RFC3869

A personal view

Name	:	Wouter Borremans
Student number	:	0461911
Course	:	System and Network Engineering
Subject	:	Classical Internet Applications

Preface

This document describes my personal view on the RFC3869, which was released in August 2004 by Atkinson and Floyed. It discusses the history of funding for Internet research, expresses concern about the current state of such funding, and outlines several specific areas that the IAB believes merit additional research.

General opinion on RFC3869

Nowadays the world is Internet and Internet is the world. Communicating means everything. The world is almost completely dependent on the Internet, it even accomplished to have some articles in the book of law! The Internet brought a whole new sector in the regular business sectors with an incredible speed. This brought many problems with it. When a mayor power down or terrorist attack will be a fact, many people will discover and feel how important the Internet is nowadays. It will even become bigger and bigger, this implies more and more problems. Research on this topic is needed, otherwise many problems will occur and will be incredible difficult to solve.

Below you can find my view on the topics discussed in the RFC3869 document.

3.2.1 Domain Name System

I agree with the stated ideas in this subchapter. In my opinion, the DNS system is not outdated, it works for now. The future isn't that bright for the current DNS system. I think that the load of the DNS system will become bigger and bigger. Just think about more and more (mobile) devices will use the Internet connectivity possibilities such as GPRS,UMTS and WiFi etc. Each device needs an IP address and get a DNS name. Those names have to be resolved. (Also note that more and more domestic devices will get an IP address; coffee machines, alarm systems, sensors, etc.)

Domain registration
The Domain Name System has been 'updated' several times now, not only top level names come and go but also the allowed structures differ from the earlier versions.

Technical issues:
- Allow longer domain names;
- Allow non-alphabetical characters like +,-,_;

Non technical issues;
- Allow not only companies to register a domain name;

A great part of the dictionary has already been claimed, the logical implication is that the number of and allowed characters had to be increased. I don't think this is a solution for the registration problem at the moment, exactly the same registration problem (no available domain names) will occur very soon. What I try to say is that adding new top level domain names or new structures will not solve the great demand of domain names. Many companies will claim every domain name possible ruining other person's businesses and whishes.

A well known problem at the moment is that the current IP system (IPv4) is running out of addresses. IPv6 has to be implemented, this implies new problems with the current DNS system. As the article says, it would be preferable to have a new DNS system. This is not very easy, I wonder how we will manage the current system to the IPv6 infrastructure. I think it will have a great impact, many companies will face great difficulties merging to the new system.

I don't think it will be preferable to design a DNS protocol or system that upgrades the current DNS infrastructure. It would be more preferable to develop a DNS system that can overtake the current DNS system in a parallel way. Maybe we can do this together with the (final) implementation of IPv6 ?

3.2.2. New Namespaces

I agree with the author of the article on the fact there must be some kind of research to new namespaces. The evolution of the Internet is somehow dependent on it. A .mobile namespace maybe? New generation of devices / media influences may introduce new namespaces in my opinion.

3.3 Routing

As the article mentions, not the algorithms and routers itself are currently facing performance problems, but the people that configure them cause the problems. I think this is not acceptable. There must come / be a set of rules which providers have to obey. This will cause the Internet to be a high performance network which is able to offer new and reliable services.

3.3.2 Routing Integrity

I don't think the focus on the security of routing messages has to be there. In most cases (as far as I know) router communication between provides is mostly implemented over internal LANs or VLANs. Implementing security features into a router will affect the performance in a device that has a great importance for the being of the Internet.

3.4 Security

The current security features that the internet offers are hard to understand for the 'regular computer user'. This causes that most users are not aware of the threads that are present. I think each operating system should have standard security features build in, in such a way that every user can understand and use it in a proper way. This implies that there must come a security standard that describes how the features have to be implemented in different kinds of GUI's.

3.4.3 Cryptography

Research on this topic needs to be continued forever. Just recently one of the –stated uncrackable- MD5 algorithm was cracked until 8 characters. Many companies use the algorithm, it will be a disaster if the whole algorithm will be cracked.

3.4.6 Denail of Service Protection

(D)DoS Attacks cause many problems in the internet sector, in my personal expierence I know that DoS attacks can be destructive for your network. It even can cost you a lot of money when your provider charges you according to the 95th percentile traffic billing system. (http://www.seanadams.com/95/)

Nowadays several DoS attack protection systems are available on the market. These system offer the so called 'secret (internal) ip system' which blocks the DoS attack entering the actual hosting network. The system pretends it is a specific host or network and analyzes the network traffic and redirects it to a very large backbone in the case of a DoS attack so the DoS attack reduces in strength. In my opinion research has to continue on this topic to precent future MAJOR DoS attacks will let the internet stop functioning.

3.5.1 Managing Networks, Not Devices

As the article mentions, more research has to funded to develop management or data mining protocols that are able not to only monitor one device, but complete (distributed) systems. Though I think the current SNMP protocol offers enough data, it would be more preferable to develop a special framework which is capable to communicate with SNMP in a proper way.

3.5.2 Enhanced Monitoring Capabilities

Why don't we reverse the whole management data mining process? Why reading the SNMP data from the devices? Why don't we standardize a protocol which makes the device itself a simple possibility to send it's management data to a centralized data mining system? This makes it easier to centralize the monitoring of large networks.

3.5.3 Customer Network Management

I think this part of the article has great idea's about informing users about current failures. On the other hand I think that the most users are not interested in that kind of information, they only want to see that their 'whishes' are fulfilled.

3.6 Quality of Service

Due to the increasing popularity of VoIP telephony systems, much effort and funding is needed to actually adding QoS to the Internet. The current infrastructure does not provide this at all. Offering QoS to the current infrastructure relies on configuring the routers properly. Companies now offering QoS only can guarantee it's quality over separate networks.

3.10 Internet Measurement

'Forcing' providers to release their infrastructure does not seem like good idea. This will make a provider even more vulnerable for attacks to it's network as it is now. I do realize that research on the networks has its advantages, but making providers to vulnerable to the internet itself is not an issue.

Topics not mentioned in this article

- *Influence of very large companies on implementing technology*
  Large companies such as Cisco,Microsoft, Juniper,Intel etc. that produce devices that 'run' the internet are able to control or slow down the implementation of new technologies. For example: Cisco does not come with IPv6 support in it's routers.

  Somehow, the (negative) influence on research or implementing new technologies by large companies should be controlled. This will prevent a delay in the evolution of the Internet.

- *Rules and planning on implementing new technology*
  Implementing for example IPv6 has such a great impact on the devices connected to the internet that it is preferable to have a set of rules and planning. Maybe this has to be supervised by the government?