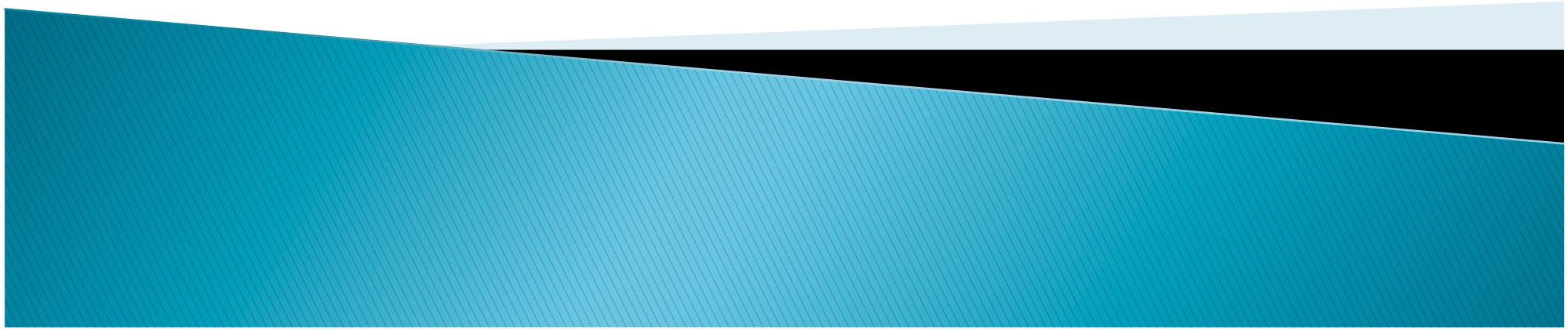
Esperienze con IPv6 al CNR di Pisa

Marco Sommani
CNR – IIT
marco.sommani@cnr.it



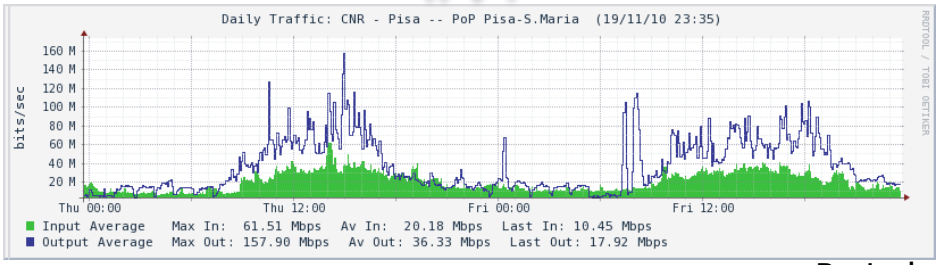
L'Area della Ricerca del CNR di Pisa: immagini

L'Area della Ricerca del CNR di Pisa: numeri

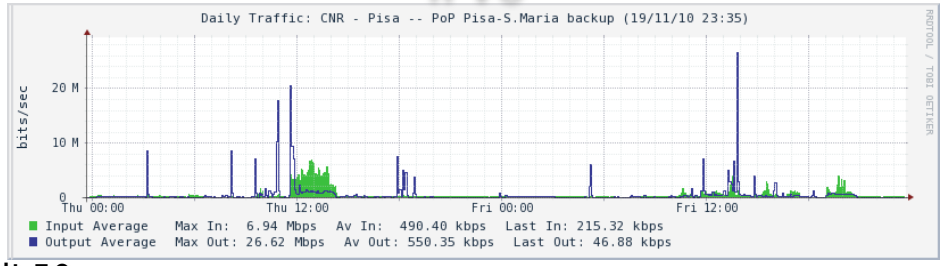
- 13 istituti
  - IIT con registro .it
  - IFC con ospedale
- circa 1100 dipendenti CNR
- circa altri 900 frequentatori a vario titolo
- circa 3500 prese dati attive
- più di 6000 indirizzi MAC sulle varie VLAN
- IPv6 globale su alcune VLAN dal 2003
- su tutte le VLAN dal febbraio 2010

Utilizzo di IPv4 e IPv6 sul collegamento fra CNR-Pisa e GARR

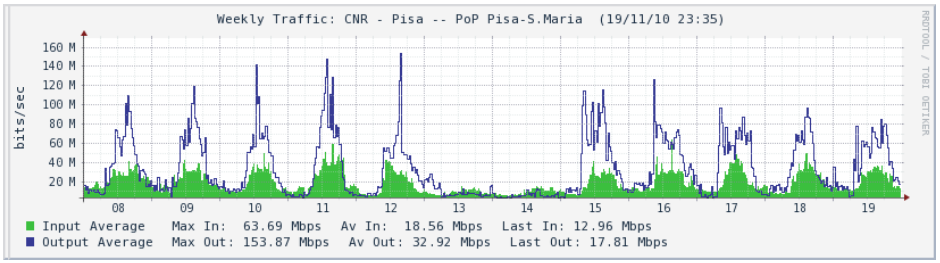
IPv4

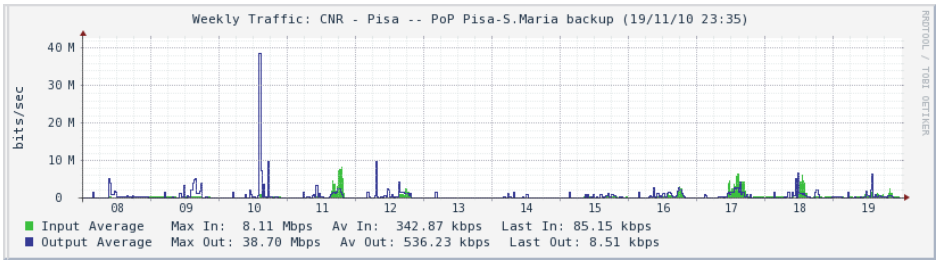


IPv6

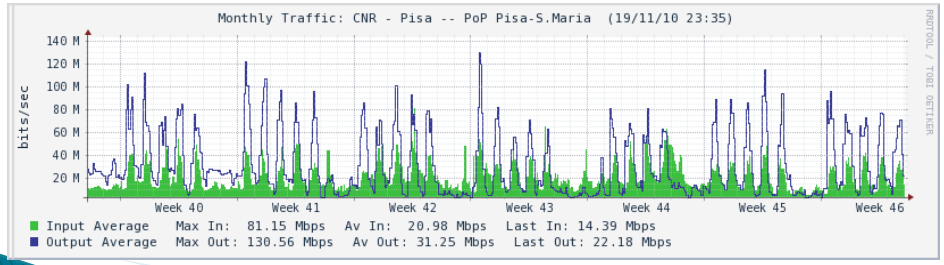


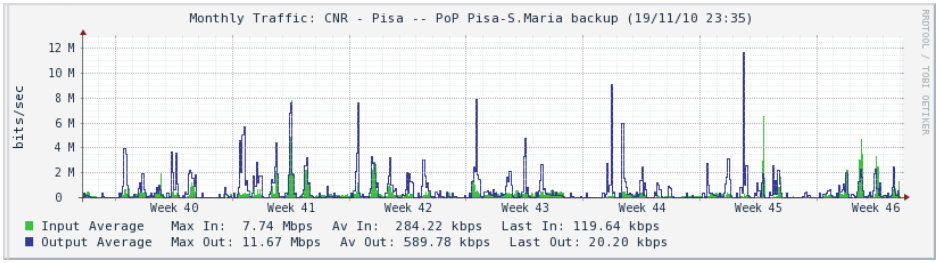
Periodo di 50 ore





Periodo di 12 giorni





Periodo di 50 giorni

Scelte tecniche

- Ogni istituto ha la sua VLAN, con una subnet per IPv4 (/24 - /21) e una per IPv6 (/64)
- Su ogni VLAN, gli stessi apparati (un Juniper M7i e un M10) fanno da router per IPv4 e IPv6
  - VRRP e VRRPv6 attivi su ogni VLAN
- I router inviano i router-advertisements su ogni VLAN, rendendo possibile l'autoconfigurazione degli host (SLAAC)
- Un firewall PA-4020 della Paloalto Networks, posizionato fra i router e le VLAN, controlla il traffico di entrambi i protocolli
- Solo alcuni server hanno l'indirizzo IPv6 riportato nel DNS (diretto e inverso)
- Il DHCPv6 non è utilizzato

Host con l'indirizzo IPv6 riportato nel DNS diretto e inverso

- dns.ilc.cnr.it
- dns2.ilc.cnr.it
- mail.ilc.cnr.it
- www.ilc.cnr.it
- mail.nic.it
- www.nic.it
- www.iit.cnr.it
- www.isoc.it
- www.igf-italia.it
- nrenum.iit.cnr.it
- pochi altri...

Chi sono gli utilizzatori?

- Chi ha un sistema operativo *dual-stack* è un utilizzatore, spesso inconsapevole, di IPv6
  - Windows Vista e Windows 7
  - Mac Os X dalla 10.2 in poi
  - Ubuntu e quasi tutti gli altri sistemi Unix
  - vari smartphones con wifi:
    - iOs4 (iPhone), Android, Windows Phone 7
    - probabilmente anche altri
- Eccezione: il comportamento default di alcuni "personal firewall" è di bloccare IPv6

Quali applicazioni?

- Il firewall PA-4020, che è “application aware”, segnala queste applicazioni IPv6:
  - dns, icmpv6, bittorrent, web-browsing, yum, smtp, ntp, flash, atom, rss, ssl, ldap, ftp, pop3, snmp
- Bittorrent, anche se soggetto a “rate limiting”, genera la maggior parte del traffico
- Le applicazioni “client-server” dual-stack scelgono IPv6 se il server ha l’indirizzo IPv6 sul DNS
- Alcune applicazioni p2p riescono a scoprire gli indirizzi IPv6 dei partner anche senza DNS
  - per ora solo bittorrent

Partner “Teredo” e “6to4”

- Più della metà delle sessioni IPv6 sono con partner con prefissi 2002::/16 (6to4) o 2001::/32 (Teredo)
- Ciò è dovuto al comportamento default di Windows Vista e Windows 7, quando nessuna interfaccia ha un indirizzo IPv6 globale:
  - se c’è almeno un interfaccia con indirizzo IPv4 pubblico, aprire un tunnel 6to4
  - se tutte le interfacce hanno indirizzi rfc1918, aprire un tunnel Teredo
- Si tratta prevalentemente di partner bittorrent

Problema 1: i rogue RA

- L'inconveniente è causato prevalentemente da macchine Windows Vista o Windows 7 configurate male, che inviano sulla LAN router-advertisements per prefissi 6to4
  - nostro rimedio: un tool – RAMon – neutralizza i rogue RA inviandone altri identici ma con router-lifetime=0
  - rimedio ideale: usare switch che permettano di bloccare in ingresso i rogue RA
  - raccomandazione: su Windows Vista e Windows 7, dare il comando:
    - netsh interface 6to4 set state state=disable
- Il problema riguarda anche le LAN prive di IPv6

Problema 2: packet too big

- Quasi tutti gli host di Internet sono configurati con MTU=1500 e inviano pacchetti con quella lunghezza
- se sul percorso c'è una tratta con MTU più piccola (p. es. un tunnel), al mittente viene inviato un ICMPv6: "packet too big"
- se sul cammino inverso c'è un apparato che elimina i "packet too big", la comunicazione non può avvenire
- si tratta di un "problema di gioventù" di IPv6, fortunatamente raro
  - basta che tutti smettano di bloccare i "packet too big"

Problema 3: individuazione dei titolari

- Gli host IPv6 si autoassegnano gli indirizzi
- Anche se si ricorre alla configurazione manuale, l'host può autoassegnarsi altri indirizzi (link-local o global-scope)
- È opportuno disporre di tool per associare rapidamente un indirizzo IPv6 al suo indirizzo MAC
- Diventa sempre più utile l'autenticazione 802.1x
- Al CNR di Pisa è in stadio di avanzato sviluppo un tool che facilita l'individuazione analizzando i multicast ed i log di Radius
  - Abraham Gebrehiwot disponibile per demo e chiarimenti

Conclusioni

- Attivare IPv6 non è difficile
- Gli inconvenienti sono rari e poco gravi
- Tutti i gestori di reti devono capire che i loro utenti utilizzano inconsapevolmente IPv6 sia localmente sia globalmente (via tunnel)
- Occorre sfruttare questi ultimi mesi di scarso traffico IPv6 soprattutto per:
  - stabilire procedure per l'individuazione degli utenti locali
  - pianificare la sicurezza IPv6

Esperienze con IPv6 al CNR di Pisa

Marco Sommani
CNR – IIT
marco.sommani@cnr.it