Working for the Internet

LINX — Est. 1994 —

Public consultation on draft BEREC Guidelines on implementation of net neutrality rules

Submission by the London Internet Exchange Ltd ("LINX")

London Internet Exchange Ltd

London Office: 24 Monument Street London EC3R 8AJ United Kingdom • Tel: +44 20 7645 3500
Peterborough Office: Trinity Court Trinity Street Peterborough PE1 1DA United Kingdom • Tel: +44 1733 207700
Email/SIP: info@linx.net Web: www.linx.net Fax: +44 20 7536 0720

Registered Office: Trinity Court Trinity Street Peterborough PE1 1DA United Kingdom • Registered in England and Wales: 3137929

About LINX

1. The London Internet Exchange (LINX) is the UK's largest membership association for Internet Service Providers and other major network operators.

2. We provide interconnection services and public policy representation to over 700 members across 68 countries. These include most major UK ISPs and most European former incumbents, and many other European operators of varying sizes.

3. LINX promotes discussion of cybersecurity best practice at our quarterly member meetings, and through participation in European Internet community institutions such as Euro-IX, RIPE and EuroISPA.

4. LINX is therefore well placed to present the views and interests from the Internet network operator industry, and to advise BEREC on relevant technical and cybersecurity issues.

Address spoofing and best current practice for prevention of DoS attacks

5. We would like to emphasise that LINX takes no position on the desirability or otherwise of network neutrality regulations. Our members take differing views on this. Accordingly, we are limiting our submission to one small but important technical point, where we believe that one paragraph of BEREC's draft guidelines would unduly interfere with network operators' ability to defend against security threats. We believe this paragraph can be amended consistently with the legislation and without in any way compromising the policy goal sought by the legislation.

6. We welcome provisions in BEREC's draft guidelines which permit networks to filter traffic in order to "protect the integrity and security of the network", and in particular the recognition of the importance of filtering spoofed addresses – an important technique for preventing common forms of denial of service (DoS) attack. Packets with spoofed source addresses are a major source of DoS attacks.

7. We also understand the reason given in paragraph 83 for the guidance in paragraph 81 that active intervention techniques be undertaken "only when security attacks are detected". Unfortunately, the effect of that when applied to filtering source address spoofing would be to eliminate long

standing best practice for the prevention of source-address spoofing, and thereby to significantly undermine efforts against DoS attacks.

8. The Internet Engineering Taskforce best practice document on this topic, BCP-38, recommends that all networks be permanently configured to detect and block packets with spoofed source addresses, before these packets leave the network of origin.

9. Network operators can only implement this recommendation with respect to traffic originating from within their own network, since only at this point is it possible to detect a mismatch between the spoofed source address and the address ranges available to the computers which send the spoofed packets.

10. Address spoofing filters must be configured to operate in a permanent and ongoing fashion. It is not possible for originating networks to trigger these filters only when a DoS attack is detected, because those in a position to detect the DoS attack are not in a position to easily discern from which networks spoofed packets are actually originating: disguising the source is the very purpose of spoofing..

11. Correct identification of packet source addresses is essential to the proper function of the network. Computers sending spoofed packets would not receive any response from the destination services, since responses will be sent to the spoofed source address, which by definition is not the IP address of the originating computer.

12. Spoofed packets are therefore not a communication in the ordinary sense. They are only used to bombard the recipient with denial-of-service packets, because this is the only function they are capable of performing. The only benefit of spoofing is to disguise the source in order to impede denial-of-service mitigation efforts and associated investigations. Accordingly, spoofed packets ought to be regarded as an attack on network management in their own right.

13. (For a more detailed technical discussion of DoS attacks and the amplification technique, we would refer you to JISC's response to this consultation.)

14. Permanent filtering of spoofed addresses should not in any way undermine network neutrality, because:

    a. There is no legitimate purpose for spoofing a network packet's source address. Therefore, blocking spoofed addresses does not have any negative effect on the service enjoyed by the originating computer.

b. It is possible to distinguish very precisely between spoofed and un-spoofed packets. This is because, as already discussed, network operators block spoofed packets originating from within their own networks, and have precise knowledge of the addresses available to the originating computers.

15. We would therefore urge BEREC to interpret source address spoofing as an attack upon the network in its own right, and that accordingly network operators may continue to maintain filters that identify and block source-spoofed packets whenever they occur.

16. This minor but important tweak to the guidance can be done while maintaining the guidance that blocking of particular IP addresses should only be done when an attack is detected, and only for as long as necessary.

For further information, please contact:
Malcolm Hutty
Head of Public Affairs
London Internet Exchange Ltd.
5th Floor, 24 Monument Street
London
EC3R 8AJ
malcolm@linx.net