Paducah Internet Exchange
Acceptable Use Policy and Peering Policy Guidelines

Paducah
Internet
Exchange

April 2025

This AUP is a community-driven guideline outlining best practices for all Paducah IX participants. It is intended to ensure a stable, cooperative peering environment for everyone.

Introduction and Purpose

Paducah IX is a community Internet Exchange Point serving networks in and around Paducah. Our goal is to foster an open and efficient interconnection environment where members exchange traffic directly for mutual benefit. This Acceptable Use Policy (AUP) describes the best-practice standards for using the exchange. By following these guidelines, all participants help maintain a reliable and collegial peering fabric.

In summary, we ask all Paducah IX participants to:

- Be technically compliant: Connect a single router (one MAC address) per port, use BGP for peering, and only send appropriate traffic over the exchange.
- Peer responsibly: Exchange routes and traffic only in intended ways – feel free to set open or selective peering policies, but avoid misuse such as transit or prefix hijacking.
- Keep information updated: Maintain your contact info (e.g. PeeringDB) and network details so others can easily peer with you.
- Cooperate in good faith: Work with the IX community to resolve issues. Our enforcement is friendly and informal – we prefer to warn and fix problems together, resorting to port disablement only if absolutely necessary.

The sections below detail these expectations in a friendly but clear manner. Remember, these rules exist to make the IX beneficial for everyone. Thank you for being a part of the Paducah IX community!

Technical Connection Requirements

Paducah Internet Exchange
Acceptable Use Policy and Peering Policy Guidelines

To ensure a smooth operation, Paducah IX has a few technical requirements for all connections. These are common standards at community IXPs and help prevent one participant's misconfiguration from affecting others:

- One Device & One MAC per Port: Connect only a single Layer-3 routing device to each Paducah IX switch port. In practice, this means only one unique MAC address should be seen from your port . (If you need to connect multiple routers or devices, please arrange additional ports or ask Paducah IX staff for guidance instead of using switches or bridges on your port.)

- One ASN per Participant: Each member should have their own registered Autonomous System Number (ASN) to peer at the exchange . BGP (Border Gateway Protocol) is the only supported routing protocol for exchanging routes, so an ASN is required. (If you don't yet have an ASN, we can advise on obtaining one.)

- Use BGP-4 for Peering: All peering at Paducah IX must be done via BGP version 4 (or its successor). Static routing or other protocols are not allowed on the IX fabric. Your router's BGP must be configured correctly to peer with others. For example, if you ever re-advertise routes learned from one peer to another (e.g. through a route server), set BGP NEXT_HOP_SELF to avoid confusing route forwarding . Also, please avoid generating unnecessary route flap or announcing overly specific prefixes that could burden others. Stable, sensible BGP announcements keep the exchange healthy for all.

- Allowed Traffic Types: Only IPv4, IPv6 unicast, and ARP/NDP traffic should traverse the exchange. No other layer-2 or link-local protocols should be sent into the IX. In particular, disable any Spanning Tree (STP), VLAN tagging (beyond the exchange VLAN), CDP/LLDP, IPv6 RA, proxy-ARP, multicast (other than ARP/NDP), or any other non-peering traffic on your port. The Paducah IX switches will drop or block unsupported protocols for safety. Normal ARP (IPv4) and ICMPv6 Neighbor Discovery are the only broadcast/multicast frames expected on the peering VLAN. Keeping to just IP peering traffic prevents accidental loops or floods.

- IP Address Assignment: Paducah IX will assign you one IPv4 address and one IPv6 address on the shared peering LAN. Please use only the IPs assigned to you on the exchange interface. Do not configure additional addresses or bring external IP space onto the IX. If you have multiple ports (e.g. a port channel/LAG or a second connection for redundancy), the IX can provide additional IPs as needed. We conserve IPv4 addresses, so typically one IP per member router is the norm.

- No Local Transit or Bridging: The Paducah IX fabric is meant for peering between networks, not as a transport network for your internal traffic. Participants should not use the exchange to carry traffic between their own routers or sites. For example, if you have two POPs connected to Paducah IX, do not forward data from one to the other across the IX (that's what your own backbone or private circuit is for). Similarly, do not extend or bridge the IX connection into your internal LAN. Each port is for one router interface only – no connecting a switch or sharing the port with third parties without permission.

- MTU and Framing: Paducah IX supports the standard Ethernet MTU (1500 bytes) on the peering VLAN. Jumbo frames may be supported on a separate VLAN if there is interest (ask the IX team). All ports are Ethernet (10Gbps/100Gbps/etc.) so make sure to use the correct optics and cable. We recommend disabling auto-negotiation and hard-setting speed/duplex on your port to avoid any mismatch (some exchanges suggest this for stability). If you do use auto-negotiation, ensure it's working properly.

Following these technical requirements will ensure that your connection to the IX is trouble-free and that you don't inadvertently cause issues for other peers. If you have any questions about configuring your equipment for Paducah IX, our operators are happy to help (we can share sample configs from similar exchanges).

Peering and Routing Policy
Paducah IX is a peering platform – networks come here to freely exchange traffic via bilateral or multilateral BGP sessions. We encourage an open peering environment while recognizing that each network can set its own policies. Below are our guidelines on peering relationships and BGP routing behavior at the exchange:

- **Open vs. Selective Peering**: Paducah IX does not mandate that you peer with everyone. Peering is voluntary and negotiated between participants . Networks may have an open peering policy (willing to peer with any other IX member), or a selective/conditional policy (peer on a case-by-case basis, possibly requiring certain criteria). We recommend indicating your peering policy on your PeeringDB entry (common options are "open", "selective/partially open", or "restrictive"). While we encourage a friendly, open peering stance to maximize the IX's value for all, we respect that some networks have selective policies. No participant is obligated to peer with any specific other participant, and bilateral peering agreements are left to

the networks involved – Paducah IX simply provides the switching fabric to make it possible.

- **BGP Announcements – Own Prefixes Only:** When advertising routes over Paducah IX, only announce prefixes that you are authorized to carry (your own routes and those of your customers, if any). Do not announce IP prefixes that belong to other Paducah IX participants or to networks that are not yours, unless you have explicit permission (this kind of unauthorized announcement is considered route hijacking and is strictly prohibited). In practice, each ASN should advertise only its own routes; the exchange's route servers and many peers will filter out unexpected prefixes. Announcing routes with a next-hop that isn't your router is not allowed without permission of that network. In short, no hijacks or improper route leaks – if it's not your prefix or you're not legitimately upstream for it, don't announce it.

- **No Transit Via the IX**: Paducah IX is for peering, not transit. This means you should only exchange traffic with networks on the IX for destinations that are advertised via the IX. You may not use one peer to reach a third-party network that isn't peering with you. Do not forward traffic across the IX to a peer unless you learned the route from that peer (or they explicitly agreed to forward it) . Similarly, do not point a default route or a static route for "everything" at an IX peer's IP. Every participant's router should send traffic to other participants only for prefixes those participants have announced on BGP. Using an IX peer as your transit provider (without their consent) is a violation. In other words, no "free transit" or proxy routing – the IX is a meeting point for mutual exchange, not a transit hub. If you need transit, arrange it outside the IX.

- **Routing Consistency and Filters**: We highly recommend all peers employ basic BGP hygiene, such as max-prefix limits and prefix filters, to avoid mishaps. Paducah IX route servers (and many peers) will use IRR/RPKI data to filter invalid routes. As a participant, you should likewise filter announcements from others to protect your network (at least set reasonable max-prefix limits for each session). Avoid advertising overly specific routes (e.g. /28s in IPv4) or rapidly changing your announcements (route flapping) as this can degrade stability . Also, honor any BGP community signals that are commonly used on the route servers (if applicable) for traffic engineering – we'll document any supported communities separately. The key point is to be a good BGP citizen: announce stable routes, and don't overload your peers with unnecessary routing churn.

- **Multilateral Peering (Route Server) vs Bilateral**: You may peer bilaterally (direct one-to-one BGP sessions with other members) and/or use the Paducah IX route servers for multilateral peering (one-to-many). These options are described more in the next section, but in terms of policy: it's entirely up to you which peers you connect with. Some networks will use the route server to automatically peer with everyone who is also on it, while others may establish direct BGP sessions with specific networks for traffic or policy reasons. Both approaches are welcome, and in fact using a combination (route server and selective direct peers) is often beneficial. Paducah IX encourages members to take advantage of the route servers for easy connectivity, and to set up direct peering where deeper coordination or performance needs exist.

- **Respect Peering Agreements**: If you do have a bilateral peering agreement or decide not to peer with someone, please respect those arrangements. Do not attempt to circumvent a peer's policy (e.g., by using the route server if they've marked "never via route server" in PeeringDB, the route server will honor that setting). Likewise, if a network prefers not to peer, please refrain from pushing the issue on the IX – reach out offline to discuss if needed. The community ethos is consent-based peering: both sides should agree on establishing a BGP session. Paducah IX just facilitates the connection and route exchange once that mutual agreement is in place.

Route Servers and PeeringDB Requirements

Paducah IX operates one or more Route Servers to make it easy to peer with many networks at once. Connecting to the route server is optional but recommended for most participants, especially newcomers, as it provides instant peering with all other route-server users. Here are the guidelines regarding route server usage and the related requirement for PeeringDB/IRR:

- **Route Server Usage**: The route server is essentially a router that "reflects" routes between all participants connected to it. If you choose to peer with the route server, you will automatically exchange routes with every other participant who is also using the route server (subject to filtering and policy controls). This is a convenient way to quickly peer with multiple networks via a single BGP session. Paducah IX maintains two route server instances (for redundancy) and we recommend setting up sessions to both. All route server sessions are IPv4 and IPv6 capable. They do not forward traffic themselves (they only exchange routes), and they do not add themselves to the AS-PATH (we use AS-transparent route servers like many IXPs, so the route server's AS does not appear in the path) . This means when you get a

route from the RS, the next hop is the origin peer, and you will send traffic directly to that peer, not through the server.

- **PeeringDB Profile – Required for Route Server Users**: In order to join the route server, you must have a PeeringDB entry with your ASN and peering details. Most IXPs make this a requirement for route-server participants, and Paducah IX does too. The route server will use your PeeringDB info (such as max prefix counts, IRR ASN or AS-SET) to help build filters . Ensure your PeeringDB record is up to date with: your ASN, NOC contacts, peering policy, and importantly an IRR entry (such as an AS-SET) that contains the prefixes you intend to announce. Paducah IX route servers perform strict filtering based on IRR and RPKI data to prevent incorrect announcements. Routes not matching your PeeringDB/IRR info will be rejected. If you need help creating or updating a PeeringDB entry or IRR records, let us know – it's crucial for smooth multilateral peering. (Note: If your PeeringDB has the setting indicating you don't want route server peering, we will honor that and not establish a session.)

- **PeeringDB – Encouraged for All Peers**: Even if you only do bilateral peering (and choose not to use the route server), we strongly encourage having a PeeringDB profile for your organization. A PeeringDB entry isn't strictly required for a direct one-to-one peering, but it is the de facto way networks find peering info about each other. By listing your ASN, peering policy, and IX connections on PeeringDB, you make it easy for other Paducah IX members to see that you're available and to contact your peering admin/NOC. Many networks will look there first before sending a peering request. It also helps advertise Paducah IX's value – prospective members might check how many networks are on the IX via PeeringDB. So please create and maintain an entry on peeringdb.com for your ASN (if you haven't already) and associate your Paducah IX connection with it. Keep your technical contact email and 24×7 support contact updated there, as those will be used for coordination (and in case of any issues). The IX operators will also use your PeeringDB contacts if we need to urgently reach you about your port.

- **IRR and RPKI for Prefixes**: As part of best practices, all peers (especially route server users) should register their routes in an Internet Routing Registry (IRR) and create ROAs in RPKI for their prefixes. The Paducah IX route servers will enforce IRR-based filtering: only prefixes that have a matching route object (or are in your listed AS-SET) and are RPKI-valid will be accepted. This protects everyone from route hijacks or leaks. Ensure that your ASN is listed as authorized origin for your prefixes in IRR/RPKI. If you use an AS-SET, put that in your PeeringDB IRR field so

our route server knows to pull it. (If all this sounds daunting, don't worry – these are standard practices, and we can assist if you're unfamiliar with IRR or RPKI.) The bottom line: route server peering requires prefix registration. For bilateral only peers, IRR/RPKI is still highly recommended, but your direct peers might handle filtering individually.

- **Route Server Communities and Options**: Paducah IX route servers support common BGP communities for controlling route propagation (e.g., to opt-out of announcing a route to certain peers, or to blackhole traffic). We will publish a separate guide on route server community controls. By default, all routes you announce to the RS are advertised to all other RS participants (except any that have set "never via RS" for you). If your policy is selective, you might prefer bilateral sessions instead of using the RS. You can also use BGP communities to simulate a selective policy on the RS (again, see documentation). We want the route server to be useful to as many members as possible, without overriding anyone's individual peering preferences.

- In summary, Paducah IX's route servers are a powerful tool for easy peering, but they come with the responsibility of maintaining accurate peering records (PeeringDB/IRR). We encourage all participants to connect to the route servers and complement that with direct peering where needed – this dual approach maximizes your reachability . If you choose not to use the route server, that's okay too – just be proactive in arranging bilaterals with other networks. In all cases, keep your info updated and follow the general routing policies outlined above.

Traffic Handling and Behavior on the Exchange

This section covers what is considered acceptable vs. unacceptable behavior in terms of traffic and use of the exchange. Paducah IX is a shared Layer-2 domain, so it's important that every participant acts in a way that doesn't adversely affect others. Here are the traffic guidelines and etiquette for using the IX:

- **Send Traffic Only to Agreed Destinations**: As emphasized before, only send traffic to a peer that is intended for that peer's networks. Do not forward packets to someone unless that someone's router has advertised a route for those packets . In practical terms, if you receive traffic from your customers destined to some prefix, you should only send it out via Paducah IX if you learned that prefix from a Paducah IX peering session. The exchange is not to be used to "trial-and-error" where to send traffic – it's for delivering on known BGP routes. Also, do not use the Paducah IX broadcast domain to reach the internet at large (e.g., no sending traffic to the

exchange hoping someone will handle it). Every packet on the IX should have a Paducah IX participant as its clear destination. This prevents abuse and confusion (like using another peer as transit without permission, which is not allowed).

- **No Traffic Flooding or Malicious Behavior**: Participants should not flood the IX with excessive traffic beyond what is normal for legitimate peering. Broadcast storms, constant ARP probing, or any form of Denial-of-Service attack emanating from your port is strictly forbidden. Our switch will rate-limit broadcasts and protect against storms, but members are expected to police their own networks. Malicious activities (scanning other peers' IPs, attempting to intercept traffic, etc.) are absolutely not tolerated. The IX is a cooperative environment – any network engaging in attacks or knowingly causing harm to others will be removed.

- **No Unapproved Third-Party Connections**: Your Paducah IX port is for your network's use only. You may not resell, extend, or give access to the IX to a third party that is not an IX member. For instance, do not plug in a switch and offer exchange connectivity to another organization through your connection. Every legal entity must have its own membership/port. If you operate on behalf of a customer, that customer needs to join the IX separately if they want direct peering. Providing exchange access to non-members violates the rules (and can cause complex technical issues). Paducah IX may allow certain approved arrangements (like a known network operator extending the fabric to remote participants) only with prior agreement and proper documentation, similar to how other IXs handle "switch extensions" . Unless such permission is granted, do not connect anyone else's equipment to the IX via your port.

- **No Exchange LAN Leakage**: Please ensure that the Paducah IX peering subnet (the IP block used for our peering LAN) is not carried into your internal network or announced to the global internet. In other words, filter out the Paducah IX IP range on your side to prevent any routing leaks. Your other routers (not connected to the IX) should not have a route to the IX LAN. Do not redistribute the IX's LAN prefix into your IGP or advertise it via BGP to others . This avoids confusion and potential security issues. If your network can reach the IX LAN from outside the exchange, implement access control lists (ACLs) to block that . All traffic for the IX LAN should stay within the exchange. (This also means you shouldn't use the IX LAN IPs for anything except IX-related communication.)

- **Bandwidth and Load**: Currently, Paducah IX does not police traffic levels – you can utilize your port up to its capacity. However, be mindful of other shared resources.

For example, sending excessive broadcast ARPs or doing constant large-scale traceroutes can have minor impact on others. It's best to use the IX for actual customer/user traffic exchange and reasonable operational traffic. If you expect extremely high bandwidth bursts (relative to port speed) or atypical usage patterns, it might be courteous to inform the IX operators or the peers, just so everyone is aware. Standard large traffic flows (CDNs, backups, etc.) are fine, that's the point of an IX! We just ask to avoid anything non-standard that could look like an attack or misconfiguration.

In essence, use the IX in the spirit it is intended: exchange traffic with your peers' networks efficiently, and nothing more. Don't abuse the platform or try to make it do something it's not meant to. If you stick to BGP-advertised traffic flows and avoid sending anything unsolicited or unusual, you'll be within the acceptable use.

Communication and Enforcement Procedure

Paducah IX's approach to enforcement is informal and cooperative. We believe most issues are unintentional and can be resolved with a quick communication. Our goal is not to be punitive but to maintain a reliable exchange. Below is how we handle rule violations or technical problems, in increasing order of severity:

1. Notification and Friendly Warning: If Paducah IX staff or the community observes a potential issue with your port (e.g. a misconfiguration or traffic abnormality that goes against this AUP), we will reach out to you via your PeeringDB contacts or email/phone on file. Expect a message describing the issue and asking for your assistance in resolving it. This is a friendly heads-up, not an accusation. We understand mistakes happen. You'll be given a reasonable timeframe to respond and fix the issue. For non-urgent matters, we typically allow up to about two weeks to hear back and see progress before considering further action. During this period, your port generally remains active so you can troubleshoot, unless the issue is critically impacting others.

2. Temporary Quarantine (if Needed for Urgent Issues): If the problem is serious – for example, your port is causing a broadcast storm, MAC flaps, or a large route leak – we might temporarily disable your port to protect the overall IX fabric . This is rare and we try to avoid it unless absolutely necessary. In such urgent cases, we will still attempt to contact you immediately. The port shutdown is not a punishment but a protective measure for everyone. We will work with you to get the issue resolved and restore connectivity as soon as possible. Once you've corrected the underlying

cause, your port will be re-enabled (and you can then verify everything is working normally).

3. Collaborative Resolution: In most cases, after contact, the member fixes the configuration (e.g., disables a rogue protocol, stops a leak) and no further action is needed. We encourage an open dialogue – Paducah IX staff can assist in diagnosing the problem. Often we might notice something before you do (thanks to monitoring) and our email is just to bring it to your attention so you can adjust. We maintain a mailing list and a Slack channel for members to discuss issues openly as well. Other participants might chime in if they see an issue (for instance, if your router is continuously flapping BGP, another peer might reach out). This peer feedback and cooperation is part of the community spirit. We prefer remediation over penalties.

4. Repeated or Egregious Violations: If a participant repeatedly violates the AUP or fails to respond to communications, Paducah IX reserves the right to suspend the participant's port indefinitely until the issues are resolved . In extreme cases (for example, willful malicious activity or complete non-compliance), the Paducah IX governance may revoke your membership. We will generally issue multiple warnings and attempts to find a solution before it ever reaches that point. Disconnection is truly a last resort. The IX may also impose conditions for reconnection (such as demonstrating the fix or agreeing to specific safeguards). Our aim is never to get to this stage – it's bad for both the participant and the IX – so we do everything possible earlier to fix problems amicably.

5. Appeals and Feedback: If you feel a notice or action was in error or unfair, you can appeal to the Paducah IX Board of Trustees. Because our process is informal, a simple conversation often clears things up. The governance board can review chronic issues if needed. We are all ultimately on the same team, wanting the exchange to run smoothly. Member feedback on these policies is welcome; the AUP itself may evolve based on community input.

Enforcement Summary: We'll warn you and work with you to sort out any problems. Only if that fails, or if there's an immediate threat to the IX, will we shut your port down. We much prefer communication and collaboration over sanctions. By keeping your contact info updated and responding promptly to IX staff inquiries, you'll find that most issues can be resolved without any downtime.

Finally, remember that this AUP is a living document – it can be updated as technologies change or new best practices emerge. We'll always notify members of any significant changes and, where possible, operate by consensus and community agreement.

Conclusion and Community Ethos
The Paducah Internet Exchange thrives on a spirit of mutual trust and cooperation. This AUP is not about ticking legal boxes; it's about building a community of networks that all benefit from a well-run exchange point. By joining Paducah IX, you're not just getting a port on a switch – you're becoming part of a local networking family that looks out for one another.

Key takeaways to keep in mind:

Do the Right Thing: If you're ever unsure whether something is allowed or a good idea on the IX, err on the side of caution or ask us. These guidelines are mostly common sense for experienced network operators. When in doubt, just remember not to harm others and to play fair.

Help Each Other: The community-driven nature means participants often assist each other – whether it's troubleshooting a BGP session or sharing guidance on PeeringDB. Don't hesitate to reach out on our member mailing list or contacts if you need help or have questions.

Benefit Together: The more networks that join and abide by these best practices, the more valuable the IX becomes for everyone. Encourage other networks in the region to consider peering, and lead by example with good etiquette.

Have Fun Peering!: Internet exchanging is one of the more enjoyable aspects of network engineering. You get to connect with many different organizations and improve internet quality for users. We hope you find your participation in Paducah IX rewarding and maybe even a bit fun!

Thank you for reading through the AUP. By adhering to these guidelines, you help ensure that Paducah IX remains a robust and friendly exchange point. If you have any questions about the AUP or suggestions to improve it, please contact the Paducah IX team.

Happy Peering!