

SAIX Technical Requirements

1. Purpose of the Document

This document is to provide SAIX technical requirements for member's connectivity.

2. Terminologies and Definitions

Terminologies used herein but not otherwise defined shall have the same meanings.

SAIX: Refers to **Saudi Arabian Internet Exchange**, where many members can peer together to interconnect their networks.

Member: Refers to a beneficiary from the services provided by SAIX, it can be any one have public ASN.

Data Service Provider (DSP): Refers to a licensed Data Service Provider in the Kingdom of Saudi Arabia, which is responsible for providing a service data circuits from one point to another point, or data communications through a switched data network, including without limitation: Broadband Services, Virtual Private (VPN) Services, Digital Leased Line Services, Internet Protocol (IP) Services, Asynchronous Transfer Mode (ATM) Services, Frame Relay Services, Wavelength Services International Data Gateway Services, and International Data Transit Traffic Services.

3. NOC Contact and Datacenter Location

The NOC team actively monitor the SAIX infrastructure 24/7, Members can report problems and inquire support from SAIX NOC via email (support@saix.sa)

Or via phone number 9200 07537.

4. Technical Requirement

4.1 Layer-1 Requirements

4.1.1 Members may install L3 device at SAIX datacenter or connect to SAIX datacenter via any licensed Data Service Provider (DSP) located at Kingdom of Saudi Arabia.

4.1.2 Interface media technology used are Ethernet only. Ethernet interfaces attached to SAIX ports shall be explicitly configured with duplex, speed, and other configuration settings and shall not be auto-sensing.

4.1.3 Physical Interfaces provided are 1G, 10G, 40G and 100G.

4.1.4 SFP single mode with 1310nm wavelength.

4.2 Layer-2 Requirements

4.2.1 Frames forwarded to SAIX ports shall have one of the following ether types

- 0x0800 - IPv4
- 0x0806 - ARP
- 0x86dd - IPv6

4.2.2 All frames of a service forwarded to an individual SAIX port shall have the same registered source MAC address, if more than one address learned by port, SAIX team has the authority to disable the port. If the member has the intention to change the registered source MAC address, he shall submit change request to SAIX support team.

4.2.3 Frames forwarded to SAIX ports shall not be addressed to a multicast or broadcast MAC destination address, except as follows:

- Broadcast ARP packets.
- Multicast IPv6 Neighbor Discovery (ND) packets.
- If explicitly allowed for that port (e.g. multicast service).

4.2.4 ARP traffic shall not exceed 20 bps per port/VLAN.

4.2.5 Allowed Ethernet MTU size = 1600 bytes

4.2.6 All members shall connect to SAIX using VLAN provided by SAIX.

4.2.7 SAIX can provide up to two links for each member, any additional links would require communicating with SAIX team to discuss different solution with member.

4.2.8 Interface connections to SAIX, from the member side, shall be a Layer-3 interface. Therefore, PBDUs will not be allowed and SAIX has the right to disable the port for any violations.

4.2.9 CDP, LLDP and VTP protocols are not permitted from SAIX side.

4.3 Layer-3 Requirements

4.3.1 Member interfaces connected to SAIX ports shall have IP addresses and netmasks assigned by SAIX. In particular:

- IPV4 & IPV6 addresses are assigned by SAIX and members are not permitted to change the IPs without SAIX team approval.
- IPv6 addresses (link & global scope) shall be explicitly configured and not auto-configured.
- IPv6 site-local addresses shall not be used

4.3.2 IP packets addressed to SAIX peering LAN directed broadcast address shall not be automatically forwarded to SAIX ports.

4.3.3 (Optional) Two EBGP sessions at least will be established with two different SAIX Route Servers (RS), to ensure service availability.

4.4 Routing

4.4.1 Routes exchange across the SAIX network shall be via BGP4 and/or BGPV6 (+) routing protocols.

4.4.2 Public AS numbers shall be used in BGP sessions across the SAIX network.

4.4.3 All Bogons or Martians IP prefixes as defined in (RFC1918, RFC5735 and RFC6598) as well as default route will be dropped if the prefixes pass through SAIX route servers.

4.4.4 All updates with ASNs in the AS-PATH as defined by (RFC5398, RFC6793, RFC6996, RFC7300 and RFC7607) will be dropped if it is passing through SAIX route servers.

4.4.7 IP address space assigned to SAIX peering LAN shall not be advertised, by a member, to other networks without explicit permission of SAIX. All routes advertised across the SAIX network shall point to the router advertising it unless an agreement has been made in advance in writing by SAIX and the members involved.

4.4.8 SAIX Route Servers will only accept routes that are registered in the RIPE database.

4.4.9 SAIX Route Servers will only accept updates that originated from members ASNs or it's behind customers. With adding customer's ASN in the member AS-SET.

4.4.10 Due to route-server functionality, All members that will peers with SAIX Route Servers have to disable the default behavior for BGP which deny incoming updates received from EBGP peers that don't list their AS number as the first segment in the AS_PATH attribute (EX. CISCO IOS "no bgp enforce-first-as").

4.5 Forwarding

4.5.1 Traffic shall be forwarded to a SAIX members when permission has been given by the receiving members by advertising a route across the SAIX network:

- Through the route servers.
- Through direct peering between members.

NOTE: Above is the basic requirements to be SAIX member, and once it is approved by MCIT other prerequisite points can be shared based on the needs.