Call Identifier: SMART 2012/0046

Full title: Study on European Internet Traffic: Monitoring Tools and Analysis

Deliverable D5: Second Experts' Workshop Report APPENDIX B

Date of preparation: June 21, 2014

List of participant organisations:

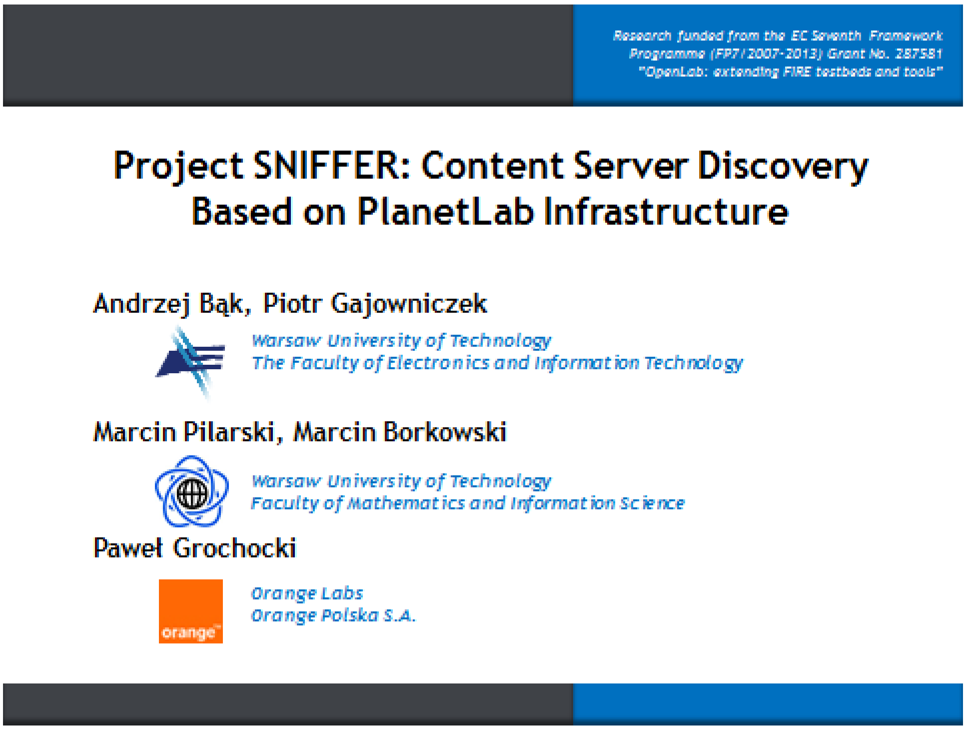
Role	Participant name	Participant short name	Country
Tenderer	Hebrew University of Jerusalem	HUJI	Israel
Supporting partner	Alcatel Lucent Bell N.V.	ALB	Belgium
Supporting partner	Martel GmbH	MAR	Switzerland
Supporting partner	Universidad Autónoma de Madrid	UAM	Spain
Supporting partner	Universite Pierre et Marie Curie – Paris 6	UPMC	France

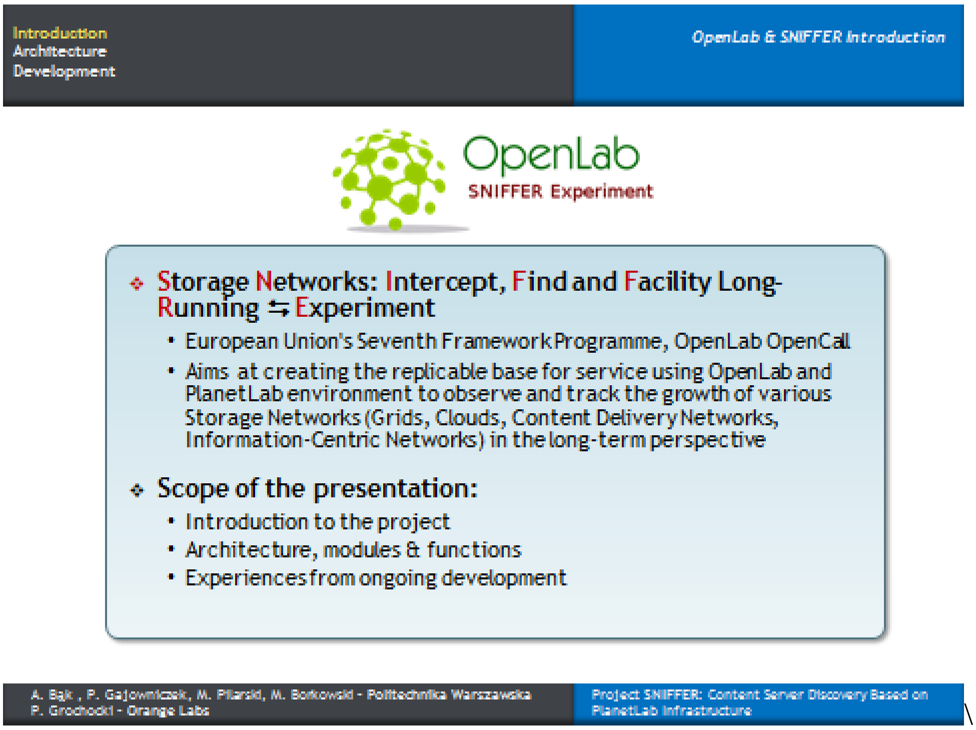
Editor of this deliverable: Professor Scott Kirkpatrick
Organisation: Hebrew University of Jerusalem
e-mail: kirk@cs.huji.ac.il

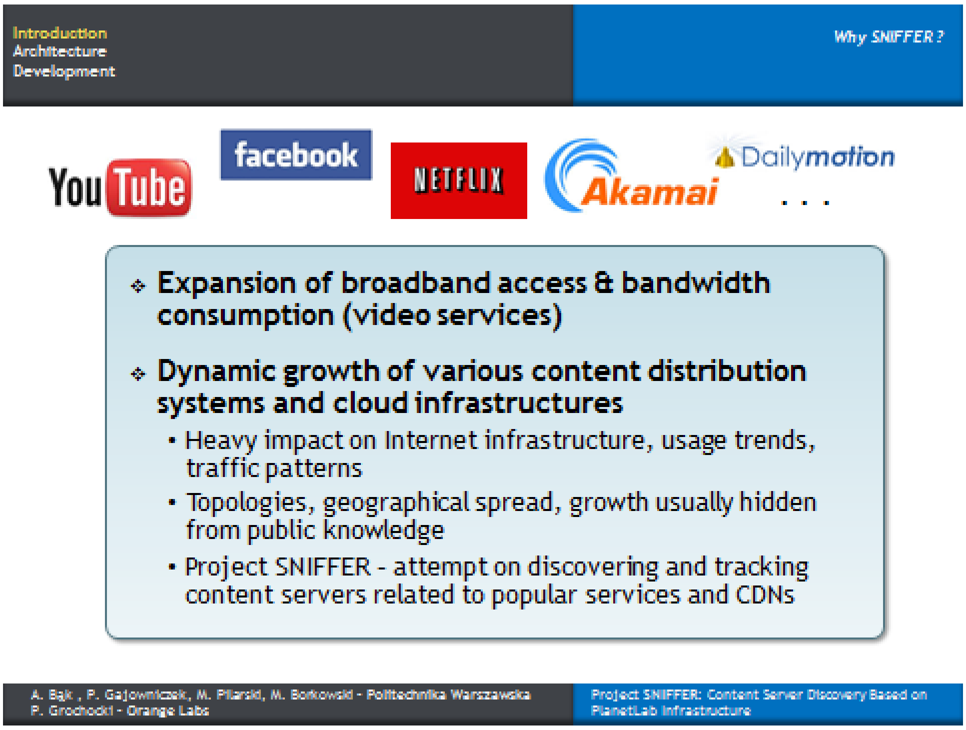
This Appendix contains the second half of the slides presented as input to the second Expert Workshop in this study. Summaries of the material appear in the main report, which is Deliverable D5 of SMART 2012/0046. Both the report and this Appendix are public material.

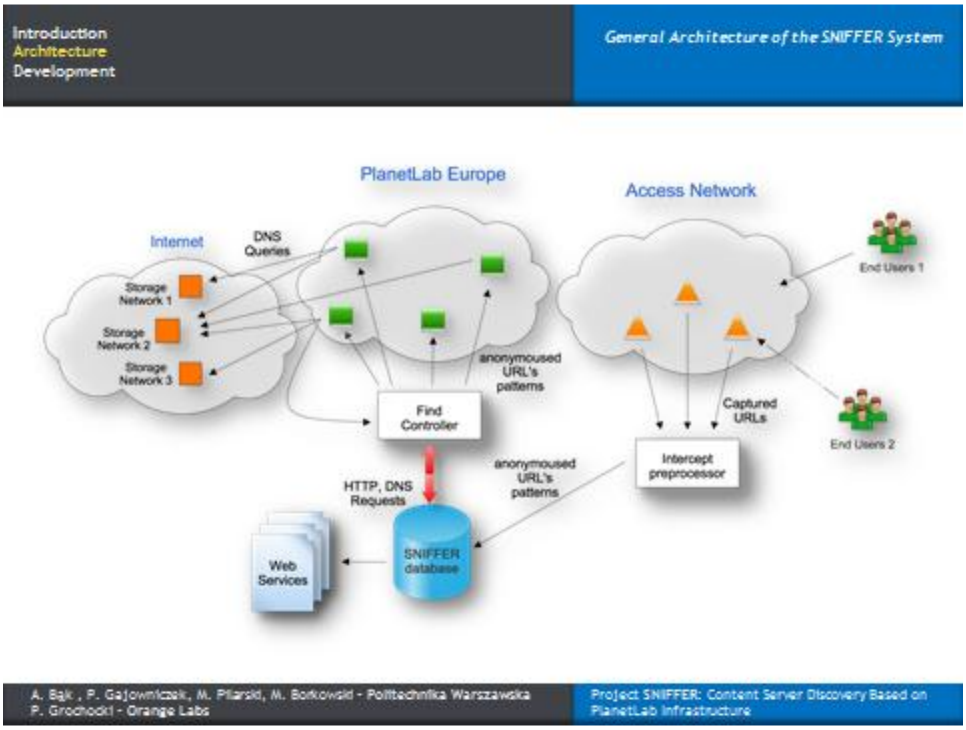
1. APPENDIX: SLIDES PRESENTED AT THE WORKSHOP

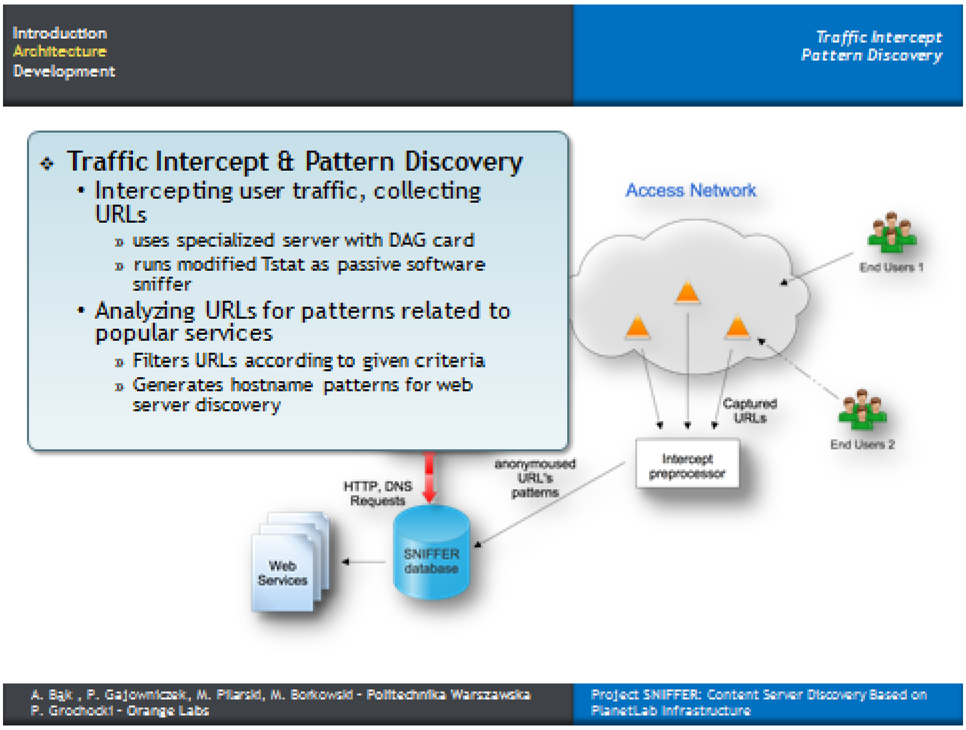
1.1 Prof. Marcin Pilarski

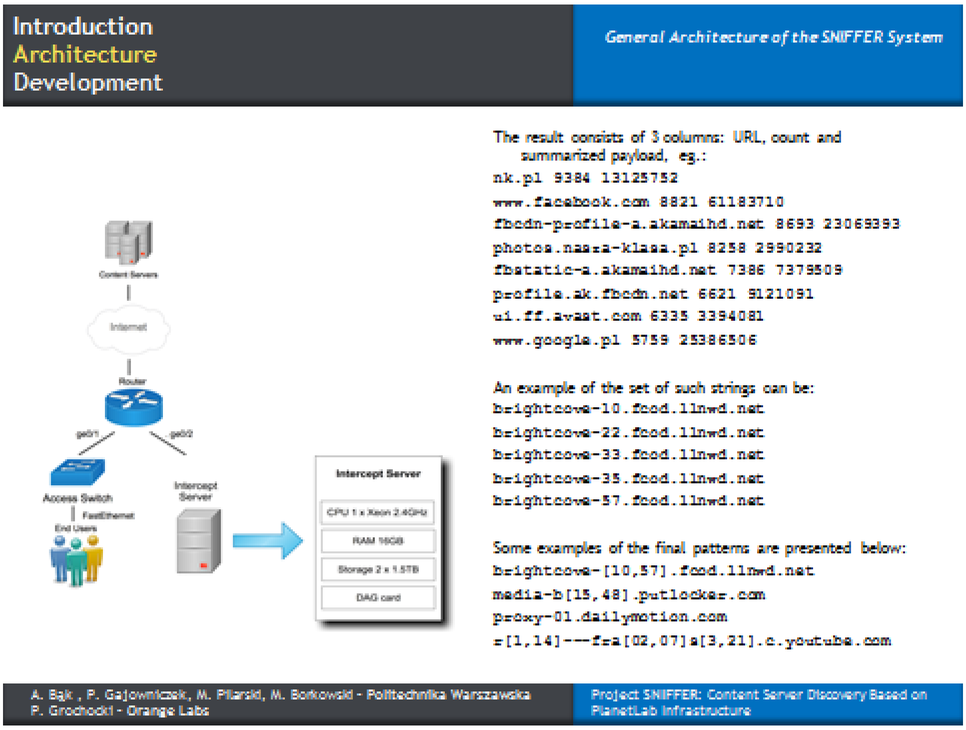


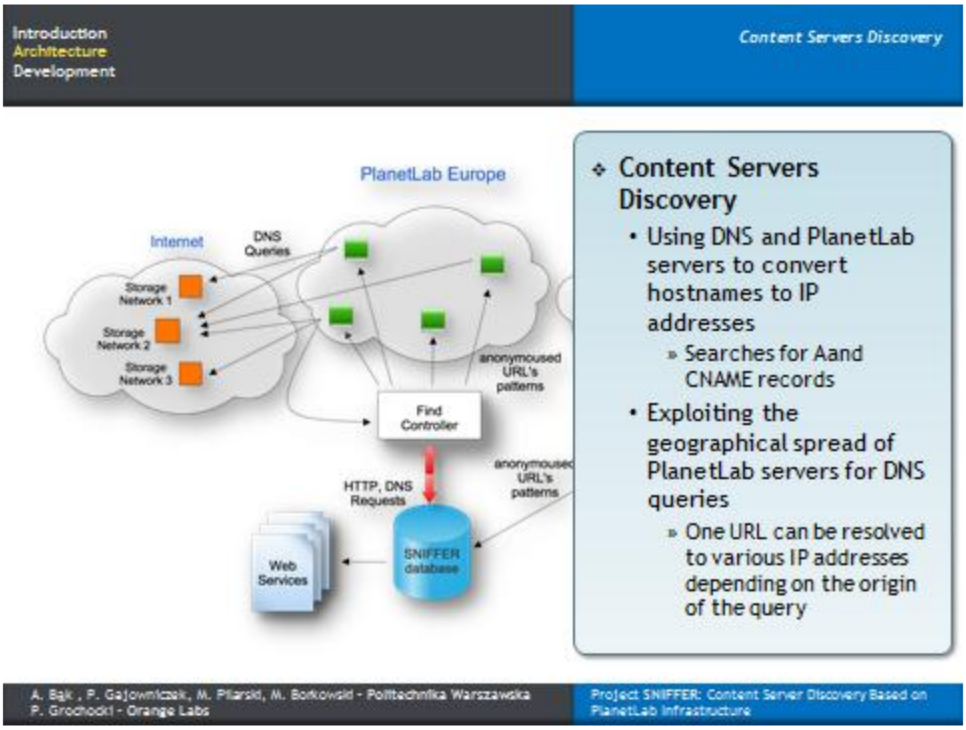


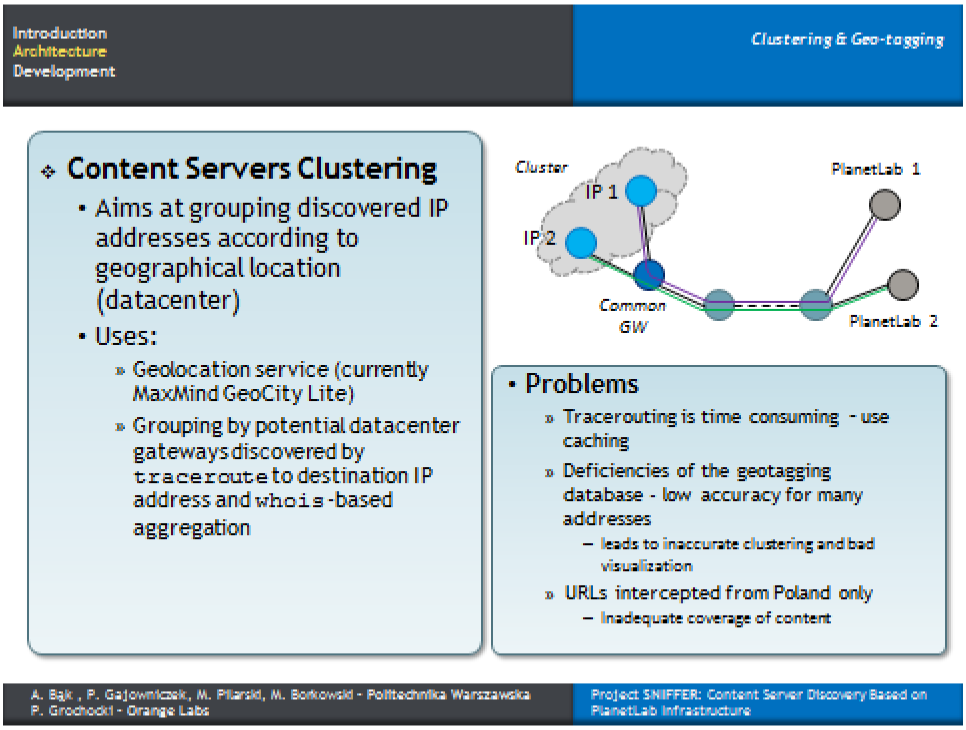

Introduction
Architecture
Development
Why SNIFFER ?
YouTube
facebook
NETFLIX
Akamai
Dailymotion
. . .
Expansion of broadband access & bandwidth consumption (video services)
Dynamic growth of various content distribution systems and cloud infrastructures
Heavy impact on Internet infrastructure, usage trends, traffic patterns
Topologies, geographical spread, growth usually hidden from public knowledge
Project SNIFFER - attempt on discovering and tracking content servers related to popular services and CDNs
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure

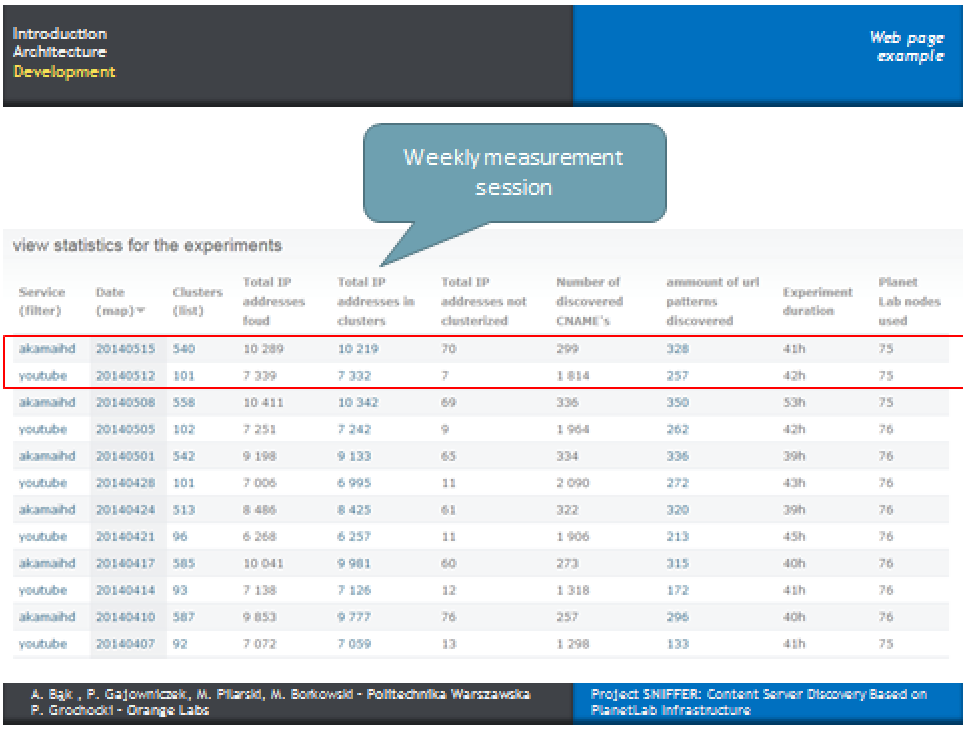

Introduction
Architecture
Development
General Architecture of the SNIFFER System
PlanetLab Europe
Access Network
Internet
DNS Queries
Storage Network 1
Storage Network 2
Storage Network 3
End Users 1
End Users 2
anonymoused URL's patterns
Find Controller
Captured URLs
Intercept preprocessor
HTTP, DNS Requests
anonymoused URL's patterns
Web Services
SNIFFER database
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure


Introduction
Architecture
Development
Traffic Intercept
Pattern Discovery
Traffic Intercept & Pattern Discovery
Intercepting user traffic, collecting URLs
uses specialized server with DAG card
runs modified Tstat as passive software sniffer
Analyzing URLs for patterns related to popular services
Filters URLs according to given criteria
Generates hostname patterns for web server discovery
Access Network
End Users 1
End Users 2
Captured URLs
Intercept preprocessor
anonymoused URL's patterns
HTTP, DNS Requests
SNIFFER database
Web Services
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure

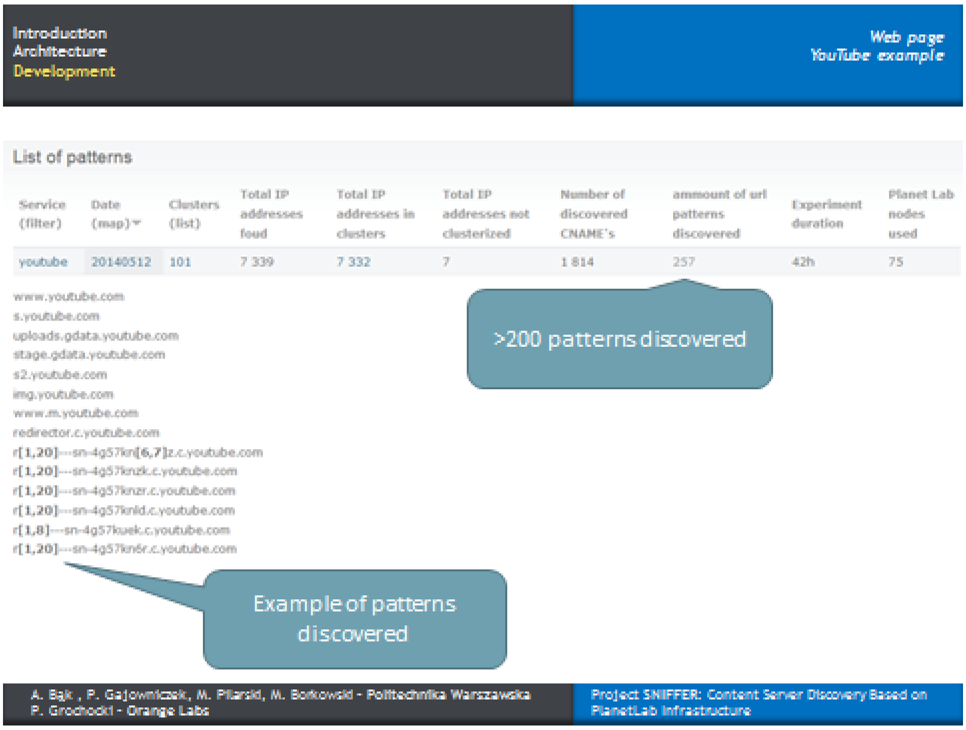

Introduction
Architecture
Development
General Architecture of the SNIFFER System
The result consists of 3 columns: URL, count and summarized payload, eg.:
nk.pl 9384 13125752
www.facebook.com 8821 61183710
fbcdn-profile-a.akamaihd.net 8693 23069393
photos.nasza-klasa.pl 8258 2990232
fbstatic-a.akamaihd.net 7386 7379509
profile.ak.fbcdn.net 6621 9121091
ui.ff.avast.com 6335 3394081
www.google.pl 5759 25386506
An example of the set of such strings can be:
brightcove-10.fcod.llnwd.net
brightcove-22.fcod.llnwd.net
brightcove-33.fcod.llnwd.net
brightcove-35.fcod.llnwd.net
brightcove-57.fcod.llnwd.net
Some examples of the final patterns are presented below:
brightcove-[10,57].fcod.llnwd.net
media-b[15,48].putlocker.com
proxy-01.dailymotion.com
r[1,14]---fra[02,07]s[3,21].c.youtube.com
Content Servers
Internet
Router
Access Switch
FastEthernet
End Users
Intercept Server
CPU 1 x Xeon 2.4GHz
RAM 16GB
Storage 2 x 1.5TB
DAG card
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure


Introduction
Architecture
Development
Content Servers Discovery
PlanetLab Europe
Internet
DNS Queries
Storage Network 1
Storage Network 2
Storage Network 3
anonymoused URL's patterns
Find Controller
HTTP, DNS Requests
anonymoused URL's patterns
Web Services
SNIFFER database
Content Servers Discovery
Using DNS and PlanetLab servers to convert hostnames to IP addresses
Searches for Aand CNAME records
Exploiting the geographical spread of PlanetLab servers for DNS queries
One URL can be resolved to various IP addresses depending on the origin of the query
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure


Introduction
Architecture
Development
Clustering & Geo-tagging
Content Servers Clustering
Aims at grouping discovered IP addresses according to geographical location (datacenter)
Uses:
Geolocation service (currently MaxMind GeoCity Lite)
Grouping by potential datacenter gateways discovered by traceroute to destination IP address and whois-based aggregation
Cluster
IP 1
IP 2
Common GW
PlanetLab 1
PlanetLab 2
Problems
Tracerouting is time consuming - use caching
Deficiencies of the geotagging database - low accuracy for many addresses
– leads to inaccurate clustering and bad visualization
URLs intercepted from Poland only
– Inadequate coverage of content
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure



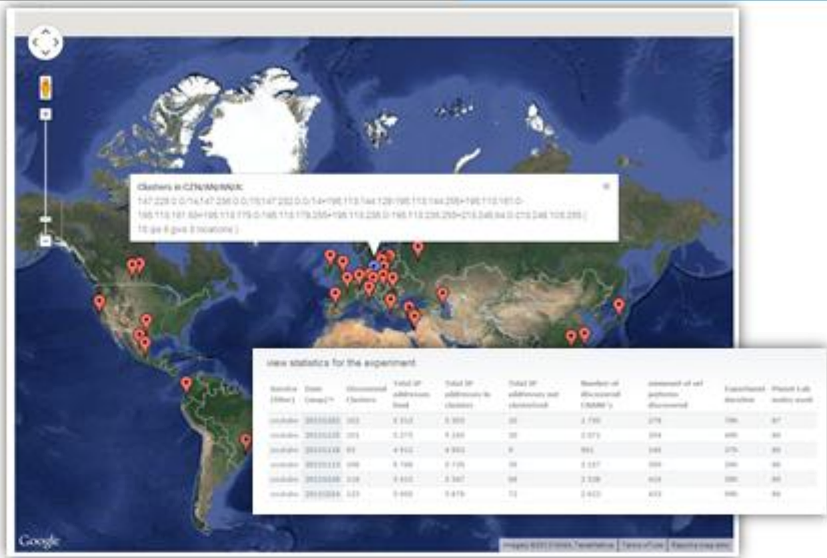
Service (filter)	Date (map)	Clusters (list)	Total IP addresses foud	Total IP addresses in clusters	Total IP addresses not clusterized	Number of discovered CNAME's	ammount of url patterns discovered	Experiment duration	Planet Lab nodes used
akamaihd	20140515	540	10 289	10 219	70	299	328	41h	75
youtube	20140512	101	7 339	7 332	7	1 814	257	42h	75
akamaihd	20140508	558	10 411	10 342	69	336	350	53h	75
youtube	20140505	102	7 251	7 242	9	1 964	262	42h	76
akamaihd	20140501	542	9 198	9 133	65	334	336	39h	76
youtube	20140428	101	7 006	6 995	11	2 090	272	43h	76
akamaihd	20140424	513	8 486	8 425	61	322	320	39h	76
youtube	20140421	96	6 268	6 257	11	1 906	213	45h	76
akamaihd	20140417	585	10 041	9 981	60	273	315	40h	76
youtube	20140414	93	7 138	7 126	12	1 318	172	41h	76
akamaihd	20140410	587	9 853	9 777	76	257	296	40h	76
youtube	20140407	92	7 072	7 059	13	1 298	133	41h	75



Service (filter)	Date (map)	Clusters (list)	Total IP addresses foud	Total IP addresses in clusters	Total IP addresses not clusterized	Number of discovered CNAME's	ammount of url patterns discovered	Experiment duration	Planet Lab nodes used
youtube	20140512	101	7 339	7 332	7	1 814	257	42h	75

Introduction
Architecture
Development

Web page
YouTube example



A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs

Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure

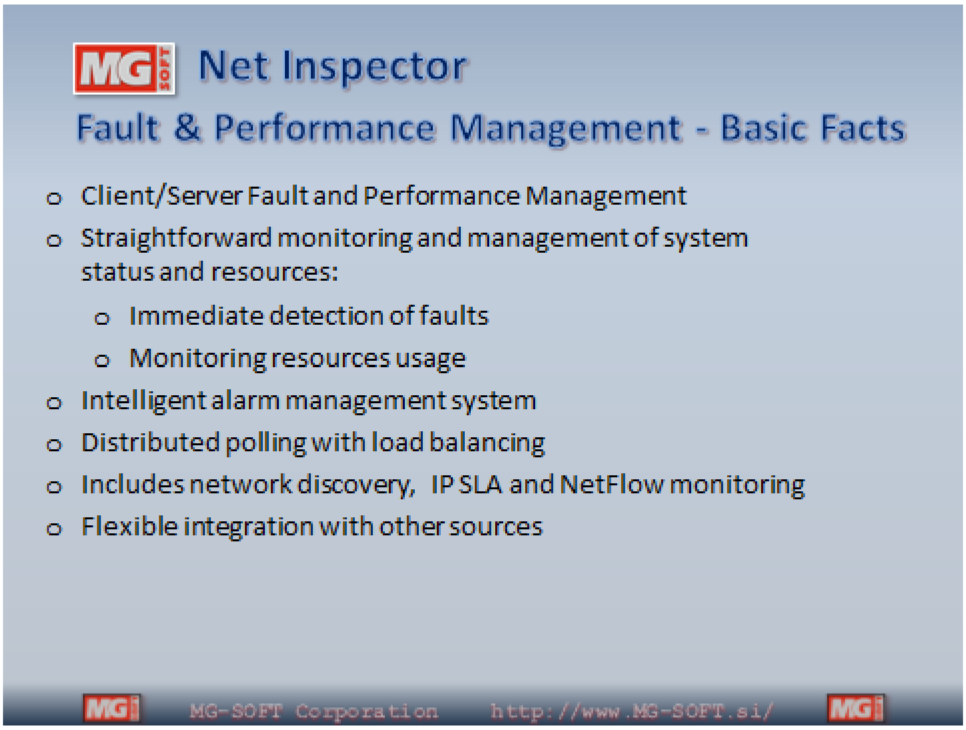
Demo

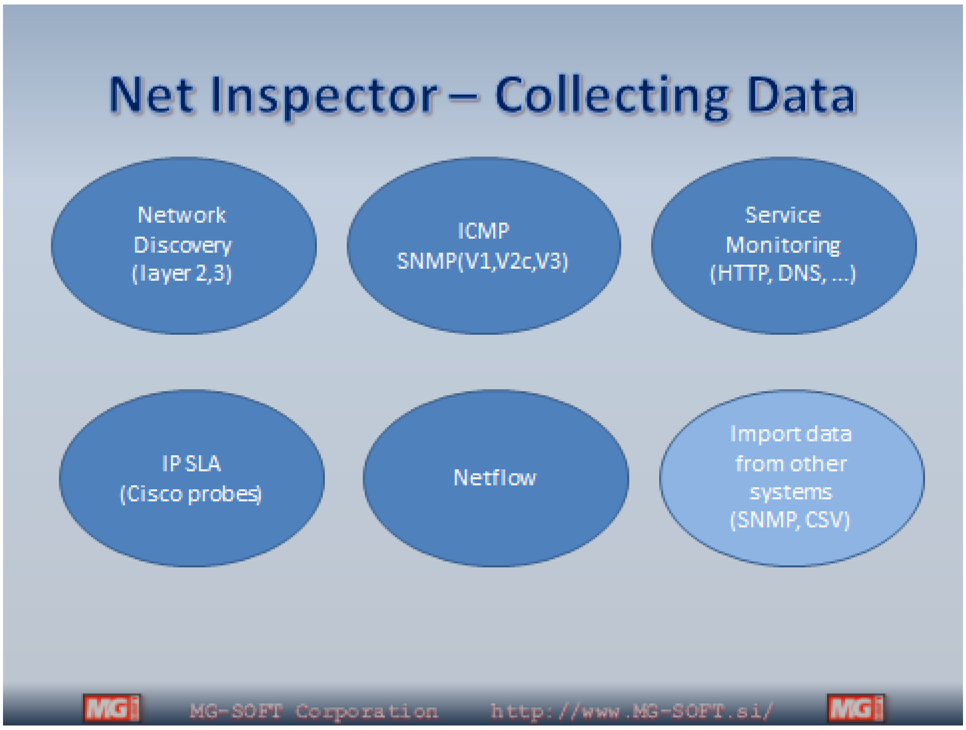
http://sniffer.mini.pw.edu.pl

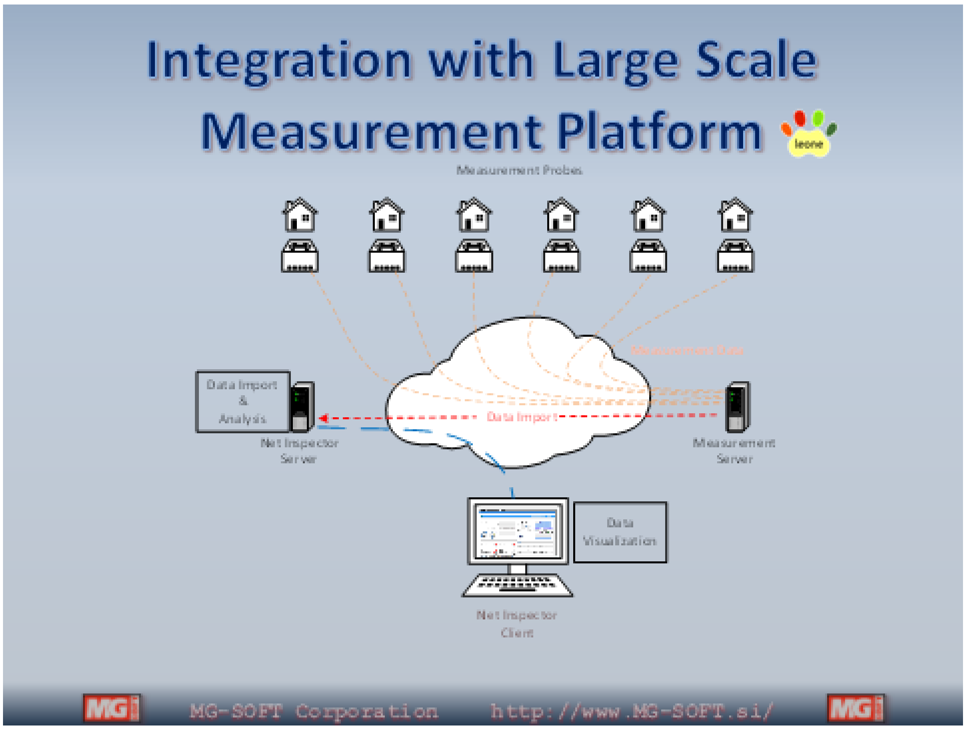
A. Bąk , P. Gajowniczek, M. Pilarski, M. Borkowski - Politechnika Warszawska
P. Grochocki - Orange Labs

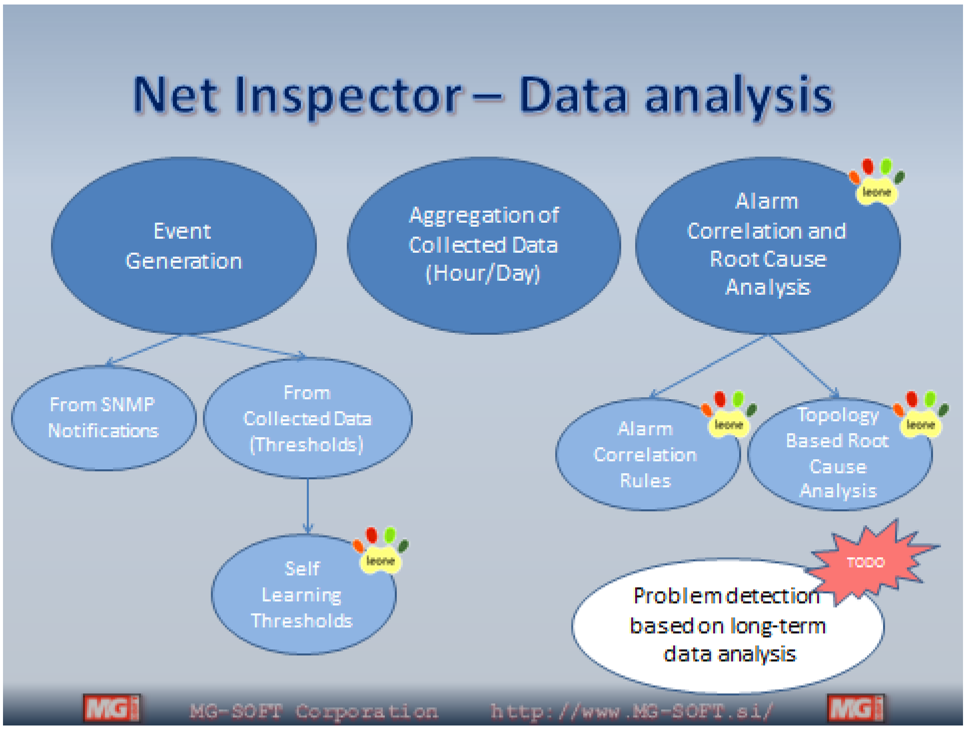
Project SNIFFER: Content Server Discovery Based on PlanetLab Infrastructure

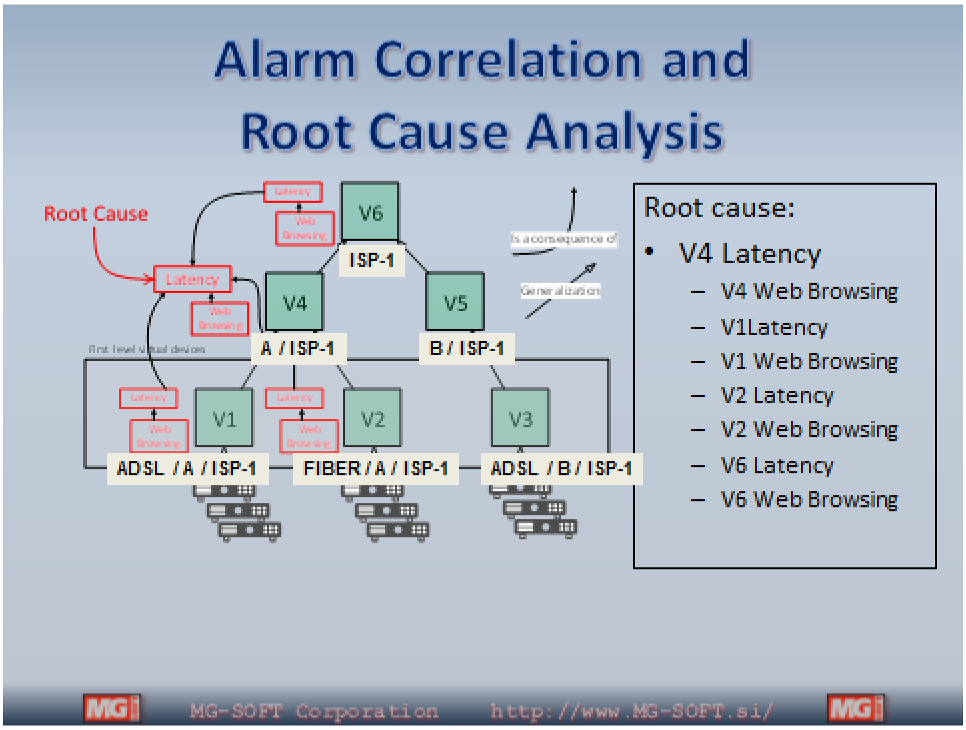
1.2 Dr. Boris Banjanin

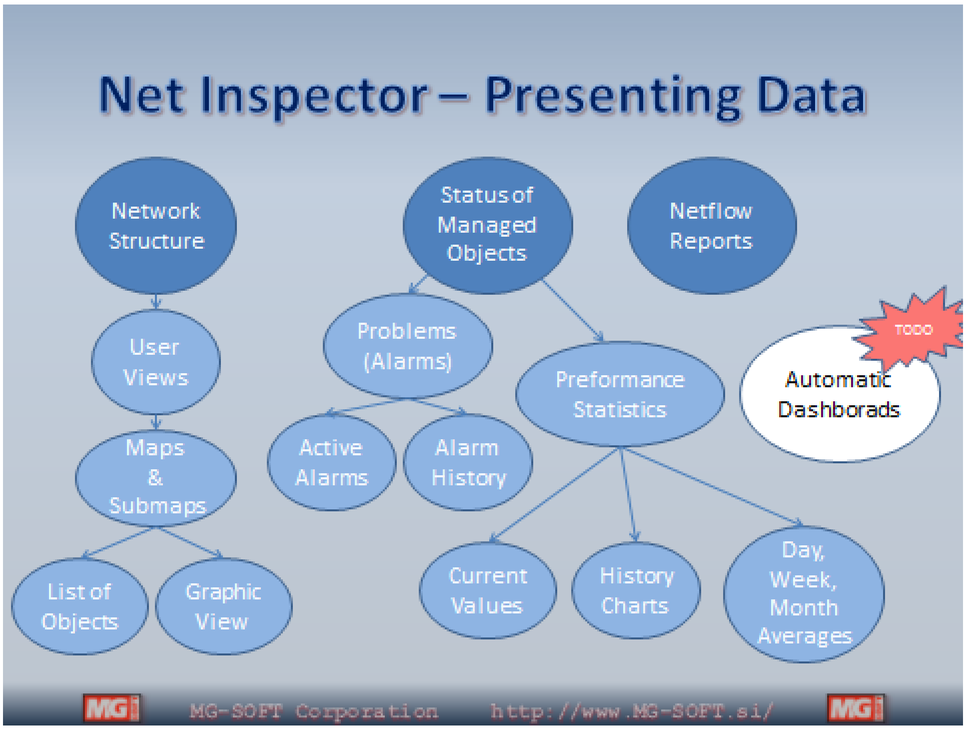


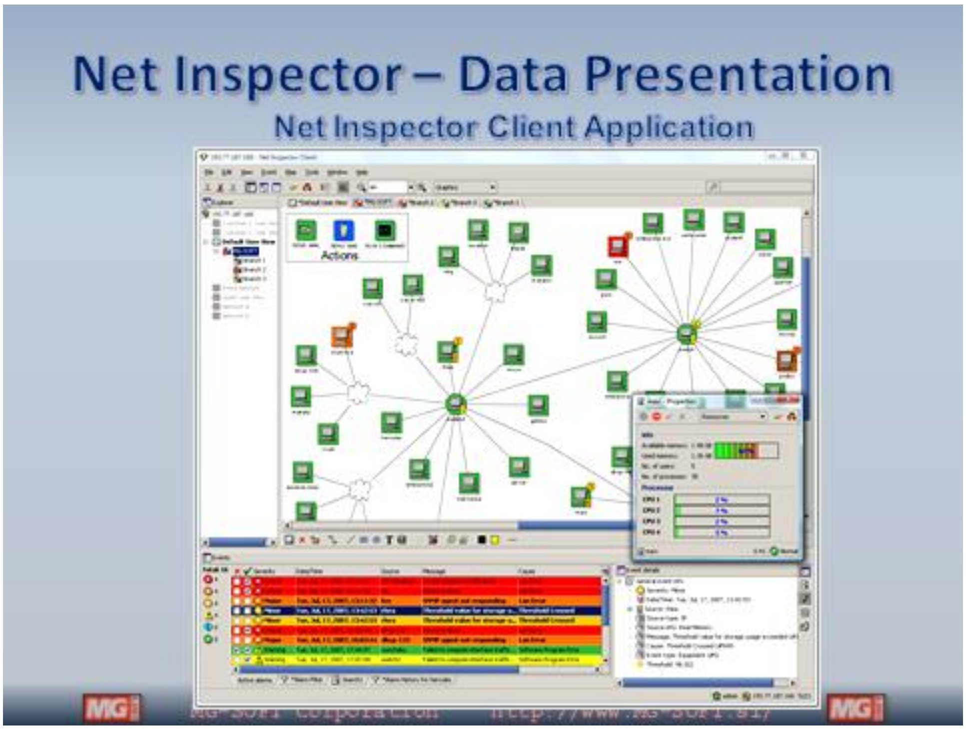

Net Inspector – Collecting Data
Network Discovery (layer 2,3)
ICMP SNMP(V1,V2c,V3)
Service Monitoring (HTTP, DNS, ...)
IP SLA (Cisco probes)
Netflow
Import data from other systems (SNMP, CSV)
MG-SOFT Corporation
http://www.MG-SOFT.si/

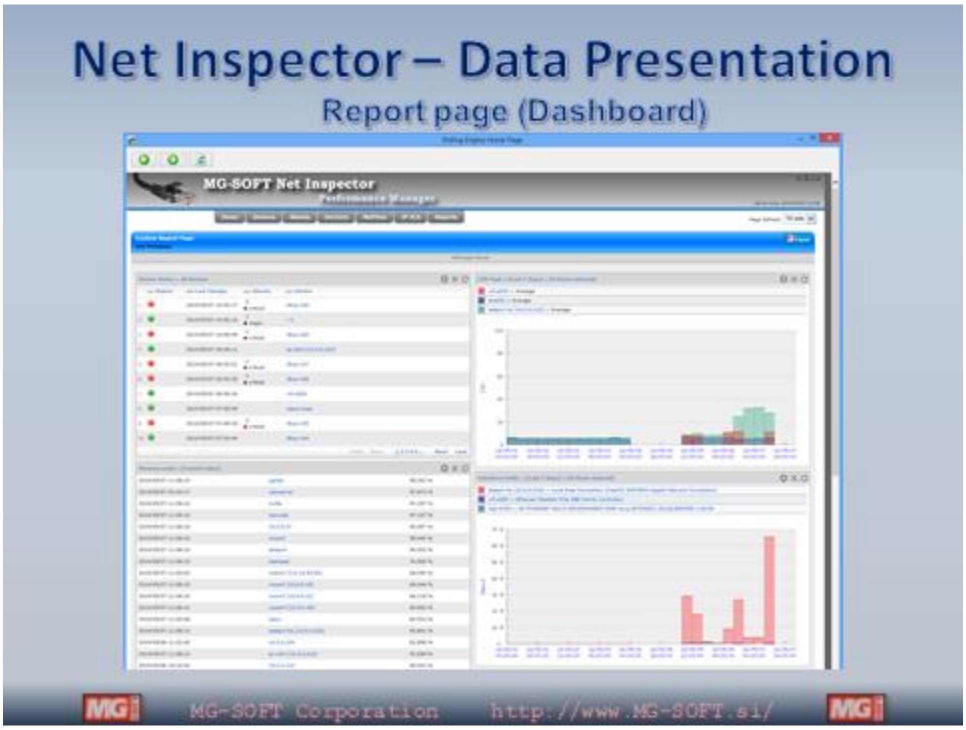

Integration with Large Scale Measurement Platform
leone
Measurement Probes
Measurement Data
Data Import & Analysis
Net Inspector Server
Data Import
Measurement Server
Data Visualization
Net Inspector Client
MG-SOFT Corporation
http://www.MG-SOFT.si/

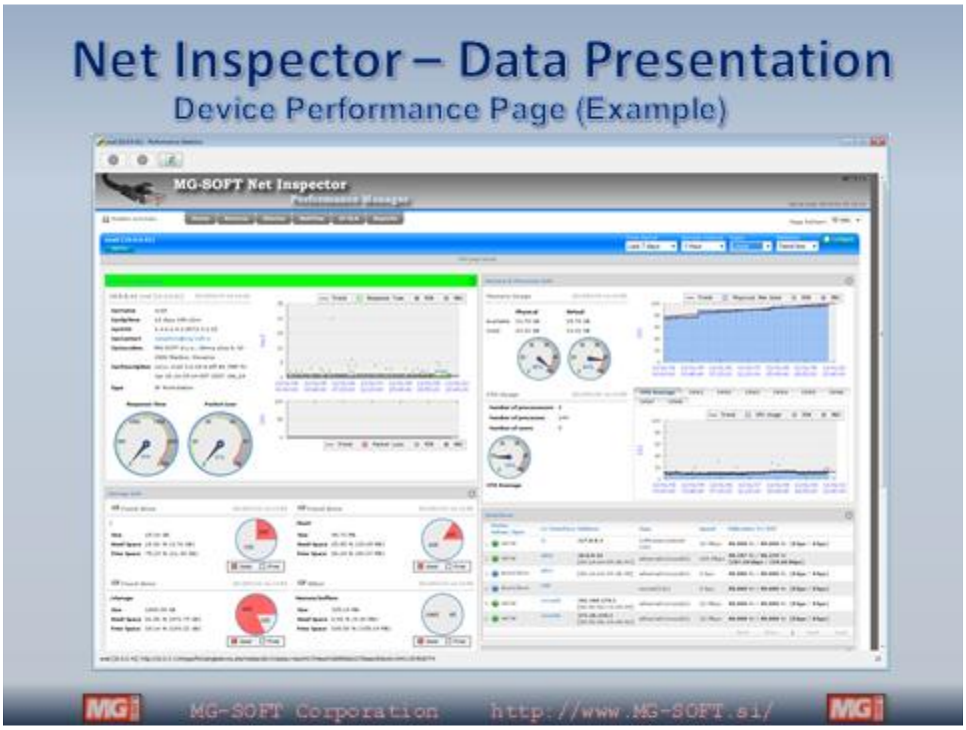

Net Inspector – Data analysis
Event Generation
Aggregation of Collected Data (Hour/Day)
Alarm Correlation and Root Cause Analysis
From SNMP Notifications
From Collected Data (Thresholds)
Self Learning Thresholds
Alarm Correlation Rules
Topology Based Root Cause Analysis
TODO
Problem detection based on long-term data analysis
MG-SOFT Corporation
http://www.MG-SOFT.si/


Alarm Correlation and Root Cause Analysis
Root Cause
Latency
V6
ISP-1
V4
V5
A / ISP-1
B / ISP-1
V1
V2
V3
ADSL / A / ISP-1
FIBER / A / ISP-1
ADSL / B / ISP-1
Root cause:
• V4 Latency
– V4 Web Browsing
– V1Latency
– V1 Web Browsing
– V2 Latency
– V2 Web Browsing
– V6 Latency
– V6 Web Browsing
MG-SOFT Corporation
http://www.MG-SOFT.si/

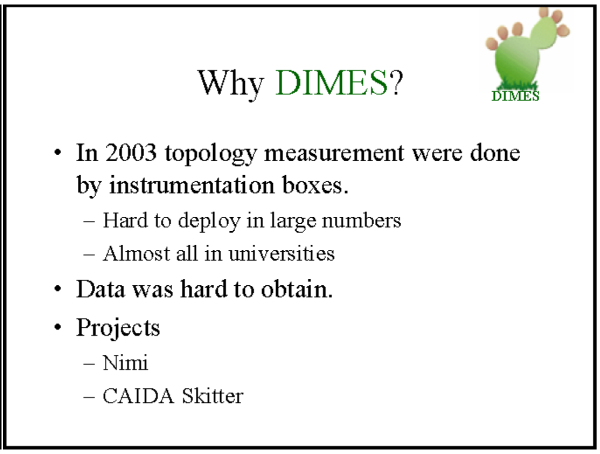

Net Inspector – Presenting Data
Network Structure
Status of Managed Objects
Netflow Reports
User Views
Problems (Alarms)
Preformance Statistics
TODO
Automatic Dashborads
Maps & Submaps
Active Alarms
Alarm History
List of Objects
Graphic View
Current Values
History Charts
Day, Week, Month Averages
MG-SOFT Corporation
http://www.MG-SOFT.si/

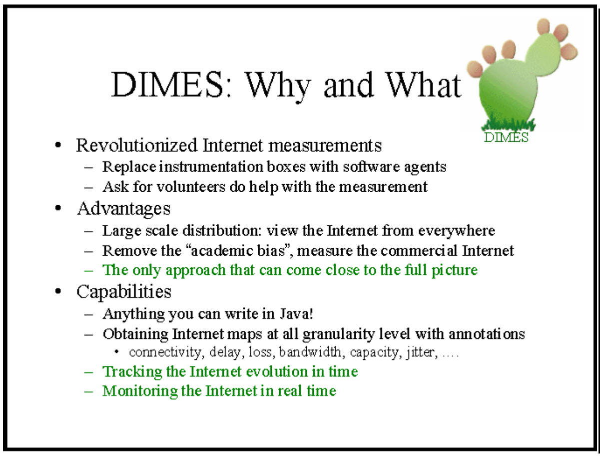

Net Inspector – Data Presentation
Net Inspector Client Application

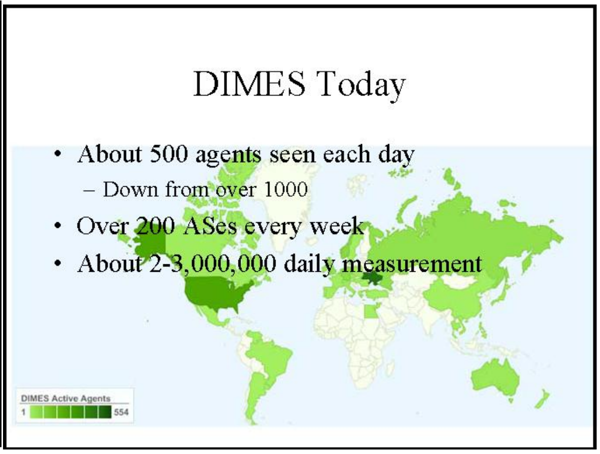

Net Inspector – Data Presentation
Report page (Dashboard)
MG-SOFT Net Inspector
MG-SOFT Corporation http://www.MG-SOFT.si/

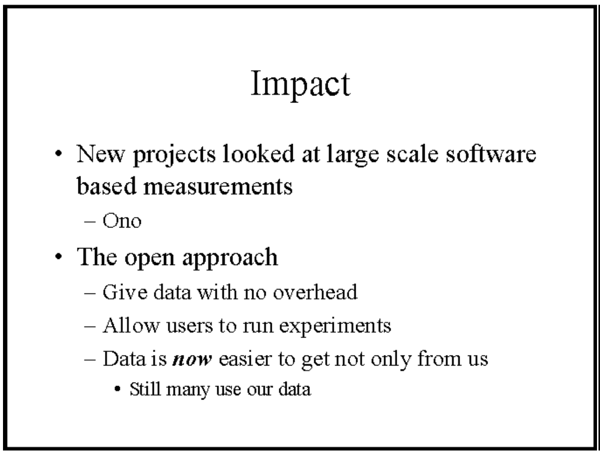

Net Inspector – Data Presentation
Device Performance Page (Example)
MG-SOFT Net Inspector
MG-SOFT Corporation http://www.MG-SOFT.si/

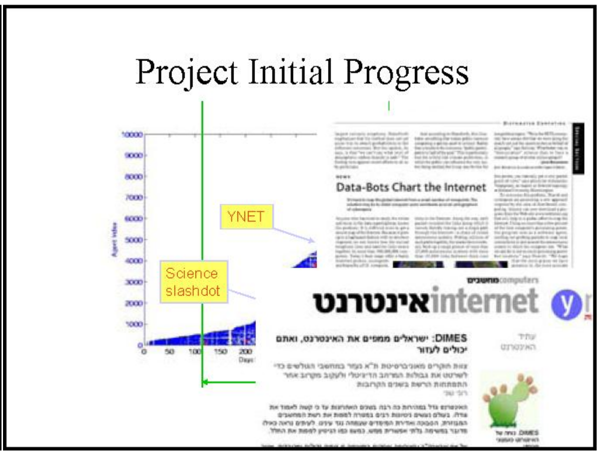
1.3 Prof. Yuval Shavitt

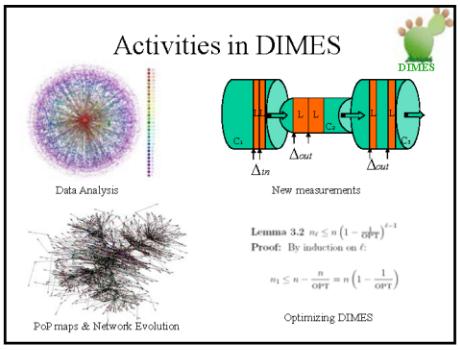


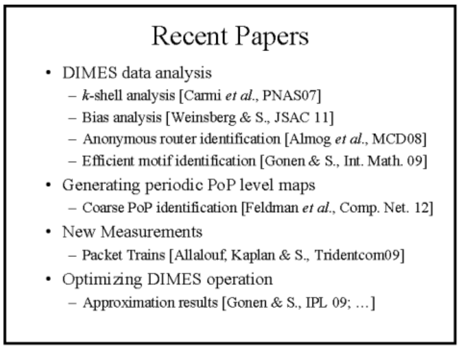


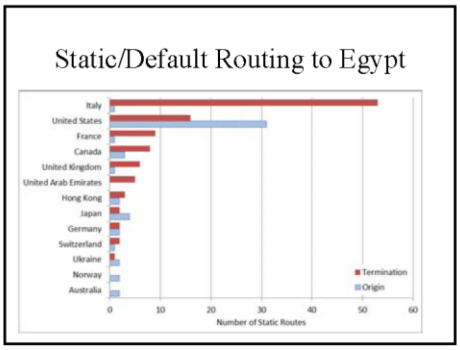


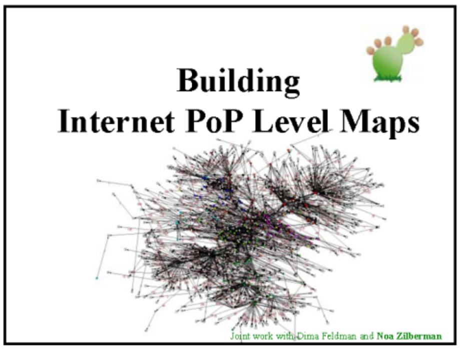


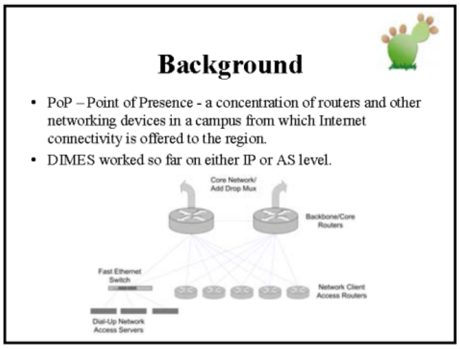


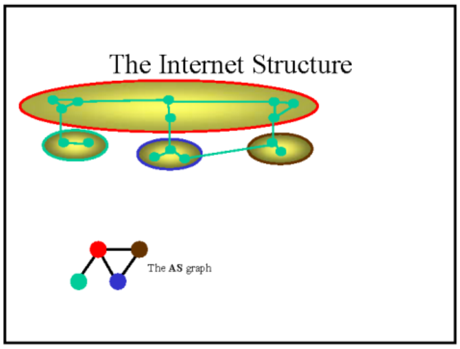

Activities in DIMES
DIMES
Data Analysis
New measurements
PoP maps & Network Evolution
Optimizing DIMES


Recent Papers
• DIMES data analysis
– k-shell analysis [Carmi et al., PNAS07]
– Bias analysis [Weinsberg & S., JSAC 11]
– Anonymous router identification [Almog et al., MCD08]
– Efficient motif identification [Gonen & S., Int. Math. 09]
• Generating periodic PoP level maps
– Coarse PoP identification [Feldman et al., Comp. Net. 12]
• New Measurements
– Packet Trains [Allalouf, Kaplan & S., Tridentcom09]
• Optimizing DIMES operation
– Approximation results [Gonen & S., IPL 09; …]

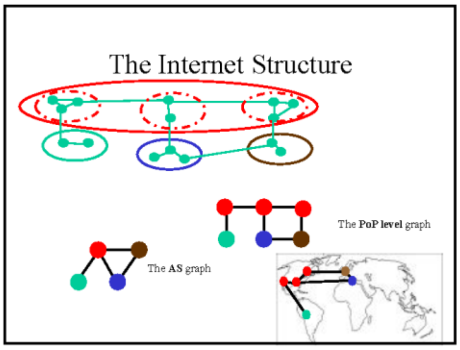

Static/Default Routing to Egypt
Italy
United States
France
Canada
United Kingdom
United Arab Emirates
Hong Kong
Japan
Germany
Switzerland
Ukraine
Norway
Australia
Termination
Origin
0
10
20
30
40
50
60
Number of Static Routes

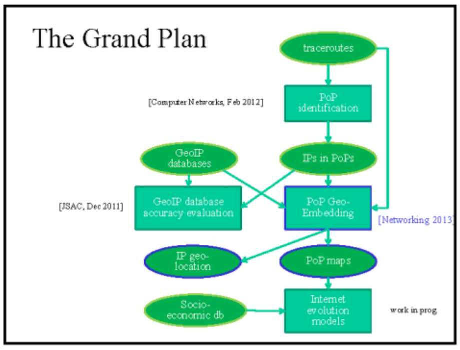

Building
Internet PoP Level Maps
Joint work with Dima Feldman and Noa Zilberman

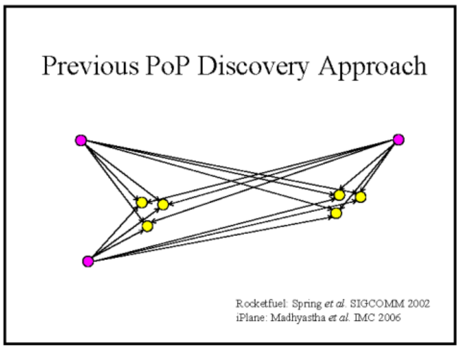

Background
• PoP – Point of Presence - a concentration of routers and other networking devices in a campus from which Internet connectivity is offered to the region.
• DIMES worked so far on either IP or AS level.

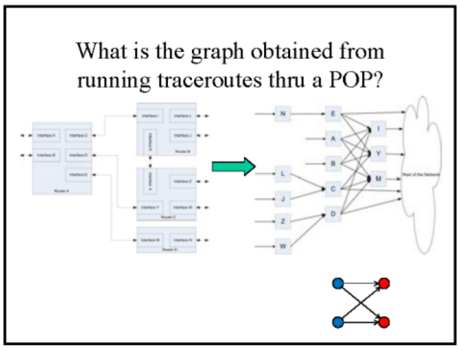

The Internet Structure
The AS graph

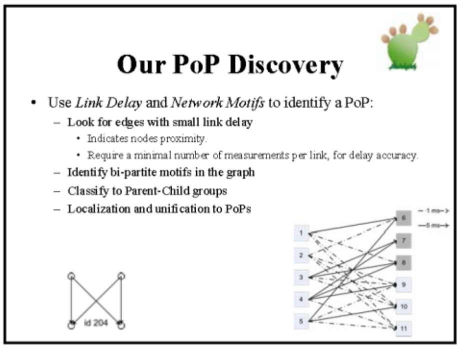
2

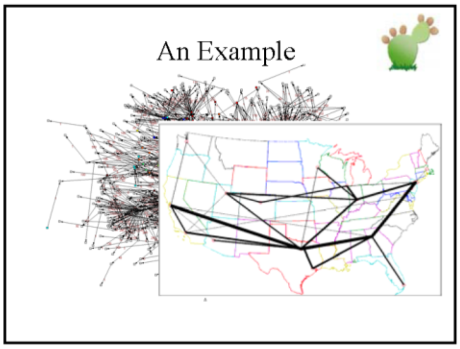

The Internet Structure
The PoP level graph
The AS graph


The Grand Plan
traceroutes
[Computer Networks, Feb 2012]
PoP identification
GeoIP databases
IPs in PoPs
[JSAC, Dec 2011]
GeoIP database accuracy evaluation
PoP Geo-Embedding
[Networking 2013]
IP geo-location
PoP maps
Socio-economic db
Internet evolution models
work in prog

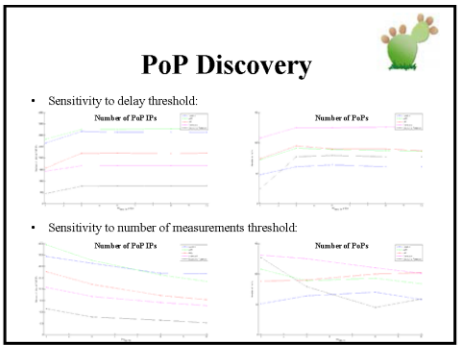

Previous PoP Discovery Approach
Rocketfuel: Spring et al. SIGCOMM 2002
iPlane: Madhyastha et al. IMC 2006

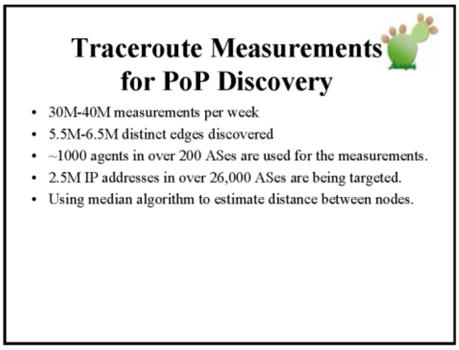

What is the graph obtained from running traceroutes thru a POP?

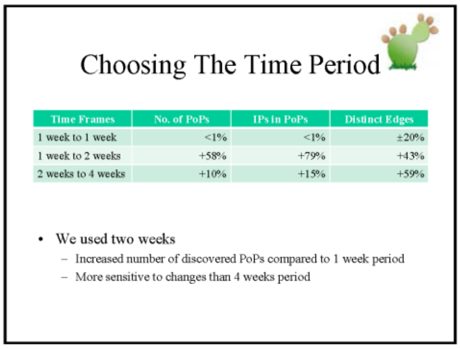

Our PoP Discovery
Use Link Delay and Network Motifs to identify a PoP:
Look for edges with small link delay
Indicates nodes proximity.
Require a minimal number of measurements per link, for delay accuracy.
Identify bi-partite motifs in the graph
Classify to Parent-Child groups
Localization and unification to PoPs
id 204
1 ms
5 ms


An Example

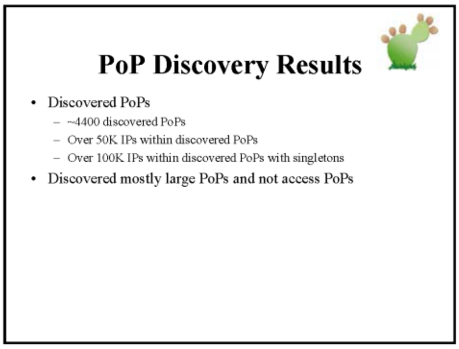
3

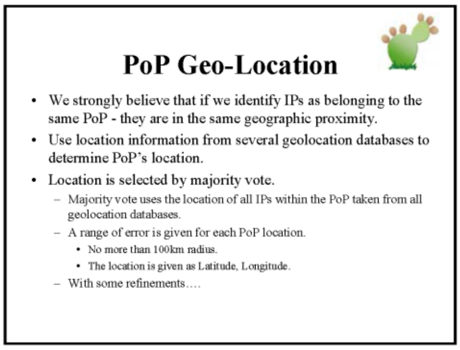


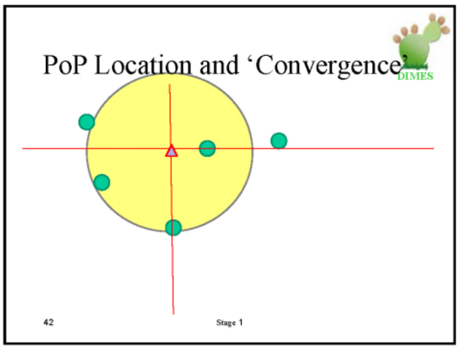




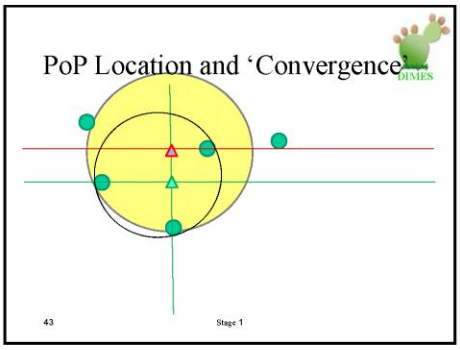
Time Frames	No. of PoPs	IPs in PoPs	Distinct Edges
1 week to 1 week	<1%	<1%	±20%
1 week to 2 weeks	+58%	+79%	+43%
2 weeks to 4 weeks	+10%	+15%	+59%



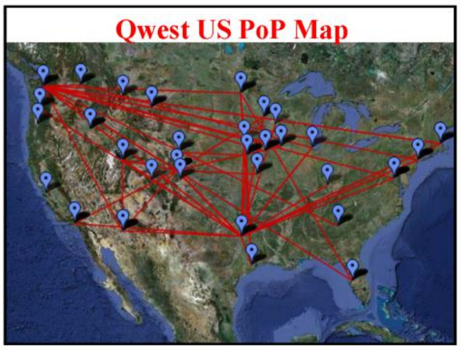


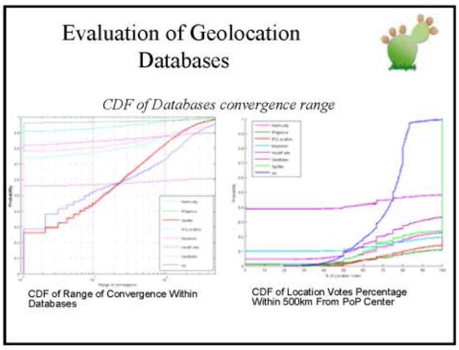


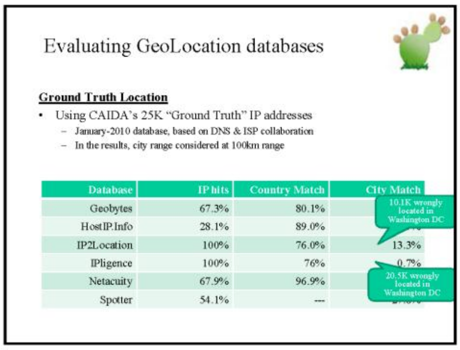
4

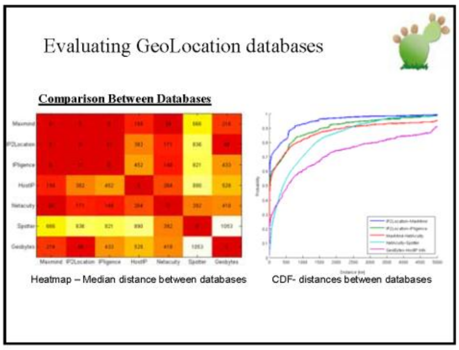

PoP Location and 'Convergence'
DIMES
43
Stage 1


World PoP Map


Qwest US PoP Map


Evaluation of Geolocation Databases
CDF of Databases convergence range
CDF of Range of Convergence Within Databases
CDF of Location Votes Percentage Within 500km From PoP Center


Evaluating GeoLocation databases
Ground Truth Location
• Using CAIDA's 25K "Ground Truth" IP addresses
– January-2010 database, based on DNS & ISP collaboration
– In the results, city range considered at 100km range
Database | IP hits | Country Match | City Match
Geobytes | 67.3% | 80.1% |
HostIP.Info | 28.1% | 89.0% |
IP2Location | 100% | 76.0% | 13.3%
IPligence | 100% | 76% | 0.7%
Netacuity | 67.9% | 96.9% |
Spotter | 54.1% | --- |
10.1K wrongly located in Washington DC
20.5K wrongly located in Washington DC


Evaluating GeoLocation databases
Comparison Between Databases
Heatmap – Median distance between databases
CDF- distances between databases

5

Evaluating GeoLocation databases

Database Anomalies - Disagreement Between Databases

Verizon/MCI/UUNET (ASN 703)
10-nodes PoP (w/Singletons)

Evaluating GeoLocation databases

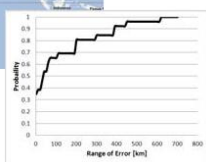
Database Anomalies - Disagreement Between Databases

Global Crossing (ASN 3549)
160-nodes PoP (w/Singletons)

Improved Geo-Location

- Many PoPs are placed in the correct location.
- How to improve the others?
- Use the connectivity between PoPs

Example Result: Telefonica Network



Testing Performance: Anchors

Crawling Stage	Number of PoPs	Same Place	Within 100km	Within 500km	Beyond 500km
Co-Location	124	100%	0%	0%	0%
Delay and Geo-Data	19	16%	47%	16%	21%
Delay Only	37	54%	0%	25%	21%
Total	180	82%	5%	7%	6%

- Attempt to locate each of the 180 anchors using the other 179.
  - 82-87% success
  - 100% success using co-locati

Crawling Algorithm Stage	Relocated PoPs 2010	Relocated PoPs 2012
Anchors	17.9%	29.3%
Co-Location	28.3%	20.1%
Delay and Geolocation Data	21.3%	13%
Delay Only	7.6%	6.1%
Not Relocated	24.8%	31.5%

Applications

- Measure cellular network performance
- Measure the routing infrastructure
  - Security applications
  - performance

6

1.4 Dr. Arjuna Sathiaseelan

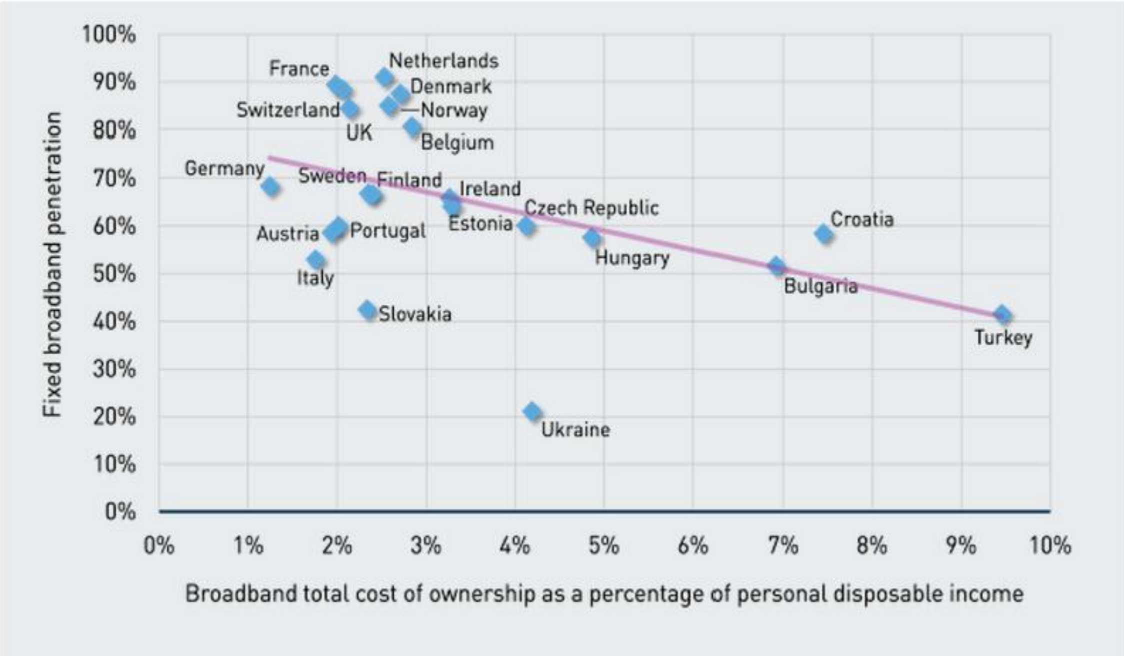
Public Access WiFi Service (PAWS)

Arjuna Sathiaseelan
Computer Laboratory

SMART Internet Measurement Study Workshop
20 May 2014

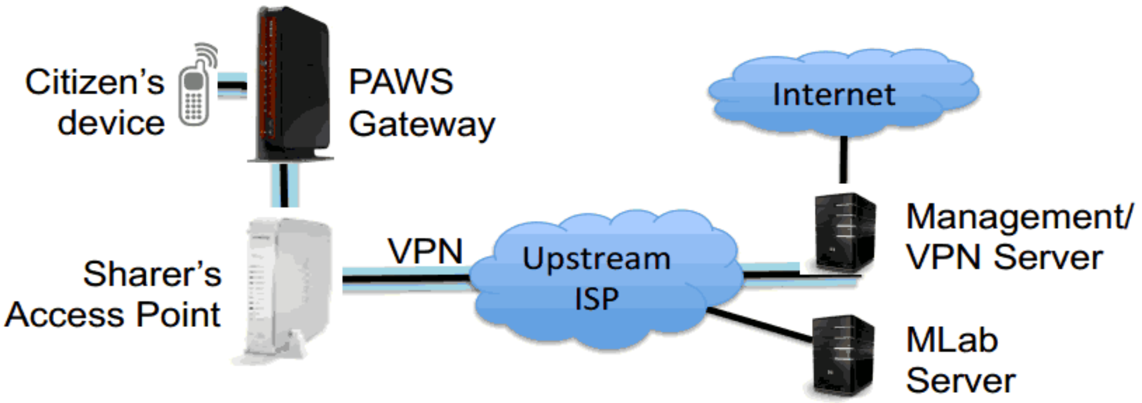
UNIVERSITY OF CAMBRIDGE

Digital divide and affordability



(Source: Analysys Mason, 2013)

Public Access WiFi Service (PAWS)



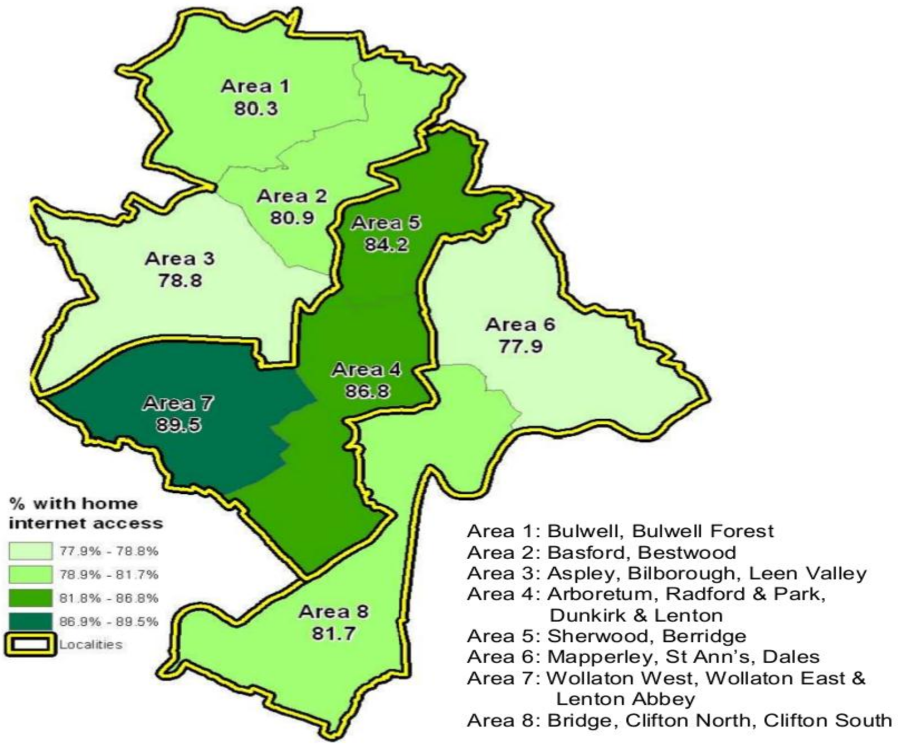
Funded by the RCUK- Cambridge (Lead), Nottingham, BT, SamKnows, BISMark, Nottingham City Council

Deployments in Nottingham, broadband performance measurements, sharing experiments and understanding PAWS usage characteristics

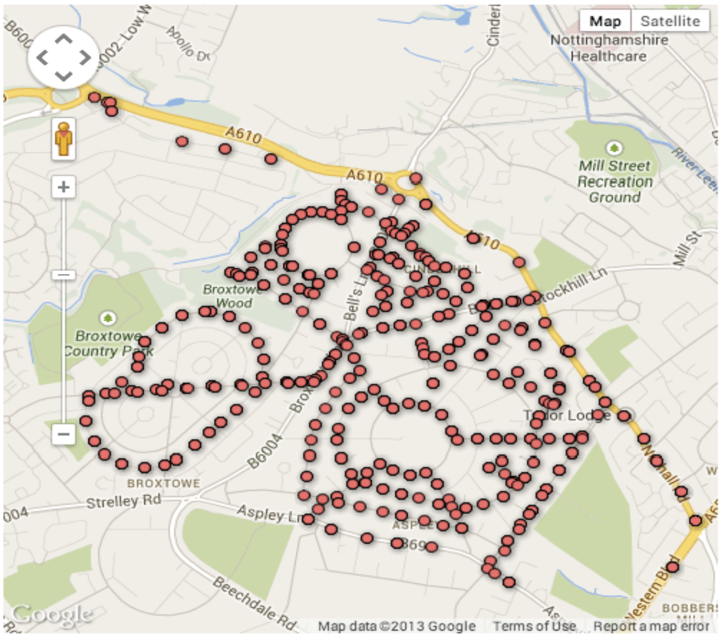
Enabling Less than Best Effort (LBE) access

- WiFi access points : lack of QoS (both upstream and wireless)
- DSLAM/MSAN: Need L2 QoS differentiation
- PAWS: We throttle at 2Mbps downstream/512Kbps upstream

Digital Divide: Nottingham



Wardrive around Aspley



Total unique SSID = 1067

Provider	Percentage
SKY	23%
Virgin	21%
BT	23%
FON	61% of BT
Unspecified	33%

of PAWS routers

ISP	Total	Measured
SKY	6	5
Virgin	10	8
Orange	1	1
TalkTalk	1	1
Tiscali/PIPEX	1	0
Griffin	1	0

20 PAWS routers deployed between July-mid November

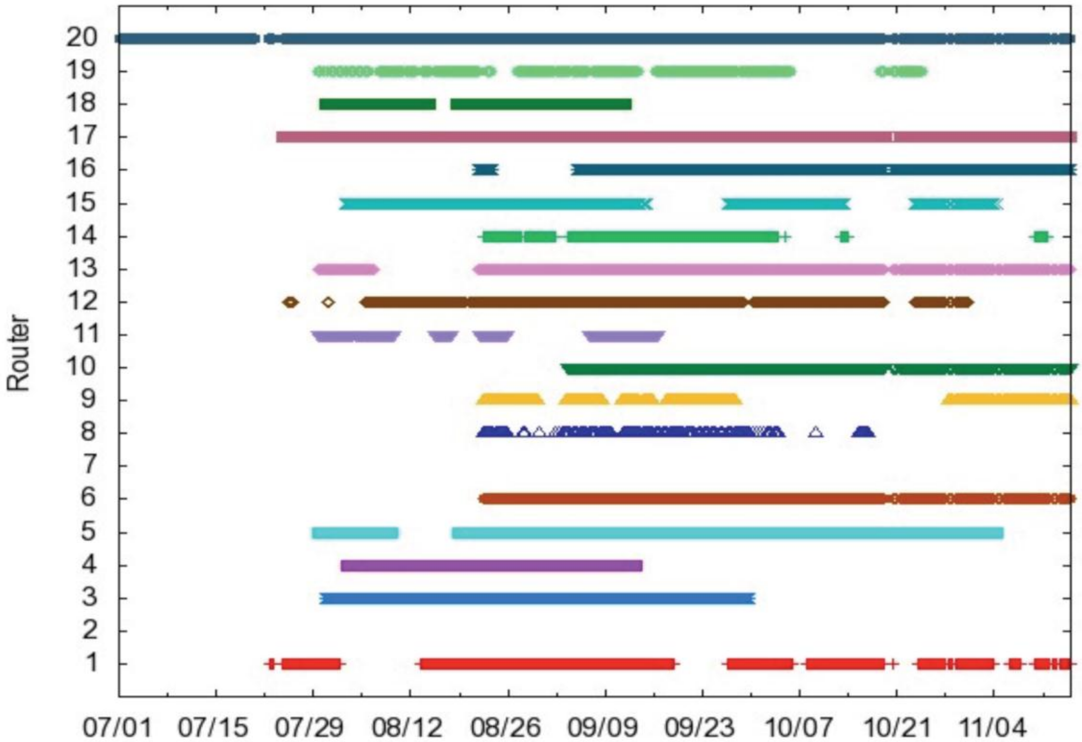
8 were used by 15 citizens: one was deployed in a public space

Remaining 12 served as measurement points

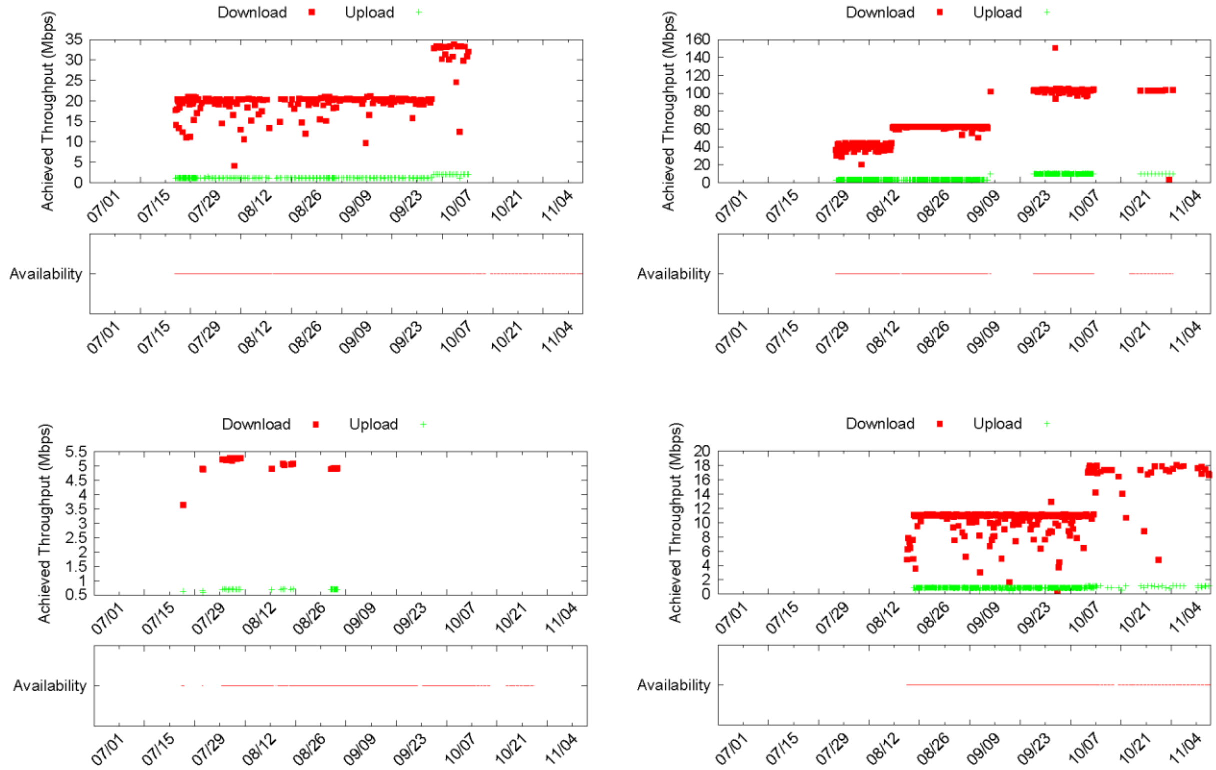
Measurement Metrics

Metric	Method	Frequency
Availability	UDP Probe (60 B)	Every min
Throughput	NETPERF (3 Parallel TCP)	6 hours
Last Mile Latency	Traceroute/Ping to first non-NATed IP	Every 10 mins
E2E RTT	Ping to different servers	Every 10 mins
Loss	D-ITG	Every 15 mins

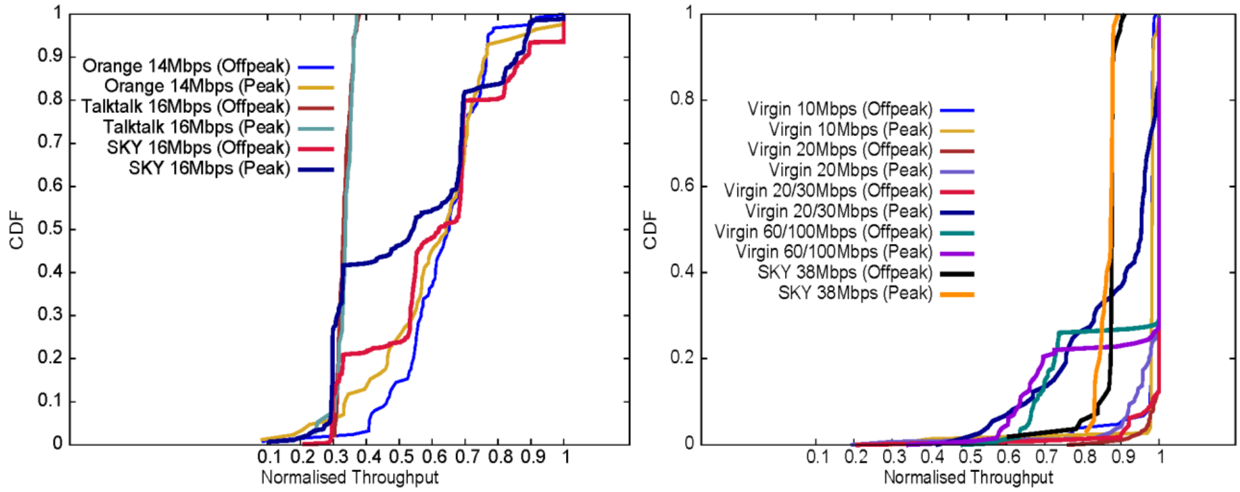
Availability



Broadband Performance



Broadband Performance (download)



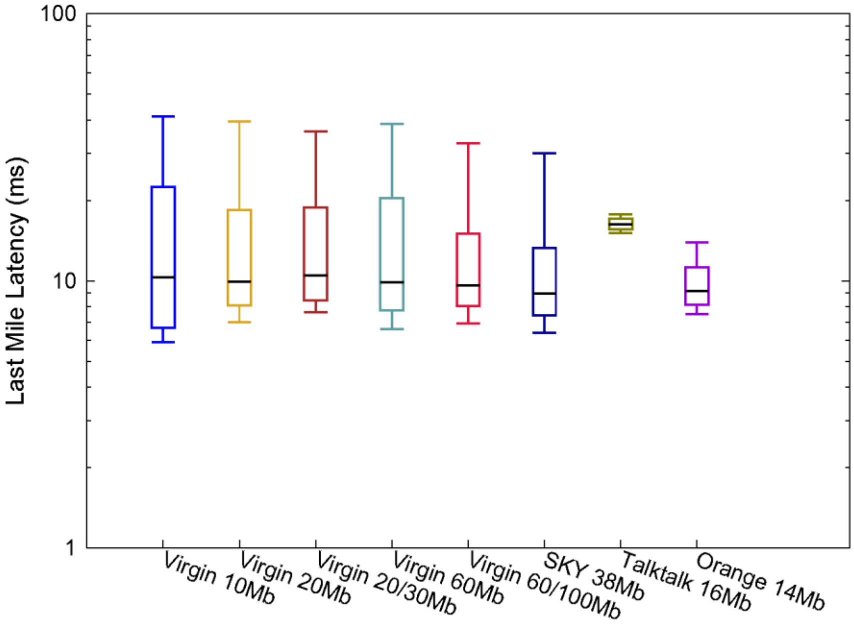
Fiber has sufficient capacity to share 2Mbps

Broadband Performance (upload)

ISP	Min (Mbps)	Max (Mbps)	Average (Mbps)
Virgin 10	0.33	1.00	0.68
Virgin 20	1.01	1.18	1.12
Virgin 20/30	1.05	2.01	1.23
Virgin 60	2.45	3.00	2.94
Virgin 60/100	2.5	9.95	5.15
SKY 38	1.05	2.33	1.97
SKY 16	0.47	1.31	0.91
TalkTalk 16	0.72	0.90	0.87
Orange 14	0.03	1.31	0.60

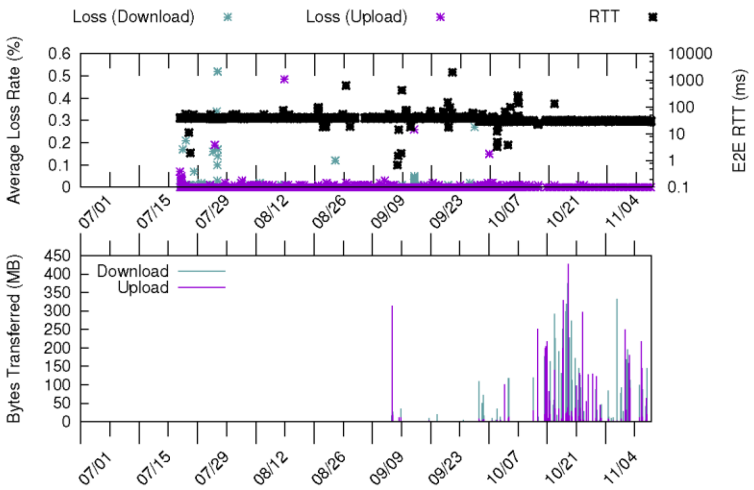
Sharing 512 Kbps on upload needs AQM/QoS on home routers/BRAS

Last Mile Latency and Loss



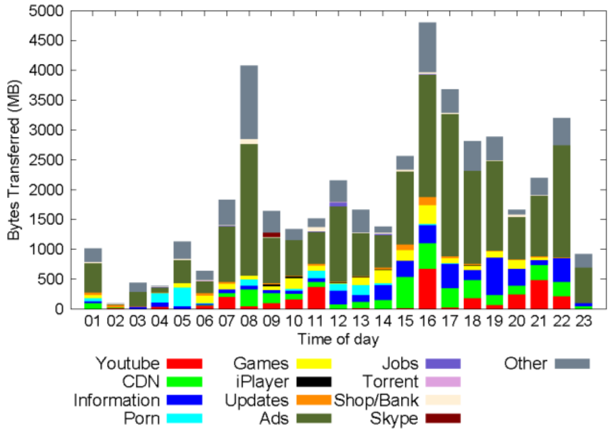
Loss was negligible <0.07%

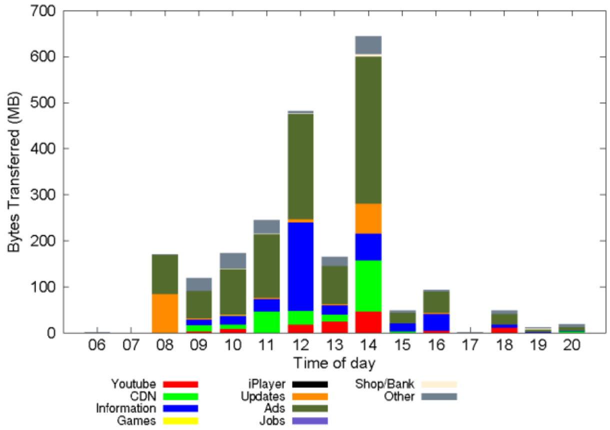
Effect of Primary Citizen Usage on Sharer



Sharer was on a 20/30 Mbps fFiber link
Throttling was sufficient

Citizen Usage





Category	%
Ads	60
Youtube	8
Games	5
Legitimate Uses	4
Porn	3
Updates	2
Other/CDN	18

Conclusions

Lessons Learnt

Deprived urban areas have network infrastructure with good capacity

Fibre networks ideal candidates for network sharing

ADSL is common - need better QoS to support

Ads are a main driver of traffic

Issues

How do we measure unused capacity?

One serious issue: Usage caps and measurements!

1.5 Dr. Walter deDonato

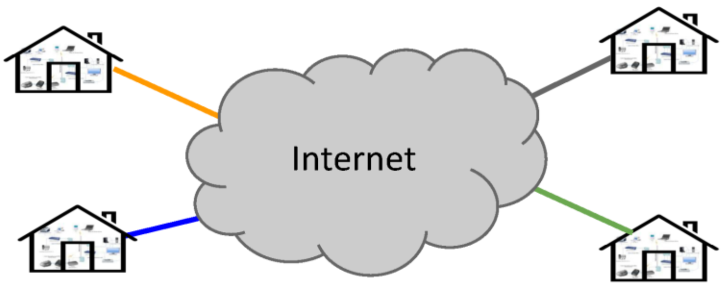
Distributed platforms for measuring and monitoring broadband access networks

Walter de Donato, Alessio Botta, Antonio Pescapé
University of Napoli Federico II, Italy

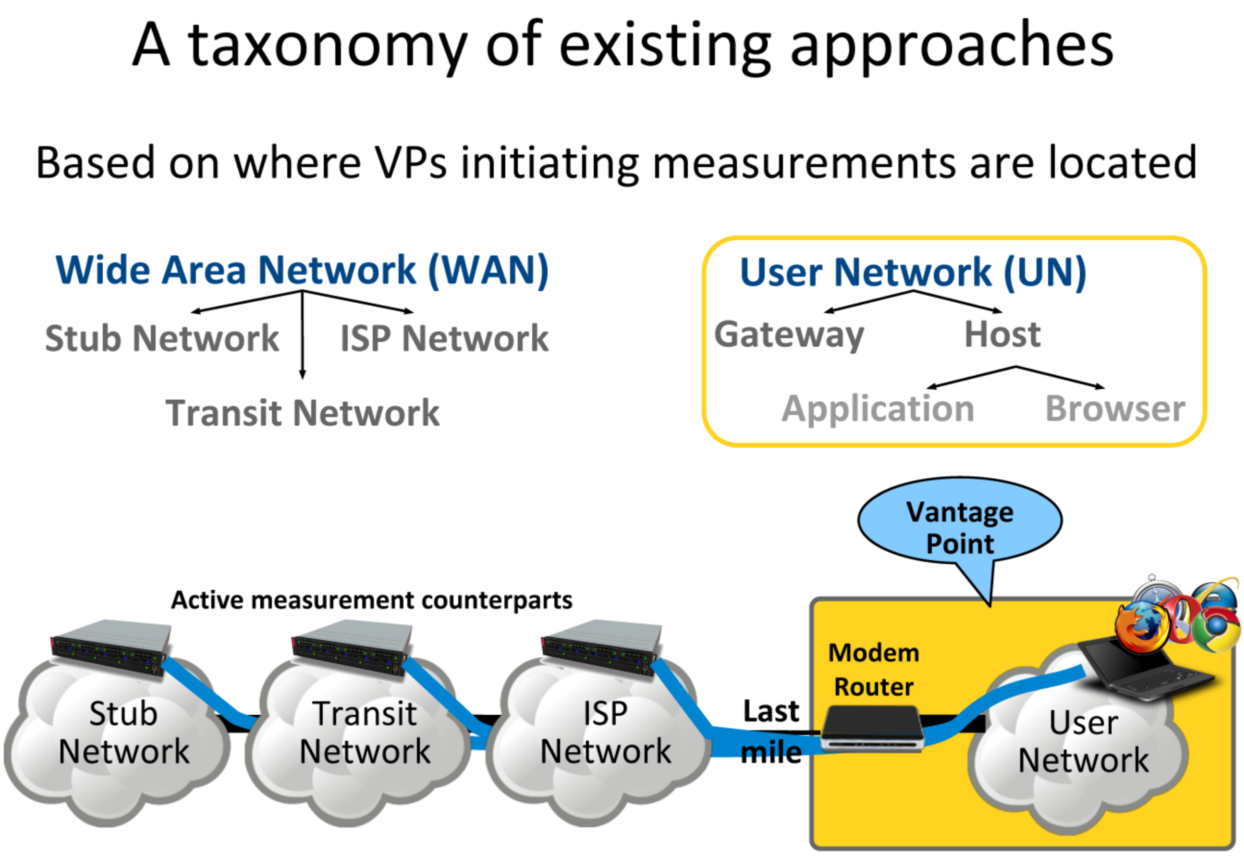
Srikanth Sundaresan, Sam Burnett, Nick Feamster
Georgia Institute of Technology, GA, USA

Introduction

Large scale measurement platforms are necessary for studying residential Internet access networks



- ➔ Several approaches and platforms have been adopted
- ➔ Standardization effort is ongoing while deployed platforms are not interoperable yet


A taxonomy of existing approaches
Based on where VPs initiating measurements are located
Wide Area Network (WAN)
Stub Network
ISP Network
Transit Network
User Network (UN)
Gateway
Host
Application
Browser
Vantage Point
Active measurement counterparts
Stub Network
Transit Network
ISP Network
Last mile
Modem Router
User Network

UN-based platform requirements

Optimal operating conditions

VPs should cover most geographic areas, ISPs, and service plans

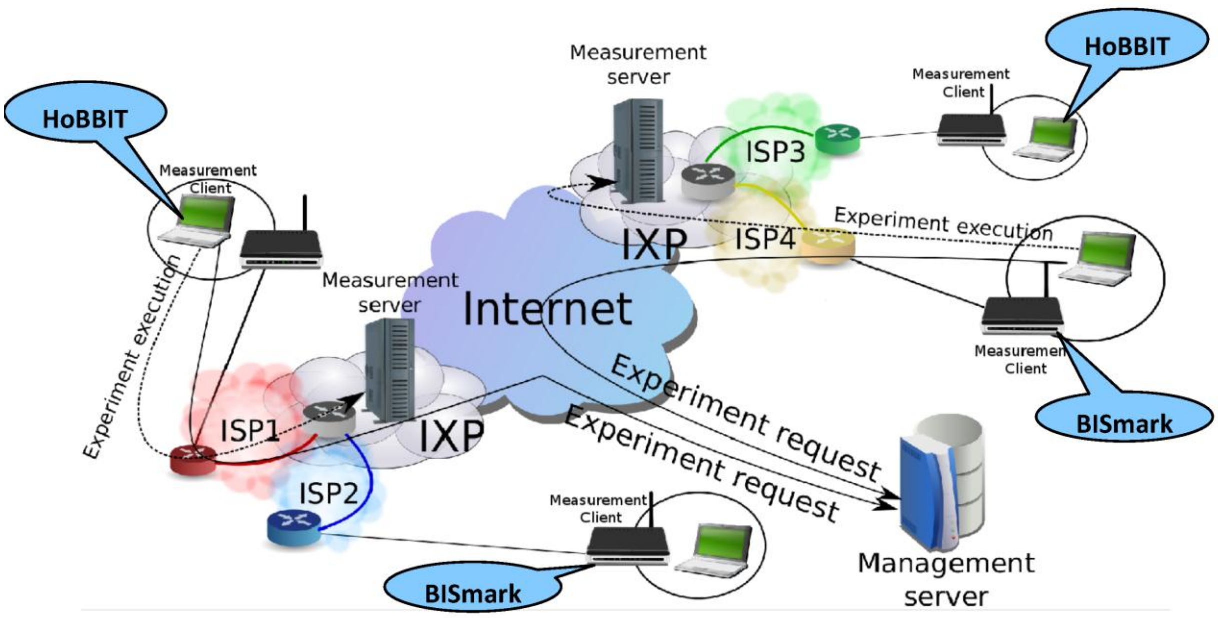
Enough measurement servers should be available at the shortest network distance to most VPs

Functional requirements

Two complementary platforms - One architecture

BISmark (Gateway-based) http://projectbismark.net

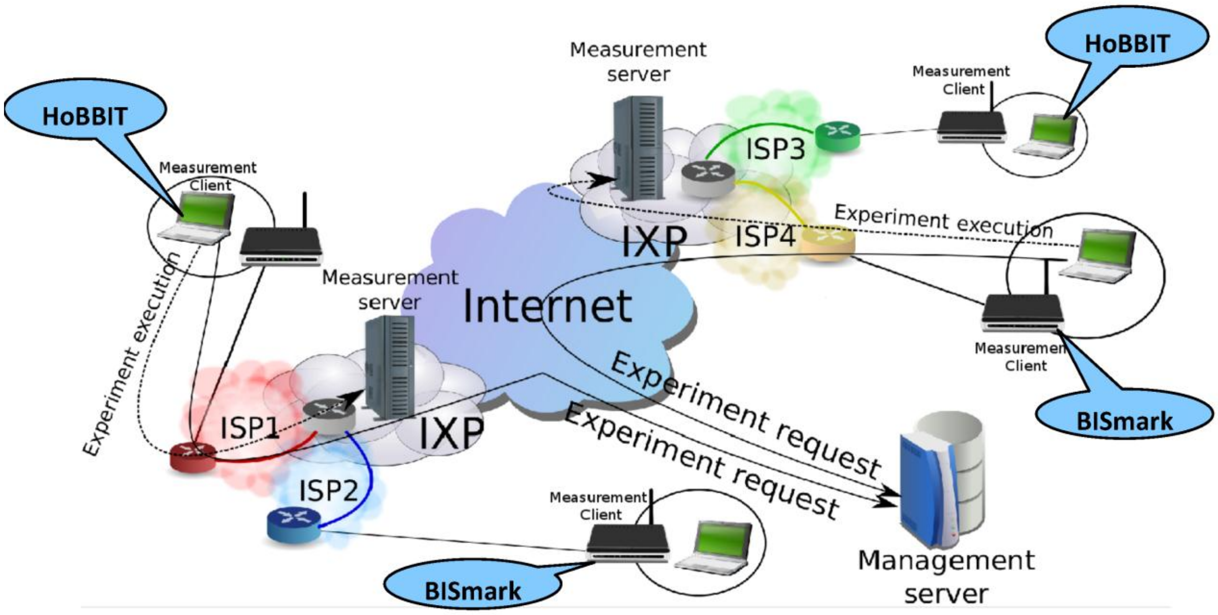
HoBBIT (Application-based) http://hobbit.comics.unina.it



Two complementary platforms - One architecture

BISmark (Gateway-based) http://projectbismark.net

HoBBIT (Application-based) http://hobbit.comics.unina.it



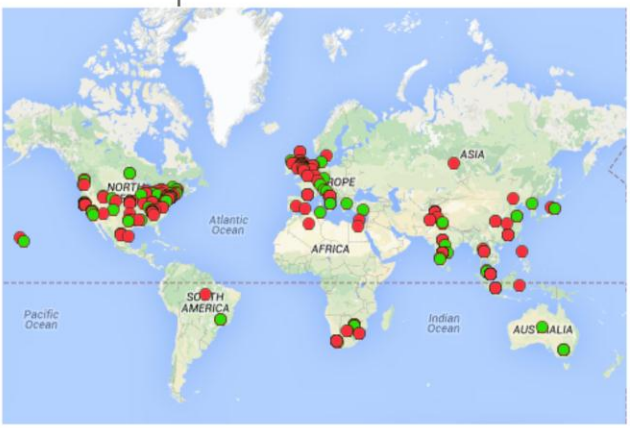
Specific features

BISmark (Gateway-based) ≠ **HoBBIT** (Application-based)

Customized OS (OpenWRT-based)	Multiplatform client based on Qt libraries and bash/awk ports
Remote access to router console for troubleshooting	Identification of connection ISP and service plan details
Captive portal-based one-time device registration	Possibility to temporarily suspend the measurements
Monitoring of gateways health	Flexible measurements (when, which tool, and how to run it)
Crosstraffic-aware measurements	Controlled-overlap scheduling algorithm for "heavy" measurements
Opt-in passive measurements	Users aware of current activities
Mutual exclusive scheduling algorithm for "heavy" measurements	

Current deployments

	BISmark (Gateway-based)	HOBBIT (Application-based)
Scope	**Worldwide**	**Italy**
Vantage Points	**417** (141 active)	**489** (57 active) – 70% / 12% / 18%
Users	**417**	**380**
Measured Access Networks	**417**	**1665**
Cities	**176**	**341**



Basic active measurements & tools

BISmark (Gateway-based)

What	How
upstream throughput (multiple TCP flows)	Netperf
downstream throughput (multiple TCP flows)	
round-trip latency (ICMP)	Ping
round-trip jitter	D-ITG
round-trip packet loss	
upstream/downstream capacity	Shaperprobe
upstream/downstream shape rate	
DNS delay	nslookup
DNS failure rate	
forward/reverse IP level path	paris-traceroute
round-trip latency under load	Netperf + ICMP

HOBBIT (Application-based)

What	How
upstream throughput (single TCP/UDP flow)	D-ITG
downstream throughput (single TCP/UDP flow)	
round-trip latency (UDP)	
round-trip jitter	
round-trip packet loss	
BitTorrent upstream throughput	
BitTorrent downstream throughput	

Other measurements and studies

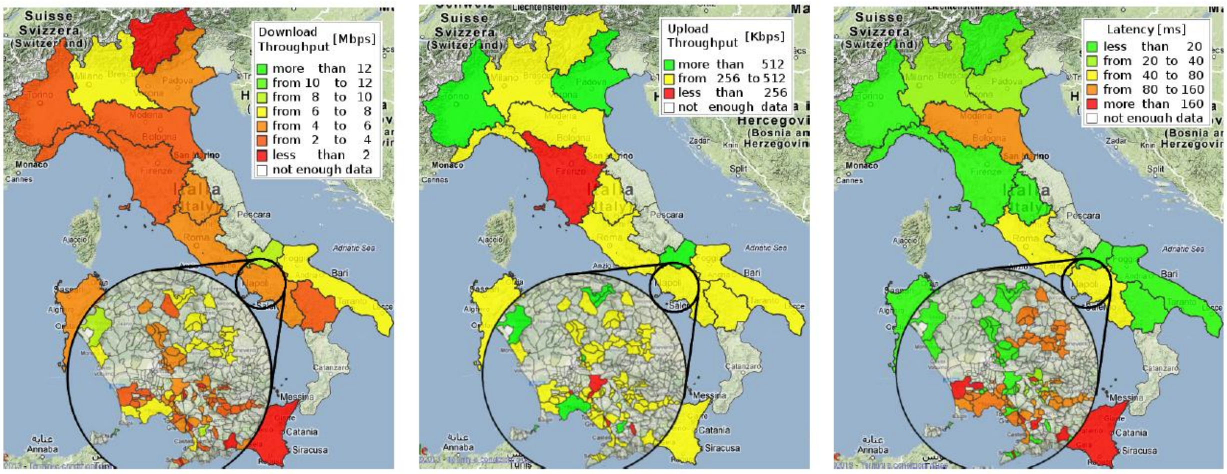
BISmark
(Gateway-based)

Project	Institution(s)	Description	Publications
	Performance Characterization		
Broadband performance	Georgia Tech, University of Napoli, INRIA, FCC/SamKnows, Research ICT Africa, National University of Sciences and Technology	Study factors affecting broadband performance in the US and in developing countries.	[10, 40], WiP
Web performance	Georgia Tech, INRIA	Characterize and mitigate last-mile bottlenecks affecting Web performance.	[41]
Home wireless performance	Georgia Tech	Study home wireless pathologies and bottlenecks in home networks	WiP
	Usage and Home Network Characterization		
Home network characterization	Georgia Tech	Understand usage and connectivity.	[18]
Home Constant Guard	Comcast	Expand Constant Guard to provide information about devices infected in home networks.	WiP
PAWS	University of Cambridge	Internet sharing in underserved communities.	WiP
	Topology and Connectivity Characterization		
Google cache measurements	University of Southern California	Study effects of Google's cache deployment on performance of Web services.	[7], WiP
Network Connectivity	Georgia Tech, USC, RIA	Characterize ISP connectivity and path inflation in Africa.	[19]
Network outages and DHCP	University of Maryland	Study effects of outages on IP address allocation worldwide.	WiP
OONI/censorship	NUST, University of Napoli	Study the extent and practice of censorship in various countries (initial focus on Pakistan).	WiP

Table 1: *Summary of various experiments (and publications) that BISmark has enabled to date. "WiP" denotes work in progress.*

The power of mapping results (Hobbit)

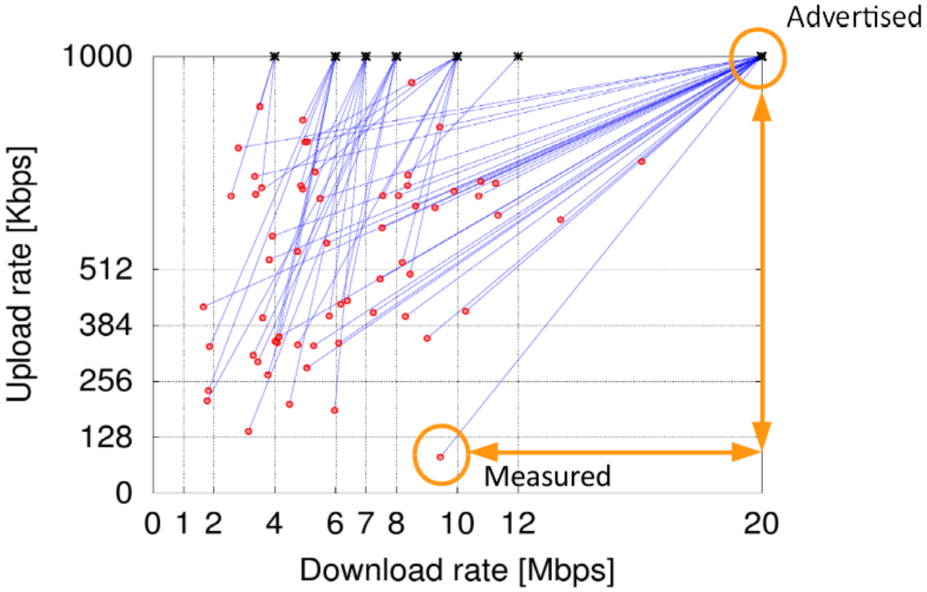
Average performance over different regions/municipalities



Maps give a quick sketch of average performance over the geographical areas

Looking for answers from collected data (Hobbit)

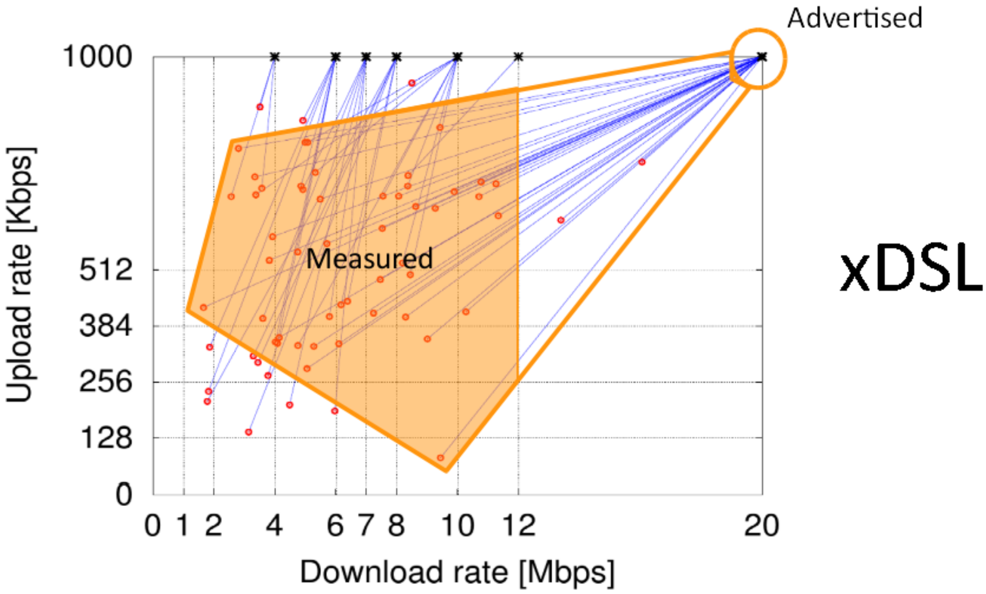
To what extent ISPs offer the advertised performance?



Often the same performance could be obtained with a cheaper service plan

Looking for answers from collected data (Hobbit)

To what extent ISPs offer the advertised performance?



Often the same performance could be obtained with a cheaper service plan

This is more evident for high-end service plans

Main lessons learned

- ➔ Gateway- and application-based approaches have complementary aspects

  they might cooperate to get more insights on performance

- ➔ Encouraging participation is challenging, while loosing it is very easy

  users give to the probe the responsibility for any problem they experience

- ➔ Form factor matters

  users often trust commodity hardware over custom hardware

- ➔ Duration of measurements makes the difference for some metrics

  long term throughput might be very different from short term one

- ➔ Using fine granularity when storing results is a good practice

Open points

- ➔ Large scale and dense deployment of VPs

  for obtaining more accurate insights on performance by geographical location and ISP

- ➔ Cooperation among available platforms

  for improving performance analysis effectiveness

- ➔ Proper scheduling of measurements

  for enabling scalability while managing overlap among measurements

- ➔ Access to technology-specific layer 2 parameters (e.g. DSL negotiated bitrate, signal attenuation, SNR, interleaving/fast)

  for tuning measurement tools and better interpreting results

- ➔ Layer 2 technology detection techniques

  for enabling technology-aware measurement techniques

More info at:

http://traffic.comics.unina.it
walter.dedonato@unina.it

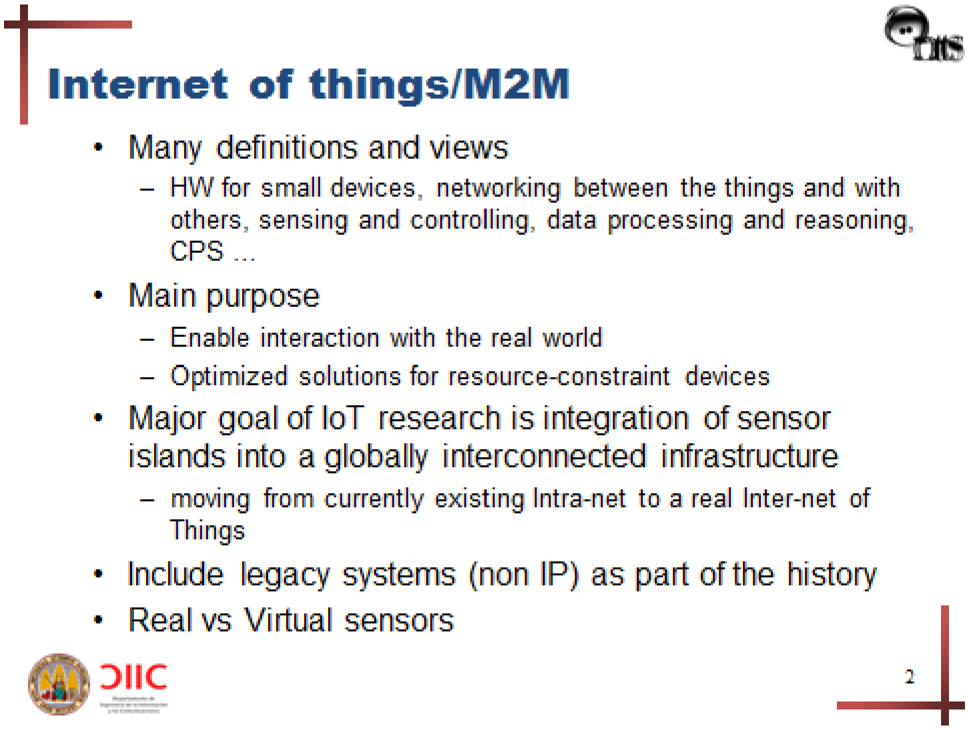
1.6 Prof. Antonio Skarmeta Gomez

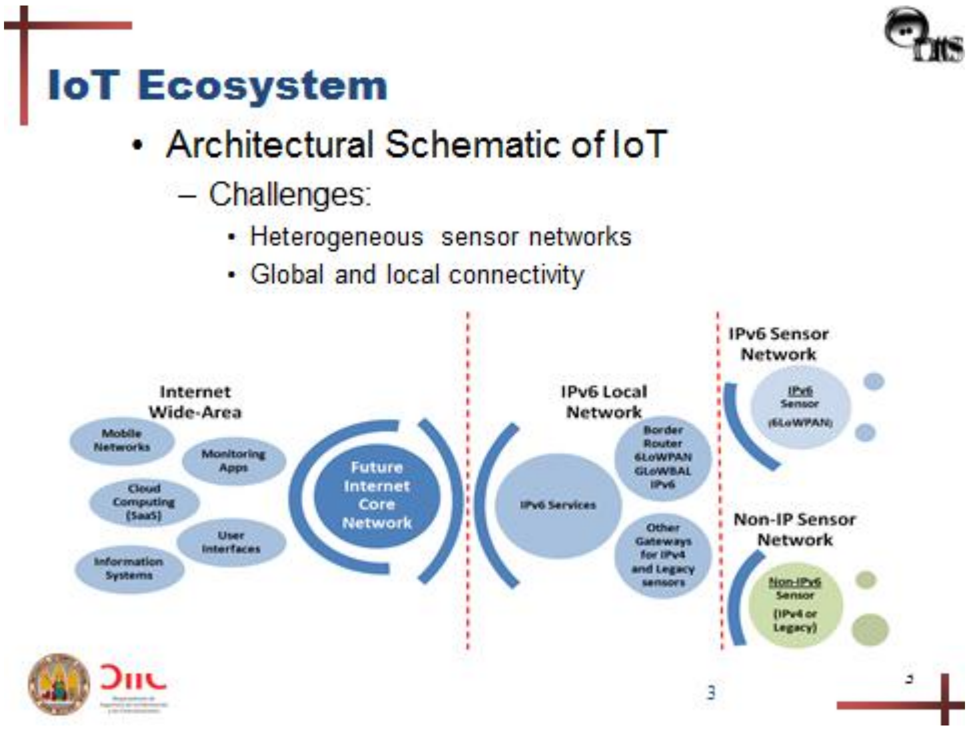
DIIC
Departamento de Ingeniería de la Información y las Comunicaciones

Monitoring and Measurement on Internet of Things Scenarios
SMART Internet Monitoring Study

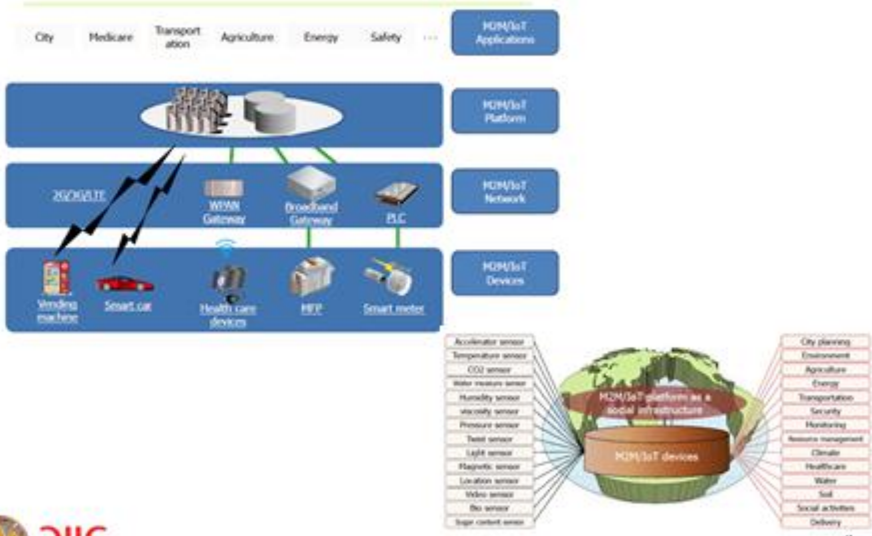
Antonio F. Skarmeta
<skarmeta@um.es>

University of Murcia (UMU)
SPAIN


Internet of things/M2M
• Many definitions and views
– HW for small devices, networking between the things and with others, sensing and controlling, data processing and reasoning, CPS ...
• Main purpose
– Enable interaction with the real world
– Optimized solutions for resource-constraint devices
• Major goal of IoT research is integration of sensor islands into a globally interconnected infrastructure
– moving from currently existing Intra-net to a real Inter-net of Things
• Include legacy systems (non IP) as part of the history
• Real vs Virtual sensors
2

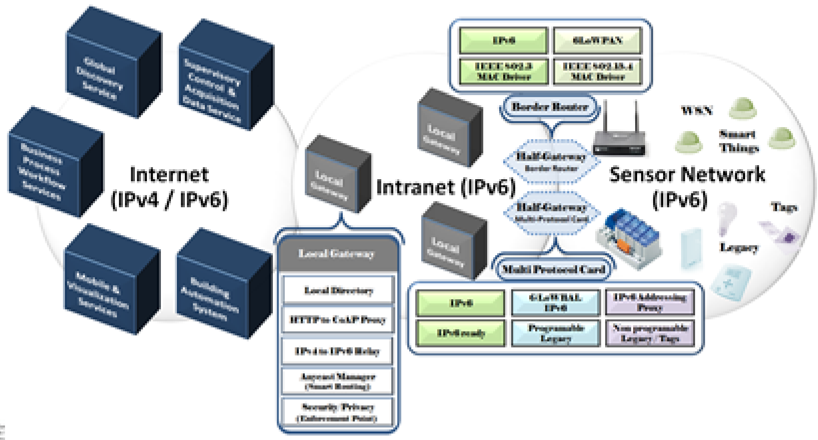

IoT Ecosystem
• Architectural Schematic of IoT
– Challenges:
• Heterogeneous sensor networks
• Global and local connectivity
Internet Wide-Area
Mobile Networks
Monitoring Apps
Cloud Computing (SaaS)
User Interfaces
Information Systems
Future Internet Core Network
IPv6 Local Network
IPv6 Services
Other Gateways for IPv4 and Legacy sensors
IPv6 Sensor Network
IPv6 Sensor (6LoWPAN)
Non-IP Sensor Network
Non-IPv6 Sensor (IPv4 or Legacy)
3

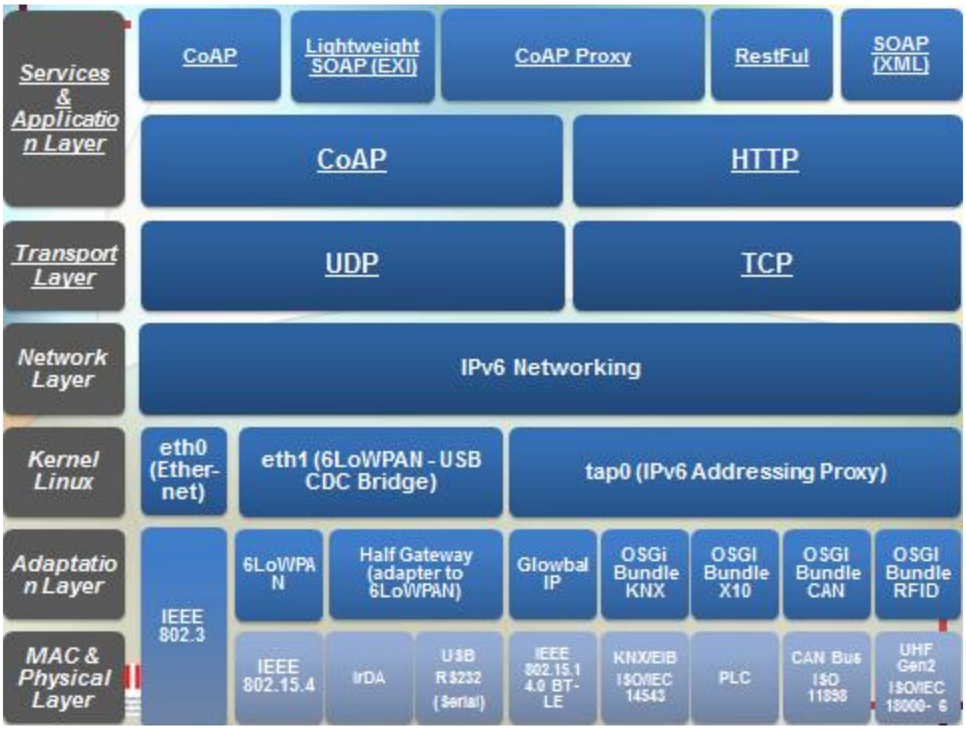
Covergence of different layers

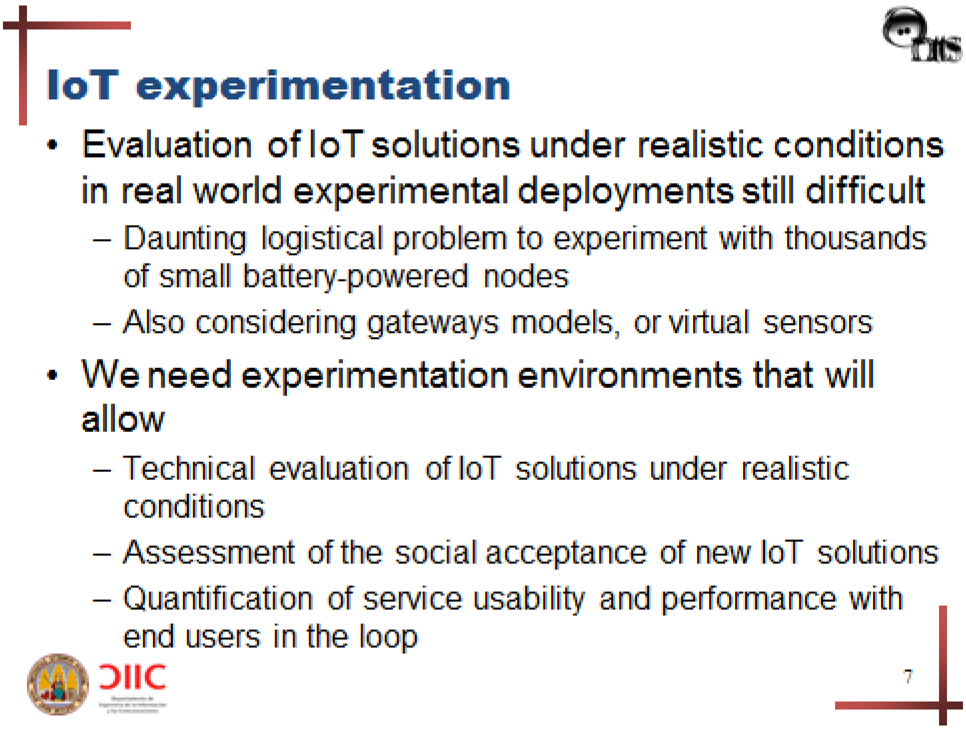


IoT Ecosystems

- Interoperability of heterogeneous networks through IPv4/IPv6 Internet based on half-gateways.

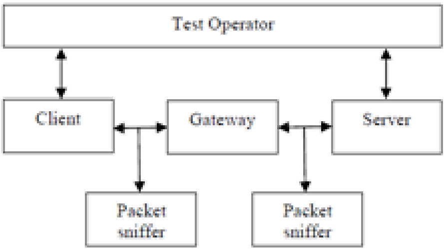



Services & Application Layer
CoAP
Lightweight SOAP (EXI)
CoAP Proxy
RestFul
SOAP (XML)
CoAP
HTTP
Transport Layer
UDP
TCP
Network Layer
IPv6 Networking
Kernel Linux
eth0 (Ether-net)
eth1 (6LoWPAN - USB CDC Bridge)
tap0 (IPv6 Addressing Proxy)
Adaptation Layer
IEEE 802.3
6LoWPAN
Half Gateway (adapter to 6LoWPAN)
Glowbal IP
OSGi Bundle KNX
OSGI Bundle X10
OSGI Bundle CAN
OSGI Bundle RFID
MAC & Physical Layer
IEEE 802.15.4
IrDA
USB RS232 (Serial)
IEEE 802.15.1 4.0 BT-LE
KNX/EIB ISO/IEC 14543
PLC
CAN Bus ISO 11898
UHF Gen2 ISO/IEC 18000- 6


IoT experimentation
• Evaluation of IoT solutions under realistic conditions in real world experimental deployments still difficult
– Daunting logistical problem to experiment with thousands of small battery-powered nodes
– Also considering gateways models, or virtual sensors
• We need experimentation environments that will allow
– Technical evaluation of IoT solutions under realistic conditions
– Assessment of the social acceptance of new IoT solutions
– Quantification of service usability and performance with end users in the loop
DIIC
7

Some examples/approaches

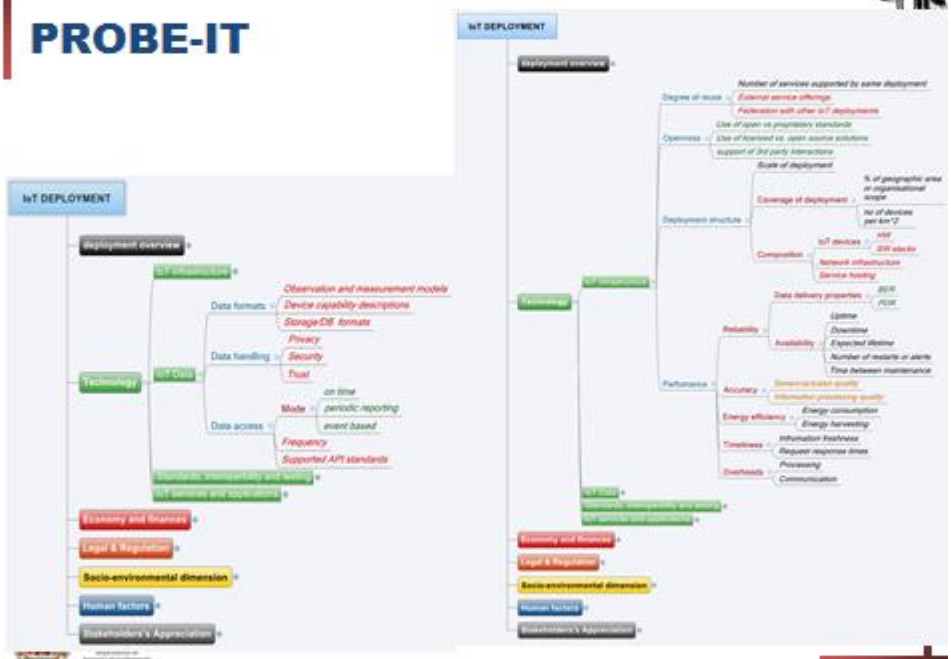
- ETSI TS 103 104 V1.1.1 (2013-04) CoAP interperability test



- ETSI Plugtest on 6LowPAN and CoAP

8

PROBE-IT



Challenges

- Up to now silos of evaluation approaches, but we need …
- Scale
  - Going up
- Heterogeneity of devices and device technologies
  - support interoperability at different layers
- Repeatability of experiments
  - on a testbed or across different testbeds difficult
- Federation of IoT testbeds with other testbeds
  - important for end to end experimentation

10

Requirements

- Scale
  - smaller-scale testbeds in the range of 10s up to hundreds of nodes were sufficient for most experiments
  - many IoT experiments will demand an order of magnitude larger scale
- Experimentation with 1000s of IoT nodes possible, but
  - minimized human intervention, maximized plug-and-play configuration, and automatic fault-management required
  - support mechanisms that ease the selection of adequate testbed resources and the composition of experiments are necessary

12

Requirements

- Heterogeneity
  - Testbeds evaluation have to include various types of devices and protocols not just CoAP
  - gateway devices should be an active part of the experimentation infrastructure.
- Achievable, but
  - Tools allowing effective configuration and execution of experiments across heterogeneous testbed resources and the corresponding management of devices required
  - Providing support to ease programmability of heterogeneous devices, which often come with diverse execution environments required

13

Requirements

- Repeatability
  - Repeat experiments within and across different testbeds
- Replayability
  - Adequate packaging of experimentation specifications, traces, and results so they can be easily re-executed and compared across different testbeds
- Heterogeneity and the wireless nature of IoT testbeds, ever changing ambient conditions ➔ both features hard to implement
- Monitoring of radio environment during experimentation and benchmarking of different testbeds required
  - providing hints for the interpretation of experimental data
- Replayability requires
  - agreement on standards for the specification of experiments, collection of traces, and the packaging of experimental results across a variety of testbeds

14

Requirements

- Federation
  - necessary to achieve scale or to add capabilities for experimentation, which are not locally available
  - viable solution to create larger and more heterogeneous facilities out of specialized, smaller-scale ones
- Requires
  - common framework for authentication, authorization, accounting, reservation, and experiment scheduling

DIIC

15

Requirements

- Concurrency
  - supporting multiple concurrent users and experiments is a necessity for an economically viable operation
  - larger-scale testbeds must support multiplexing of concurrent experiments
- IoT devices are substantially resource-constrained
  - virtualization at the hardware-layer very difficult
- "Virtualization" at the testbed level more feasible
  - advanced mechanism allowing selection of testbed resources to minimize interference of concurrently executing experiments, while satisfying the requirements of the experiment required

DIIC

16

Requirements

- Experimental environment:
  - IoT technologies heavily depend on ambient environmental conditions in which they are deployed
    - so does the service logic of the diverse IoT applications
- Outdoors deployments, in the real, wild world
  - require more robust techniques for realizing out-of-band management and control planes ➔ wired solutions have to be replaced by wireless
  - Increased robustness important due to the increased overhead of the maintenance of testbed equipment
    - access is often traded off against the threat of physical tempering, deliberate damage, or theft

17

Requirements

- Mobility
  - Real world is moving, so are the IoT devices attached to them
- Handling such mobility and the associated system dynamics is thus a key requirement for future IoT solutions
  - mechanisms to control and exploit realistic mobility of both IoT devices and real world entities during experimentation are necessary
- Privacy and security

18

Requirements

- User involvement and impact
  - Many IoT applications centered on human users or require their active participation ➔ experimentation more difficult to control and may invalidate results
- Required mechanisms allowing for
  - evaluating social impact and acceptance of IoT solutions and applications
    - Automated detection of situations when user behavior influences the validity of collected data
  - provision of efficient multi-modal mechanisms for user feedback

DIIC

19

ANA4IoT experiments, measurements

- Objetive: Analysis for Future Internet architectures for the Internet of Things
  - Connection setup time, transit time of packets (latency), available bandwidth over time, average time to transfer a file
    - one vs. many connections (bandwidth and scalability)
  - Handover delay, packet delay, packet loss (if any), effects on the transmitting and non-transmitting connections
  - With malicious nodes, measure interference (delay, broken connections)

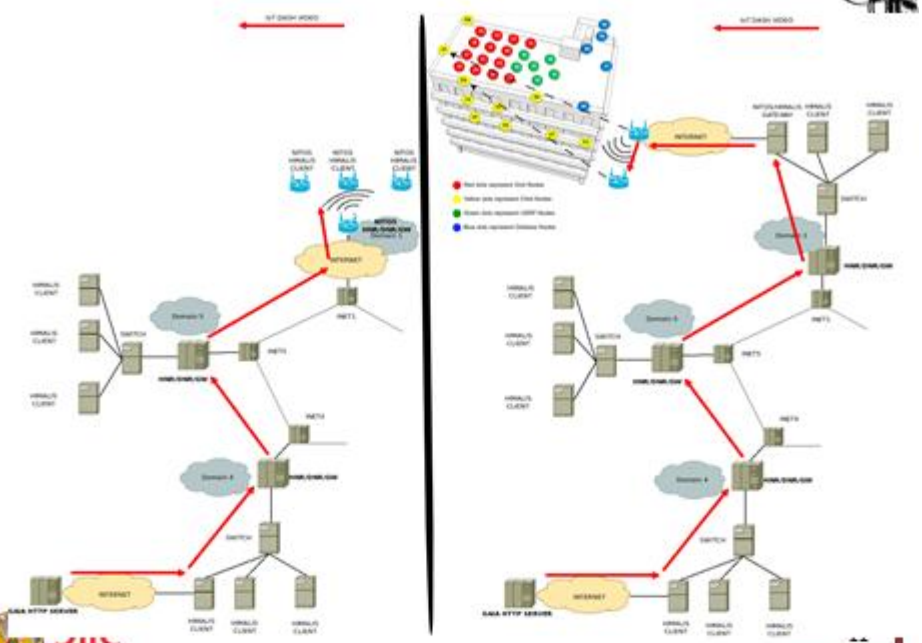
DIIC

20

Experimentation environment

- Four different levels of:
  - IoT devices (things) connected to enabled edge networks with mobility capabilities.
  - Medium-power devices (normal hosts, nodes) connected to the edge networks.
  - Interconnection equipment (gateways and routers) forming part of the global transit network or interfacing it with the edge networks or IoT enabled edge networks.
  - Specific equipment to provide the control and management planes.

21



IoT6 Monitoring parameters Scalability

- The following performance metrics have been considered:
  - **Delay**: The delay have been taken measuring the time since a request is sent to the response is received, either positive or negative.
  - **Packet error**: If the packet is lost, the result shows a negative delay, so this negative delay is represented as a connection error.
  - **Memory usage**: While the test is being performed, an application is taking RAM usage values every second from server side.
  - **CPU usage**: While the test is being performed, an application is taking CPU usage values every second from server side.
  - **Network usage**: While the test is being performed, an application is taking network usage values every second from server side. The network usage is composed by RX and TX.

DIIC

23

Conclusions

- Wider background: IoT for large scale monitoring (i.e. Smart Cities domains)
- reliability + security + scalability
- real-time / secure IoT applications are hard to achieve besides bespoke solutions
- diverse feature-set of IoT data sources
  - IoT devices can produce data-streams in a wide bit-rate spectrum (ON/OFF → CCTV video streams, legacy,gateways)
  - for real-time applications low latency transport needed
- private nature of generated data
  - need to link data source with well defined user / application and dynamically secure those pipes to prevent "knowledge leaks"

DIIC

24

Proposed experimentation

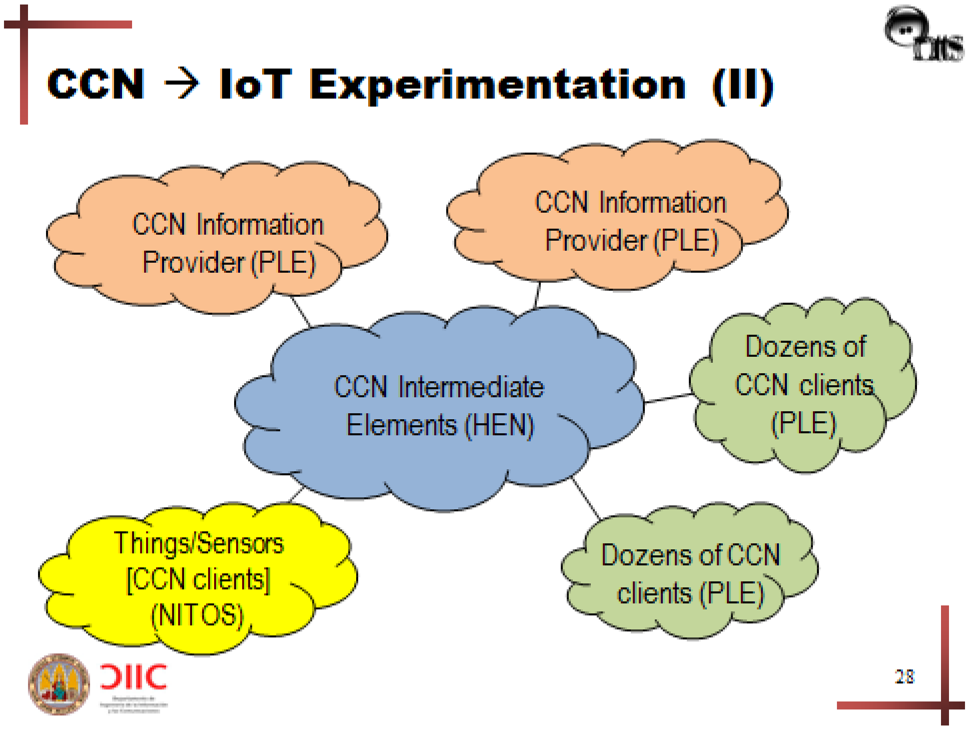
- As the central output of the experiment we propose to measure the bandwidth, throughput, and delay of the communications established with the low-powered devices connected to the edge networks for the different protocols.
- Get the behavior of different communication combinations, including the *thing-to-thing*, *thing-to-host*, *host-to-thing*, and even *host-to-host*.
- Experiment with the mobility support of the different approaches to get the particularities of each handover operation.
- Evaluate the security of communications with *simulated* intruders, denial-of-service attacks, robustness of security infrastructure, etc.
- Overhead of the integration of some approaches with a security-oriented, identity-based control plane

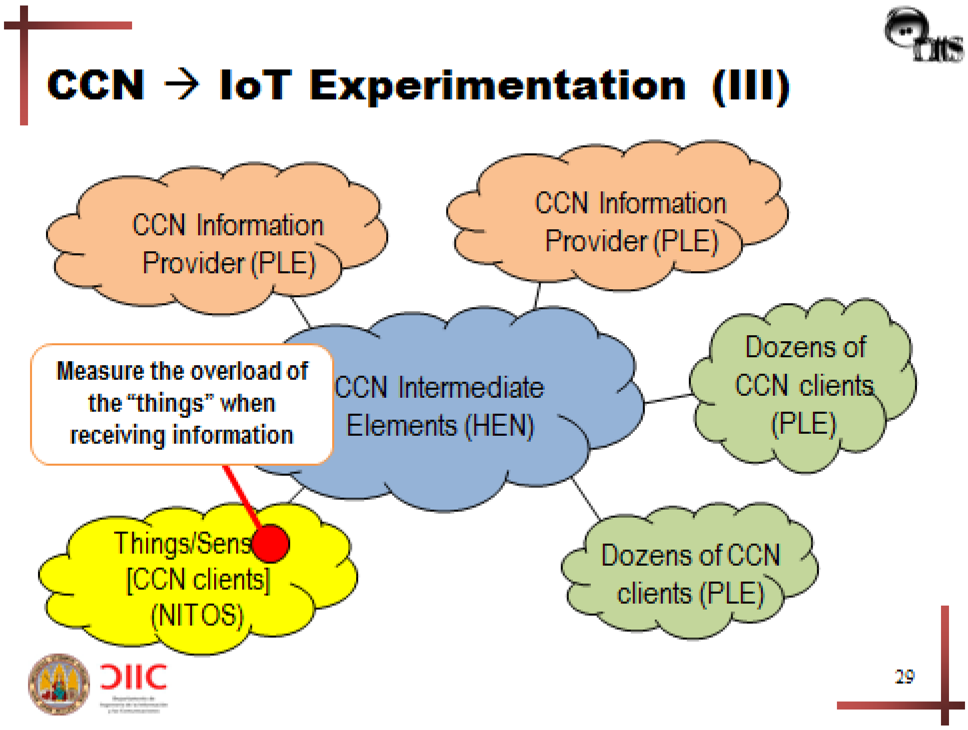
25

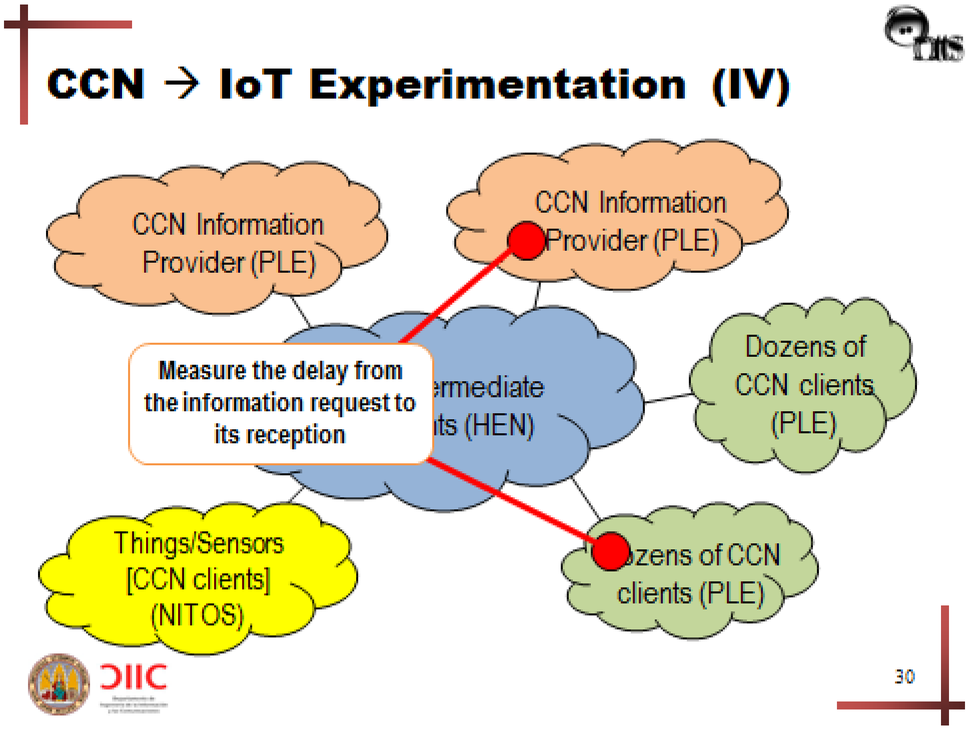
Tests and measurements

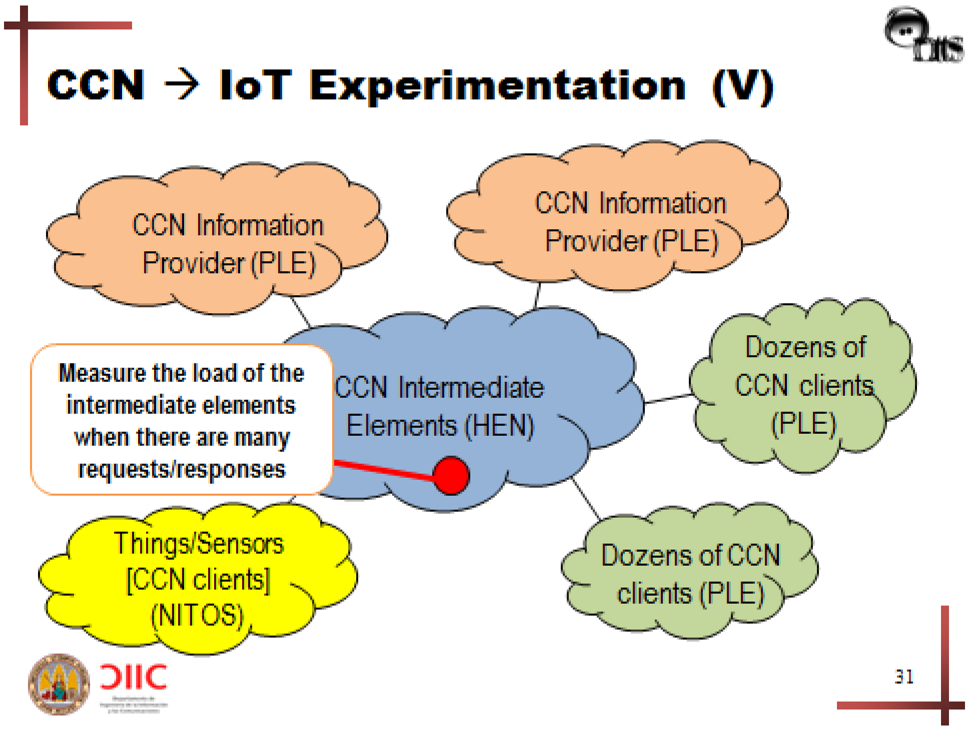
- The first experiment just consists in incrementally making many end-nodes of different types establish many communications with each other and send/receive a big file, evaluating:
  - latency
  - bandwidth and scalability
  - throughput
- The second experiment consists on evaluation communication and handover process by moving a node from one network to:
  - Handover delay,
  - packet loss
- The third experiment consists in selecting some nodes and configuring them as attackers which intercept the communication between other pair of nodes.
- The fourth experiment consists in introducing security extension on the architectures based on identity-based control plane

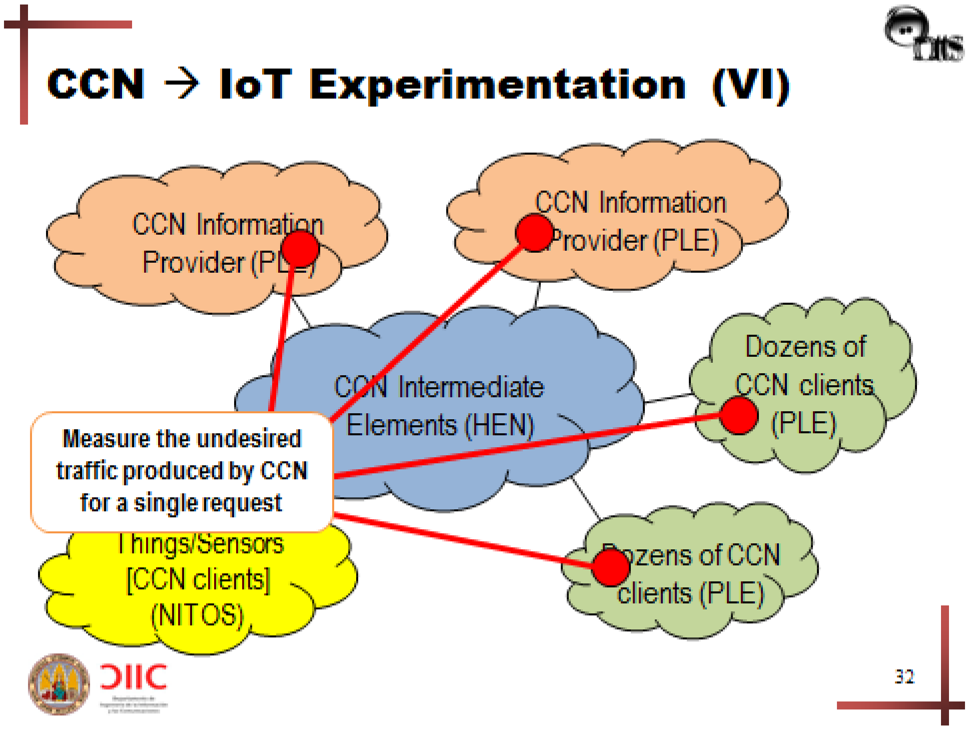
26


CCN → IoT Experimentation (II)
CCN Information Provider (PLE)
CCN Information Provider (PLE)
CCN Intermediate Elements (HEN)
Dozens of CCN clients (PLE)
Things/Sensors [CCN clients] (NITOS)
Dozens of CCN clients (PLE)
DIIC
28


CCN → IoT Experimentation (III)
CCN Information Provider (PLE)
CCN Information Provider (PLE)
Measure the overload of the "things" when receiving information
CCN Intermediate Elements (HEN)
Dozens of CCN clients (PLE)
Things/Sens [CCN clients] (NITOS)
Dozens of CCN clients (PLE)
DIIC
29


CCN → IoT Experimentation (IV)
CCN Information Provider (PLE)
CCN Information Provider (PLE)
Measure the delay from the information request to its reception
Dozens of CCN clients (PLE)
clients (PLE)
Things/Sensors [CCN clients] (NITOS)
30


CCN → IoT Experimentation (V)
CCN Information Provider (PLE)
CCN Information Provider (PLE)
Measure the load of the intermediate elements when there are many requests/responses
CCN Intermediate Elements (HEN)
Dozens of CCN clients (PLE)
Dozens of CCN clients (PLE)
Things/Sensors [CCN clients] (NITOS)
31


CCN → IoT Experimentation (VI)
CCN Information Provider (PLE)
CCN Information Provider (PLE)
CCN Intermediate Elements (HEN)
Dozens of CCN clients (PLE)
Measure the undesired traffic produced by CCN for a single request
Things/Sensors [CCN clients] (NITOS)
Dozens of CCN clients (PLE)
32


FOTsis
ITSSv6
FOTsis 2012 ITS World Congress demo
Overview of the demo
ITSSv6 sensor network
Roadside ITS-S Router
Central ITS-S Host (FOTsis Road Safety Management Centre)
Roadside ITS-S Router
Vehicular ITS-S Host (Smartphone)
802.11p
Vehicular ITS-S Router
WiFi
Central ITS-S Host (ITSSv6 Roadside Monitoring Centre)
CAM (802.11p)
FOTsis
ITSSv6
Far demo area
Stand area (Hall B)
Launch Area (Hall A)
33
FOTsis/ITSSv6 2012 Vienna ITS World Congress Joint demo