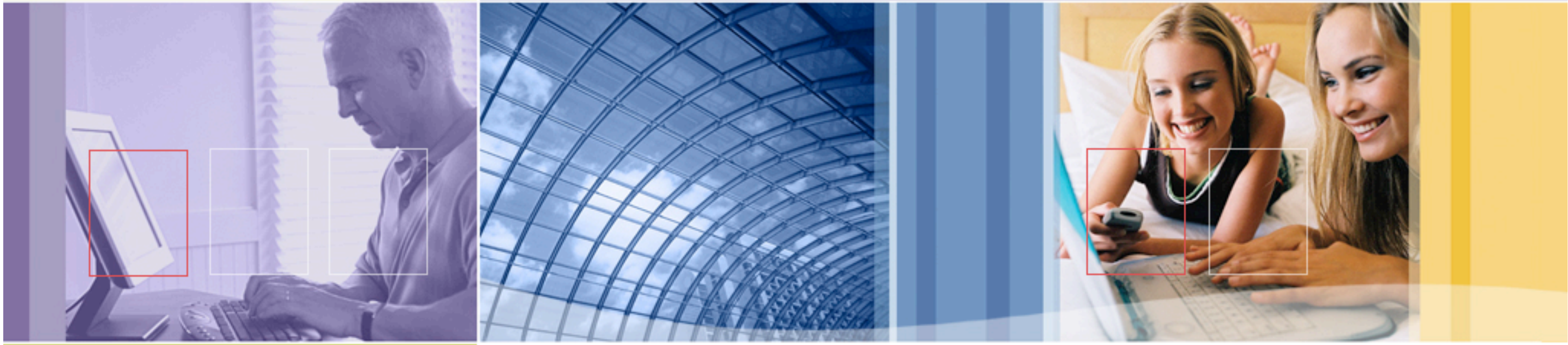
Messaging Anti-Abuse Working Group

ITU/WSIS Thematic Meeting on Cybersecurity, June 28 2005



luc.mathan@francetelecom.com

Messaging operator experience today…

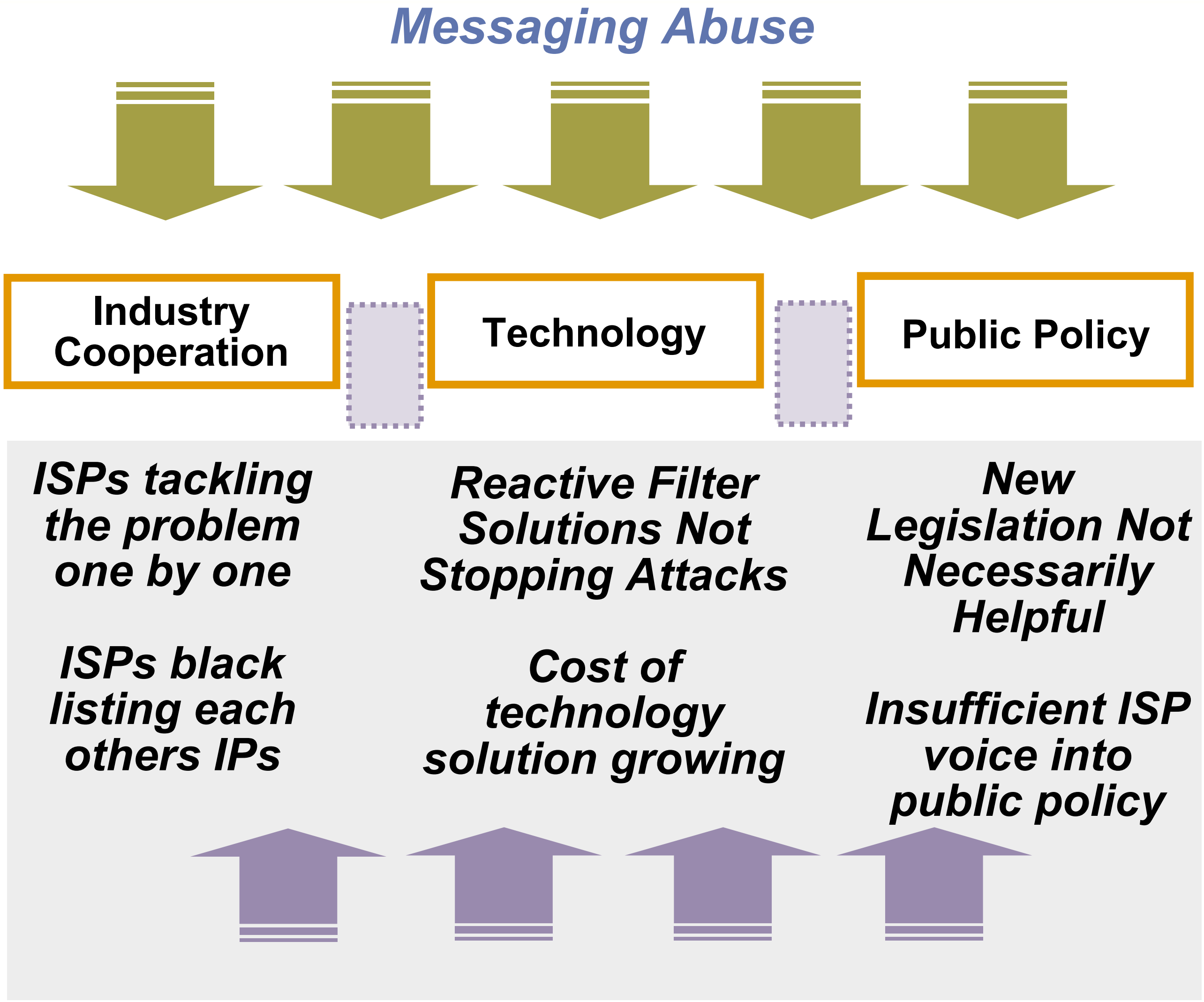
Incoming spam trafic
=> End user complaints
=> Strain on infrastructure

Outgoing spam trafic
=> Protective reactions from other operators
=> Strain on backbone

Anti-abuse teams: overwhelmed
Messaging platform teams: continuous emergency state
Cost of anti-abuse technology and expert staff
General decrease of margins for ISPs

User experience severely degraded
Devaluation of email as universal communication tool

Change this:



Messaging Abuse

Industry Cooperation

Technology

Public Policy

ISPs tackling the problem one by one

ISPs black listing each others IPs

Reactive Filter Solutions Not Stopping Attacks

Cost of technology solution growing

New Legislation Not Necessarily Helpful

Insufficient ISP voice into public policy

2 of the problems currently

Zombies (compromised PCs belonging to unsuspecting broadband customers)

Source of ~ 80% of spam

Also used for viral or ddos attacks

Must inhibit smtp server function (port 25)

Must clean customer’s PC

Education is key

Forged headers (obfuscation of path taken by email)

Is sender known and approved ?

Is he really who he claims he is ?

Sender Authentication Protocols (SAP), 2 methods:

Secure headers

Sign contents

Purpose of Messaging Anti-Abuse Working Group

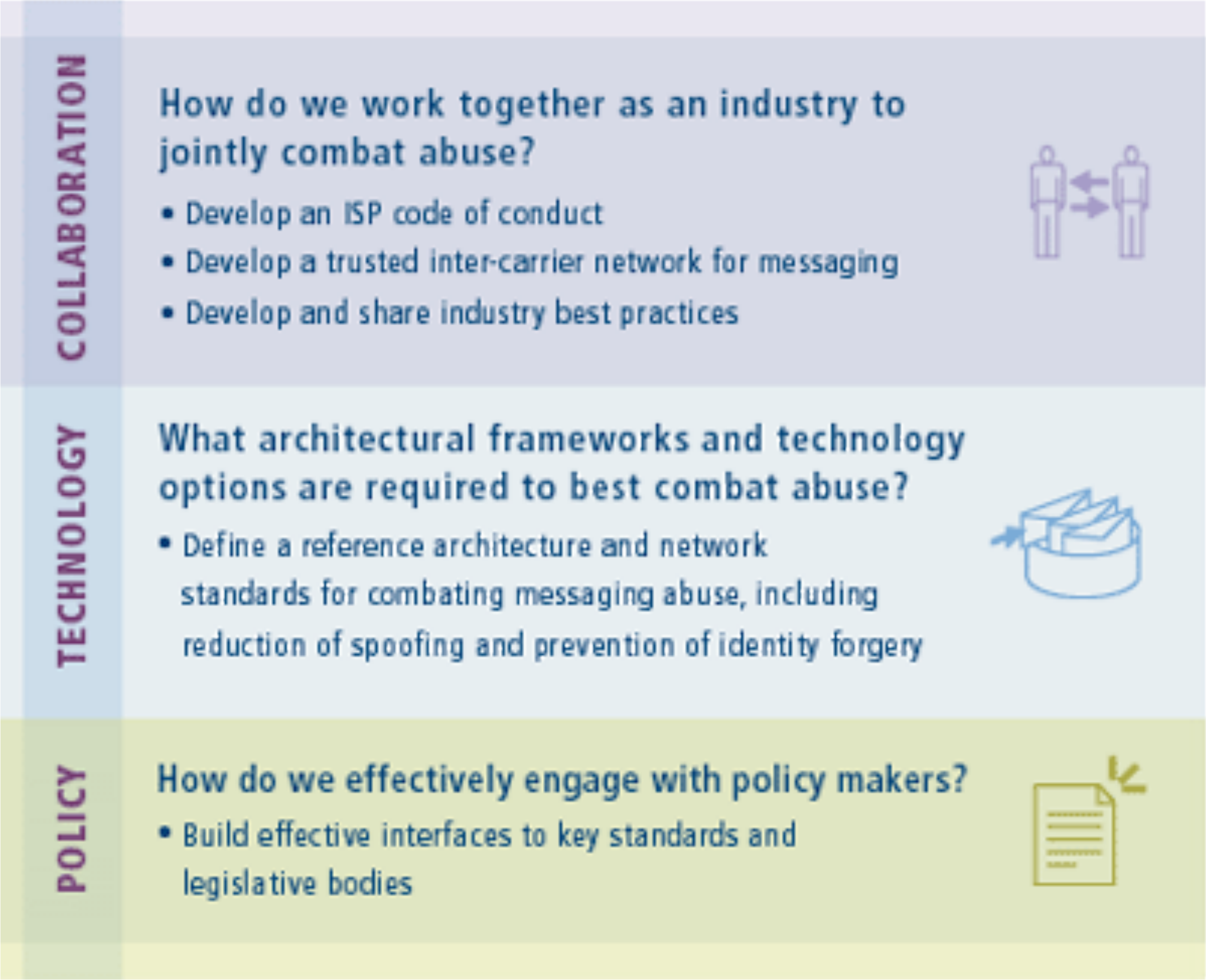
- Bring the messaging industry *together* to effectively address the growing problem of messaging abuse
  - Minimize abuse and the impact on legitimate messaging uses and operations

- *Open, global, industry organization* to facilitate *collaborative work* to address messaging abuse
  - Global geographically
  - Fixed line and wireless messaging (currently focusing on email)

- Work with other industry organizations with related goals & objectives

- MAAWG does NOT engage in certification or conformance activities

MAAWG approach



COLLABORATION

How do we work together as an industry to jointly combat abuse?

- Develop an ISP code of conduct
- Develop a trusted inter-carrier network for messaging
- Develop and share industry best practices

TECHNOLOGY

What architectural frameworks and technology options are required to best combat abuse?

- Define a reference architecture and network standards for combating messaging abuse, including reduction of spoofing and prevention of identity forgery

POLICY

How do we effectively engage with policy makers?

- Build effective interfaces to key standards and legislative bodies

Currently 45 members and growing over 500M addressable subscribers

SPONSOR MEMBERS

AOL.COM

Bell

BELLSOUTH Listening. Answering.℠

cingular WIRELESS

CLOUDMARK

COX

EarthLink

france telecom

comcast.

swisscom

Charter get hooked.

GoodmailSystems restoring trust in email

OPENWAVE

verizon

YAHOO!

FULL MEMBERS

IIJ Internet Initiative Japan

Sprint.

CABLEVISION

mx LOGIC

CISCO SYSTEMS

IRONPORT SYSTEMS

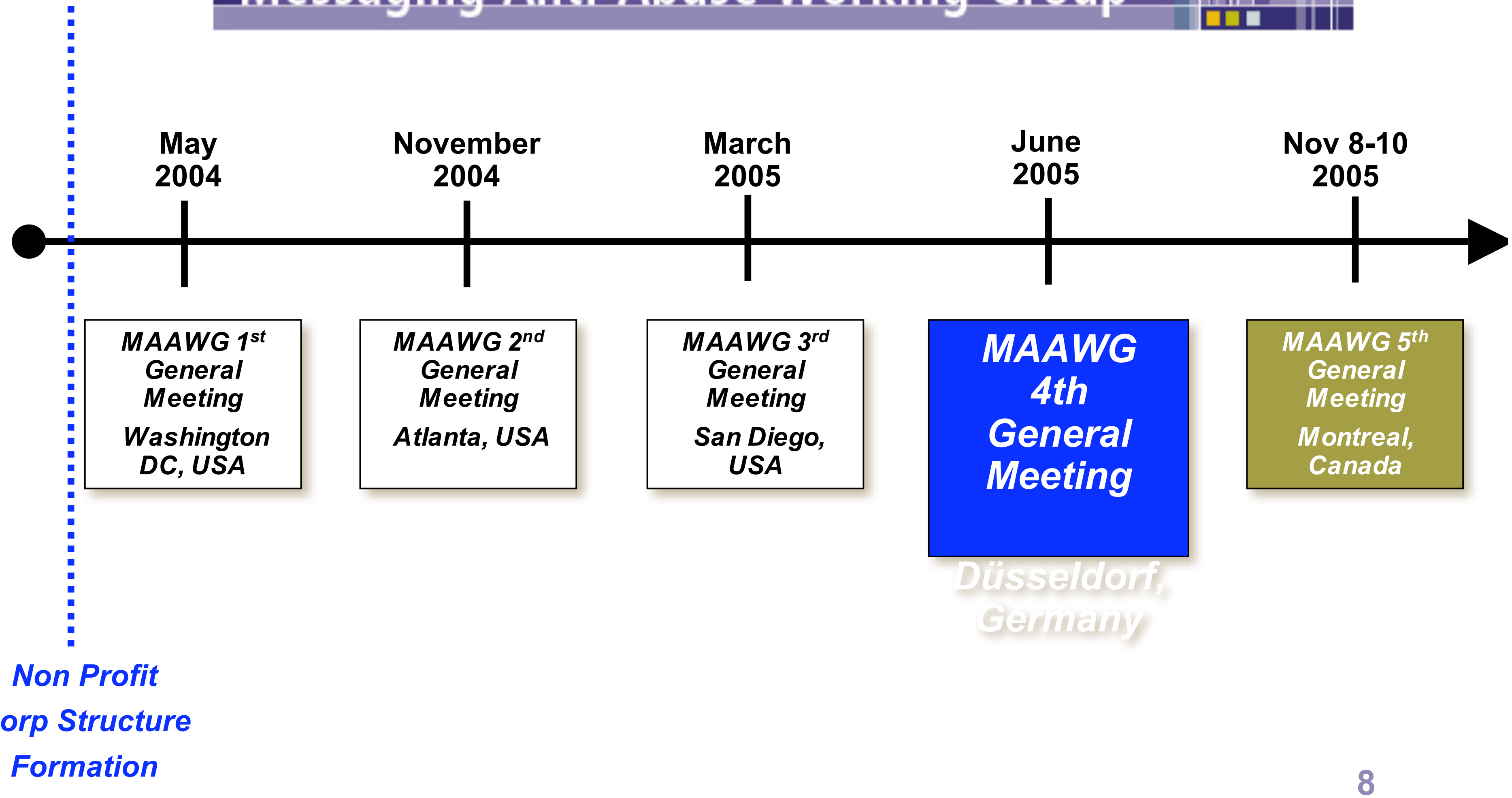
VeriSign

symantec.

22 SUPPORTER MEMBERS

MAAWG timeline

Messaging Anti-Abuse Working Group



May 2004

MAAWG 1st General Meeting

Washington DC, USA

November 2004

MAAWG 2nd General Meeting

Atlanta, USA

March 2005

MAAWG 3rd General Meeting

San Diego, USA

June 2005

MAAWG 4th General Meeting

Düsseldorf, Germany

Nov 8-10 2005

MAAWG 5th General Meeting

Montreal, Canada

Non Profit Corp Structure Formation

MAAWG Organization - Committees

- Board of Directors
  - Comprised of Sponsors & 2 Full members – operators and vendors
  - Fiduciary and governance responsibility for the organization
  - Approval of new initiatives, public documents/reports and new Committees
- Technical Committee
  - Responsible for the technical work including evaluation of new technology based upon testing and specification development as needed
- Collaboration Committee
  - Responsible for developing collaborative policies and procedures to address messaging abuse
- Public Policy Committee
  - Responsible for interacting with other industry organizations and government agencies
- Wireless Abuse Committee
  - Responsible for addressing mobile abuse needs in conjunction with other Committees and organizations

General meetings: Committee meetings + public panels

Technical Committee

- Deployment and Testing of SAP by Operators
  - shared results
  - SPF, SenderID, DomainKeys, IMM, etc
- SPF and SenderID Comparison
  - Published document in July
  - A “cheat sheet”, not a recommendation
- Outbound Guidelines (e.g.: Port 25, SMTP Auth)
  - Collaboration Committee review for Best Practices
  - Draft available for members
  - Additional inputs from non-members
- Feedback Loop Messaging Format
  - MIME Content-Type: message/feedback-report
  - Developed based upon real deployments
  - Members and Nonmembers have and are contributing
  - Finalize version 1.0 at November meeting

Collaboration Committee

- Code of Conduct
  - 4 points
  - Approved and Published on MAAWG web site
- Best Current Practices
  - Currently under member review
  - Version 1.0 in November
  - Followed by non-member reviewing, IETF
- Feedback Loop Testing ISP to ISP
  - Expanded Testing Framework in November
  - Recommendations / Best Practices based upon Expanded testing
- Contact Databases
  - Voluntary Members Contact database for improved anti-abuse communications and resolution
  - Expand to non-members based on usage results
  - Members version complete by end of year

Public Policy Committee

- Port 25 blocking advocacy document
  - Directed at regulators and non-technical execs
  - What is port 25
  - Why it is a necessary step
  - What are the accompanying steps
- New Board of Directors initiative on spam metrics
  - Common Definitions for Abuse and Anti-Abuse Metrics
  - Aggregate reporting from MAAWG based upon Members reporting
  - Agreement in November Meeting and reporting will follow
- Fact based inputs to Agency Requests
  - Example, FTC request for technology inputs for Sender Authentication technology approaches: MAAWG SPF / SenderID comparison

Wireless Committee

Current focus on messaging anti-abuse techniques for open Internet interfaces. Many wireless messaging operators counter this problem by closing the interface to all traffic. Alternative solutions are needed.

- Addresses gaps not covered in other organisations

- Reference Architecture
  - Used for common terminology and reference for practices
  - Seeking expanded input and comments

- Best Current Practices: email to mobile
  - Seeking expanded input and comments

MAAWG Committees - Summary

• TECHNICAL	• *Deployment and Testing of SAP* • *SPF and SenderID Comparison* • *Outbound Guidelines (e.g.: Port 25, SMTP Auth)* • *Feedback Loop Messaging Format*
• COLLABORATION	• *Code of Conduct* • *Best Current Practices* • *Feedback Loop Testing ISP to ISP* • *Inter-ISP Contact Databases*
• PUBLIC POLICY	• *Governmental and Regulatory Interfacing* – *US-FTC / OECD / Others* • *Aggregate Metrics*
• WIRELESS	• *Reference architecture* • *Best Current Practices*

MAAWG Code of Conduct

Voluntary set of principles directed at member and non-members ISPs/ESPs

In summary:

- Explain to your users the permissible/prohibited uses of the messaging services and include them in the AUP
- Enforce your AUP (acceptable use policy)
- Protect your users and your network from abuse resulting from the non-enforcement of prohibited uses at other ISPs
- Communicate with the ISP(s) impacted by your protective measures

Thank you !

Our 4th General Meeting in Düsseldorf, Germany
had 120 Attendees from16 Countries:
Australia, Austria, Croatia, Denmark, Egypt, France,
Germany, India, Italy, Japan, Netherlands, New Zealand,
Poland, Switzerland, UK, USA

We invite your Comments and Participation in MAAWG.
Please sign up for our Interest Group mailing list for future information.

http://www.maawg.org/home/

If you would like additional information or have questions, please contact us
jerry.upton@maawg.org, or luc.mathan@francetelecom.com

Attend our next meeting in
Montréal, Canada on November 8-10, 2005.