# REGULAMENT TEHNIC

**I Recomandari**

1. Participantii la trafic sunt incurajati sa anunte toate rutele proprii si sa accepte toate rutele provenite din InterLAN. Pentru o conectivitate mai buna si mai simpla este recomandat ca participantii sa efectueze sesiuni BGP cu route-serverele InterLAN. Participantilor la peering li se recomanda instituirea unei pagini pe propriul site web (de exemplu website.com/peering), in care procedura de acces la peering sa fie explicitata in detaliu pentru cei interesati.

2. Se recomanda ca dispozitivele utilizate pentru interconectare sa fie echipamente specializate, din clasa routere sau switch-uri Layer III.

**II. Obligatii**

1. Tot traficul care se desfasoara prin Infrastructura InterLAN ca rezultat al schimbului de informatii dintre participanti nu trebuie sa fie filtrat sau alterat. Interceptarea sau examinarea acestui trafic se va face doar cu aprobarea scrisa a departamentului tehnic InterLAN sau la cererea scrisa a organismelor abilitate, in conditiile legii in vigoare.

2. Potentialii participanti sunt in intregime responsabili in ceea ce priveste conectivitatea cu POP-ul InterLAN unde urmeaza sa se desfasoare interconectarea.

3. InterLAN este singurul care decide traseul pe care vor fi transferate pachetele de date provenite de la partener in reteaua InterLAN.

4. Nu se va actiona in scopuri ilegale sau care impiedica utilizarea peering-ului InterLAN de catre ceilalti parteneri (de exemplu: ARP spoofing, instalare de sniffere etc.).

5. Cadrele Ethernet trimise catre porturile de acces in InterLAN de catre parteneri vor avea doar urmatoarele tipuri:
   a. 0x0800 – IPv4
   b. 0x0806 – ARP
   c. 0x86dd – Ipv6
   d. 0x8100 – 802.1q

6. Este interzisa activarea Proxy ARP pe interfetele spre InterLAN.

7. Toate cadrele Ethernet reprezentand traficul de Internet Xchange trimise catre un port de acces in InterLAN vor avea in mod obligatoriu adresa/adresele mac asociate cu adresele IPv4 si IPv6 alocate de catre departamentul tehnic InterLAN;

8. Fiecarui participant la peering i se va aloca o adresa IP folosita pentru interconectarea cu RS-urile InterLAN si parteneri. Numarul de adrese IP alocate unui participant la traffic se poate modifica in functie de necesitatile de interconectare pe baza documentatiei justificative prezentate.

   Alocarea de adrese IP suplimentare se face de catre departamentul tehnic InterLAN in urmatoarele cazuri:
   a. Necesitatea unor sesiuni BGP de back-up
   b. Realizarea de sesiuni private de BGP
   c. Sesiuni active simultane ale aceluiasi partener de trafic (identificat prin ASN)

9. Traficul specific protocoalelor locale nu trebuie trimis catre porturile de acces in InterLAN.

10. Nu sunt permise urmatoarele tipuri de trafic si protocoale:
    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. Protocoale pentru trunking: VTP,DTP
j. Protocoale proprietare ce includ dar nu limitate la: CDP,EDP,LLDP
k. Protocoale de routare: OSPF,ISIS,IGRP,EIGRP,RIP
l. IGMP nu trebuie sa ruleze pe VLAN-ul afferent IEX-ului
m. Protocolul xSTP nu se ruleaza pe interfata conectata la infrastructura InterLAN

11. Traficul broadcast emis de catre un port nu trebuie sa depaseasca 20 pps/port/vlan.

12. Numar adrese MAC:
    a. Pe porturile dinspre client se accepta doar o singura adresa MAC pentru fiecare adresa IP alocata atat timp cat clientul nu foloseste alte servicii in afara de cel de IX. Daca traficul va fi originat de mai mult de o adresa MAC portul se va dezactiva pentru 5 minute.
    b. Pe porturile dinspre client se accepta mai mult de o adresa MAC in functie de serviciile folosite (tranzit, multicast, routere multiple). Limita se va stabili impreuna cu clientul si daca se va depasi se va aplica regula de la subpunctul anterior. Limita se poate creste cu aprobarea Interlan.

13. Schimbul de rute se va realiza doar prin sesiuni BGP IPv4 si IPv6.

14. Lungimea maxima a unui prefix anuntat de catre participanti nu trebuie sa depaseasca 24 de biti in cazul IPv4 si 96 biti in cazul IPv6.

15. Toate rutele anuntate in InterLAN originate din AS-uri publice ale participantilor la trafic trebuie sa fie inregistrate in baza de date a RIR-ului care le gestioneaza (sa existe route-objects).

16. Fiecare participant la peering trebuie sa detina un ASN public si cel putin o clasa de adrese IP originata din ASN-ul propriu.

17. Se vor anunta prin sesiunea BGP numai clasele de adrese IP proprii sau ale clientilor si nu ale altor provideri fara acordul expres al InterLAN si al acestora.

18. Spatiul de adrese IP rezervat peering-ului in InterLAN nu va fi anuntat in alte retele decat cu aprobarea scrisa prealabila a departamentului tehnic InterLAN.

19. Toate rutele anuntate in InterLAN vor avea nexthop setat la partenerul care face anuntul, cu exceptia cazului in care s-a obtinut acordul departamentului tehnic pentru membrii care anunta rute cu nexthop la alti parteneri.

20. Nu se permite anuntarea de clase de adrese private (RFC1918) in InterLAN.

21. Un participant va trimite trafic catre portul unui alt participant doar in cazul in care a obtinut permisiunea celui din urma prin intermediul unei rute anuntata prin route-serverele Interlan sau a unei sesiuni BGP private.

22. Nu se permite folosirea rutelor statice. Toate deciziile de a ruta sau nu traficul prin legatura cu InterLAN se vor lua pe baza rutelor primite prin sesiunea/sesiunile BGP.

23. Lucrarile de mentenanta, trebuie notificate catre departamentul tehnic al InterLAN cu minimum 48 de ore inainte de producerea evenimentului, in scopul luarii tuturor masurilor necesare pentru a preintampina eventuale probleme de compatibilitate si/sau conectivitate ale participantilor. In cazul inlocuirii fortuite a echipamentelor in urma defectarii acestora, este necesara anuntarea imediata, prin orice mijloace a departamentului tehnic al InterLAN.