The.nlyst

No 3, Q2 2011

The.nlyst

THE IP ADDRESS PROBLEM

The pros and cons of a temporary solution

Over the last few years, there have been increasingly frequent media references to IPv4 addresses running out. Without new IP addresses, difficulties would soon arise and unrestrained growth of the internet would come to an end. However, the IP address problem is nothing new. It has been with us for nearly twenty years. During that time, everything has been kept running smoothly by a number of temporary workarounds. However, the success of those emergency measures is now hampering the introduction of a structural solution: IPv6.

Unique identification codes

Billions of machines are connected to each other via the internet. They include everything from computers and web servers to mobile phones and digital cameras. And they all send information to one another. To ensure that sent information arrives at the right machine, each device has a number, called an IP address. Like domain names and phone numbers, IP addresses have to be unique.

The principle that each connected device has its own unique IP address is referred to as end-to-end connectivity. Developed in the early 1970s, the end-to-end connectivity concept was one of the basic principles underpinning the internet's design. The idea behind it is that network intelligence is best positioned at the periphery, in the 'end devices' that run the applications. The role of the intermediate equipment is merely the efficient transmission of data packages. Not until the point of delivery are the separate packages combined to form a coherent body of data that an application can make use of. Having the internet set up this way is the most efficient arrangement.

Growth and shortage

With a view to giving every device its own unique IP address, version 4 of the Internet Protocol was developed in the 1970s using a 32-bit system. This allowed for the creation of nearly 4.3 billion IPv4 addresses. At the time, that sounded like enough addresses to last for ever. Little did the protocol's inventers realise what the future held. The internet grew beyond anyone's expectations, so that even in the late 1980s

IANA

IP addresses are assigned under the auspices of IANA, the Internet Assigned Numbers Authority. IANA gives large blocks of addresses to RIRs (Regional Internet Registries). The RIRs then divide up those blocks between the affiliated LIRs (Local Internet Registries). Finally, the LIRs allocate the addresses to users. Users can't choose their own IP addresses; that could interfere with the smooth running of the internet. On 3 February 2011, IANA assigned the final remaining IPv4 address blocks to the RIRs. There should be enough addresses in the system to enable user assignment to continue for a while, possibly until 2013.

Foreword

On 3 February 2011, IANA assigned the last remaining IPv4 addresses to Regional Internet Registries (RIRs) such as RIPE-NCC. Without some way of generating more addresses, the end of IANA's IPv4 stock would ultimately have had serious implications. Once the RIRs and ISPs had used up the addresses assigned to them by IANA, further growth of the internet would not have been possible. When it was first realised, twenty years ago, that the supply of IPv4 addresses would run out at some point, Network Address Translation was thought to be the solution. However, as this edition of The.nlyst explains, NAT would have afforded only a temporary respite. The long-term answer to the internet address problem is IPv6. The main difference between IPv4 and IPv6 is the number of possible addresses. IPv4 is a 32-bit system, which can generate enough addresses for 4.3 billion machines to connect to the internet. By contrast, IPv6 is based on 128-bit technology, enabling it to generate an almost infinite number of addresses. With IPv6, it is unlikely that the internet will ever run out of addresses. However, in 1977 people thought the same about IPv4, of course.

IPv6 is important to SIDN, as it is to all registries. We are responsible for the registration and performance of all .nl domain names. On its own, though, a unique domain name is not enough. Without that other unique identifier, the IP address, e-mails wouldn't arrive in the right mailboxes, people couldn't find the websites they wanted and smartphones couldn't connect to the internet. We therefore attach a great deal of importance to a smooth transition to IPv6. SIDN is committed to the development of the internet, and protocol migration problems could threaten that development.

Against that background, SIDN has been internationally involved with the introduction of IPv6 for some years – through active participation in the RIPE and IETF communities, for example. In the Netherlands, we sponsor the IPv6 Awards, which recognise the achievements of IPv6 trendsetters and thus focus attention on the new protocol. In 2010, XS4ALL won the SIDN-sponsored Internet Service Provider category award for taking the initiative to offer its clients native IPv6. Fortunately, more and more ISPs and registrars are following suit. SIDN itself now operates largely on IPv6. Our name servers, websites and DNS check are all IPv6-ready. The registration system and Whois will follow in the course of 2011.

Finally, I would like to draw your attention to the .nl domain's silver jubilee. Our national domain is 25 years old –quite an age in the world of internet- and a variety activities that pay tribute to its success are planned, starting on 26 April 2011. Details are available at www.de25jaarvan.nl and, of course, in a later edition of The.nlyst.

Roelof Meijer

CEO, SIDN

people began to fear that the world would run out of IP addresses. Vinton Cerf, one of the people behind the Internet Protocol, said in 2011: "I am a little embarrassed about that, because I was the guy who decided that 32-bit was enough for the Internet experiment. My only defense is that that choice was made in 1977, and I thought it was an experiment. The problem is… the experiment didn't end."

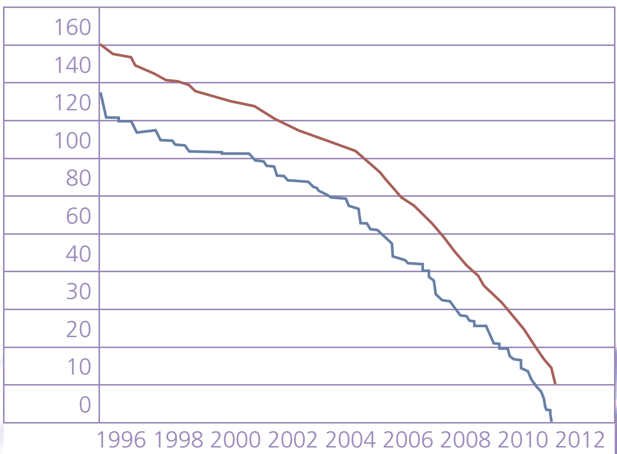
The IP address problem is not new

In 1991, the Internet Architecture Board, part of the IETF, published a review document, RFC1287, which warned about an IP address shortage. Although no specific solutions were put forward, a number of general options were identified. One was increasing the scope for address creation by bolting additional bits onto the basic 32-bit model. Another idea was the method ultimately to become known as NAT (Network Address Translation), which was developed further in a later document (RFC1335). A whitepaper published in 1993 eventually led to a new informative document, RFC1631 (in May 1994), in which NAT was first properly defined. Notably, this RFC begins by pointing out that an IP address shortage may develop and that a structural solution should be sought. NAT was presented as a short-term solution, for use until a much higher-capacity addressing system became available. NAT's interim character is an important historical fact.

Network Address Translation (NAT)

NAT makes it possible for many internet-connected computers to share a single IP address. The machines in question are assigned non-unique IP addresses, known as 'internal addresses'. Special address series are reserved for this purpose (see, for example, RFC1918). Between these machines and the internet is a NAT device, which does have a unique IP address and is connected directly to the net. The routers that

Legend	Free/8
(blue)	IANA
(red)	RIR pool + IANA



Vinton G. Cerf, 'father of the internet'

many people use to connect their home computers, tablets and smartphones to the internet are NAT devices. A NAT device has both an internal address and an external address and handles the translation of internal addresses into external addresses and vice versa. NAT therefore constitutes a departure from the end-to-end connectivity principle.

The advantage of NAT is that for every unique IP address you can have dozens – sometimes hundreds – of computers with internet access. So it reduces the demand for unique IP addresses enormously. However, NAT does have its disadvantages, especially for use in combination with protocols that work on the basis of end-to-end connectivity and make no allowance for IP address translation. If a computer is going to offer an internet service – operate as a web server or mail server, for example – having a NAT device between the computer and the internet can create a lot of sometimes insurmountable technical challenges. Problems can also arise with some peer-to-peer applications, VoIP applications and online games. So, for example, a teleworker may not be able to connect to his/her employer's mail server via a VPN link, because the server's address is in the same IP address series as the worker's laptop. The router does not recognise that a remote address is being sought, requiring a connection to be effected over the VPN system.

Disagreement

Although the use of NAT became increasingly common in the early 1990s, most IETF participants favoured seeking a structural solution in the form of a next-generation Internet Protocol (IPng). In the latter part of 1993, a newly formed IPng working group accordingly started on the development of IPv6, the successor to version 4 of the protocol. The initiative,

coupled with a more cautious approach to IP address allocation and certain other measures, was expected to ensure that a solution to the address problem would be ready in plenty of time.
Meanwhile, more and more NAT applications were appearing. NAT was proving to be an excellent way of connecting more systems to the internet without undue hassle. NAT was therefore an ideal solution at a time when internet service providers (ISPs) found it hard to get hold of IPv4 addresses in any great quantities. `End users weren't normally inconvenienced by having just one unique IP address and had no problem giving complete PC networks access to internet. So the years went by. All the time that IPv6 was under development, NAT was a huge success. So successful, in fact, that the supply of IPv4 addresses was made to last a lot longer than had at one point seemed likely. Contrary to previous predictions, it was not until 3 February 2011 that the last IPv4 addresses were assigned. NAT had enabled the internet to keep on growing at an extraordinary rate throughout the intervening years. Its effectiveness also diminished the urgency of IPv6 adoption, which was consequently put off longer and longer. In other words, the very success of NAT gave rise to problems.

Interim solution becomes established

NAT has therefore been in use for so long that an entire generation has grown up with it. Ironically, most members of the 'internet generation' – quite possibly including you – have never been connected directly to the net at all. It is very common to have a NAT device between a home computer or office workstation and the internet. End-to-end connectivity, once a foundation stone of the internet, is for many people nothing more than an abstract concept. The problems associated with NAT are circumvented with varying degrees of success by port forwarding, 'smart' firewalls, external STUN-servers and countless other tricks and gadgets. The ingenuity of these workarounds often prevents us seeing just how much more complex NAT has made the internet. Some people argue that NAT contributes to network security, but experts agree that it provides only an illusion of security. Meanwhile, fewer and fewer people recognise NAT for what it has been from the start: an interim arrangement introduced to buy time while a new higher-capacity addressing system (IPv6) was developed. NAT did not therefore ever become an official standard.

The IETF and its RFCs

The Internet Engineering Taskforce (IETF) develops and promotes internet standards. It is an open organisation, with no formal membership requirements. Decisions are made on the basis of rough consensus (and running code). SIDN is an active participant in the IETF, particularly in DNS-related working groups.
The IETF publishes RFCs ('Requests for Comment'). RFCs may relate to internet standards or to other matters. Some RFCs are therefore purely informative.

What next?

The internet is far from done growing. With ever more mobile devices entering use and development of the 'internet of things', the demand for IP addresses is set to go on increasing. Fortunately, we already have a structural solution in the form of IPv6. That is not to say that by switching to the new protocol, we will resolve all our IP-related problems at a stroke. For one thing, IPv6 is not compatible with IPv4. Each version of the protocol is associated with its own distinct world. And, because the changeover to IPv6 has proved so protracted, IPv4 will probably still be around for years. But is that a good reason for clinging on to an outmoded protocol? A move away from NAT will ultimately be needed in any case, because the system assumes that every end user can at least access the net via a NAT device with a globally unique IP address. At the current rate of growth, the time will soon come when that is no longer possible. Only IPv6 can then satisfy the long-term demand for addresses. However, although the big ISPs have already made the switch to IPv6, many hosting firms and ISPs catering for private customers are delaying. It is very important that these organisations think very carefully about the options open to them.

Option 1: higher-level NAT

No business can turn away prospective customers, but giving every new end user a unique IPv4 address simply isn't possible. The solution is NAT, but at a higher level in the system, enabling a very large number of end users to share a unique IPv4 address. This arrangement is sometimes referred to as

'carrier-grade NAT', or 'large-scale NAT'. Unfortunately, it implies the gradual escalation of NAT's inherent drawbacks. What's more, without special translation systems, users remain isolated from the inexorably expanding world of IPv6. The general assumption is that, in the long term, the NAT path must lead to a dead end.

Option 2: invest in IPv6

IPv6 is ready to use right now. Affordable hardware and software that support the new protocol have been available for some time. Although it isn't yet in very widespread use, IPv6 is gaining considerable ground year on year. Also, the adoption of IPv6 enables a return to the old principle of end-to-end connectivity. That will take some getting used to; there will have to be a fundamental rethink of network security, for example. However, the inconvenience is outweighed by the many advantages. IPv6 is an attractive and future-proof solution. What's more, good techniques are available (such as NAT64 and DNS64, based on NAT) that make it possible to create a bridge between the new IPv6 world and the legacy IPv4 protocol. Investing now in IPv6 therefore makes sense.

Conclusion

Policy-makers tend to be somewhat indifferent to warnings about IPv4 addresses running out. That is not surprising, given that those warnings have been common currency for twenty years, during which time the internet has continued to thrive. It is hard to square the huge growth and evident adaptability with alarming statements about there soon being no more IP addresses. Hopefully, this article has explained why there are genuine grounds for concern and how the internet has managed to cope for so long by adopting a series of temporary workarounds, of which NAT has been the most successful.

The last of the IPv4 addresses really have now been allocated to the RIRs. The time that NAT bought us is all but spent. Before long, the internet will not be able to grow any further using IPv4. And there are various developments in the pipeline that will stimulate demand for addresses. Putting off the inevitable a little longer using techniques such as carrier-grade NAT is simply not a sensible approach. The only real way forward is IPv6.

Many readers of The.nlyst are to some degree dependent – financially or otherwise – on the existence of a reliable, stable and unconstrained internet, which can go on growing into the future. Securing that growth will require collective commitment, and all parties must accept their responsibility. SIDN is seeking to do just that by, for example, promoting and supporting the use of IPv6.

IPv6 World Day

On 8 June 2011, various leading companies will be demonstrating their commitment to a future-proof internet at the IPv6 World Day. For 24 hours, they will be showing that they are ready for IPv6 by taking part in a global IPv6 experiment. In the Netherlands too, various things will be happening that day. You can join in by, for example, making sure that you are IPv6-enabled before the big day arrives. Options for getting IPv6 support include applying to your ISP or a tunnel broker for native IPv6 or an IPv6 tunnel. Before long, consumers who are buying new hardware will also be well advised to check whether it is IPv6-compatible.

More information:

http://www.ipv6dag.nl/
http://www.ripe.net/internet-coordination/ipv6
http://www.ipv6-taskforce.nl/
http://isoc.org/wp/worldipv6day/

Internet of things

In the future, all kinds of devices are expected to be connected to the internet and to each other. Sensors, thermostats, refrigerators, scales, toys and alarm systems, to name just a few. There will be nano devices that monitor our vital signs and alert a doctor if there is anything untoward. Domestic appliances will connect to a 'smart grid' via smart meters, and will switch themselves on when electricity is cheapest. Car tyre sensors will relay data to an onboard computer, enabling it to adjust the braking system to compensate for under- or over-inflation. It will, in short, be an 'internet of things'.

.NL Analysed

.NL Analysed features facts and figures that shed light on national and international developments involving the .nl domain and the world in which we operate. Different topics will be covered in each edition. If there is anything that you feel we should focus on in .NL Analysed, please send your suggestions to communicatie@sidn.nl.

TLD top 25 ranking Q1 2011

	TLD		Count Q1*	Growth	
1	.com	Generic	93,956,551	2.7%	=
2	.de	Germany	14,311,082	1.9%	=
3	.net	Generic	13,826,975	1.9%	=
4	.uk	United Kingdom	9,317,393	3.5%	=
5	.org	Generic	9,094,389	3.7%	=
6	.info	Generic	7,657,006	5.3%	=
7	.nl	Netherlands	4,367,635	4.2%	↑
8	.cn	China	3,388,575	-22.1%	↓
9	.eu	European Union	3,381,398	1.5%	=
10	.ru	Russia	3,249,139	3.9%	=
11	.br	Brasil	2,412,455	4.0%	=
12	.ar	Argentina	2,280,825	2.6%	=
13	.it	Italy	2,148,180	4.7%	=

	TLD		Count Q1*	Growth	
14	.biz	Generic	2,082,948	1.7%	=
15	.pl	Poland	2,072,751	4.0%	=
16	.au	Australia	2,030,277	4.6%	=
17	.fr	France	1,985,298	4.6%	=
18	.us	United States	1,679,071	4.2%	=
19	.ca	Canada	1,654,702	4.9%	=
20	.ch	Switzerland	1,563,262	2.5%	=
21	.es	Spain	1,295,217	2.2%	=
22	.jp	Japan	1,210,843	1.1%	=
23	.be	Belgium	1,127,628	2.4%	=
24	.dk	Denmark	1,115,408	1.8%	=
25	.kr	Korea	1,085,013	0.8%	=
	*By March 31, 2011				

The .nl domain's strong growth over the last quarter has enabled it to move up a place in the global TLD 'league table', overtaking China's national domain. Although .cn shrank by nearly a million domain names, it looks as though its period of contraction has now ended. For the first time in fifteen months, .cn has started to grow again albeit only slightly. Otherwise, the top 25 TLDs remained in the same order as before. Next quarter, however, things are set to change. South Korea's .kr has come under further pressure and is very likely to lose 25th place to .se when the next quarterly figures are published. In addition, .biz is about to surrender 14th spot to .pl.

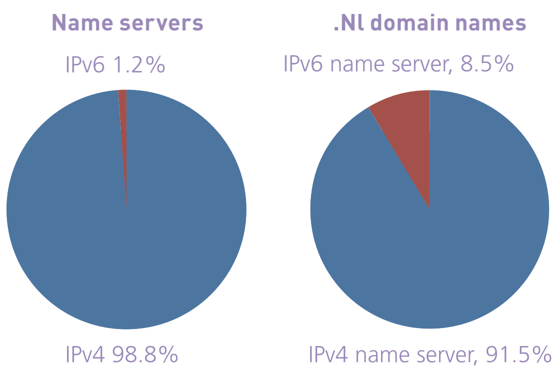
IPv6 support

Name servers

As the diagram shows, the proportion of name servers in the .nl zone that can currently be contacted using IPv6 is still very low, at 1.2%. Nevertheless, that figure is a 151% increase on a year ago, when the percentage of name servers with IPv6 support was just 0.5%. Clearly, though, there is a long way to go. At the current rate of expansion, it will be the middle of 2021 before all name servers in the .nl zone support IPv6.

Domain names

Although the name servers using IPv6 account for only 1.2% of all the name servers, they represent a substantially larger portion of .nl domain names: 8.5% of all .nl domain names have at least one IPv6 name server. However, the annual rate of increase is not as strong as it might be, at 19% over the last twelve months.



Unreachable .nl domains

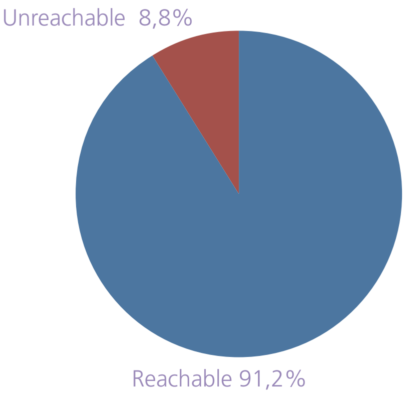
Fortunately, the vast majority of .nl domains – more than 90 per cent – are reachable. The rest are unreachable either because no website has been configured, or because there are DNS errors or HTTP errors associated with the name. An unreachable domain isn't necessarily non-operational; it may be used purely for e-mail or FTP, or may have simply been 'reserved' (e.g. for a planned campaign or a business start-up).

Nearly a third of the unreachable domains are unreachable because no web server has been configured for the name. Another third are unreachable because of a DNS configuration error, which prevents the domain ever being reached.

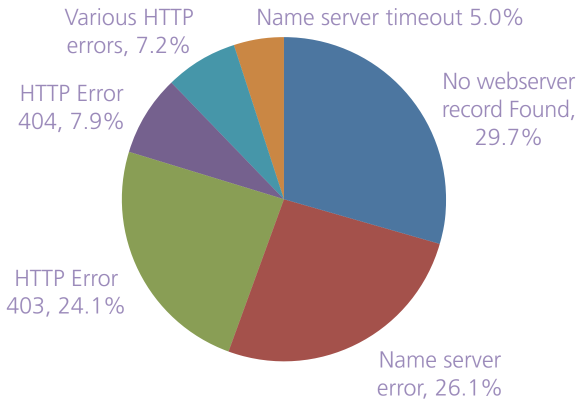
And, in some cases, a domain merely appears unreachable. That is the case, for example, if a valid request is sent, but access is denied for whatever reason, resulting in the familiar HTTP 403 error message.

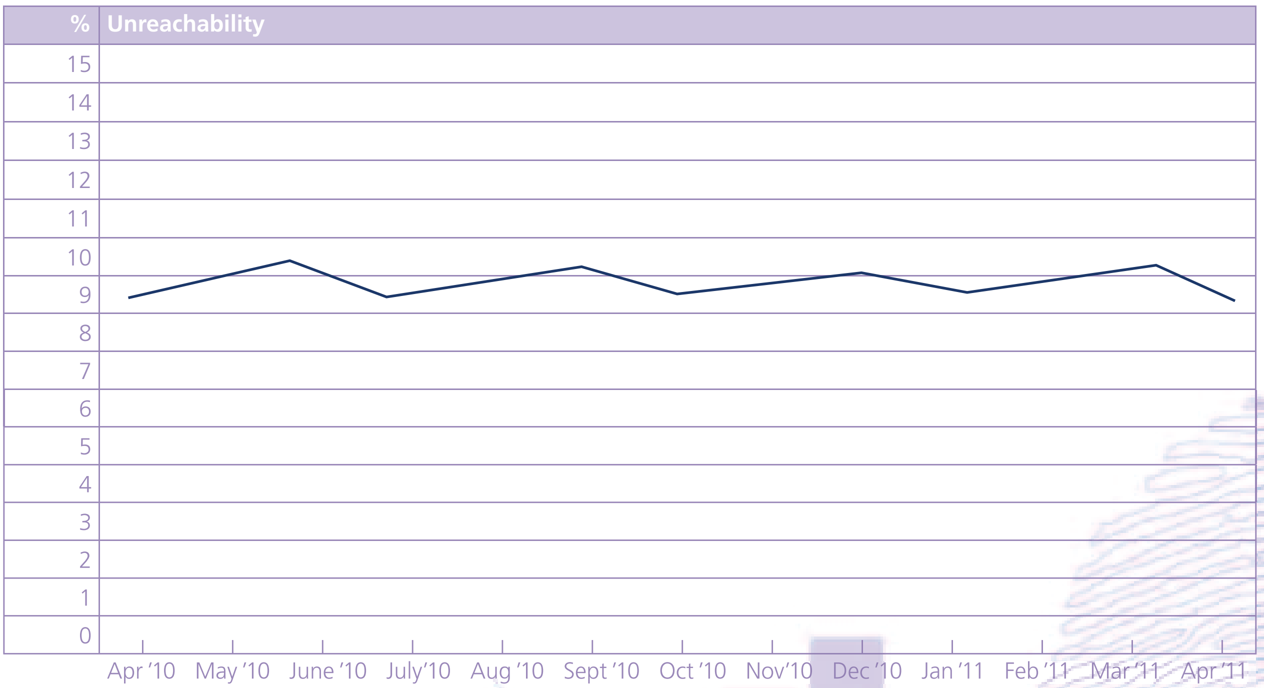
The percentage of unreachable domain names has in recent years remained fairly stable. However, there is always a rise in the percentage towards the end of each quarter. This is likely to be linked to the cancellation cycle: the content and name servers are removed before the domain name is formally cancelled with effect from the end of the quarter.

Reachability of .nl domain names



Unreachable .nl domains





Did you know...?

Facebook

An easy way to check whether your internet service provider already gives you IPv6 support is to try visiting a website that can only be reached using IPv6. The popular social networking platform Facebook has for some time operated a website www.v6.facebook.com. If you have IPv6 support, you will be able to view the site; if you don't have the necessary support, you will get the message 'Server not found'. A neat detail: Facebook's IPv6 address is 2620:0:1cfe:**face**:b00c::3.

IPv6 on 'apply or explain' list

The Dutch government has what is known as an 'apply or explain' list of open standards. This means that whenever a government body is planning to purchase an ICT product or service, it has to either go for an option that applies the listed open standards, or it has to explain why it hasn't done so. IPv6 has been included on the list for some time, in order to encourage government bodies to make the switch to the new protocol.

Event calender

SIDN frequently sends representatives to national and international congresses. We undertake these activities in our capacity as the registry for the .nl domain and the Dutch ENUM zone. In doing so, we seek to represent the Dutch internet community and our registrars. In addition, we ourselves organize regular gatherings for our registrars.

In the coming months, SIDN is represented at the following conferences:

Date	Event	Place
07-06 to 08-06	23rd Centr Admin Workshop	Trondheim, Norway
08-06	World IPv6 day	Amsterdam, The Netherlands
08-06 to 09-06	45th CENTR GA	Trondheim, Norway
10-06	NL IGF Event	Den Haag
19-06 to 24-06	41st ICANN Meeting	Singapore
19-06 to 24-06	EURO-SSIG	Meissen, Germany
24-07 to 29-07	81st IETF	Quebec City, Canada
26-09 to 30-09	IGF KENYA 2011	Nairobi, Kenya

The .nlyst

In the next issue:

- the (Dutch) Internet Governance Forum
- ages of .nl domain names

Colophon
The.nlyst is a platform for information about (.nl) domain names. It is published four times a year and distributed free of charge to associates of SIDN.

Editorial address
SIDN
PO Box 5022
6812 AR ARNHEM, the Netherlands
communicatie@sidn.nl

Additional input
Marco Davids, Jaap Akkerhuis, Miek Gieben, Lycke Hoogeveen, Roelof Meijer, Sieger Springer, Sean Schuurman van Rouwendal, Martin Sluijter

Design & production
ARA Direct, Rotterdam – www.ara.nl

Translations
G & J Barker Translations – www.gandjbarker.co.uk

Print run
Approximately 3000

Subscriptions
The.nlyst is distributed free of charge to associates of SIDN. If you wish to be added or removed from the distribution list, please contact communicatie@sidn.nl.