Evaluating the Progress towards IPv6 Implementation

Best Practice Document

Produced by CESNET-led Working Group
on Network Monitoring
(CESNET CBPD118)

Author: Martin Pustka
September 2011

Document No:	GN3-NA3-T4-CBPD118
Version / date:	September 1, 2011
Original language :	Czech
Original title:	English title
Original version / date:	September 1, 2011
Contact:	martin.pustka@vsb.cz

CESNET bears responsibility for the content of this document. The work has been carried out by a CESNET led working group on IPv6 as part of a joint-venture project within the HE sector in the Czech Republic.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Introduction

IPv6 implementation can be evaluated by many approaches, but none of them, in and of themselves, describe the actual state of the implementation in the network exactly and objectively, in comparison with other networks.

The implementation of IPv6 involves more than just setting it up on active network components but also includes its practical application in workstations and server systems. For this reason, characteristics need to be defined that best reflect the degree of IPv6 implementation in the relevant networks and that can be collected automatically.

Procedures are proposed in this document that can be centralised and integrated and that can be applied within the NREN network.

One of the targets of the methodology is to define those procedures that enable the greatest automation of the collection of data and that minimise the resources required for their collection. This monitoring should also be realised centrally, within the NREN network.

1 Characteristics of an Academic Network

Academic and university networks are typically connected into the national core network (NREN), which provides Internet for all of its members and all connected networks. This enables a relatively simple and centralised overview of data, without the need for direct participation of the end networks. This is particularly beneficial for institutions that are not properly equipped or that lack experience in the advanced monitoring of network operations. This also makes it possible to integrate all of the methods and procedures required to evaluate IPv6 implementation across the networks of connected academic university institutions.

Academic networks have different types of users - employees (teaching, research, and administrative) and students. Students usually make up the bulk and the most significant group of active IT users. Almost all of them work actively with computer equipment, so their number can be used as a parameter to define the institution's size.

2 Network and Institutional Records

For continued monitoring of the progress of IPv6 implementation in the individual networks, record keeping of the monitored networks must be implemented. The following data is the minimum that must be recorded for these institutions:

- the name of the institution;
- the IPv6 address range;
- the domains that contain the required information about the infrastructure
- the DNS servers that provide access to the contents of the domain;
- a parameter describing the institution's size (such as the number of users).

This list must be updated constantly, since the information changes over time.

Practice has shown it is worthwhile to automatically monitor changes in WHOIS databases. Usually the NIC operator of the national core network is responsible for administering the allocation and use of IPv4/6 addresses. Because of this, data in the RIPE database can be considered as authoritative, without the need to update it or compare it against other records.

3 Characteristics Describing the Extent of IPv6 Implementation in the Network

The extent of implementation can be evaluated from several perspectives:

- the expansion of IPv6 infrastructure within the network;
- support of transitional mechanisms;
- the expansion of central server services;
- an increase in the number of in end stations;
- the number of AAAA records in DNS domains;
- the volume of traffic.

3.1 Network Infrastructure: the Number of End IPv6 Networks

The current practice is to award end institutions with 48 bit prefix addresses. After this, the individual institution end subnets are awarded 64 prefix address blocks. Therefore, the number of subnets with a 64 prefix length indicates the degree of expansion of the IPv6 network infrastructure.

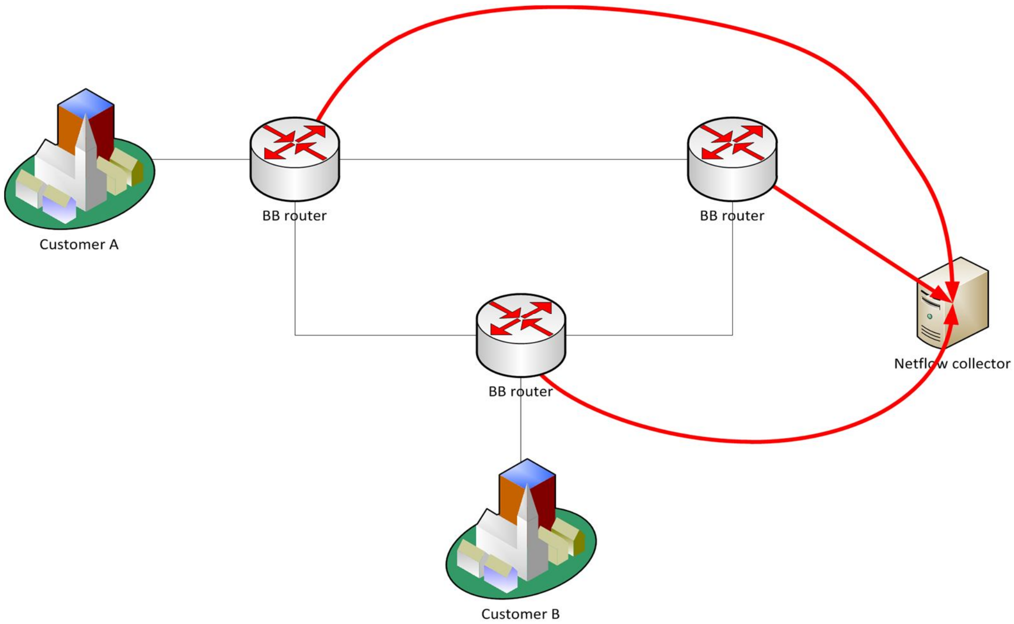
Further expansion or use of address space can be accomplished in two ways. The first option is to consider the use of a network with 64 bit prefix in DNS. However, even though end stations might have IPv6 addresses, they are not integrated into DNS, making this technique less than effective.

A better solution, although technically more difficult to implement, is to monitor active addresses, which can be acquired from the NetFlow statistics of the core network routers of the NREN. Even though an IPv6 address does not always belong to a single machine, the list of active addresses can serve as a good basis to determine the number of subnetworks.

These days, most NREN networks collect some form of statistics of generated traffic, usually based on NetFlow technology. If we use these core statistics, aggregated according to an IPv6 subnet, we can easily acquire a list of end IPv6 networks.

Routers are usually able to export traffic information. The NetFlow protocol, developed by Cisco Systems and standardised in RFC 3954, can also be used for this purpose. Routers regularly send statistical information about the through-traffic to collectors on the network. This data can be aggregated in such a way that it can record source IPv6 addresses from defined ranges of connected networks sufficiently and from the recorded addresses, use only those within the network (those with first 64 bit IPv6 addresses).

If we use routers of core network operators (NREN) for this purpose, no active participation by the monitored network is necessary, because the NREN has precise statistical information that can be monitored and evaluated over time.



3.2 Support of Transitional Mechanisms

Transitional mechanisms are primarily used during the initial phase of implementation of the IPv6 protocol. In practice, their use has proved justified.

The existence of an ISATAP server can be confirmed by a DNS query to FQDN isatap.<domain>. This DNS record usually serves internal network needs and can be filtered. In practice, such filtering is not usually applied. If it is applied, the active participation of the monitored networks is not necessary.

3.3 Central Server Services

This area focuses on the type and number of implemented server services and reflects the degree of implementation and accessibility of IPv6 services within the network's central infrastructure. Therefore, the following are recorded:

- the NS domain records of institutions referring to IPv6 addresses;
- the MX domain records of institutions referring to IPv6 addresses.

DNS is the source of such information. All records should be accessible with common DNS queries. The exception to this rule would be the ISATAP.<DOMAIN> DNS record, which may be filtered out, although this is rarely done.

For this method, the active participation of the monitored networks is not usually necessary.

3.4 End Stations

The number of end stations in operation in the computer network is most certainly an interesting statistic, but these statistics can be relatively difficult to obtain. The first complication is that many operating systems change their IPv6 address regularly, so that, over a period of time, one station can generate several addresses.

Another possible statistic is the number of end stations shown in AAAA records from DNS. DNS zone transfers are required in order to acquire AAAA records, but this transfer is often blocked, so access to the zone must be granted by the DNS administrator. However, even this list is not always accurate because the station within the DNS may not be listed due to the constantly changing addresses, even though it has adopted IPv6.

The main reason for not implementing AAAA station records into DNS is the practical necessity to autoconfigure the end stations. During autoconfiguration, end stations change their addresses over time, so the only option is to update the DNS zones of the end station dynamically. The problem is that only a very limited number of computer networks actually support the dynamic updating of DNS zones.

In this case, the active participation of the monitored networks is necessary.

3.5 Volume of Traffic

Traffic volume is a major characteristic that can reveal the extent of the application of the IPv6 protocol. Technically, it is possible to determine the volume of traffic from the router statistics of an NREN end station.

It makes sense to compare the volume of IPv4 and IPv6 traffic of the institutions in order to monitor developing trends in traffic volume.

For this monitoring, the active participation of the monitored networks is not usually necessary.

3.6 Difficulties

Some institutions may have a complicated internal network structure. For example, universities may be divided into different faculties, which operate their own end stations. In these cases, it would not be possible to find the DNS records of second-order domains, which may make it appear that the institution does not have a well-supported IPv6 implementation. It is also possible that the IPv6 implementation in the individual subnetworks (such as in faculties) is different.

In such cases, one would have to consider whether to include the individual subnetworks into the total, or to treat the institution's entire network as a single unit.

4 Evaluating the Progress towards IPv6 Implementation

When monitoring expansion and implementation, it is necessary to collect specific data regularly, which produces the following types of document:

- a comparison of IPv6 implementation at different institutions;
- an overview of an institution's progress over time.

Textual reports can be supplemented with graphical representations. When comparing institutions, it is advisable to compare the networks that are similar in character, scope and number of users.

The human factor is significant when evaluating. It is advisable to compare not only absolute values but also relative ones, when equivalent values are compared under IPv4.

4.1 How Not to Evaluate

When comparing the state of networks among institutions of different sizes, the comparisons should take the difference in size into consideration. The progress in absolute terms may appear to be less in a small network than in a larger network, but their implementation of the IPv6 protocol in end networks of the small network may be relatively larger.

Sometimes it is not possible to compare IPv6 to IPv4. If we attempt to collect data automatically, independent of information provided us by administrators of the end networks, we may find that some networks may or may not use NAT technology. Therefore, this is not an advisable approach.

Comparing the number of IPv6 and IPv4 subnets in individual networks is also not advisable, because some networks divide themselves into subnetworks by different means. In IPv6, each end subnetwork uses 64 bit length masks, while in IPv4 a subnetwork can use a different network mask. This makes the estimation of the number of IPv4 subnetworks rather difficult, and thus, comparing networks in this manner is also not advisable.

4.2 Evaluating the Number of End Networks - a Mathematical Model

Mathematical models require the quantification of measurable values. The following values must be obtained for each monitored network:

- the number of end IPv6 subnetworks with a prefix of length /64;
- the number of users.

The number of users reflects the size of an institution. These details are required when comparing individual institution networks. This data can usually be obtained from publicly accessible sources (such as the number of employees or students), or by direct query to the institution.

As has already been mentioned, the number of end IPv6 subnetworks can be obtained from network traffic statistics on the national core network.

These two fundamental peaces of data can help determine the *computer network score, SC.* In this formula, we divide the number of 64 bit prefix length IPv6 subnetworks $NETS_i(t)$ by the size of the institution $S_i(t)$, which in our case, is the number of network users. The same calculation can be made for all institutions.

$$SC_i(t) = \frac{NETS_i(t)}{S_i(t)} \quad (1)$$

We calculate the *SC* for all institutions and then the *Average Score* SC_{avg} of all compared institutions:

$$SC_{avg}(t) = \frac{1}{N(t)} \sum_{i=0}^{N} SC_i(t) \quad (2),$$

where N(t) is the number of institutions during the monitoring period and $Sc_i(t)$ is each institution's score during the monitoring period.

From the above formulae, we get a numerical rating of the *SC* of each institution and the average SC_{avg}. For a more appropriate evaluation and, subsequently, an easier comparison, we propose the table below, which categorises the networks of the individual institutions into groups:

Rating	**Required Score**
RATING-A+	$SC_{avg}(t) * 1.5$
RATING-A	$SC_{avg}(t) * 1.25$
RATING-B+	$SC_{avg}(t) * 1$
RATING-B	$SC_{avg}(t) * 0.75$
RATING-C+	$SC_{avg}(t) * 0.5$
RATING-C	$SC_{avg}(t) * 0.375$
RATING-D+	$SC_{avg}(t) * 0.25$
RATING-D	$SC_{avg}(t) * 0.125$
RATING-0	0

The division is not linear so the progress of institutions which are beginning to implement IPv6 is more visible.

To prevent confusion between evaluations across different groups of institutions, the rating should be labelled according to the measured group, such as, CZEDU-A+ or EUEDU-A+.

5 Conclusion

The proposed method is suitable for comparing similar types of institution, but may not yield accurate values comparing different networks in different types of institution. The success of this method increases with an increase in the number of compared networks and could be applied for the record keeping and comparison of academic networks across Europe.

These procedures and methods could also be applied to non-academic institutions, although a different method would need to be chosen, in particular, taking the size of the monitored networks into consideration.

Obtaining the necessary data can be automated relatively effectively and manual updating does not need to be performed often. A great advantage is that the results are not dependent on data provided by the institutions. It requires only simple and one-time technical participation of the institutions (permitting the transfer of zones to the DNS servers).

This method will produce an overview and a comparison of individual institutions. The approach not only examines each institution but, thanks to the comparison, it also indicates their progress in the implementation of IPv6 compared with other institutions ranked in the same category of the overview.

6 Appendix 1: Institutional overview

Records should be kept in order to develop an overview of the individual institutions and their progress. This sample shows an *Institutional Overview,* which includes the necessary technical and administrative data, as well as determined states. A quick glance at this sheet will provide the necessary information on that institution's progress towards and support of IPv6. The overview shown here depicts a non-existent institution.

Institution

DNS servers for AXFR:	dns1.domain.eu / 1.2.3.4
Searched names:	domain.eu
IPv6 address range	2011:0004:cafe::/48
Contact person	Stojan Jakotyč, Stojan.Jakotyc@domain.eu phone 123 456 789
Institution size (number of users)	12345 (31.2.2011)

Centralised Services

Service	**State**
ISATAP	Yes, since 2010/10
WWW	No
NS	Yes, since 2010/12
MX	No

Date	**COUNTRY-Rating**	**IPv6 Subnets**	**Services**	**Comments**
1 January, 2011	A	15	-	
1 February, 2011	A+	17	-	
1 March, 2011	B	17	NS	
1 April, 2011	B+	18	NS, WWW	

7 Appendix 2: Rating Academic Institutions in the Czech Republic

This annex describes a one-month rating of institutional academic networks in the Czech Republic. This method has been used in the Czech Republic for several months to compare the implementation of IPv6 in the networks of academic institutions.

The data was obtained automatically from DNS and from NetFlow statistics provided by CESNET as an operator of the national research network, connected to the CESNET2 network or the Internet of university and other academic networks.

The size of an institution is rated by the number of its employees and students. This data was obtained from official sources published by the Ministry of Education, Youth and Sports.

For illustration, only a few groups and categories of institutions have been selected for the table.

Institution / Network	Number of Users	IPv6 Network	Score (*10^{-3})	CZEDU Rating
VUTBR	22849	99	4.33	CZEDU-A+
TUL	10389	31	2.98	CZEDU-A+
CVUT	23059	57	2.47	CZEDU-A
VSB	23159	42	1.81	CZEDU-B
VSE	19401	32	1.65	CZEDU-B
SLU	9187	15	1.63	CZEDU-B
CUNI	53466	39	0.73	CZEDU-C
...				

The average score was calculated as: SC_{avg} = 1.849.

The following table depicts the values of individual groups with their calculation:

Rating	**Score**	**Score Value**
CZEDU-A+	$SC_{avg}(t)$ * 1.5	2.77
CZEDU-A	$SC_{avg}(t)$ * 1.25	2.31
CZEDU-B+	$SC_{avg}(t)$ * 1	1.85
CZEDU-B	$SC_{avg}(t)$ * 0.75	1.39
CZEDU-C+	$SC_{avg}(t)$ * 0.5	0.92
CZEDU-C	$SC_{avg}(t)$ * 0.375	0.69
CZEDU-D+	$SC_{avg}(t)$ * 0.25	0.46
CZEDU-D	$SC_{avg}(t)$ * 0.125	0.23
CZEDU-0	0	0

The data was obtained from statistics provided by the operator of the CESNET2 core network, generated from NetFlow statistics for the relevant calendar month. The resulting data was aggregated according to an IPv6 network of 64 bit prefix length and those networks, in turn, were assigned to the individual institutions/networks.

SC values were then calculated for the individual networks, and from these values, the SC_{avg} value was calculated.

Finally, concrete ratings were assigned to the individual institutions based on the scores attained.