TECHNICAL REGULATIONS

I Recommendations

1. Traffic Participants are encouraged to announce all their routes and accept all routes from InterLAN. For a better and easier connectivity it is recommended that participants perform BGP sessions with InterLAN route-servers. Participants in peering are advised to establish a page on their own website (e.g. website.com/peering), where the peering access procedure is detailed for whoever may be interested.

2. It is recommended that the devices used for interconnection be specialized equipment such as routers or Layer III class switches.

II. Obligations

1. The traffic that runs through the InterLAN infrastructure as a result of the exchange of information between participants should not be filtered or altered. The interception or the examination of this traffic will be made with the written approval of InterLAN technical department or at the written request of qualified authorities, according to the law in force.

2. Potential participants are entirely responsible in terms of connectivity with InterLAN POP where the interconnection will take place.

3. InterLAN alone will decide the route to transfer data packets from the partner in the InterLAN network.

4. Traffic participants will not act send illegal traffic or other traffic that hinders InterLAN peering use by other partners (e.g. ARP spoofing, sniffers installation, etc.).

5. Ethernet packets sent to the access ports in InterLAN by the partners will have only the following types:
   a. 0x0800 – IPv4
   b. 0x0806 – ARP
   c. 0x86dd – Ipv6
   d. 0x8100 – 802.1q

6. It is forbidden to activate Proxy ARP on the interfaces towards InterLAN.

7. All Ethernet frames representing Internet Exchange traffic sent to an access port in InterLAN will have necessarily the mac address/addresses associated with IPv4 and IPv6 allocated by InterLAN technical department.

8. An IP address used for the interconnection with InterLAN RSes and with the other partners will be assigned to each peering participant. The number of IP addresses assigned to a traffic participant can be altered according to interconnection needs, supported by submitted documents.

The assignment of additional IP addresses is done by the InterLAN technical department in following situations:

   a. The need for back up BGP sessions
   b. Private BGP sessions operation
   c. Simultaneous active sessions of the same traffic partner (identified by ASN)

9. The traffic specific to local protocols should not be sent towards the access ports in InterLAN.

10. The following type of traffic and protocols are not allowed :

    a. ICMP redirect
    b. IEEE802 STP
    c. IRDP – (Internet router discovery protocol)
    d. BOOT/DHCP
    e. DVMRP
    f. UDLD
    g. L2 keepalive
    h. ICMPv6 ND-RA
    i. Trunking protocols: VTP,DTP
    j. Proprietary protocols, including but not limited to: CDP,EDP
    k. Rounting protocols: OSPF,ISIS,IGRP,EIGRP,RIP

11. The outgoing broadcast traffic of a port should not exceed 20 pps / port / vlan.

12. The routes exchange will be achieved only via BGP IPv4, IPv6 sessions.

13. The maximum length of a prefix announced by participants should not exceed 24-bit in the case of IPv4, and 96-bit in the case of IPv6.

14. All routes announced in InterLAN which originate from traffic participants public ASes must be registered in RIR's database managing them (route-objects must exist).

15. Each peering participant must have a public ASN and at least one IP address class originated from his own ASN.

16. BGP sessions will announce only own IP address classes or customer's classes and not those of other providers without their express consent along with InterLAN's consent.

17. InterLAN's peering reserved IP address space will be not announced in other networks except with the prior written approval of InterLAN technical department.

18. All routes announced in InterLAN will have set the nexthop to the partner making the announcement, unless the consent of technical department was obtained for the members announcing the routes with nexthop to other partners.

19. The announcement of private address classes (RFC1918) in InterLAN is not permitted.

20. A participant will send traffic to another participant's port only in case when he has obtained permission from the latter via a route announced through InterLAN route-servers or a private BGP session.

21. The use of static routes is not allowed. All traffic routing decisions through the connection with InterLAN will be taken on the basis of by BGP session received routes.

22. Maintenance works must be notified to the InterLAN technical department at least 48 hours prior to the event, with a declared goal to take all necessary measures to prevent any compatibility and/or connectivity issues of the participants. In case of accidental equipment replacement as result of their failure, it is required to announce immediately, by any means, the InterLAN technical department.