: Chiarmo Prof. Sergio Palazzo
Correlatore: Giuseppe Sava

Anno Accademico 2012-2013


UNIVERSITÀ DEGLI STUDI DI CATANIA
FACOLTÀ DI INGEGNERIA
Corso di Laurea in Ingegneria delle Telecomunicazioni
DIPARTIMENTO DI INGEGNERIA ELETTRICA, ELETTRONICA E INFORMATICA

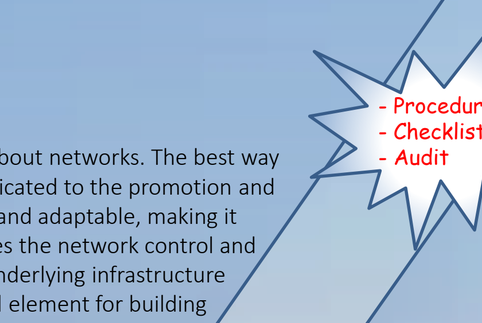
Ronald Vincenzo Field

ANALISYS AND MIGRATION TO IPv6 OF A DEPARTMENTAL RESEARCH NETWORK

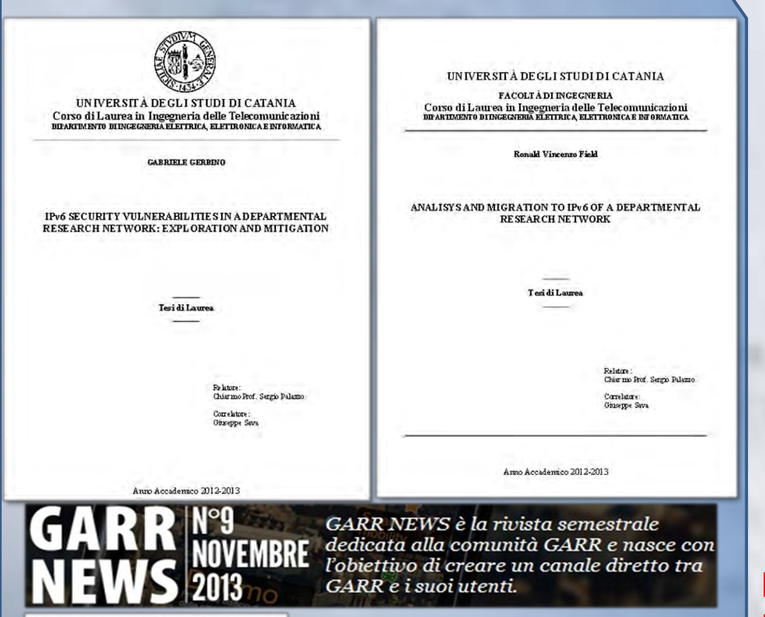
Tesi di Laurea

Relatore: Chiarmo Prof. Sergio Palazzo
Correlatore: Giuseppe Sava

Anno Accademico 2012-2013




Website trend during 2013 and 2014.


GARR NEWS N°9 NOVEMBRE 2013

*GARR NEWS è la rivista semestrale dedicata alla comunità GARR e nasce con l'obiettivo di creare un canale diretto tra GARR e i suoi utenti.*


''Nella comunità GARR, tra le varie istituzioni che sono già passate al nuovo protocollo, un esempio virtuoso è quello della sezione di Catania dell'INFN che ha adottato IPv6 all'interno della propria LAN grazie anche al supporto di un tesista dell'Università di Catania che ha svolto il proprio lavoro supportando i colleghi nell'analisi e nella migrazione della rete dipartimentale ad IPv6 e guadagnando il punteggio massimo e la lode. Questa modalità potrebbe essere ripetuta anche in altre strutture, visto che ci sono ancora tanti aspetti che riguardano il nuovo protocollo da affrontare...''

## PLAN

**Division of Catania**
**Computation and Network Service**
**Training Program 2013-2014 with**
**Cycle of Deming approach**
**for students with a scholarship**
**and thesis students.**

# IPv6 and SDN


Alessio Fichera, Ronald Field,
Gabriele Gerbino, Marco Borzì,
Filadelfo Cristaudo,
Giuseppe Sava (Network Coordinator),
Giuseppe Andronico (IT Service Manager)

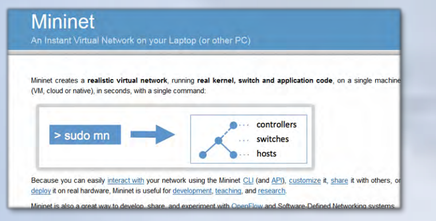

Workshop CCR, 27-30/05/2014, LNS, Catania

## ACT

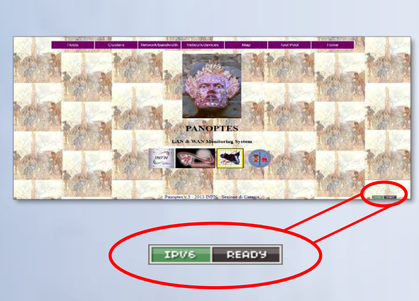
## DO

## CHECK

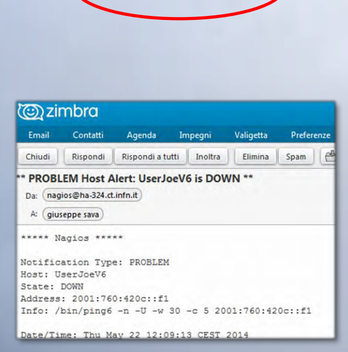
Mininet as a ''First Step'' to study SDN and OpenFlow.



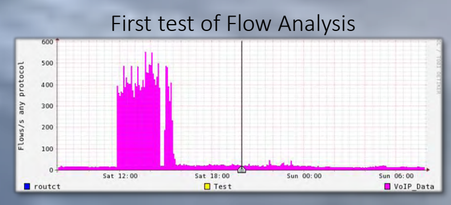

The Panoptes Monitoring System now supports IPv6 too.

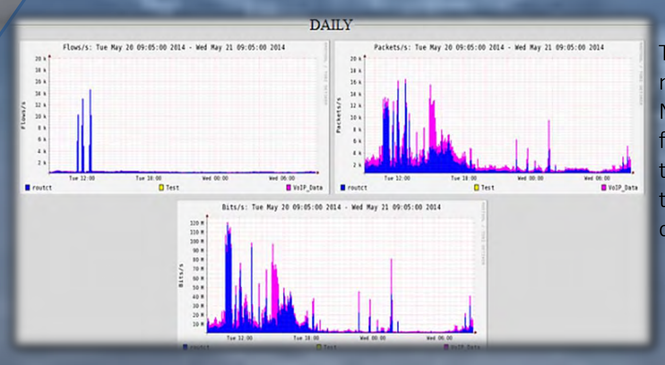



Alarm notification for an IPv6 node down.




First test of Flow Analysis



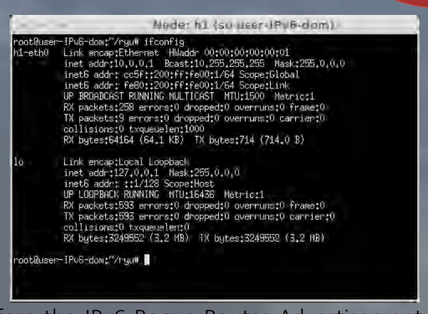

The nfdump tools collects and process netflow data on the command line. NfSen is a graphical web based front end for the nfdump netflow tools. It allows you to display your netflow data, easily navigate through the netflow data, process the netflow data within the specified time span, set alerts, etc.

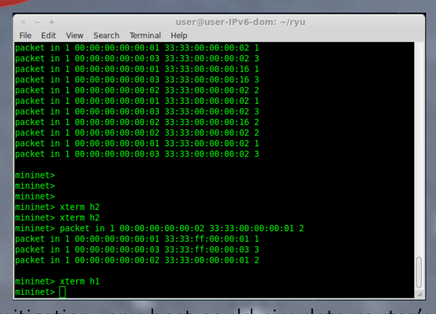
## AFTER

```
From the controller:
[ALERT] packet contains a Router Advertisement!
[WARNING] Intrusion Detection System detected a Rogue Router Advertisement!
 fe80::200:ff:fe00:2 != fe80::200:ff:fe00:1

[SUSPECT] SUSPICIOUS state has changed!
packet in 1 ipv6:fe80::200:ff:fe00:2 00:00:00:00:00:02 33:33:00:00:00:01 2

[DROP] SUSPICIOUS packet was dropped!
```

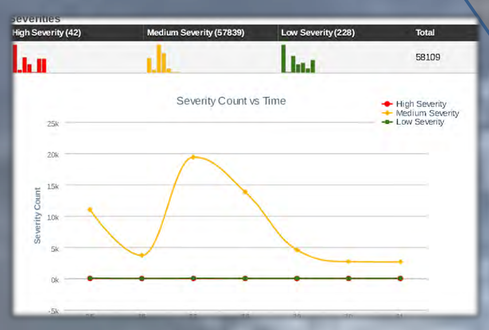
By using SDN and Python programming, we gave the controller a method to reveal fake RAs and to drop them when received. During all the attack session, none of the hosts will receive or notice anything. As shown in the picture above, the controller will also send email notifications to the IT Network Group with all the useful information needed to investigate and to identify the attacker.

## BEFORE




Before the IPv6 Rogue Router Advertisement (RA) mitigation, any host could simulate router's RAs and send them to anybody in the network. As shown in the picture on the left, the receivers will consider the fake RAs as valid and will assign themselves an address of the network the attacker wants them in. Depending on the amount of RAs sent, this can be considered both as Man In The Middle or DOS attack. In a massive RA flood, almost all vulnerable hosts will crash or will be getting extremely slow.




Snorby is an intuitive IDS frontend for Snort. It uses Ruby On Rails, and offers a nice web GUI, customizable severities and events. Snorby also allows you to create custom rules for email notifications. By default, it regularly sends you daily, weekly, monthly and yearly reports, in order to help you continuously monitoring and improving your network security and performances. Last but not least, Snorby is Free, Open Source and constantly updated.

ISO and OHSAS Management Systems are based on model Plan-Do-Check-Act (PDCA)

Process Approach