
TECHNICAL SPECIFICATIONS

This Annex describes the obligations of the participants to traffic, as well as the rules that must be observed during the operation of the interconnection agreement.

I Obligations

- 1) Each participant to Peering is bound to inform the other participants to the Peering of all its clients' routes, only by means of the InterLAN Route-Servers, but also to accept in its turn all routes announced by the other participants to the Peering, in accordance with the official registrations kept in the whois servers held by the Regional Internet Register;
- 2) Participants are bound to allow the free traffic exchange with the other participants.
- 3) Participants are bound to empower a contact person for technical issues, who should be in change of any technical problems concerning the interconnection;
- 4) Participants are bound to empower a contact person for administrative issues who can answer to any organizational or financial problem concerning the interconnection;
- 5) All traffic performed through the InterLAN Infrastructure as a result of the exchange of information among participants must not be filtered or altered. Such traffic shall be intercepted or examined only with the written approval of the InterLAN Technical Department or at the written request of the competent bodies, under the laws in force.
- 6) Potential participants are entirely liable for the connectivity with the InterLAN POP where the interconnection is to take place;

II Rules

This paragraph sets forth the rules which must be observed by all participants:

- 1) INTERLAN is the only one to decide the route on which the data packages from the PARTNER are to be transferred within the INTERLAN network.
- 2) No one shall act for illegal purposes or purposes which prevent the use of the Interlan peering (e.g: ARP spoofing, sniffer set-up, etc.).
- 3) The Ethernet frames sent to the Interlan access ports by the members shall only have the following types:
 - 0x0800 – IPv4
 - 0x0806 – ARP;
- 4) Proxy ARP cannot be activated on the Interlan interfaces.
- 5) Participants to peering are allowed a single MAC address on the ports of the Interlan equipment, that of the equipment designated for interconnection;
- 6) All Ethernet frames sent to an Interlan access port shall compulsorily have the same source MAC address;
- 7) The traffic specific for local protocols must not be sent to Interlan access ports. Examples of unacceptable traffic:
 - a. redirect ICMP
 - b. IEEE802 STP
 - c. Router discovery protocols (e.g. CDP)
 - d. Broadcasts/multicasts belonging to interior routing protocols (OSPF, IS-IS, IGRP, EIGRP)
 - e. BOOTP/DHCP;

- 8) It is prohibited to activate the Spanning-Tree protocol on the connections to Interlan.
- 9) The traffic broadcast to a port must not exceed 10pps / port.
- 10) The route exchange shall only be made through BGPv4 by means of the Route-Servers owned by InterLAN;
- 11) Each peering participant shall allot a single IP address used for interconnection;
- 12) The maximum length of a prefix announced by the participants must not exceed 24 bytes;
- 13) All routes announced by Interlan originating from public AS must be registered in the RIPE data base (route-objects should exist).
- 14) Each peering participant must own a public ASN and at least an IP address class originated from its own ASN.
- 15) By the BGP session only own IP address classes or the clients' addresses shall be announced, not those of other providers without their express consent and the express consent of Interlan.
- 16) The IP address space reserved for peering in Interlan shall not be announced in other networks unless with the prior written approval of the InterLAN Technical Department.
- 17) All routes announced in InterLAN shall have a nexthop set by the member who makes the announcement, save for the case when the approval of the technical department was obtained for the members announcing nexthop routes to other members.
- 18) The announcement of private address classes (RFC1918) is not allowed in InterLAN.
- 19) A participant shall send traffic to the port of another participant only if the latter gave its permission by means of a route announced by Interlan route-servers or of a private BGP session made through approved vlans.
- 20) The use of static routes is not allowed. All decisions to route the traffic or not through the connection with Interlan shall be taken based on the routes received through the BGP session from route-servers.
- 21) Private BGP sessions between members on the Interlan traffic vlan are not allowed. If an exchange of traffic of another type than the one originated from the direct peering AS, the Technical Department shall make available VLANs committed to this, after obtaining the prior approval of the Interlan Board of Directors.
- 22) The interfaces of the routers connected in an Interlan port shall use only the settings of IP/netmask and VLAN address which were assigned by the InterLAN Technical Department.
- 23) It is recommended that the devices used for the interconnection be specialized equipment, of the router or Layer III switch class.
- 24) The replacement of the equipment (with another equipment of the same type or with another one of other type) or the change of the configuration thereof, must be notified to the Technical Department of InterLAN at least 48 hours before the occurrence of the event, for the purpose of taking all necessary action for preventing eventual problems of compatibility and/or connectivity of the participants. In case of accidental replacement of the equipment following its break-down, it is required to immediately inform the InterLAN Technical Department by any means.