

Africa

DataCentres

Africa Data Centres

The **heartbeat** of your business

Advantages of

peering in carrier and cloud-neutral data centres

Version 1.00

Advantages of peering in carrier and cloud-neutral data centres

Internet exchange points (IXPs) are a crucial part of the Internet, enhancing connections for citizens and organisations alike, and helping economies thrive. Most major cities in developed countries have an internet exchange or two, because as data travels across the internet, it is re-routed and re-directed between different networks. Often, traffic on one network has to switch to a different network which might be owned and controlled by another party. IXPs enable this type of data transfer through a process called “peering,” which enables networks to hand off customer traffic between each other’s networks without the cost of having to pay a third party to carry it across the web for them.



Keeping traffic local

Without IXPs, traffic switching from one network to another has to depend on intermediary networks or transit providers, to transport the data from its source to its destination, which results in notable latency. Moreover, there would be fewer routes for data to travel, and the ability to easily switch onto whichever network happens to be fastest at the time would be compromised should there be any issues with the transit provider’s network, including traffic surges, slow connections, or packet loss. Peering through internet exchanges addresses all of these challenges by ensuring the shortest possible route is used to reach a given destination. It keeps traffic as local as possible, which improves performance and enables faster connections between networks, facilitating high-speed data transfer, lower latency, increased bandwidth and improved fault tolerance.

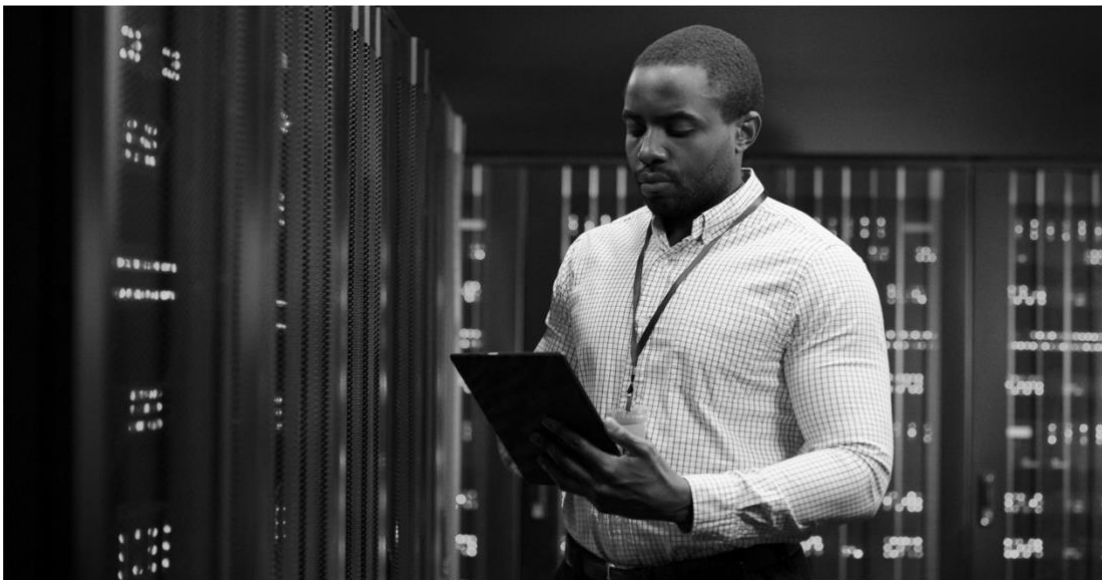
One IXP can serve a wide range community, based on the size of their digital market and geographic limitations. However, in Africa, many countries have had to pay international carriers to exchange “local” traffic on their behalf. This was an expensive and inefficient way of handling the exchange of traffic between African nations, because for an efficient and functional Internet, traffic needs to stay as local as possible to keep in line with data residency regulations and keep Internet costs low.

Addressing the IXP issue

Several initiatives have been formed to address this issue. Heads of State and Government of the African Union, meeting in the Fourteenth Ordinary Session of the AU Assembly, adopted a declaration that undertook to strengthen national programmes and regional cooperation for the development and interconnection of broadband infrastructures and the deployment of regional IXPs. The establishment of the African Internet Exchange System (AXIS) aimed to lower communications costs, reduce the cost of financing trade and ultimately the price of goods. Moreover, affordable and accessible bandwidth is said to fuel regional trade integration and new "think work" industries like business process outsourcing (BPO) and call centres will create employment, lower poverty, and generate wealth for the continent.

Encouragingly, [The Internet Society](#) conducted a broad overview of the members of the African IXP Association (Af-IX), and a number of IXPs that are not members. In 2021, over half of Africa's countries had an IXP (Internet Exchange Point), with six countries having multiple IXPs (Angola, Democratic Republic of Congo, Kenya, Nigeria, South Africa, and Tanzania). However, 20 countries in Africa still lacked an IXP, missing out on its benefits.

The report also revealed that some regions were outperforming others in terms of Internet adoption, despite having similar income levels. This, the report said, can be attributed to these countries' positive enabling environments, including support for the IXP ecosystem, which has become a proven contributor to lowering the cost of Internet access and improving access to content and services connected to an IXP. It is obvious then, that it is in the interests of all countries in Africa to find ways to optimise internet traffic, to support intra-continental traffic flows, and create opportunities for private sector investment in these areas.



Instant network optimisation

However, while the need for IXPs is clear, they are not all created equally. IXPs are charged with bringing content closer to business and consumer customers, so these deployments require a network architecture that can connect many peers together at very high bandwidths. This helps to drive faster service creation, content delivery and better customer experience by combining the ability for massive scale with the intelligence of routing.

Peering in a cloud- and carrier-neutral data centres offers several significant advantages for businesses and service providers. These facilities act as central hubs where multiple networks interconnect, enabling efficient and cost-effective data exchange. For one, when IXPs and content providers take up space together in colocation data centres, they ensure that local traffic remains local, something that is becoming increasingly important in today's stringent regulatory environment that is forcing organisations to be compliant when it comes to data residency and sovereignty.

In addition, peering in neutral data centres facilitates direct interconnection between networks without having to traverse multiple hops through the public internet. This direct connectivity lowers latency and boosts network performance, resulting in faster data transfer speeds and lower packet loss. By avoiding congested public internet routes, businesses can provide a more reliable and responsive user experience for their customers.

Scalability, cost-saving and reliability

Peering in neutral data centres can help organisations realise dramatic cost savings too. By exchanging traffic directly with other networks, organisations can reduce their dependence on internet service providers (ISPs) for data transit. Peering agreements often involve settlement-free arrangements, where participating networks agree to exchange traffic without charging fees. This can result in fairly substantial cost savings when it comes to bandwidth and data transfer expenses.

Another compelling benefit is increased reliability. Cloud- and carrier-neutral data centres are designed with redundancy in mind, guaranteeing high levels of availability and resilience. By peering in these facilities, entities can reap the benefits of diverse connectivity options and redundant network paths. If one connection or provider experiences an outage or performance

issue, traffic can be automatically rerouted through alternative paths, minimising disruptions and maintaining service availability.

Peering in neutral data centres also enables organisations to scale their network capacity rapidly and efficiently. As these facilities serve as interconnection points for multiple networks, adding or increasing network capacity becomes straightforward. This scalability is key for businesses undergoing growth spurts or for those who experience seasonal fluctuations in network demands, as it enables them to scale their infrastructure to changing requirements without the need for major investments or disruptions.

Flexibility, security

Businesses are also allowed the flexibility to choose their network and service providers based on their unique requirements. They are not locked into a single provider and are able to negotiate peering agreements with a range of networks to ensure redundancy, performance, and cost savings. This flexibility enables companies to gain more control over their network infrastructure and tailor their connectivity options to meet their specific needs.

Enhanced security is another major benefit. Peering in cloud- and carrier-neutral data centres is more secure, as exchanging data directly with trusted networks can help businesses reduce the exposure to potential security risks associated with traversing public internet routes. Moreover, these data centres have top security standards in place, such as ISO 27001 and PCI DSS, and have robust physical security measures in place, including 24/7 monitoring, access controls, and multiple layers of authentication, to ensure that sensitive data and infrastructure are protected.

Finally, peering in cloud- and carrier-neutral data centres gives businesses access to a rich and broad ecosystem of interconnected networks, cloud service providers, content delivery networks (CDNs), and other service providers. This ecosystem comes hand in hand with many opportunities for collaboration, content delivery optimisation, and the creation of value-added services. By leveraging this interconnected environment, businesses can expand their reach, improve service quality, and foster partnerships that enhance their overall offering.