NIX·CZ

REGISTERED OFFICE
NIX.CZ, z. s. p. o.
Milešovská 1136/5
130 00 Praha 3
Czech Republic

CONTACT ADDRESS
NIX.CZ, z. s. p. o.
Americká 525/23
120 00 Praha 2
Czech Republic

CONTACT
info@nix.cz
www.nix.cz
+420 246 083 460

OPERATING RULES OF NIX.CZ ASSOCIATION

(Version 10.0 dated 2016/06/02 with effect from 2016/08/01)

Article I.
PREREQUISITES FOR MEMBERSHIP IN ASSOCIATION

1.1 Each legal entity applying for membership in NIX.CZ Association shall comply with the following conditions:

a) has been assigned their own Autonomous System Number (ASN). In case any legal entity applying for membership in NIX.CZ Association have not been assigned their own ASN, it is necessary to provide written permission from the owner of the ASN.

Article II.
PREREQUISITES FOR ENTERING INTO CUSTOMER CONTRACT WITH ASSOCIATION

2.1 Each legal entity requesting to enter into a customer contract with NIX.CZ Association shall comply with the following conditions:

a) Has been assigned their own Autonomous System Number (ASN).

b) In case the entity applying for membership in NIX.CZ Association has not been assigned their own ASN, it is necessary to provide written permission from the owner of the ASN or evidence of providing IPTV or VOD services.

c) Undertakes to comply with the conditions set out in these Operating Rules of NIX.CZ Association and in the Price list of NIX.CZ Association.

Article III.
OPERATING CONDITIONS

3.1 Connection to NIX.CZ nodes shall be permitted after the relevant membership fee has been paid (by a member of the Association) or the service contract has been signed (by a customer of the Association).

3.2 Each member/customer is obliged to cooperate with the employee of NIX.CZ Association who is in charge of establishing or maintaining the connection to NIX.CZ nodes (from now on "**responsible employee of the Association**").

3.3 Before connecting to the NIX.CZ infrastructure, each member/customer is obliged to enter and keep updated the following information on the Extranet of the Association:

a) operation contact including:
   i) a telephone number available 24 hours a day, 7 days a week
   ii) e-mail address to their NOC (Network Operation Centre);

b) e-mail addresses to be listed in the NIX.CZ contact register for the purpose of correspondence between members/customers;

c) Autonomous System Number (ASN) assigned to the relevant member/customer;

d) full canonical name for member's/customer's router to be registered in the reverse domains (in-addr.arpa and ip6.arpa) within the domain name system assigned to NIX.CZ Association;

e) URL to member's/customer's website, if the member/customer requires a link from the website of the Association;

f) e-mail address for sending peering requests;

g) member's/customer's contact information.

3.5 In case the stability and functionality of NIX.CZ equipment is jeopardized by an equipment/connection belonging to a member/customer, the Association shall be entitled to block the relevant member's/customer's port until the problem has been resolved by the member/customer. Association employees will, in such a case, immediately inform the NOC contact (as registered on the Association extranet) by e-mail. This obligation to inform does not apply to the automatic port blocking pursuant to Item PI/131 hereof.

3.6 Technical operating conditions for public peering (VLAN) are set out in Annex I to these Operating Rules. Technical operating conditions for private VLAN are set out in Annex II to these Operating Rules. Technical operating conditions for the multicast segment (VLAN) are set out in Annex III to these Operating Rules.

Article IV
OTHER CONDITIONS OF USING NIX.CZ NODE

4.1 Members/customers shall make sure that their connection to the NIX.CZ node does not hamper the use of NIX.CZ services by other members/customers.

4.2 Members/customers shall not use NIX.CZ to carry out any illegal activities.

Article V
INSURANCE AND LIABILITY

5.1 In the event of any claims for damage caused by any member/customer of the Association to another member/customer or to the Association itself, the case shall proceed pursuant to the provisions of the Commercial Code.

Annexes:
Annex I – Technical Operating Conditions for public peering segment.
Annex II - Technical Operating Conditions for private VLAN.
Annex III - Technical Operating Conditions for multicast peering.

NIX·CZ

Annex I

TECHNICAL OPERATING CONDITIONS FOR PUBLIC PEERING SEGMENT

PI/1. The common network segment of the NIX.CZ nodes is based on Ethernet technology (IEEE 802.3).

PI/2. NIX.CZ offers the following interfaces:

a) metallic port 1Gbps port 1000BASE-T; optical 1Gbps port with 1000BASE-SX or 1000BASE-LX module;
b) optical 10Gbps port with 10GBASE-SR or 10GBASE-LR module;
c) optical 10Gbps port with 100GBASE-SR10 or 100GBASE-LR4 module;
d) if requested other, not mentioned modules, as specified by responsible employees of the Association (especially modules ER, ZR, xWDM etc.).

PI/3. Members/customers are not allowed to use peering infrastructure of NIX.CZ for internal transit of their networks.

PI/4. Several physical ports of one member/customer terminated on the same NIX.CZ switch can be grouped into one logical port (EtherChannel). Ports group is configured statically or via LACP (Slow LACPDUs).

PI/5. Each member/customer single-channel link is limited to 2 source dynamic MAC addresses. A multiple channel connection (Etherchannel) is according to applied technology limited to 1 static MAC address (configured by Association employees) or 2 dynamic MAC addresses on the logical port. In the case of a 802.1Q encapsulation, each segment (VLAN) belonging to the member/customer is limited to 2 source dynamic or static MAC addresses (depending on the technology used).

PI/6. Ethernet frames forwarded by the connected equipment into the common network segment shall have of one of the following ether-types:

a) 0x0800 – IPv4;
b) 0x0806 – ARP;
c) 0x86dd – IPv6;
d) 0x9000 – loopback/keepalive.

PI/7. All frames forwarded into the common network segment shall not be addressed to the multi-cast or broadcast MAC address, with the following exceptions:

a) ARP broadcast;
b) IPv6 neighbour discovery
c) others based on permission by NIX.CZ Association

PI/8. Broadcast and multicast frames sent to shared segment are limited.

PI/9. Traffic for link-local (see Item PI/10) protocol shall not be forwarded into the common network segment, with the following exceptions:

a) ARP (except Proxy-ARP);
b) IPv6 neighbour discovery.

PI/10. Link-local protocols (PI/7) include but are not limited to the following list: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols (CDP etc.), internal routing protocols (OSPF, ISIS, EIGRP), BOOTP/DHCP, PIM-SM/PIM-DM, DMVRP, IPv6 router advertisement and others.

PI/11. Traffic generated by ARP shall not exceed 20 packets per second.

PI/12. Newly installed ports are initially connected to the isolated testing segment to verify whether the member's/customer's equipment is configured correctly. Connection to the production network is possible only after all detected defects are removed.

PI/13. In the event of exceeding the maximum number of allowed MAC addresses at one port/link, the related switch port is automatically blocked to ensure stability for the switches of the Association.

PI/14. Ports connected to the common network segment shall use only the IP address and network mask assigned by the responsible employee of NIX.CZ Association. One physical (logical) port is assigned with one IP address IPv4 and one IPv6 address.

PI/15. IPv6 addresses shall be statically configured (no use of automatic configuration). IPv6 site local addresses shall not be used.

PI/16. Member's/customer's port shall not forward to the common network segment any IP packets with the broadcast address of the common network segment.

PI/17. The routing protocol of NIX.CZ nodes is BGP-4 (RFC-4271) with possible extension to MP-BPG-4 (RFC4760, RFC-2545) – only unicast IPv4 and IPv6.

PI/18. Addresses of the common network segment shall not be advertised to other networks without explicit permission of NIX.CZ Association.

PI/19. Traffic from the port of one member/customer can be forwarded to the address of another member/customer only upon peering agreement and only via BGP-4 protocol (see PI/17).

PI/20. All routes advertised across the common network segment shall point to the router advertising them, with the sole exception of deploying the RTBH filtering function (see PI/21) or based on a prior agreement made in writing by NIX.CZ and all members/ customers involved.

PI/22. In order to prevent (D)DoS attacks, it is possible to deploy, following a written agreement of the responsible employee of NIX.CZ Association, the RTBH filtering function. This function allows members/customers to announce routers with an altered next-hop pointer to bh.nix.cz or bh-ipv6.nix.cz and filter traffic in this way.

The members/customers are recommended to:

a) register their routing policy for each connected ASN in the RIPE database and keep it updated;
b) for all networks advertised via BGP register a route (or route6) object in the RIPE database or similar register and keep it updated;
c) not generate useless "route flap";
d) not advertise useless specific routes when peering with other members/customers of the NIX.CZ Association;
e) use an as-set object registered in RIPE database or similar register.
f) use the MTU setting for 1500B switches.

PI/23. The load on the port/ports used by members and customers may not exceed 90% based on a 5-minute average.

NIX·CZ

Annex II

TECHNICAL OPERATING CONDITIONS FOR PRIVATE VLAN

PII/1. The common network segment of the NIX.CZ nodes is based on Ethernet technology (IEEE 802.3).

PII/2. NIX.CZ offers the following interfaces:

a) metallic port 1Gbps port 1000BASE-T; optical 1Gbps port with 1000BASE-SX or 1000BASE-LX module;
b) optical 10Gbps port with 10GBASE-SR or 10GBASE-LR module;
c) optical 10Gbps port with 100GBASE-SR10 or 100GBASE-LR4 module;
d) if requested other, not mentioned modules, as specified by responsible employees of the Association (especially modules ER, ZR, xWDM etc.).

PII/3. Link for Private VLAN must be set on 802.1Q encapsulation and it is not allowed to use any other configuration (ISL, QinQ etc.)

PII/4. Several physical ports of one member/customer of at least 1GB link speed terminated on the same NIX.CZ switch can be grouped into one logical port (Etherchannel). Ports group is configured statically or via LACP (Slow LACPDUs)

PII/5. Each VLAN is limited to 2 source dynamic or static MAC addresses (according to applied technology).

PII/6. Ethernet frames forwarded by the connected equipment into the common network segment shall have of one of the following ether-types:

a) 0x0800 – IPv4;
b) 0x0806 – ARP;
c) 0x86dd – IPv6;
d) 0x9000 – loopback/keepalive.

PII/7. Broadcast and multicast frames forwarded into the common network segment are limited.

PII/8. Frames forwarded into common network segment must not be of the following types: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols (CDP etc.), internal routing protocol PIM-SM/PIM-DM, DMVRP, and others.

PII/9. Traffic generated by ARP shall not exceed 20 packets per second.

PII/10. Newly installed ports are initially connected to the isolated testing segment to verify whether the member's/customer's equipment is configured correctly. Connection to the production network is possible only after all detected defects are removed.

PII/11. In the event of exceeding the maximum number of allowed MAC addresses at one port/link or breaching section PII/8 of this Annex, the related switch port is automatically blocked to ensure stability for the switches of the Association.

PII/12. The load on the port/ports used by members and customers may not exceed 90% based on a 5-minute average.

PII/13 Members/customers are recommended to:

a) Apply direct connection to their own edge router without further L2 equipment.

b) Private VLAN is designed for broadcasting internal protocols like OSPF, ISIS, EIGRP, iBGP, BOOT/DHCP, IPv6 router advertisement and other.

PII/14 Following a written agreement of the responsible employees of the Association, ports using the services of a private VLAN can increase their MTU switch settings to up to 9216 B. Members/customers shall comply with keeping the MTU size in the the peering segment in accordance with PI/22. f.)

Annex III

TECHNICAL OPERATING CONDITIONS FOR MULTICAST VLAN

PIII/1. The common network segment of the NIX.CZ nodes is based on Ethernet technology (IEEE 802.3).

PIII/2. NIX.CZ offers the following interfaces:

a) metallic port 1Gbps port 1000BASE-T; optical 1Gbps port with 1000BASE-SX or 1000BASE-LX module;
b) optical 10Gbps port with 10GBASE-SR or 10GBASE-LR module;
c) optical 10Gbps port with 100GBASE-SR10 or 100GBASE-LR4 module;
d) if requested other, not mentioned modules, as specified by responsible employees of the Association (especially modules ER, ZR, xWDM etc.).

PIII/3. Link for Private VLAN must be set on 802.1Q encapsulation and it is not allowed to use any other configuration (ISL, QinQ etc.)

PIII/4. Several physical ports of one member/customer terminated on the same NIX.CZ switch can be grouped into one logical port (Etherchannel). Ports group is configured statically or via LACP (Slow LACPDUs)

PIII/5. Each physical/logical port is limited (depending on the technology used) limited to 50 source dynamic or static MAC addresses. The number of MAC addresses can only be changed based on a written agreement of the responsible employees of the Association.

PIII/6. Ethernet frames forwarded by the connected equipment into the common network segment shall have of one of the following ether-types:

a) 0x0800 – IPv4;
b) 0x0806 – ARP;
c) 0x9000 – loopback/keepalive.

PIII/7. Broadcast and frames forwarded into the common network segment are limited.

PIII/8. Frames forwarded into common network segment must not be of the following types: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protocols (CDP etc.), and others.

PIII/9. Traffic generated by ARP shall not exceed 20 packets per second.

PIII/10. Newly installed ports are initially connected to the isolated testing segment to verify whether the member's/customer's equipment is configured correctly. Connection to the production network is possible only after all detected defects are removed.

PIII/11. In the event of exceeding the maximum number of allowed MAC addresses at one port/link or breaching section PII/8 of this Annex, the related switch port is automatically blocked to ensure stability for the switches of the Association.

PIII/12. The load on the port/ports used by members and customers may not exceed 90% based on a 5-minute average.

PIII/13. The multicast VLAN uses a point-to-point topology (source-target).

PIII/14. Members/customers shall comply with the addressing of the multicast traffic determined by the IANA, i.e. class D group - 224.0.0.0/4

PIII/15. Members/customers shall use the IGMpv2/3 or PIMv1/2 protocols to manage multicast traffic distribution in the segment.

PIII/16. Each physical/logical port that belongs to a member/customer is limited to 100 multicast groups. The number of groups can only be changed based on a written agreement of the responsible employees of the Association.

PII/17 Members/customers are recommended to:

a) Apply direct connection to their own edge router without further L2 equipment.

b) Not use overlapping multicast addresses in mapping multicast IP onto MAC addresses 32:1.

Examples of overlapping addresses:

224.1.1.1
224.129.1.1
225.1.1.1
225.129.1.1
.
.
.
238.1.1.1
238.129.1.1
239.1.1.1
239.129.1.1

PIII/18.

c) Multicast VLAN can be used to distribute IPTV, VoD etc.

On ports using multicast VLAN services, the MTU switch settings can be increased, provided the responsible employees of the Association give a written agreement, to 9216B. Members/customers must comply with the size of the MTU in the peering segment in accordance with PI/22.f.