Amateur Virtual Internet Exchange (AvIX) Connection Policy

Version: 1.0
Effective Date: July 5, 2025

1. Introduction

This document outlines the connection policy for the Amateur Virtual Internet Exchange (herein referred to as "the AvIX"). The AvIX is established to facilitate direct, settlement-free interconnection and traffic exchange between autonomous networks operated by licensed amateur radio operators utilizing 44Net (AMPRNet) address space and major Internet Service Providers (ISPs)/content providers. The goal is to enhance connectivity, reduce latency, and improve the overall resilience and performance for both communities.

2. Purpose

The primary purposes of this policy are to:

- Define the technical and operational requirements for connecting to the AvIX.
- Ensure the stability, security, and integrity of the AvIX infrastructure.
- Promote efficient and equitable traffic exchange among participants.
- Foster a collaborative environment between amateur radio operators and commercial internet entities.
- Outline the responsibilities and expectations of all connected participants.

3. Scope

This policy applies to all entities seeking to connect or currently connected to the AvIX, including:

- Licensed amateur radio operators with assigned 44Net (AMPRNet) IP address allocations.
- Major Internet Service Providers (ISPs), Content Delivery Networks (CDNs), and other large network operators. For the purpose of this policy, "Major Carriers" shall be defined as any carriers designated as Tier 1 providers or any others as deemed fit by the establishing organization of the AvIX.

4. Connection Requirements

All applicants for connection to the AvIX must meet the following criteria:

4.1 General Requirements

- **Legal Entity/Licensed Operator:**
  - **44Net Participants:** Must be a licensed amateur radio operator with a valid callsign and a legitimate allocation of 44Net IP address space from ARDC

(Amateur Radio Digital Communications) or a recognized delegate.
    - **Major Carriers:** Must be a legally registered entity with a valid Autonomous System Number (ASN) assigned by a Regional Internet Registry (RIR).
- **Public ASN:** All participants, regardless of type, must operate a public Autonomous System (AS) and use a public ASN.
- **Public IP Addresses:** All participants must possess and announce at least one block of public IPv4 and/or IPv6 addresses (independent of any upstream provider) assigned by a RIR or a legitimate 44Net allocation.
- **Technical Capability:** Participants must have the technical expertise and equipment (e.g., edge routers capable of BGP) to configure and manage BGP interconnections.
- **24/7 Operational Contact:** Participants must provide and maintain a 24/7 operational contact (e.g., NOC contact, email, phone) for technical issues, maintenance notifications, and abuse complaints. This information should be kept current in a public database such as PeeringDB (for major carriers) or a designated AvIX contact registry (for 44Net participants).
- **Acceptable Use:** All traffic exchanged over the AvIX must comply with all applicable local, national, and international laws and regulations. Illegal activities, denial-of-service attacks, spam, or any other abusive traffic are strictly prohibited.

4.2 Technical Requirements

- **Border Gateway Protocol (BGP):** All peering sessions will be established using BGP-4 (RFC 4271).
    - Participants must support both IPv4 and IPv6 unicast traffic (dual-stack operation is highly recommended).
    - BGP sessions will be established directly between participant routers and the AvIX route server(s).
    - Participants must announce only their own prefixes and those of their legitimate downstream customers. The announcement of transit or third-party routes is strictly prohibited.
    - Participants are strongly encouraged to implement BGP Route Origin Authorizations (ROAs) and utilize Resource Public Key Infrastructure (RPKI) validation for all announced prefixes.
    - BGP communities may be used to convey routing information, and participants are encouraged to implement a comprehensive BGP community scheme.
    - The AvIX will operate route server(s) to simplify peering. Participants are encouraged to peer with the route server(s) to maximize interconnection with

other AvIX members.
    - Participants must not point static or default routes towards the AvIX infrastructure.
    - Participants must configure their BGP sessions to prevent the propagation of private ASNs (RFC 6996) or bogon routes.
- **Filtering:** Participants must implement strict ingress and egress filtering to prevent the advertisement of incorrect or unauthorized routes. This includes filtering based on IRR (Internet Routing Registry) entries.
- **Capacity:** Participants are responsible for ensuring sufficient capacity on their connection to the AvIX to handle their traffic volumes without causing congestion or impacting other participants. The AvIX reserves the right to request capacity upgrades if a participant's connection consistently shows signs of overutilization.
- **Link-Local Protocols:** Participants must disable or prevent any link-local protocols (e.g., CDP, LLDP, vendor discovery protocols) or interior routing protocol broadcasts (e.g., OSPF, EIGRP) on their AvIX facing interfaces.
- **MAC Address Limits:** Participants must adhere to any specified MAC address limits per port to maintain the stability of the virtual switching fabric.
- **Time Synchronization:** Participants are encouraged to synchronize their network devices with a reliable NTP source.

4.3 Operational Requirements

- **Maintenance:** Participants must provide advance notice (at least 72 hours for planned maintenance) of any work that may affect their AvIX connection or traffic flow. Emergency maintenance should be communicated as soon as possible.
- **Troubleshooting:** Participants are expected to actively participate in troubleshooting efforts for any issues affecting their connection or the AvIX.
- **Abuse Handling:** Participants must have a clear process for handling abuse complaints originating from their network and respond to such complaints in a timely manner.
- **Security:** Participants are responsible for the security of their own network and equipment connected to the AvIX. This includes implementing appropriate security measures to prevent unauthorized access, malicious activity, and the spread of malware.
- **PeeringDB/Contact Information:** Major carriers are required to maintain an up-to-date PeeringDB entry. 44Net participants should maintain current contact information with the AvIX administration.

5. Peering Policy

The AvIX operates on a settlement-free peering model, meaning no money is

exchanged for the exchange of traffic between participants.

- **Open Peering:** The AvIX encourages an open peering policy among its participants. However, the decision to establish a bilateral peering relationship remains at the discretion of individual participants.
- **Route Server:** The AvIX provides a route server to facilitate multilateral peering. Participants connecting to the route server agree to peer with all other participants connected to the route server, subject to any explicitly defined filtering policies.
- **Direct Peering:** Participants may also establish direct bilateral BGP sessions with other participants on the AvIX fabric, independent of the route server.
- **Traffic Exchange:** Participants are expected to exchange traffic for their own networks and their legitimate customers only. The AvIX is not intended for transit services to third parties.
- **Approved Transit Provider:** Notwithstanding the general traffic exchange policy, AS17290 is an approved transit provider for specific connectivity requests within the AvIX. Participants may utilize AS17290 for transit services as required, provided such usage adheres to all other policies and agreements.

6. Abuse and Disconnection Policy

The AvIX reserves the right to suspend or terminate a participant's connection for violations of this policy.

- **Violations:** Examples of violations include, but are not limited to:
  - Sending abusive, illegal, or unauthorized traffic.
  - Failure to maintain operational contact information.
  - Persistent technical issues impacting the AvIX or other participants.
  - Failure to comply with BGP filtering requirements.
  - Unauthorized transit of third-party traffic.
- **Notification:** In most cases, the AvIX administration will attempt to contact the participant to resolve the issue before initiating a suspension or disconnection.
- **Immediate Disconnection:** In cases of severe abuse or immediate threat to the AvIX's stability or other participants, the AvIX reserves the right to disconnect a participant immediately without prior notice.
- **Reconnection:** Reconnection after a suspension or termination will be at the sole discretion of the AvIX administration and may require a review of the participant's network, a commitment to rectify past issues, and potentially a re-application process.

7. Amendments

This policy may be amended from time to time by the AvIX establishing organization.

Participants will be notified of any changes via email or through the AvIX's official communication channels. Continued connection to the AvIX after notification of changes constitutes acceptance of the revised policy.