Primeres experiències d'ús de l'SMAЯTxAC

Trobada de l'Anella Científica (TAC'04)

CENTRE DE COMUNICACIONS
AVANÇADES DE BANDA AMPLA

Pere Barlet Ros
Josep Solé Pareta
Jordi Domingo Pascual

Barcelona, 2 de Juny de 2004

Agraïments: Aquest treball està finançat parcialment pel CESCA (conveni SMAЯTxAC) i pel MCyT (ref. TIC2002-04531-C04-02)

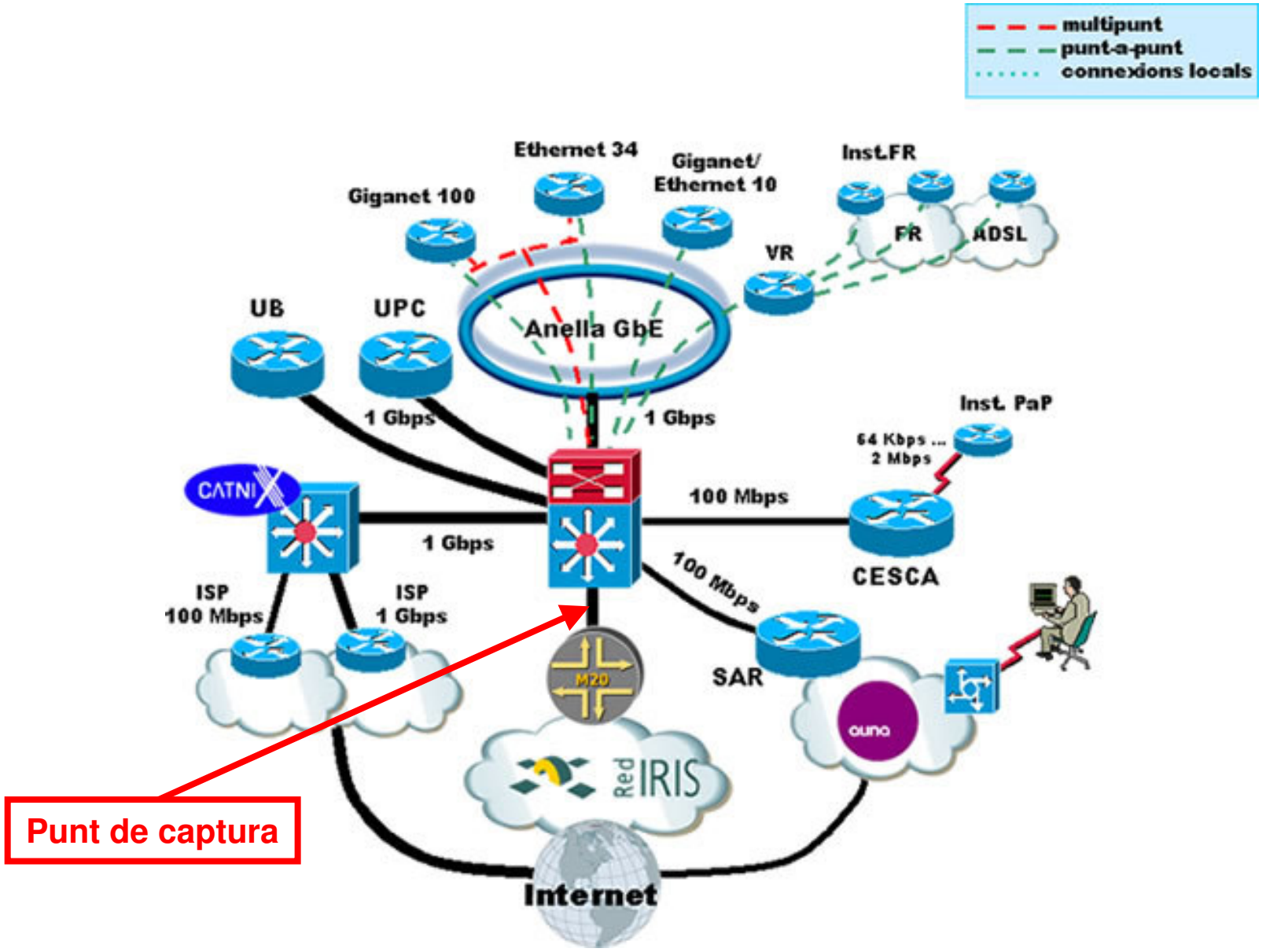
Índex

- Sistema SMAЯTxAC
- Perfil de tràfic de l'Anella Científica
- Gràfiques de situacions irregulars
- Treball actual
- Referències

Conveni SMAЯTxAC

- SMAЯTxAC: “Sistema de monitorització i anàlisi de tràfic per a l’Anella Científica”
- Conveni de col·laboració entre CESCA i Centre de Comunicacions Avançades de Banda Ampla (CCABA) de la UPC
- Objectius
  - Monitorització i anàlisi permanent de l’enllaç entre l’Anella Científica i RedIRIS
  - Conèixer l’ús que es fa dels recursos de xarxa disponibles
  - Obtenir informació que ajudi al CESCA a les taques de gestió de la xarxa
  - Detecció d’anomalies, usos irregulars i atacs (seguretat reactiva)

Anella Científica (GigE)

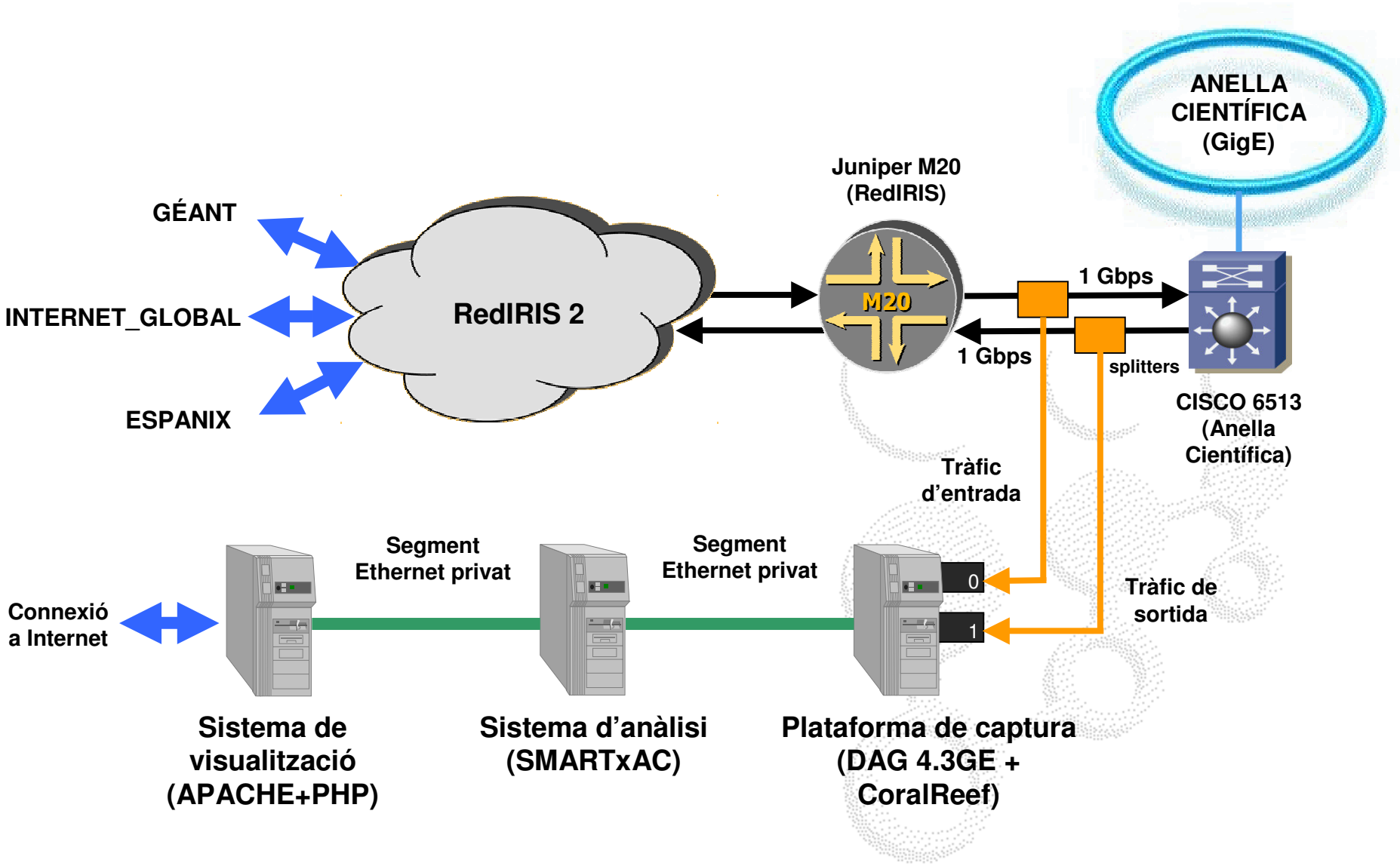


Plataforma SMARTxAC

- Característiques
  - Captura passiva
  - Anàlisi del 100% del tràfic en temps real
  - Captura únicament de capçaleres IP
  - Agregació en fluxos IP
  - Visualització de resultats en temps real via web
- Hardware
  - Endace DAG 4.3GE (+ splitters òptics)
  - 2 PCs estàndard (+1 servidor web)

- Software
  - Captura: CAIDA CoralReef (+ versió especial de libpcap)
  - Anàlisi+visualització: desenvolupat íntegrament CCABA-UPC

Escenari de treball

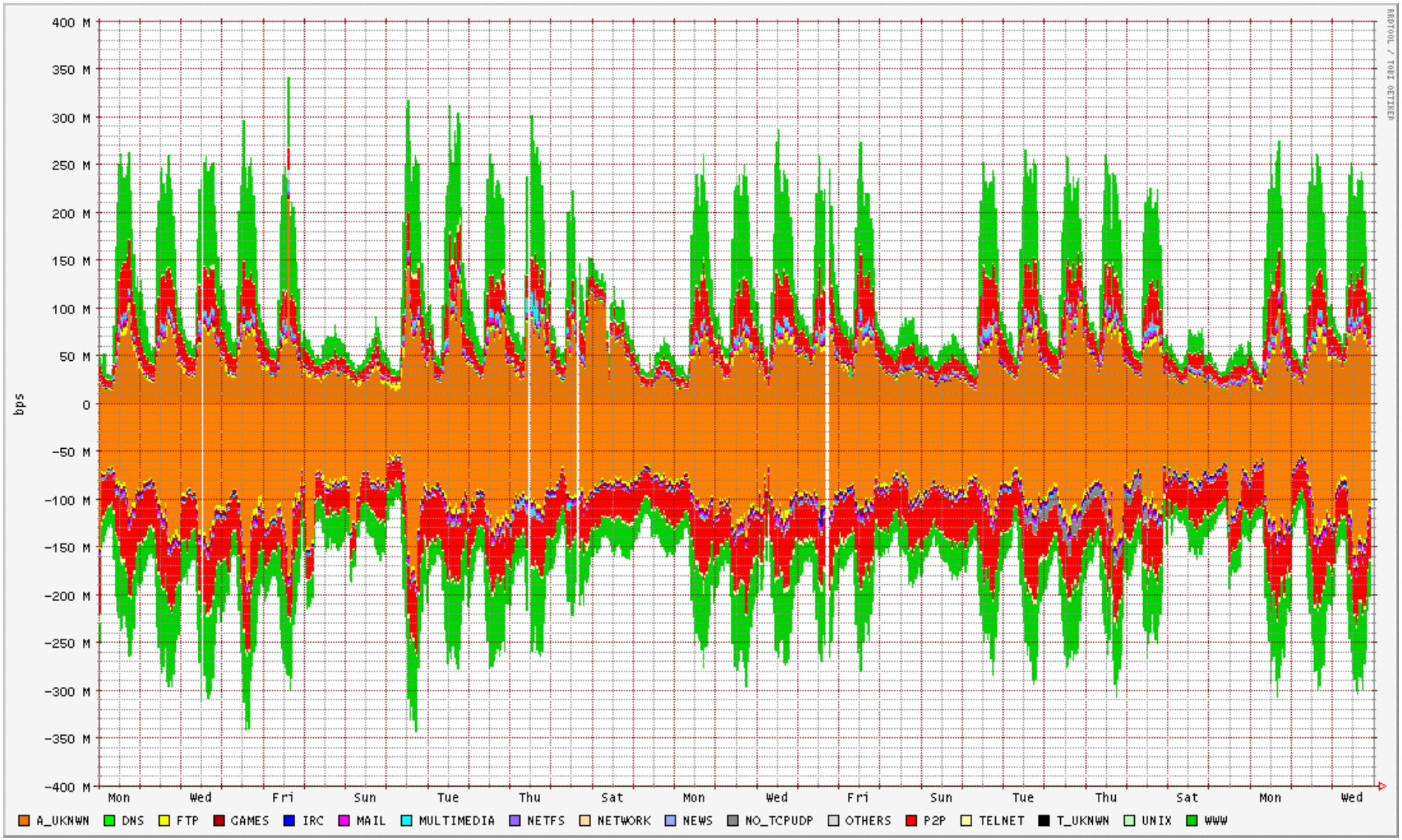


Interfície gràfica

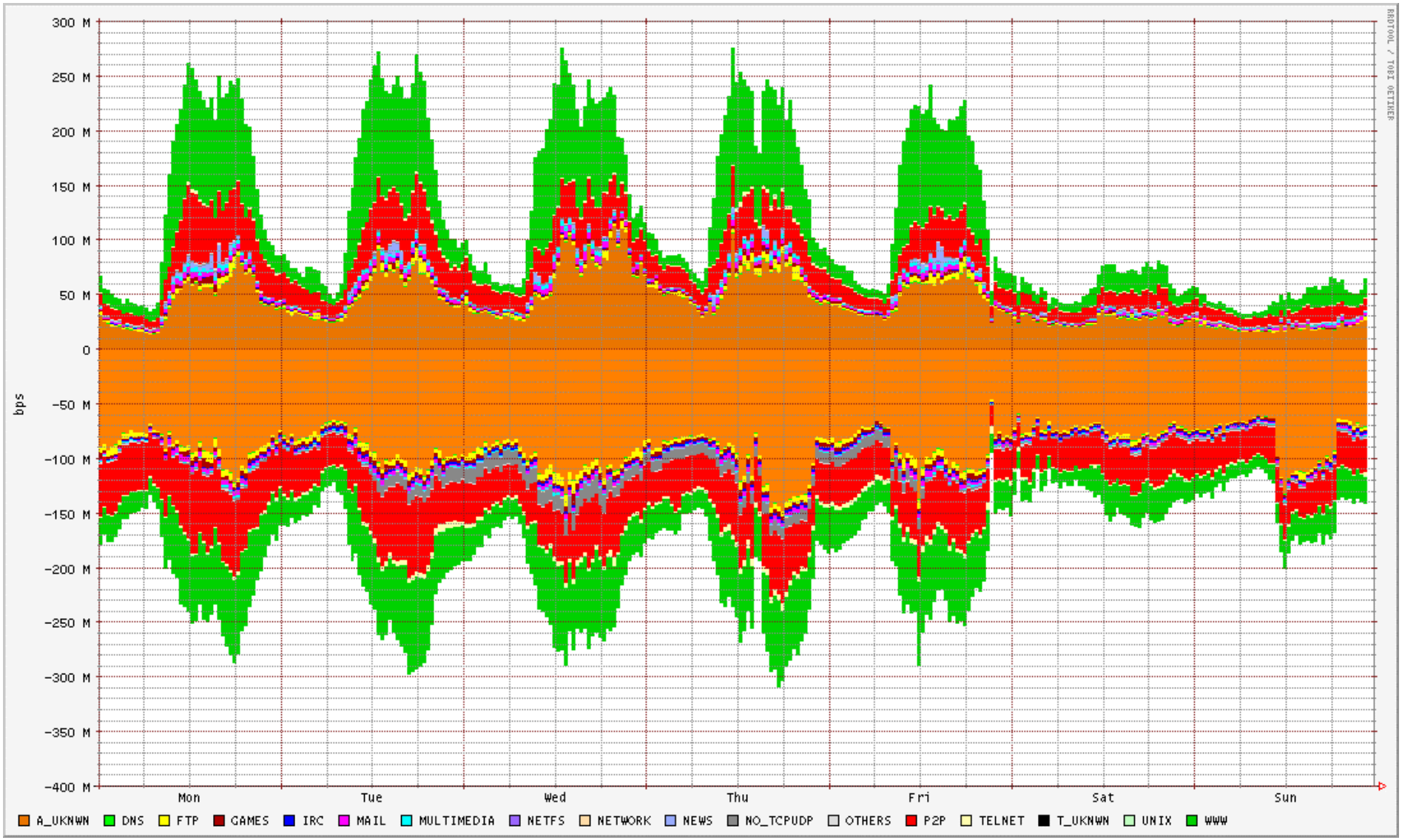
Índex

- Sistema SMAЯTxAC
- Perfil de tràfic de l'Anella Científica
- Gràfiques de situacions irregulars
- Treball actual
- Referències

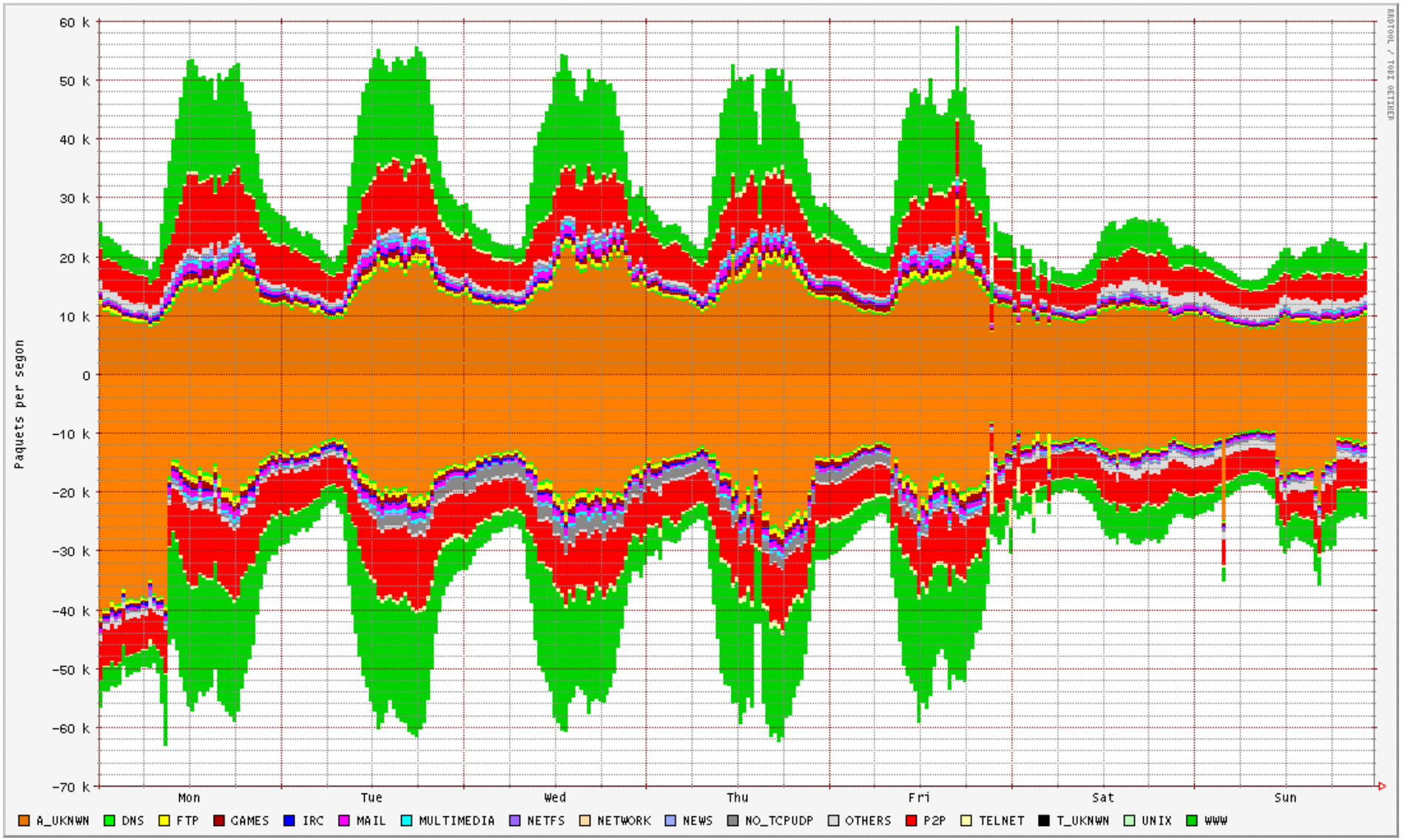
Tràfic mensual per aplicacions (bits/sec)



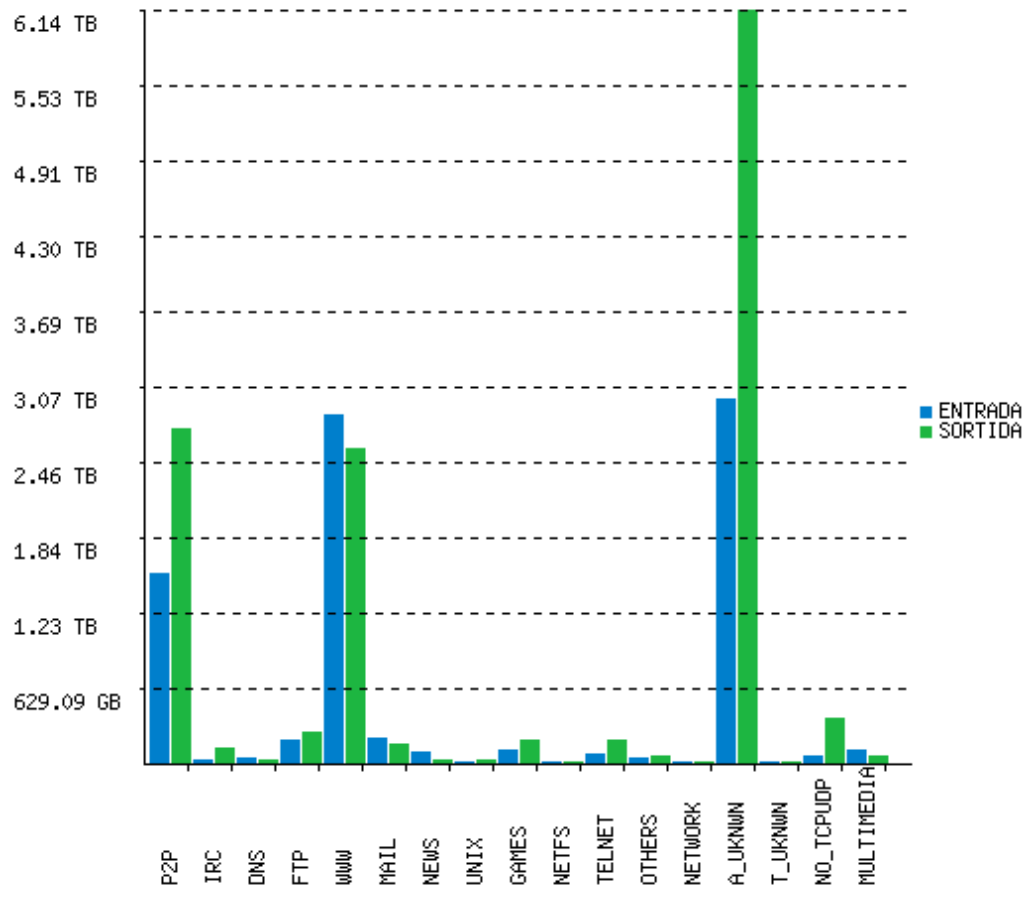
Tràfic setmanal per aplicacions (bits/sec)



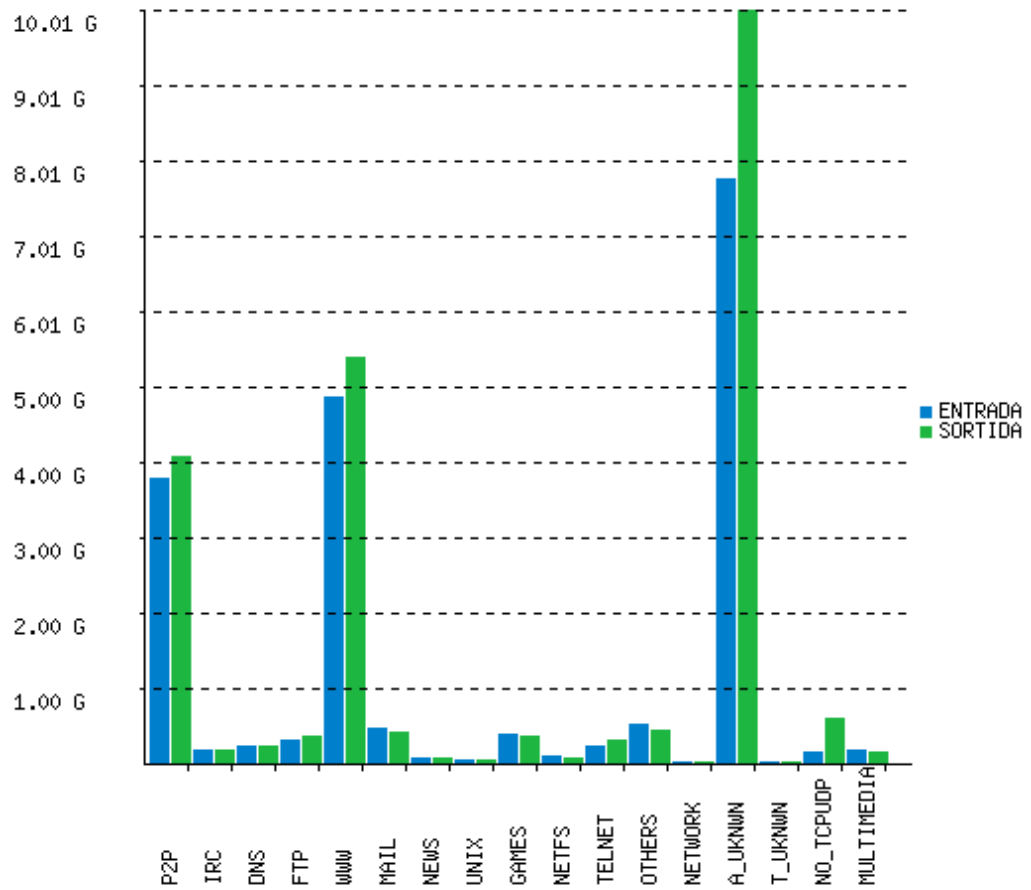
Tràfic setmanal per aplicacions (pkts/sec)



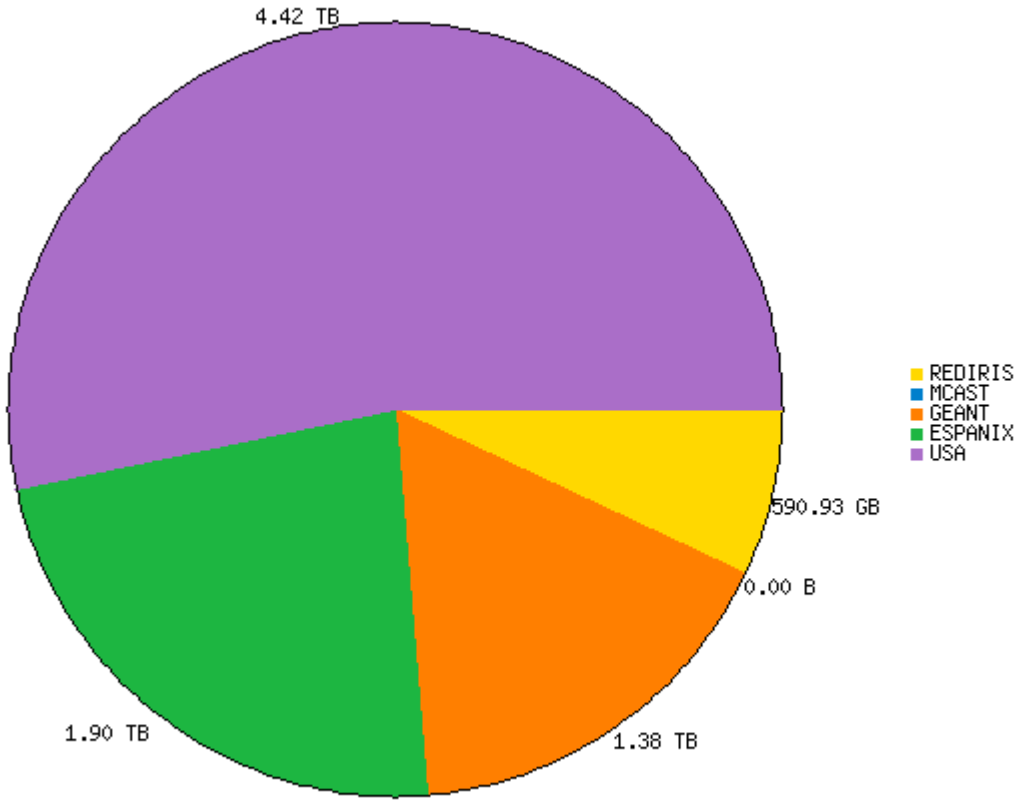
Tràfic setmanal per aplicacions (bytes)



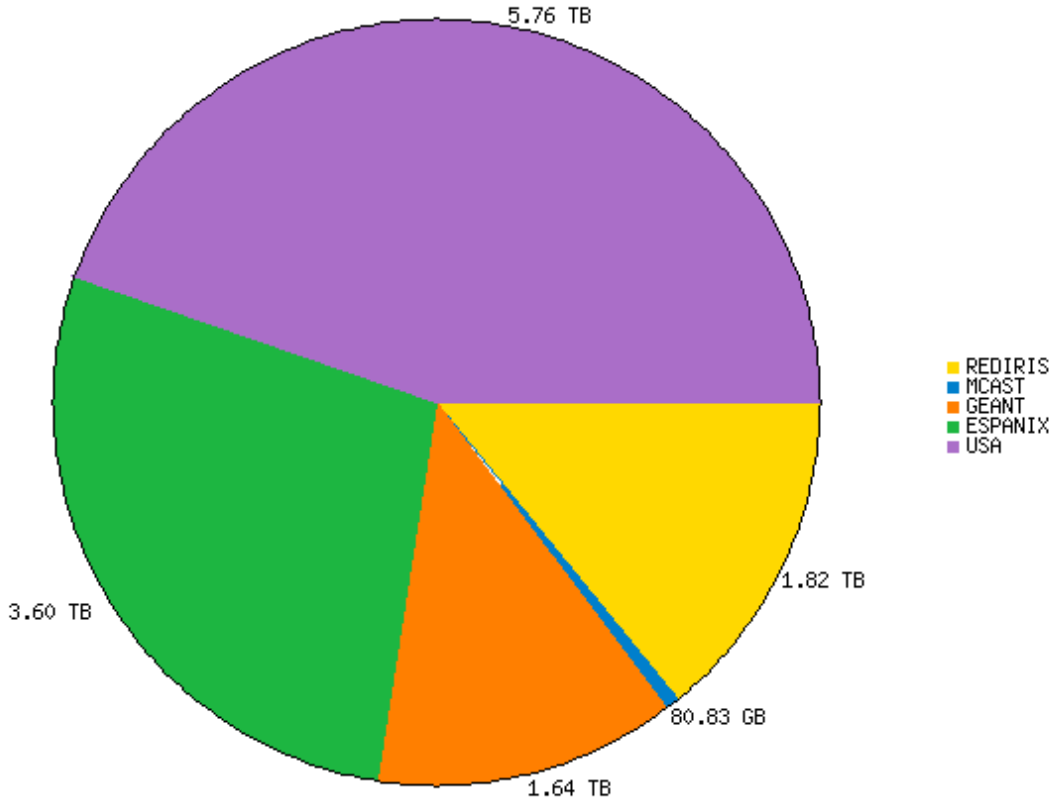
Tràfic setmanal per aplicacions (pkts)



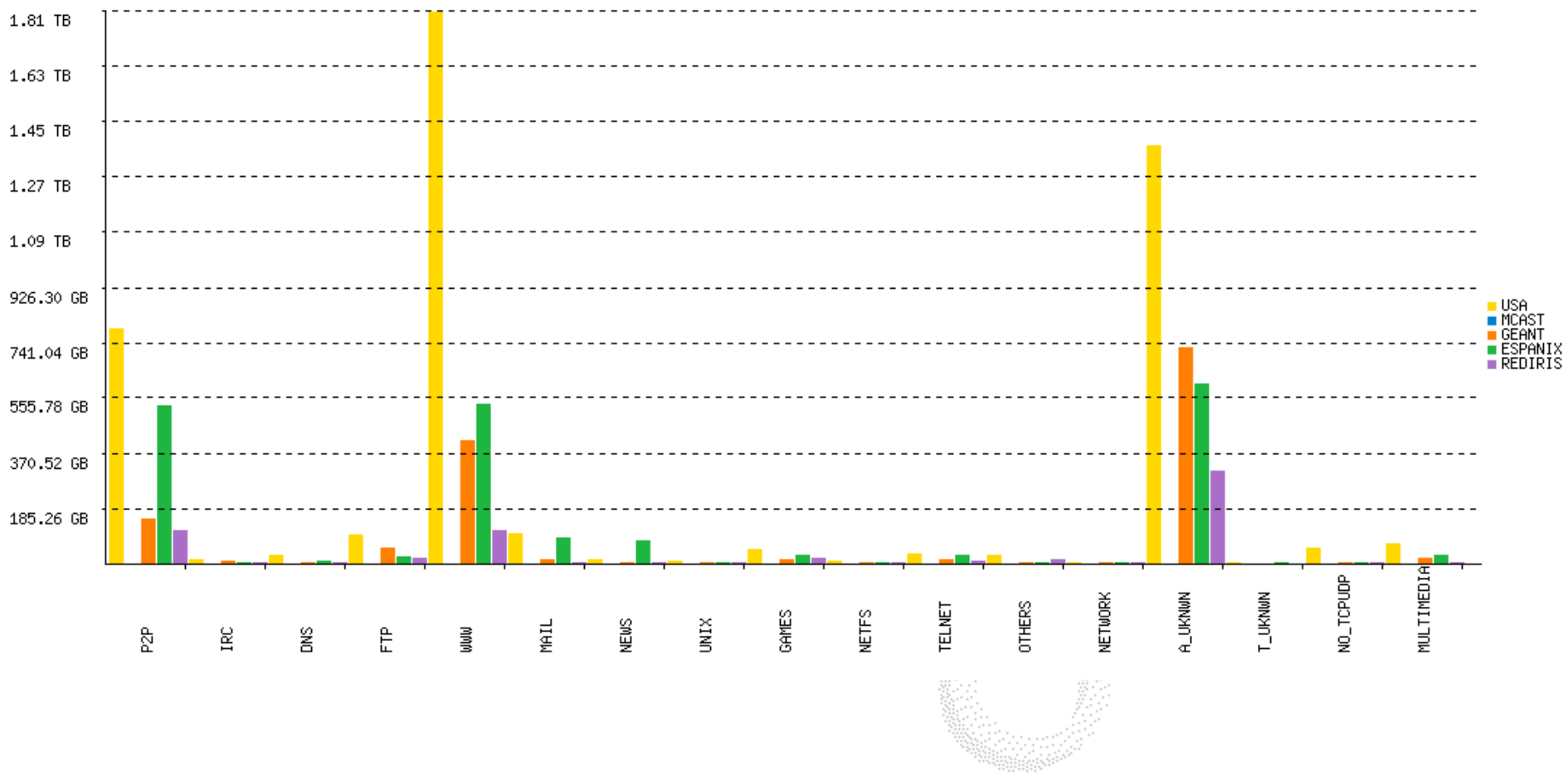
Tràfic setmanal per destinació (bytes ent.)



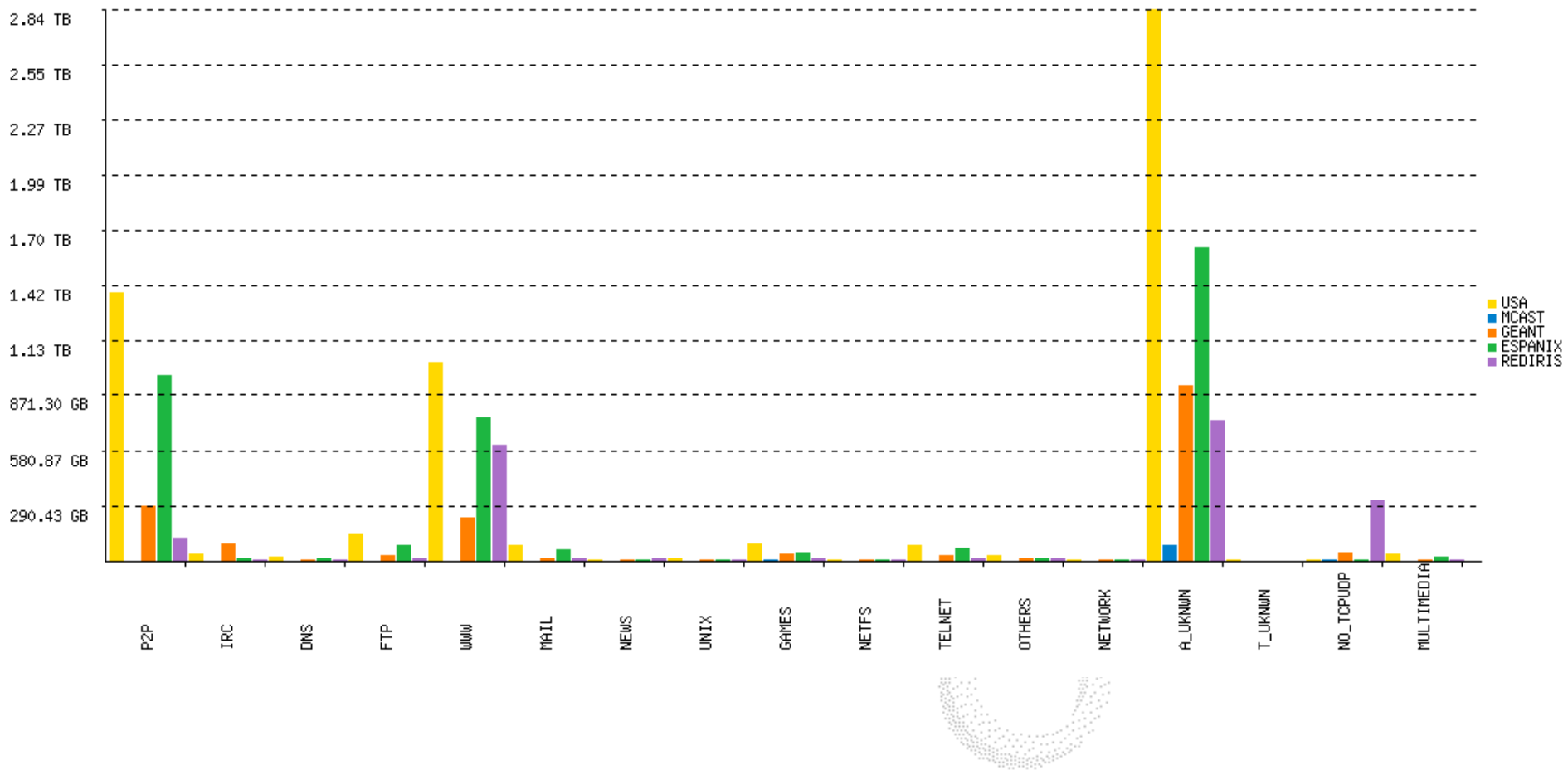
Tràfic setmanal per destinació (bytes sortida)



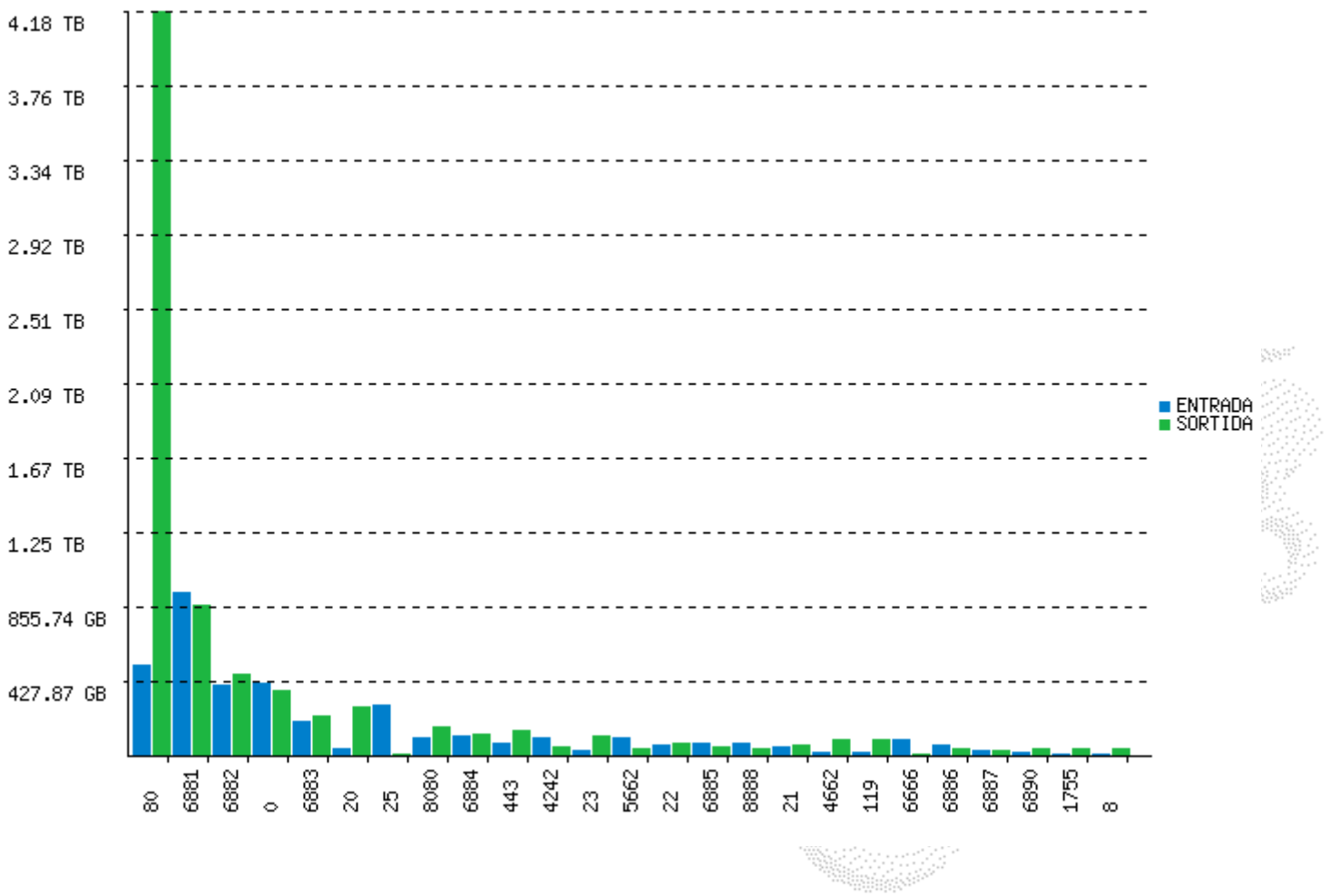
Tràfic per destinació i aplicació (bytes ent.)



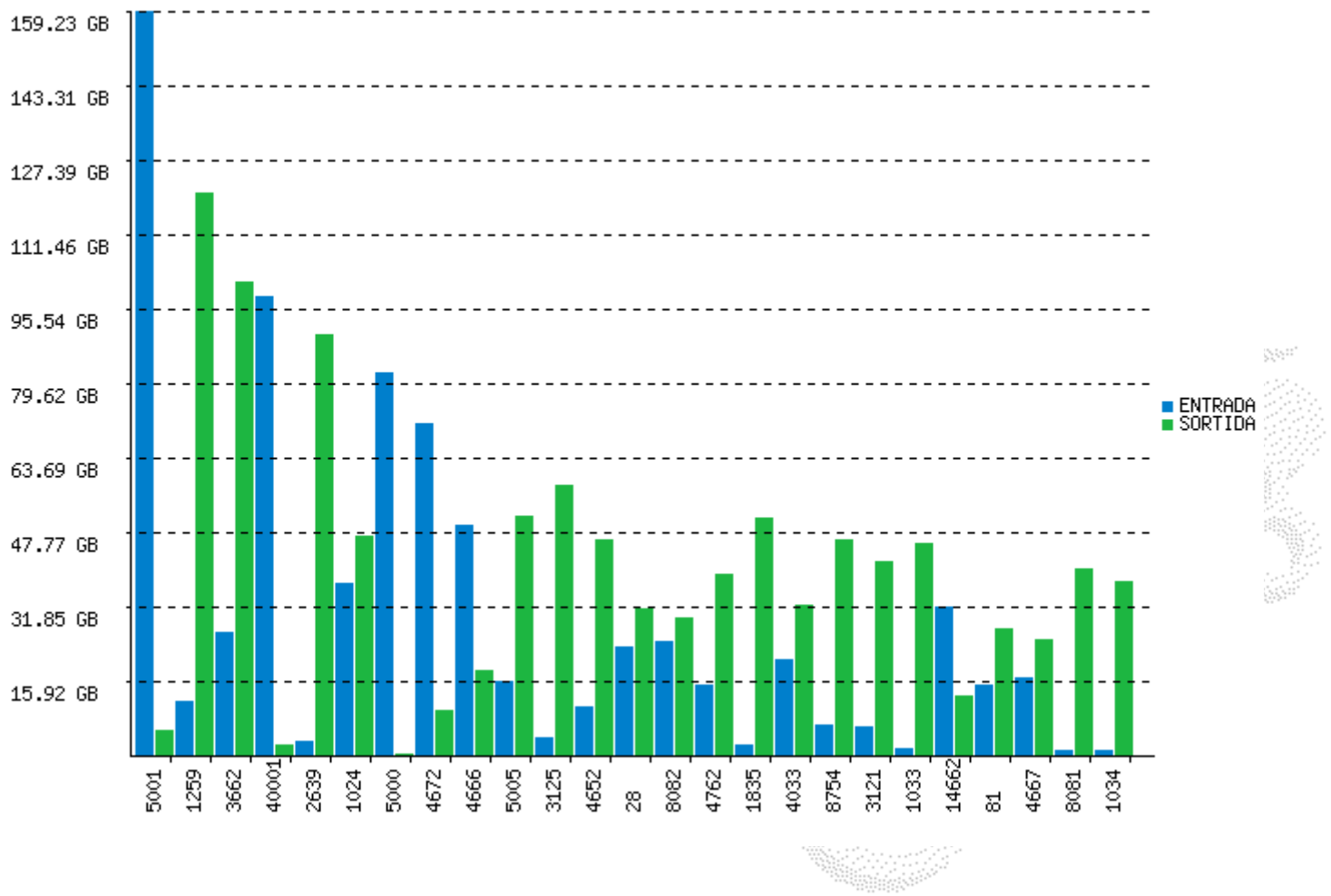
Tràfic per destinació i aplicació (bytes sor.)



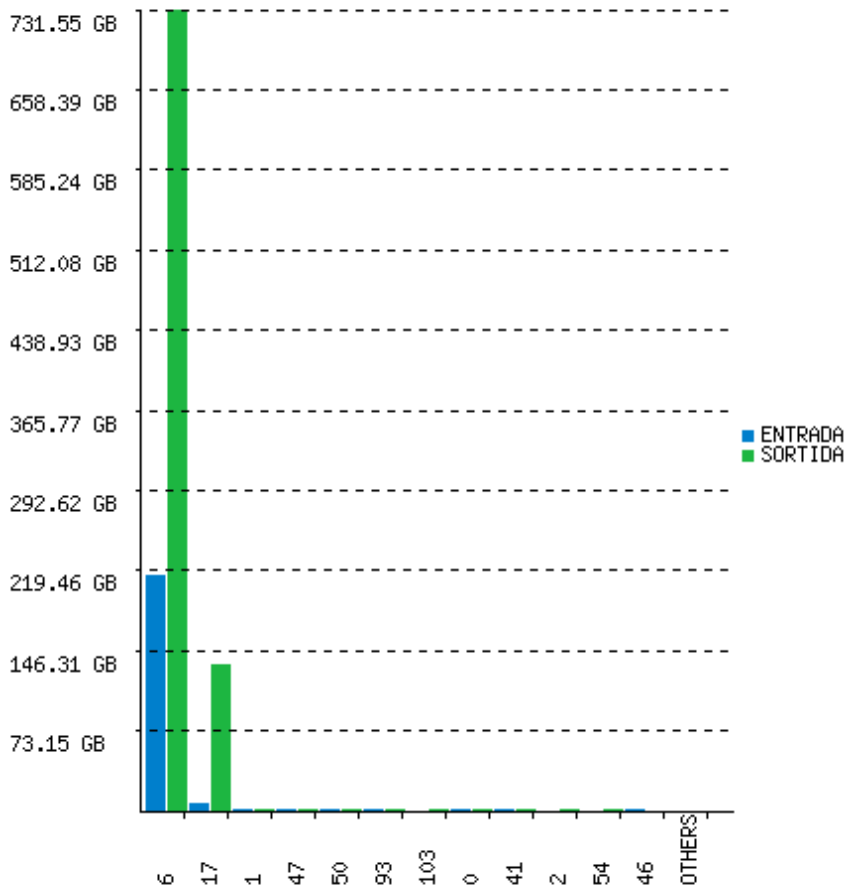
Top-N ports coneguts (bytes)



Top-N ports desconeguts (bytes)



Top-N protocols (bytes)



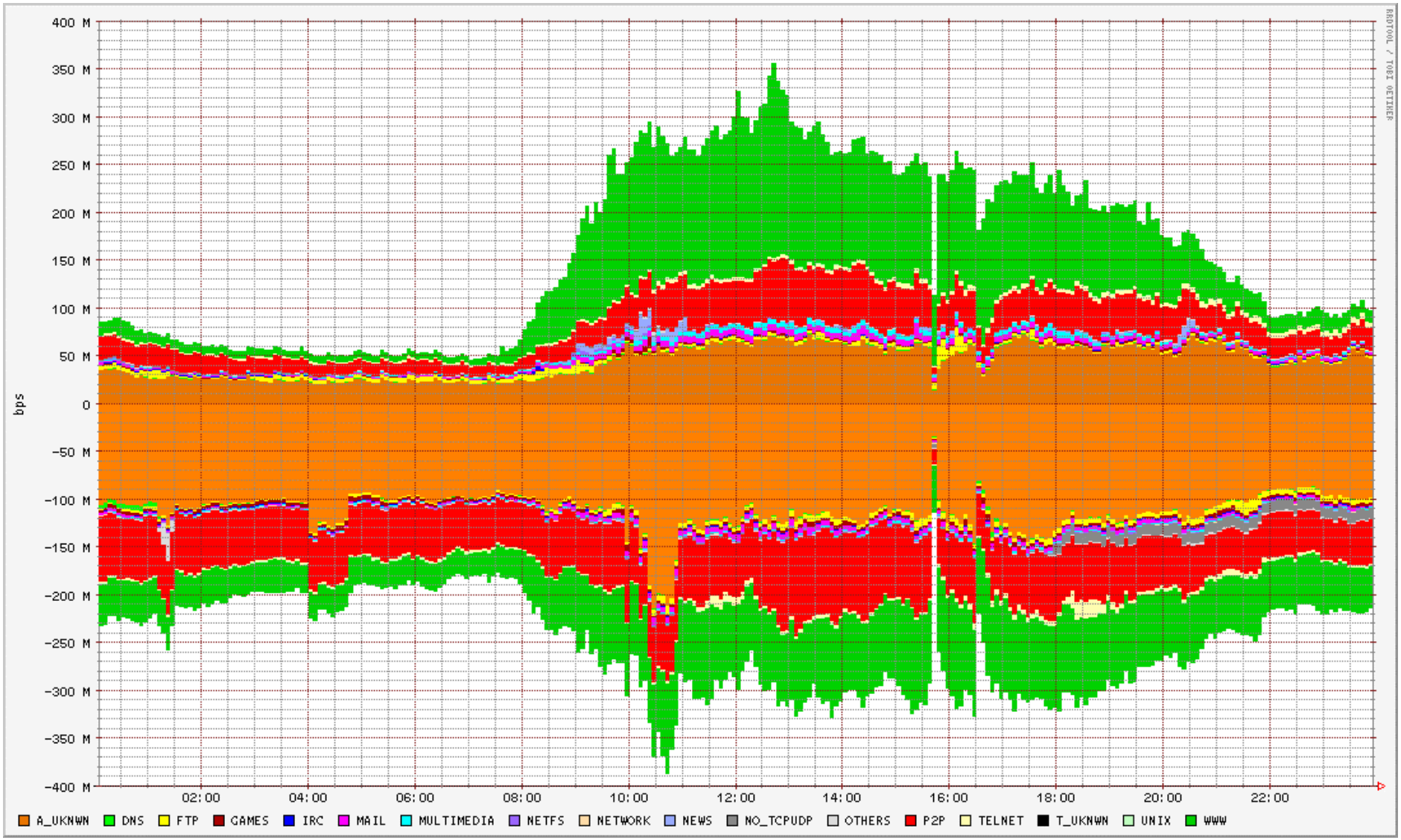
Altres gràfiques

- Gràfiques anteriors per institucions/punts d'accés
- Top-N d'adreces IP
- Top-N d'adreces IP desconegudes
- Top-N protocols no TCP/UDP
- Top-N protocols desconeguts
- Tràfic per institució/punt accés
- Destins per institucions/punts accés
- Comparativa aplicacions institucions/punt accés

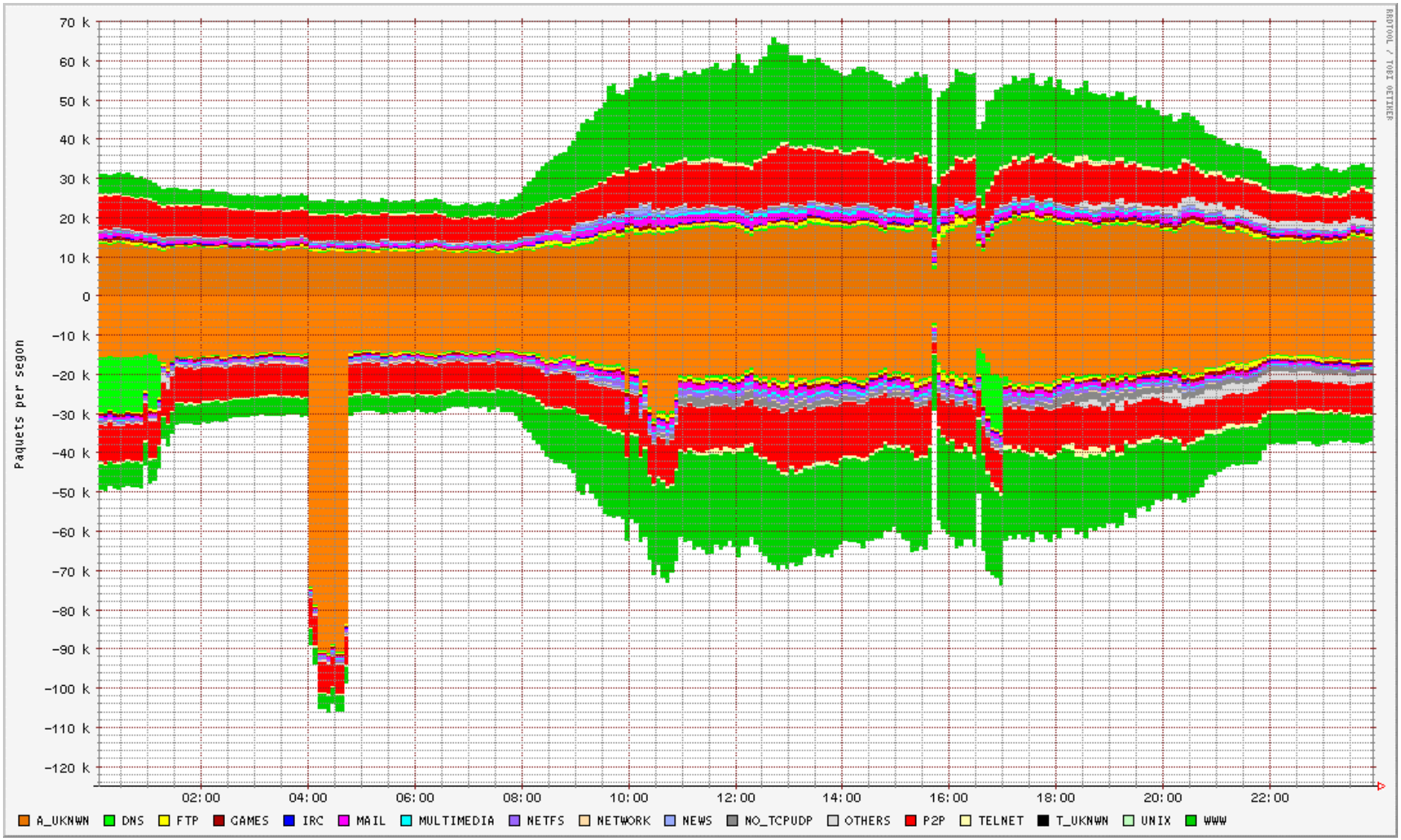
Índex

- Sistema SMAЯTxAC
- Perfil de tràfic de l'Anella Científica
- Gràfiques de situacions irregulars
- Treball actual
- Referències

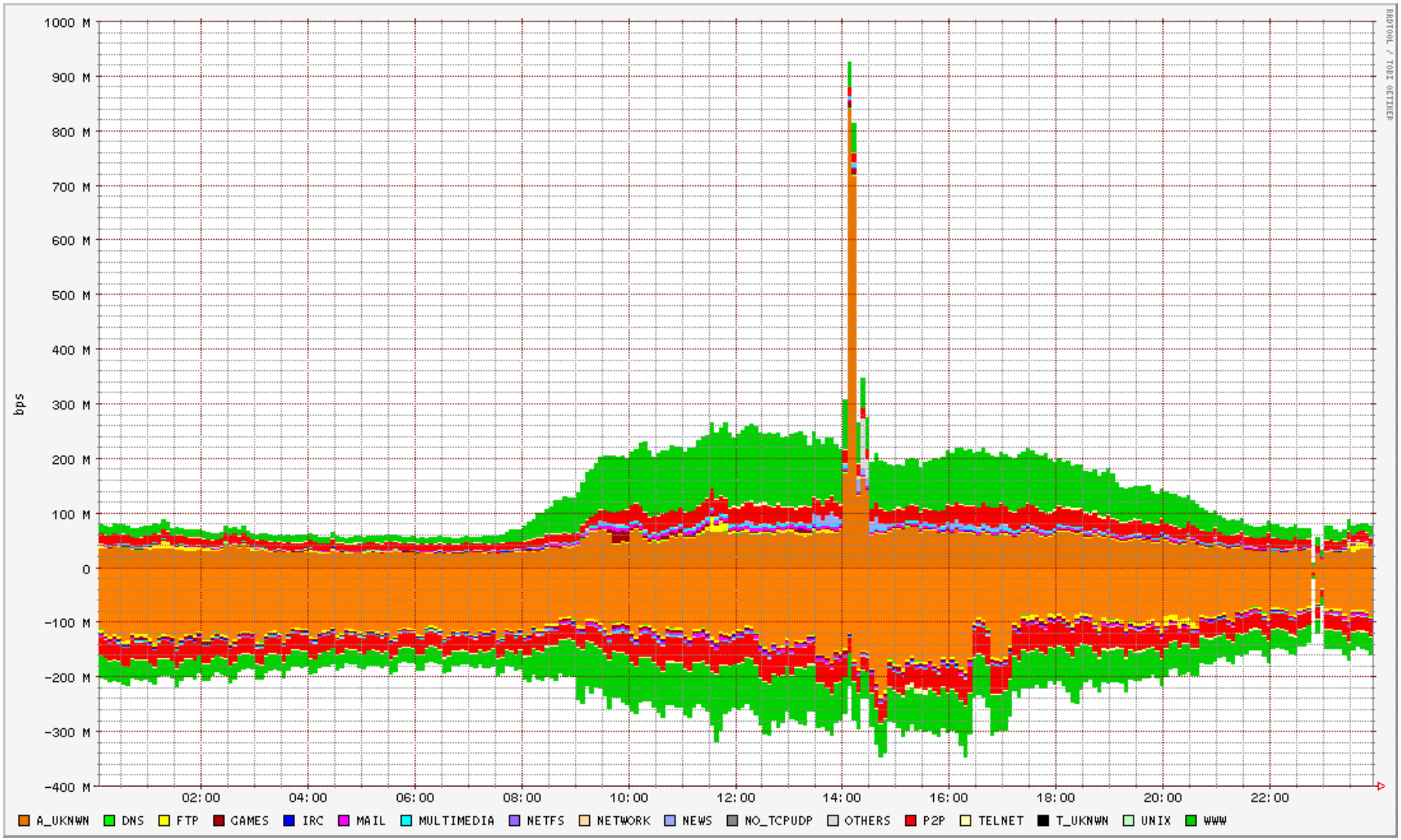
Situació irregular 1 (bits/sec)



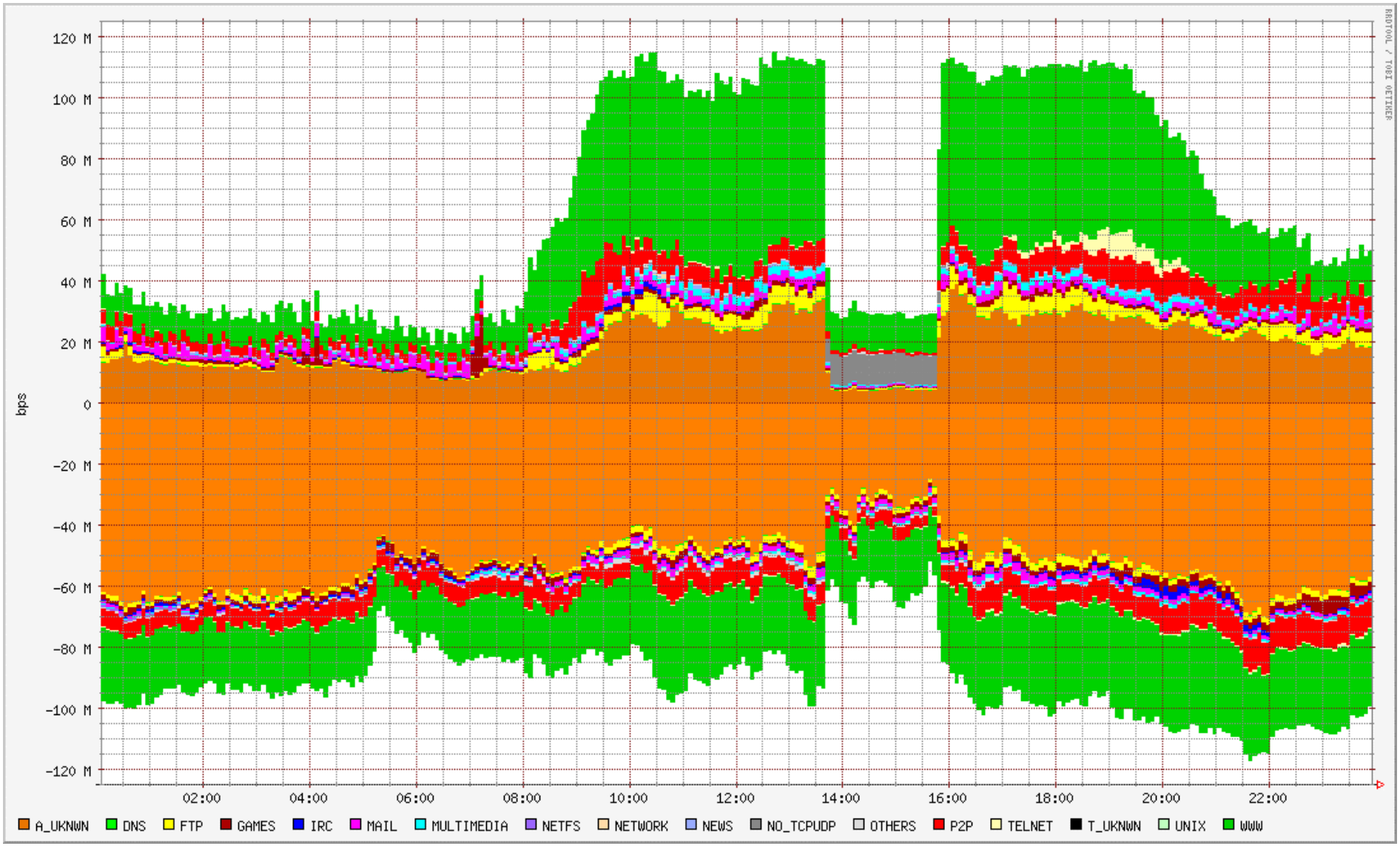
Situació irregular 1 (pkts/sec)



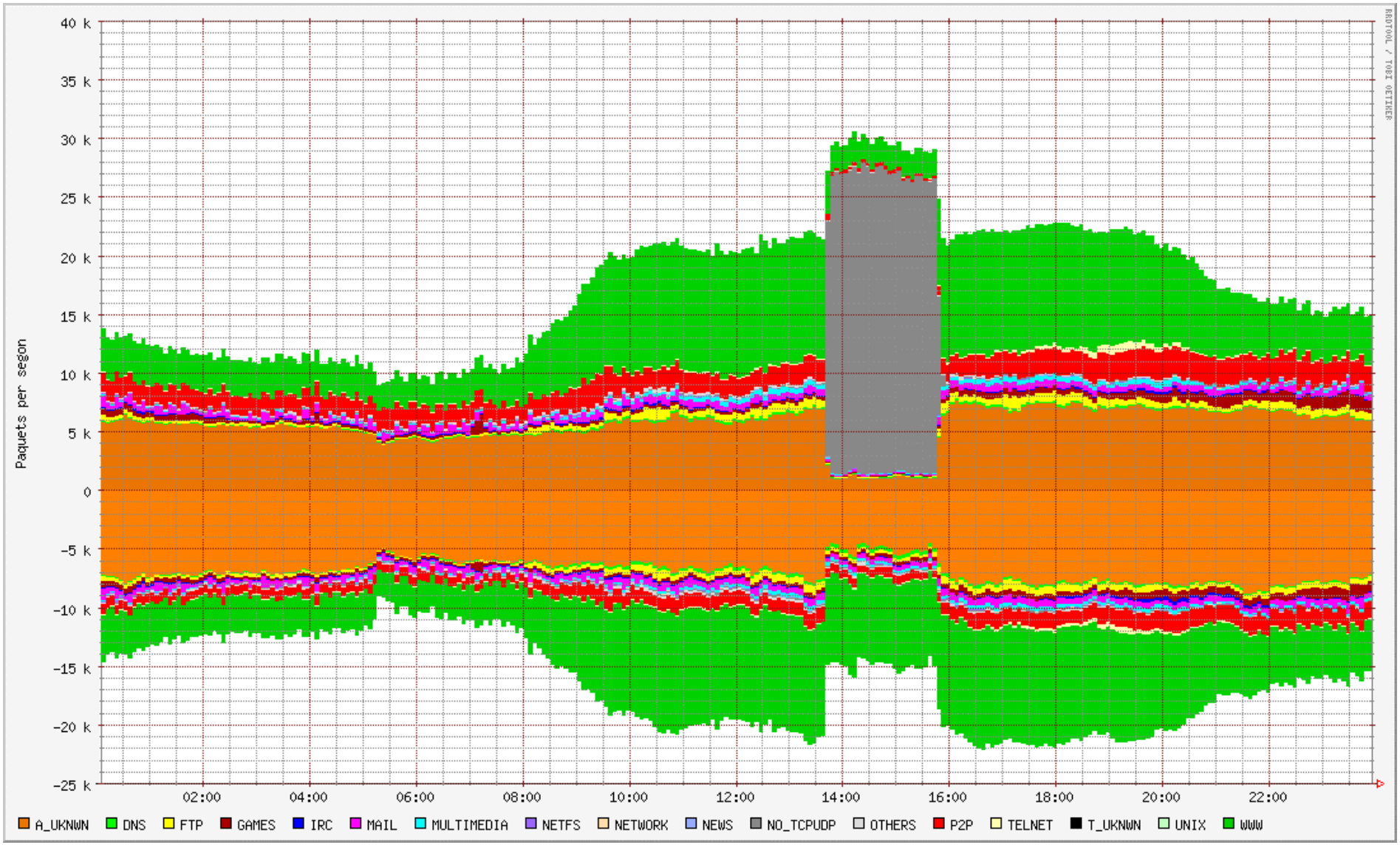
Situació irregular 2 (bits/sec)



Situació irregular 3 (bits/sec)



Situació irregular 3 (pkts/sec)



Índex

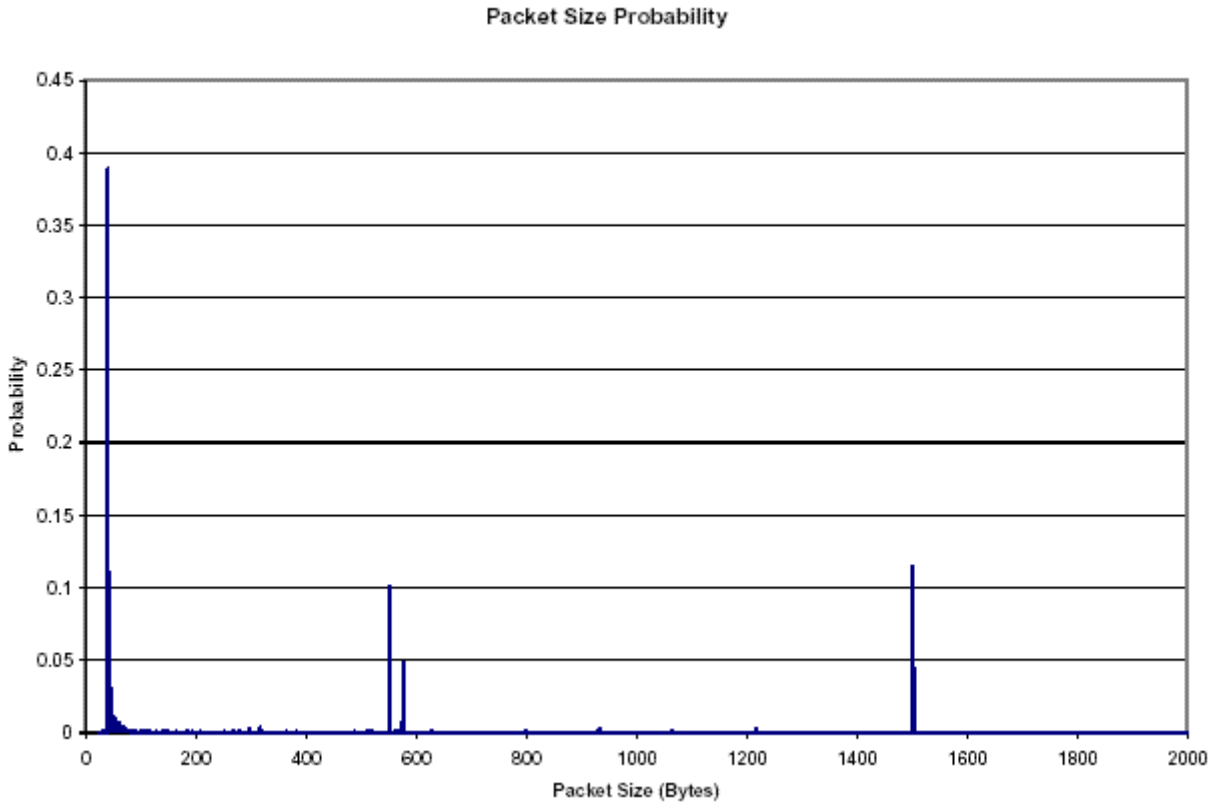
- Sistema SMAЯTxAC
- Perfil de tràfic de l'Anella Científica
- Gràfiques de situacions irregulars
- Treball actual
- Referències

Treball actual

- Detecció automàtica de situacions/usos irregulars
  - Canvis en els patrons habituals de tràfic per institució
  - Atacs (DoS, DDoS, etc.)
  - Us d'aplicacions P2P o equivalents
- Reaccions davant situacions irregulars
  - Generació d'alarmes per avisar a l'administrador
  - Guardar informació addicional sobre el tràfic sospitós
  - Anàlisi *off-line* para descobrir les possibles causes
- Detecció d'anomalies basada en:
  - Llindars per institució/punt d'accés
  - Predictors de tràfic
  - Característiques del tràfic

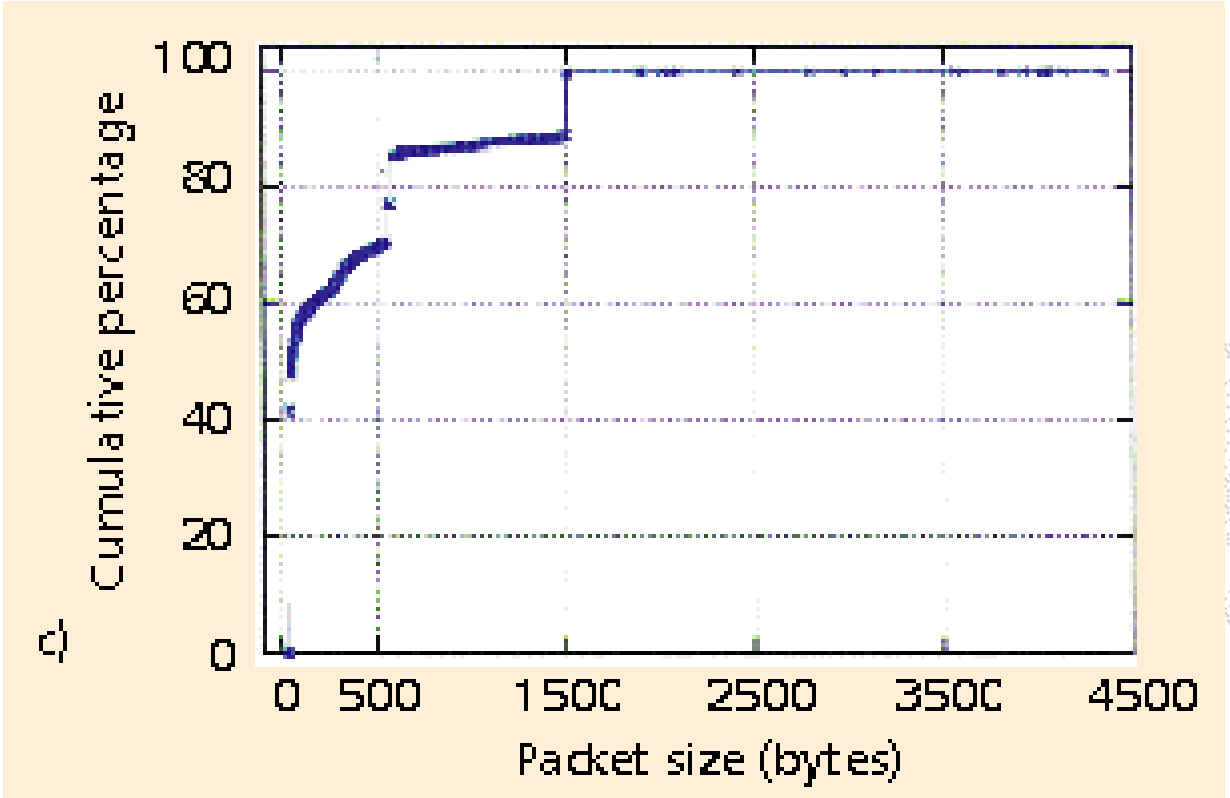
Distribució longitud de paquets

- Enllaç OC-3 del MCI (NLANR, 1998)



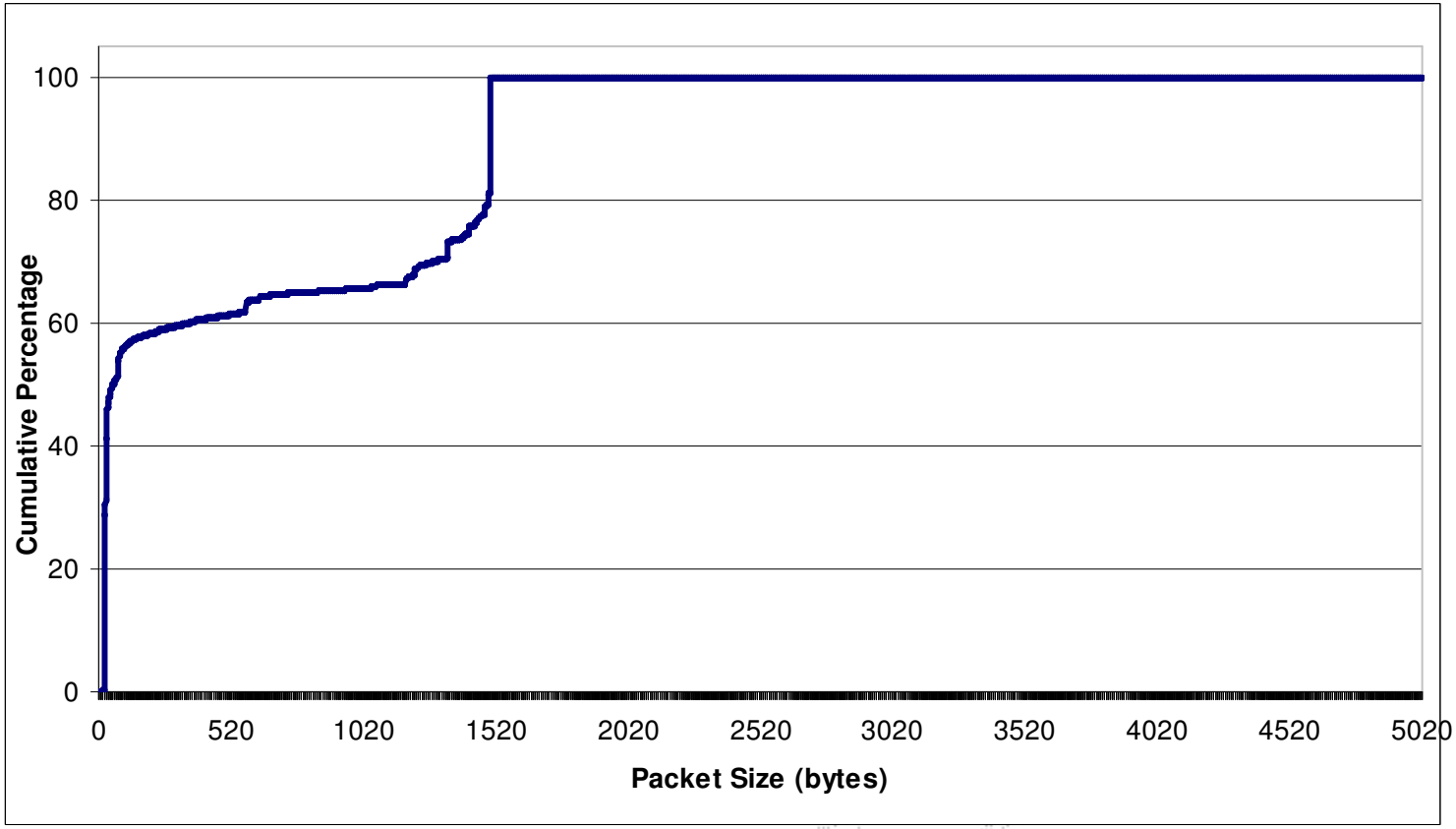
CDF longitud de paquets

- Entorn residencial (IEEE Network, Nov-Dec 1997)



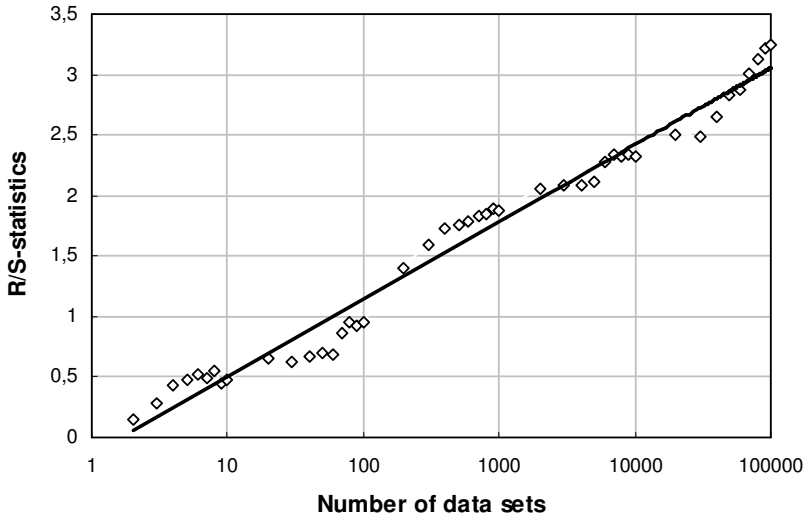
CDF longitud de paquets

- Anella Científica (2003)

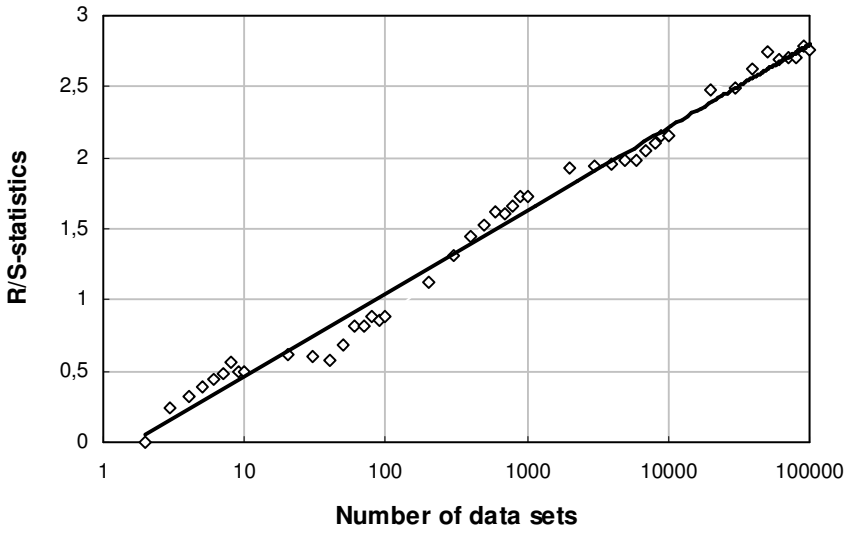


Estimació de self-similaritat

- Anella Científica (2004)
  - Gràfiques R/S plot: el pendent de la gràfica dóna una estimació del paràmetre de Hurst (H)
    - *H = 1.0 → Self-Similar*
    - *H = 0.5 → Exponencial*



Tràfic d'entrada (H=0.64)



Tràfic de sortida (H=0.58)

Índex

- Sistema SMAЯTxAC
- Perfil de tràfic de l'Anella Científica
- Gràfiques de situacions irregulars
- Treball actual
- Referències

Referències (I)

- Informació general del sistema SMAЯTxAC
  - http://www.ccaba.upc.es/smartxac
- Proves SMART (evolució del SMARTxAC) en un enllaç 10Gbps OC-192 del NLANR
  - http://pma.nlanr.net/Special/tera2.html
- Traça de l'Anella Científica sincronitzada amb GPS (traça únicament de capçaleres i anonimitzada)
  - http://pma.nlanr.net/Special/cesc1.html
- Ponència a les "Jorndas Técnicas de RedIRIS 2003"
  - http://www.rediris.es/jt/jt2003/archivo-jt

Referències (II)

- **CCABA** “Centre de Comunicacions Avançades de Banda Ampla”
  - http://www.ccaba.upc.es
- **CESCA** “Centre de Supercomputació de Catalunya”
  - http://www.cesca.es
- **ENDACE** “Endace Measurement Systems”
  - http://www.endace.com
- **CAIDA** “Cooperative Association for Internet Data Analysis”
  - http://www.caida.org
- **NLANR** “National Laboratory for Applied Network Research”
  - http://www.nlanr.net

Referències (III)

- BARLET, P.; SOLÉ-PARETA, J.; DOMINGO-PASCUAL, J. "SMARTxAC: Sistema de Monitorización y Análisis de Tráfico para la Anella Científica". Jornadas Técnicas RedIRIS. 2003. Mallorca (Spain).
- VECIANA-NOGUÉS, C.; DOMINGO-PASCUAL, J.; SOLÉ-PARETA, J. "Cost-sharing and Billing in the National Research Networks: the MIRA Approach". In proc. of: Terena Networking Conference. 2002. Limerick (Ireland).
- LIZCANO, P.J.; AZCORRA, A.; SOLÉ-PARETA, J.; DOMINGO-PASCUAL, J.; ÁLVAREZ-CAMPANA, M. "MEHARI: A System for Analyzing the Use of the Internet Services". "Computer Networks". 31(21):2293-2307.
- MOORE, D; KEYS, K.; KOGA, R.; LAGACHE, E.; CLAFFY, K. "The CoralReef Software suite as a tool for system and network administrators". 2001.
- ENDACE MEASUREMENT SYSTEMS. "DAG 4.3GE Network Monitoring Interface Card". 2003. (http://www.endace.com/dag4.3GE.htm)