

## REGULAMENT TEHNIC

Aceasta anexa descrie obligatiile participantilor la trafic precum si regulile care trebuie respectate in cadrul operarii contractului de interconectare.

### I Obligații

1. Fiecare participant la Peering este obligat să anunțe toate rutele clienților săi către ceilalți participanți la Peering, numai prin intermediul Route-Server-elor InterLAN, dar și să accepte la rândul său toate rutele anunțate de către ceilalți participanți la Peering, în conformitate cu înregistrările oficiale menținute în severele whois deținute de către Registrul Regional Internet;
2. Participanții sunt obligați să permită schimbul liber de trafic cu toți ceilalți participanți.
3. Participanții sunt obligați să mandateze o persoană de contact tehnic, care să răspundă la orice problemă de natură tehnică care privește interconectarea;
4. Participanții sunt obligați să mandateze o persoană de contact administrativ care să poată răspunde la orice problemă organizatorică sau financiară, care privește interconectarea;
5. Tot traficul care se desfășoară prin Infrastructura InterLAN ca rezultat al schimbului de informații dintre participanți nu trebuie să fie filtrat sau alterat. Interceptarea sau examinarea acestui trafic se va face doar cu aprobarea scrisă a Departamentului Tehnic InterLAN sau la cererea scrisă a organismelor abilitate, în condițiile legii în vigoare.
6. Potențialii participanți sunt în întregime responsabili în ceea ce privește conectivitatea cu POP-ul InterLAN unde urmează să se desfășoare interconectarea;

### II Reguli

Acest paragraf conține regulile care trebuie respectate de către toți participanții:

1. INTERLAN este singurul care decide traseul pe care vor fi transferate pachetele de date provenite de la PARTENER in rețeaua INTERLAN
2. Nu se va acționa în scopuri ilegale sau care împiedică utilizarea peering-ului Interlan de către ceilalți membri (de exemplu: ARP spoofing, instalare de sniffere, etc.).
3. Cadrele Ethernet trimise către porturile de acces în Interlan de către membri vor avea doar următoarele tipuri:
4. 0x0800 – IPv4
5. 0x0806 – ARP;
6. Nu se permite activarea Proxy ARP pe interfețele spre Interlan.
7. Pe porturile echipamentelor Interlan către participanții la peering se permite o singură adresă MAC, cea a echipamentului desemnat spre interconectare;
8. Toate cadrele Ethernet trimise către un port de acces în Interlan vor avea în mod obligatoriu aceeași adresă MAC sursă;
9. Traficul specific protocoalelor locale nu trebuie trimis către porturile de acces în Interlan. Exemple de trafic inacceptabil:
10. ICMP redirect
11. IEEE802 STP
12. Protocoale de router discovery (ex. CDP)
13. Broadcasturi/multicasturi aparținând protocoalelor de rutare interioare (OSPF, IS-IS, IGRP, EIGRP)
14. BOOTP/DHCP;

15. Este interzisă activarea protocolul Spanning-Tree pe legăturile spre Interlan.
16. Traficul broadcast emis de către un port nu trebuie să depășească 10pps / port.
17. Schimbul de rute se va realiza doar prin BGPv4 prin intermediul Route-Server-elor proprietate a InterLAN;
18. Fiecărui participant la peering i se va aloca o singură adresă IP folosită pentru interconectare;
19. Lungimea maximă a unui prefix anunțat de către participanți nu trebuie să depășească 24 de biți;
20. Toate rutele anunțate în Interlan originare din AS-uri publice ale membrilor trebuie să fie înregistrate în baza de date a RIPE (să existe route-objects).
21. Fiecare participant la peering trebuie să dețină un ASN public și cel puțin o clasă de adrese IP originată din ASN-ul propriu.
22. Se vor anunța prin sesiunea BGP numai clasele de adrese IP proprii sau ale clienților și nu ale altor provideri fără acordul expres al Interlan și al acestora.
23. Spațiul de adrese IP rezervat peering-ului în Interlan nu va fi anunțat în alte rețele decât cu aprobarea scrisă prealabilă a Departamentului Tehnic InterLAN.
24. Toate rutele anunțate în InterLAN vor avea nexthop setat la membrul care face anunțul, cu excepția cazului în care s-a obținut acordul departamentului tehnic pentru membrii care anunță rute cu nexthop la alți membri.
25. Nu se permite anunțarea de clase de adrese private (RFC1918) în InterLAN.
26. Un participant va trimite trafic către portul unui alt participant doar în cazul în care a obținut permisiunea celui din urmă prin intermediul unei rute anunțată prin route-serverele Interlan sau a unei sesiuni BGP private realizată pe vlan-uri aprobate.
27. Nu se permite folosirea rutelor statice. Toate deciziile de a ruta sau nu traficul prin legătura cu Interlan se vor lua pe baza rutelor primite prin sesiunea BGP de la route-servere.
28. Nu sunt admise sesiuni BGP private între membri pe vlan-ul de trafic Interlan. Dacă se dorește schimb de alt tip de trafic decât cel originat din AS-urile de peering direct, Departamentul Tehnic va pune la dispoziție VLAN-uri dedicate acestui lucru, după ce s-a obținut aprobarea prealabilă a Consiliului Director al Interlan.
29. Interfețele routerelor conectate într-un port Interlan vor folosi numai setările de adresă IP/netmask și VLAN care le-au fost atribuite de către Departamentul Tehnic InterLAN.
30. Se recomandă ca dispozitivele utilizate pentru interconectare să fie echipamente specializate, din clasa routere sau switch-uri Layer III.
31. Înlocuirea echipamentului (cu un alt echipament de același tip sau cu unul de alt tip) sau modificarea configurației acestuia, trebuie notificată către Departamentul Tehnic al InterLAN cu minimum 48 de ore înainte de produce-rea evenimentului, în scopul luării tuturor măsurilor necesare pentru a preîntâmpina eventuale probleme de compatibilitate și/sau conectivitate ale participanților. În cazul înlocuirii fortuite a echipamentelor în urma defectării acestora, este necesară anunțarea imediată, prin orice mijloace a Departamentului Tehnic al InterLAN.