Promoting the Use of Internet Exchange Points: A Guide to Policy, Management, and Technical Issues By Mike Jensen

Summary

Internet Exchange Points (IXPs) are vital elements of Internet infrastructure that enable networks to exchange traffic with each other. Multiple Internet service providers (ISPs) can connect at a single IXP, creating the potential for a range of technical and economic benefits for the local Internet community. By keeping local traffic local and avoiding international links, local operators and users can reap substantial cost savings, provide substantial local bandwidth, and significantly improve local Internet performance. In this paper, Mike Jensen describes the role and technical operation of IXPs; explains the most common IXP operational models, including advantages and impediments to their establishment; and provides examples of successful, working IXPs in several countries.

Mike Jensen is an independent ICT consultant who has assisted in the establishment of information and communications systems in developing countries for more than 20 years. Drawing on his hands-on experience in 40 African countries, Sri Lanka, and Brazil, Jensen offers advice to international development agencies, the private sector, NGOs, and governments in the formulation, management, and evaluation of Internet and telecommunication projects. A go-to expert and public speaker at international meetings, Jensen's primary focus is on policy and technology developments in rural telecommunication projects, community access, fibre, wireless, and satellite connectivity.

1775 Wiehle Avenue, Suite 201
Reston, VA 20190-5108, U.S.A.
+1 703 439 2120

Galerie Jean-Malbuisson 15
CH-1204 Genève, Suisse
+41 22 807 1444

03/09

INTERNET SOCIETY REPORTS

Introduction

The Internet is not a single entity. It is a large group of independent networks that agree to share traffic with each others' customers using a common Internet protocol (TCP/IP). Without this agreement, it would be impossible for users of two different networks to send each other email. The key task of an Internet provider is to ensure that its users are able to most cost-effectively connect to any point in the world that is connected to the Internet, be it a web site on the local network or a user connected to another network in the same city or in a distant part of the world.

Internet exchange points (IXPs) are a vital part of this system. Without them, the Internet could not function because the different networks that make up the Internet would not be able to exchange traffic with each other. The simplest form of an exchange point is a direct connection between two Internet Service Providers (ISPs). When more than two providers operate in the same area, an independent switch operates more efficiently as a common interconnection point at which to exchange traffic between the local networks. This is similar to the development of regional airport hubs where many different airlines are served. At these locations, airlines exchange passengers between their flights in much the same way that networks exchange traffic across the IXP.

For Internet providers and users, there are many advantages to local routing of Internet traffic via a common exchange point:

- Substantial cost-savings are made by eliminating the need to put all traffic through the more expensive long-distance links to the rest of the world.
- More bandwidth becomes available for local users because of the lower costs of local capacity.
- Local links are often up to 10 times faster because of the reduced latency in traffic, which makes fewer hops to get to its destination.
- New local content providers and services, which rely on high-speed low-cost connections become available, further benefiting from the broader user-base available via the IXP.
- More choices for Internet providers become available on which to send upstream traffic to the rest of the Internet—contributing to a smoother and more competitive wholesale transit market.

So far, more than 300 IXPs have so far been set up worldwide—an increase of more than 50 percent since 2006. Regionally, Latin America has experienced the fastest recent growth in numbers of IXPs, reaching 20 by the end of 2007—almost double the number of the previous year. However, developing countries have generally lagged behind the rest of the world in establishing IXPs. The Asia-Pacific region grew the slowest in 2007 at 15 percent, bringing the total number of IXPs in that region to only 67. Africa has the fewest IXPs—only 17 of the 53 nations had IXPs in 2007—and growth was only 21 percent over the previous year.

Due to the limited amount of local online content and services in many developing countries, most of the Internet traffic generated by users is international, resulting in large capital outflows paid to foreign Internet providers. Local content providers in these countries tend to operate offshore, where it is cheaper to host them due to the lack of low-cost local infrastructure of which an IXP is an integral part. Thus, the presence of an IXP helps to encourage more local content development and creates an incentive for local hosting of services. This is both because of the lower cost and the larger pool of local users, who are able to access online services faster and more cost effectively.

From a public policy perspective, ensuring the presence of local IXPs is becoming increasingly important. It ensures online services are equally accessible to all local users, enhances competitive opportunities, and improves the quality and affordability of Internet services.

In May 2007 88 countries still did not have even one IXP. As a result, networks in most of these countries must exchange traffic via expensive international links, although in some cases they may pay high prices for local transit through what is often a monopoly telecommunication provider. This occurs despite the fact that one of the largest costs for network operators in developing countries is that of international capacity, and the fact that IXPs are relatively inexpensive to set up. By one estimate, an expenditure of approximately USD 40,000 is all that is required to establish a national IXP. Indeed, some network operators have managed to set up IXPs for a fraction of this cost using donated equipment and facilities. Yet many countries without IXPs pay much more than this amount every few weeks to foreign operators for carrying local traffic—a situation that further and unnecessarily increases foreign capital outflows.

The barriers to establishing IXPs in countries where they do not yet exist are largely non-financial: there is often a lack of mutal appreciation of benefits among all stakeholders, as well as resistance from those providers with market dominance. In addition, limited technical skills and a lack of open competitive markets in telecommunication and Internet services make it more difficult to establish an IXP.

This guide provides an introduction to IXPs by outlining their role as a key component of Internet infrastructure and covering the policy, management, and technical issues, which must be considered in their establishment. An description of selected IXPs is provided, as is a glossary of terms.

The Role of Internet Exchange Points

Commercially, the Internet consists of a hierarchy of global, regional, national, and local providers. These either sell transit services to other operators for traffic they pass through their networks or, when two networks of similar market position exchange roughly equal amounts of traffic, they enter into a settlement-free arrangement called peering. Peering and transit take place directly between two networks or via an independent exchange point.

The term *Internet exchange point (IXP or IX)* is often used interchangeably with *exchange point (EP), Internet peering point (IPP),* and *network access point (NAP).* While there are no formally agreed definitions for these different terms, the most commonly used are *IXP, IX,* and *peering point. NAP* is an older term, originally used for the first four exchange points, which, prior to the global development of the Internet, provided access to NSFNET, the Internet backbone operated by the U.S. National Science Foundation.

As the Internet developed, the original NAPs were joined by commercial and nonprofit exchange points, first within the United States and then in other nations wherever significant amounts of local traffic were generated by more than one network operating in the same area.

As shown in Figure 1, any network connect to the Internet via a connection to the Internet cloud. This enables it to pass traffic between its users and others on different networks.

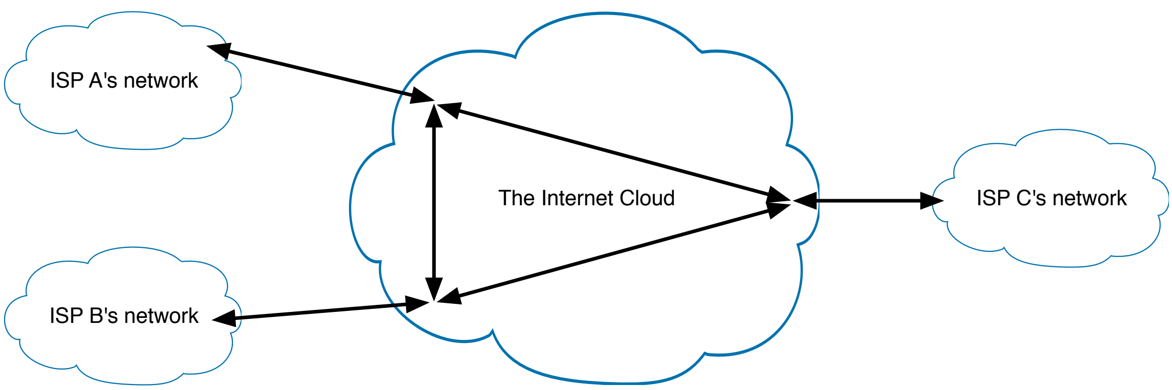

Figure 1.

If two networks that are independently connected to the Internet are close to each other—e.g., in the same city or country—it may be faster and cheaper to use a separate connection to send local traffic directly between the two networks. See in Figure 2.

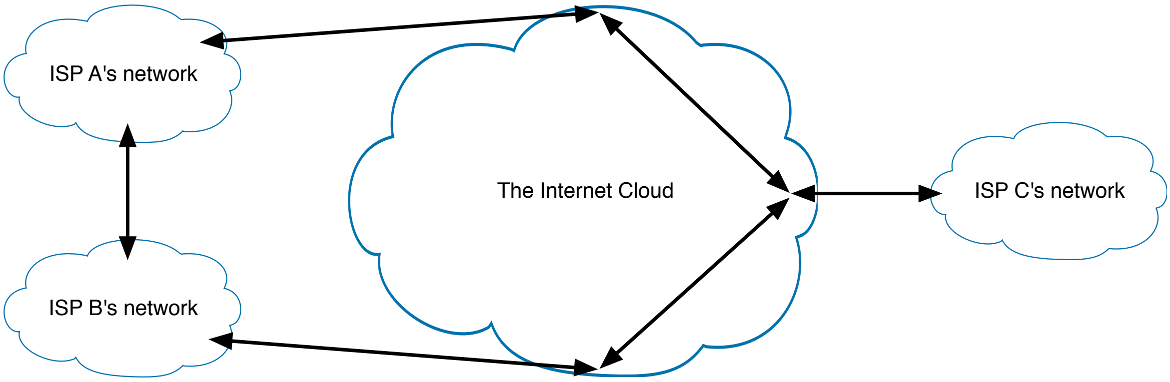

Figure 2.

When there are more than two local networks, which need to exchange traffic, it becomes more efficient to establish a switch (IXP) to which each network can connect. Figure 3 shows how three ISPs may share a local IXP to route all of their local traffic. An IXP can thus be viewed as the centre of a star network that makes it possible for local traffic from any local network to traverse through a single connection to the switch. This decreases the telecommunication and management costs of multiple direct links between each network and increases the speed of local traffic by minimising the number of network hops required to reach any other local network.

While Figure 3 shows the most simple example of an exchange point used to route traffic, various local factors affect the viability of an IXP and create a wide range of permutations in the implementation of this basic model. The key factors in connecting to or setting up an IXP are: (1) the amount of traffic that is likely to flow between the local networks, and (2) the cost of the physical connection between the network and the IXP versus the cost of the connection to the upstream Internet cloud.

To take a simple example, assuming that each of the three networks above have 10Mbps connections to the upstream Internet cloud, in a developing country this could cost them each about USD 30,000 per month (that

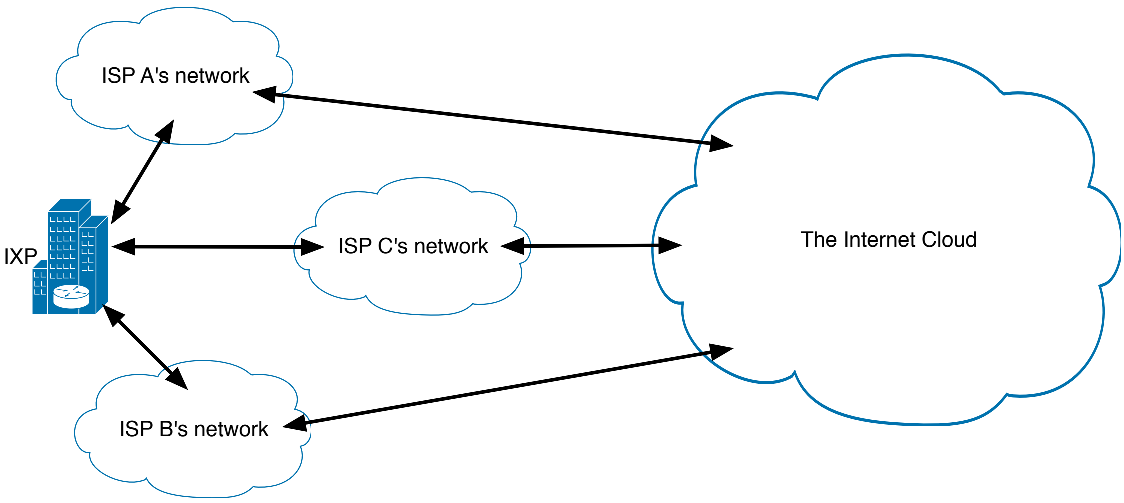

Figure 3.

is, a total annual cost for all three networks of 3 x USD 30,000 per month x 12 months = USD 1,080,000. Assuming only 20 percent of the traffic is local means that roughly USD 216,000 per year is spent on routing local traffic via the upstream Internet link. If the three networks can self provide their links to the IXP at no cost, such as via a wireless circuit or sharing facilities located in the same building, an IXP would pay for itself in a few months.

In practice, networks may need to lease connections from a licensed telecom provider to reach the IXP, in which case the cost for local bandwidth might be as much as USD 1,000 per Mbps per month in a developing country. This equals an annual cost for local links of 20 percent x 30 Mbps x USD 1,000 per month x 12 months = USD 72,000—an annual savings of almost USD 150,000 (although a portion of this would need to be applied to maintaining the IXP). Naturally, if there are increases in the number of local networks, in the size of their upstream links, or in the proportion of local traffic, much greater savings can be provided by an IXP.

In most countries, the first step is to set up a national exchange point to keep traffic within the country. Additional exchange points might then be established to serve smaller geographic areas where it is more cost effective to keep traffic local. This is particularly the case in developing countries where national telecom backbone infrastructure is poorly developed, congested, or particularly costly—a common situation where cities are still connected via satellite links and when monopoly pricing is in force. As a result, IXPs are often needed in the secondary cities, as well.

By contrast, IXPs situated in locations where competitively priced international optic fibre links are available can attract international membership. Networks from other countries may be generating sufficient traffic with members of the foreign IXP to warrant the cost of a direct international link versus paying another network for transit. For example, The London Internet Exchange (LINX), an IXP in the United Kingdom has members from 40 countries (see The London Internet Exchange below).

Reducing operating costs by establishing a local IXP decreases Internet access prices to the end user and provides faster response times from local web sites and other local interactive services. This is especially the case when international links are congested and when international traffic is carried over satellite links. This is because the latency (delays) caused by routing local traffic via satellites can be cut from seconds to milliseconds when two local networks are directly connected. As a result, response times for local web sites are dramatically improved and more advanced local services which require low-latency connections (VPNs, multimedia streaming, and VoIP) become viable. When links between networks rely on satellite connections, many of these services cannot be provided with acceptable quality and some do not run at all. A local interconnection point is critical to ensuring their availability to users.

The establishment of an IXP also has indirect benefits on the pricing of telecom capacity. In Nigeria the IXP negotiated lower rates for international connectivity for its members. In July 2007 the price for 1 Mbps of capacity on the international fibre cable (SAT3) was reduced from USD 6,300 to USD 2,800 per month for networks participating at the Internet Exchange Point of Nigeria (IXPN). Such a reduction could have been negotiated independently of the IXP, but it can be argued that the creation of the IXP had a catalytic effect and by having a group of networks at the same location, IXPN could negotiate a better deal with the upstream provider.

A further advantage of an IXP is that it reduces transactional costs and improves choice for its members. If a network decides to switch transit providers at an IXP, they can do so in a matter of hours and without physical intervention. In the past, this would have involved having a new circuit installed, as well as incurring significant waiting time and financial charges. The fluidity available by the IXP promotes cooperative behaviour from providers and encourages greater price competition—further driving down costs for access providers and end users. While some IXPs do not yet allow transit agreements, this position is now generally seen to be counter productive and these restrictions are becoming less common.

Once an IXP is established, it becomes a natural location to host a variety of other services that reduce bandwidth requirements and improve the speed and reliability of Internet access for local users. The most important of these include domain name servers, root server mirrors, time servers, web caches, and news servers. In addition, a variety of administrative facilities for network operators are often hosted at an IXP, such as looking glass and traffic measurement facilities. While some IXPs may only allow access providers to be members, in many cases content providers are permitted to connect to IXPs.

The presence of an IXP can attract telecommunication operators that may establish a point of presence at an IXP in order to easier sell services to potential customers located at the exchange, as all parties are reachable at low cost. In this respect, IXPs help to encourage the development of telecom infrastructure (such as national and international fibre cables).

Using an IXP to provide its members with a single shared connection to the Internet cloud and to interconnect national IXPs have been suggested as possible ways to cut costs and keep traffic in the same region. In general, these strategies have not been successful—they negatively affect the business of the IXP members that sell such links to clients. This does not mean that interconnections among IXPs or transit sharing cannot be implemented. In some specific cases, if there is agreement among the members of the IXPs and appropriate business models can be found, implementation is feasible. Also, to improve reliability, prior agreements may be made so that in the event of a disruption to a network's upstream Internet link, the IXP could be used as a temporary route to the Internet cloud via another member.

Institutional and Operational Models for IXPs

A variety of institutional models have been adopted to operate IXPs. They fall into four categories:

1. Nonprofit industry associations of ISPs
2. Operator-neutral commercial and for-profit companies
3. University and government agencies
4. Informal associations of networks

Of these models, the most common is one in which IXPs are operated by a nonprofit industry association of ISPs. This is the case in Europe where many IXPs are typically mutual, nonprofit organisations in which members collectively own the facility or it is owned by the industry association. Operating costs are shared among members who will pay a one-off joining fee, plus a monthly, quarterly, or annual operating fee. The fee is normally determined by the speed (bandwidth) of their connections to the IXP or, less commonly, by the volume of traffic that passes across the exchange. In the United States, commercial IXPs are more prevalent and are operated by specialised companies such as CIX, Any2, and Equinex. They are almost always provider neutral and do not compete with ISPs in providing services to end-users.

Note should be made of the presence of phony IXPs where the dominant Internet operator provides local exchange points in one or two major cities. In these cases, the IXP is used more as a marketing term by the commercial transit provider, but is really no more than a router offering BGP4 peering for the sale of local or international transit.

IXPs are usually formed by a founding group of network operators who decide which model best fits the local environment. Key questions to address include:

1. Will the IXP have permanent staff or be operated by volunteers?
2. Will the IXP be a nonprofit or for-profit organisation?
3. Will the IXP be entirely cooperatively owned by its members or will it have external ownership?
4. Where will the IXP be hosted?
5. What cost-recovery method will be used?

In developing the appropriate institutional policies for the IXP, a variety of choices must be made. A common requirement to connect a network to an IXP is that its operator must be a recognised legal entity and must be licensed to operate a network (if a license is required). In some cases it is a policy that member network operations include transmission of third party content or services. In other cases this is not a requirement and any entity that needs to exchange traffic with the IXP members is allowed to join. This option allows the operators of large private networks that provide services to the public—such as hosting providers, government departments, or banks—to take advantage of only having to establish a single link in order to reach the users of other local networks.

Technically, there are two predominant models for IXP operation. In the simplest model, Layer 3 IXP, IXPs exchange traffic between member networks inside a single router. In the other model, Layer 2 IXP, each network provides its own router and traffic is exchanged via a simple Ethernet switch. Overall, the Layer 3 model may be less costly and simpler to establish initially, but it limits the autonomy of its members and has generally been superseded by the Layer 2 model. The Layer 3 model also offers providers less control regarding with whom they can peer and makes them dependent on a third party to correctly configure and maintain routes—which requires greater technical skills from the IXP staff. In contrast, the Layer 2 model does not require the staff to have any routing knowledge.

The requirements for traffic routing agreements between IXP members vary depending on the IXP's institutional model and other local policies. Many require a Mandatory Multilateral Peering Agreement (MMLPA), in which those who connect with the IXP must peer with everyone else who is connected. This creates a disincentive to large ISPs to interconnect and may reduce incentives to keep technical operation in top condition.

Other IXPs may require each network to enter into Bilateral Peering (BLP) arrangements with the other network members. And some IXPs may limit the use of the facility for such transit traffic.

Although MMLPAs are common among many IXPs, flexible peering policies that permit the coexistence of multilateral and bilateral peering arrangements will allow peers at an IXP to enter into separate bilateral peering or transit agreements. It is usually acceptable for IXP members to restrict (filter) traffic originating from or destined for any member's network in accordance with the member's policies, which are normally specified in the Internet Routing Registry (IRR).

Other important policies and strategies that IXPs and their member networks normally adopt include:

1. Payment for the cost and management of the link between the network and the IXP (including a redundant link if required) is usually the responsibility of the member. However, some IXPs have adopted policies to smooth these costs so that each member pays the same amount to access the IXP. This helps to ensure that commercial operators who happen to be located in the same building as the IXP do not have an unfair advantage.
2. It is not usually acceptable to pass traffic to the IXP that is destined for networks that are not members of the IXP unless transit is allowed and there are specific agreements with the IXP and the members providing transit.
3. Monitoring or capturing the content of a member's data traffic is limited to data required for traffic analysis and control. Members usually agree to keep this data confidential.
4. IXPs may make the provision of routing information and looking-glass sites mandatory.
5. Routing and switch-port information can either be made public or restricted to members only.
6. Provisions are made for responses in the event of security problems, infrastructure failures, routing equipment failures, and software configuration mistakes.

Practical Considerations in Establishing IXPs

At the outset, as described above, the first step in considering the establishment of an IXP is to determine need. This would be based on a provisional assessment of the number of providers (at least three) that are willing to support and use the IXP, the amount of traffic that would be exchanged, and the likely cost of connecting to the IXP. A meeting of local network operators and technical advisers should be sufficient to establish this.

If the outcome of this assessment proves positive, the next step would be to build support for the project among all stakeholders and identify any potential policy problems or market barriers to establishing an IXP. These usually arise from either the potential members themselves or as a result of incompatible government policies.

The establishment of a local IXP is often seen as a threat by competing commercial providers who may not be aware of the full advantages of collaboration and local traffic exchange. There can be lack of trust and a fear of making business cheaper for (or even subsidising) competitors, and concerns that *interconnection* means stealing customers. These issues may need some time to be discussed and supported by awareness raising on the role of IXPs before all relevant parties are in full support of the IXP.

There may also be outstanding issues regarding participation in the IXP when there is a dominant commercial Internet service provider in the market. Such providers may be resistant to participation or they may participate but severely under-provision the link to the IXP. This is known as the Thin Pipe Stratagem. Here, the customers of competitors encounter slow connections to dominant provider's customers and, understandably, they fault the competitor for the poor connection. This creates a strong incentive for users to switch to the dominant service provider. If unsolvable by other means, this problem may be cause for regulatory intervention.

Some network providers may be concerned that IXPs are overly complicated for their needs. This is frequently the case for small ISPs with only one connection to the rest of the Internet and without sufficient technical expertise to implement multipath routing. This may be amplified by contact with large, developed-country IXPs, which have more sophisticated switches and powerful routers. Equipment vendors can contribute to this view by trying to sell sophisticated equipment that may not be appropriate for the needs of a small IXP. To address these issues, awareness raising and training activities may be necessary. At a minimum, potential members will need to be familiar with the border gateway protocol (BGP), which is used for routing between the networks, and each network will need to have a publicly registered autonomous system number (ASN) for their exchange communications (obtained from the relevant Regional Internet Registry). The use of open-source routing software systems, such as the Quagga routing suite, is an inexpensive deployment option for small ISPs and IXPs.

In most markets, exchange points are not regulated by government policy and, as most activity within an exchange is considered entirely private between the parties, should be free from government regulatory oversight. However, in many developing countries, government policies can restrain the establishment of an IXP in a variety of direct and indirect ways. Because IXPs only exist where there are multiple providers needing to exchange domestic traffic, in many countries the presence of a monopoly service provider is probably the major reason for the lack of an IXP. Alternatively, the lack of an IXP may indicate the existence of a single player with monopoly power over certain infrastructures or rights of way, such as international gateways. If low levels of competition exist, networks may have little choice but to exchange domestic traffic via the dominant player rather than directly between themselves. In the immediate term, there may be little that can be done by potential IXP members to address this problem. Continued lobbying of government policy makers and regulators should ultimately help to open markets and relax restrictions on new entrants.

Even where the market is more open, incumbent telecom operators may still resist the establishment of an IXP. The incumbent operators' views often carry great weight with regulatory authorities, for a variety of reasons ranging from close personal relationships to corruption. They also reflect the concerns of developing-country policy makers whose governments are often heavily dependent on revenues from the state-owned telecom operator and are reluctant to sanction activities which are thought to limit profits. Some policy makers may even see IXPs as a form of anti-competitiveness on the part of industry. Often, statutory or other licensing requirements exist which can arguably be applied to IXPs and, in most cases, the regulatory authority is, at least initially, unfamiliar with the technical and economic aspects of Internet facilities and ISP traffic exchange.

IXP founders need to ensure that policy makers, regulators, and incumbent operators appreciate that reducing the cost of Internet connectivity for domestic consumers will generate much greater investment, more users, and thus greater internationally leased line revenues. In fact, a strong case can be made that increased domestic use of the Internet, leads to even greater use of international direct-dial telephony to foster commercial and personal international relationships that are supported through the Internet.

In view of these factors, some governments, such as the one in Chile, have tended to the other extreme and have made it mandatory for networks to establish a peering point. Superficially this seems like a good policy, but could actually hinder growth by removing the incentives for an ISP to competitively grow beyond a single exchange.

Other government policies, which effect strategies for establishing an IXP include any limitations on self-provisioning of links between network members and the IXP. This could include limitations on use of radio frequencies and on use of space on telephone poles, and rights to dig up streets and lay cables (rights-of-way).

Once the IXP's founding members have addressed these issues, it will be necessary to decide on management structure and policies, as outlined above. Then, the required technical expertise needs to be identified and a technical committee established to design the IXP, budget it, and find the most appropriate location to host it. This may include an assessment of existing facilities and comparing their use to the cost and effort involved in setting up a new, independent facility. In many countries, costs associated with leasing space, purchasing power, and hiring staff can be high. Hosting an IXP in an existing data facility can substantially reduce these operating expenses. Existing facilities that may be considered include the premises of telecom operators, university networks, data-hosting centres, and city emergency services.

The most important features to consider for potential sites include:

- Proximity to the networks of the potential members. This may also depend on whether the IXP is to be centralised in one room, located in a campus of adjacent buildings, or more widely dispersed across a broader area, such as by using fibre channel switched fabric.
- Availability of electric power, including a backup supply or generator
- Availability of air-conditioning
- Availability, capacity, and reliability of telecommunication links to the site
- Access to fibre facilities or rights-of-way
- Ability to build antenna towers or dig trenches for fibre
- Ease of access (independent 24x7x365 access for IXP member staff is highly desirable)
- Quality of security (CCTV, 24 hour monitoring, fire and break-in detection is desirable)
- Availability of ancillary equipment and services, such as equipment cabinets and telephones

Once the design of the IXP is complete and the institutional structure and site(s) have been identified, a detailed business plan may be developed that details set-up and maintenance costs, proposed revenue, and cost recovery projections.

To help establish IXPs in developing countries where they do not exist, financial support may be available from development agencies or donors. Since the financial assistance needed for the start-up costs of an IXP are relatively modest compared with the potential long-term economic benefits, a strong case can be made for development assistance. As the majority of IXPs are nonprofit facilities, financial aid can be said to assist market growth versus distort its natural development. And as the majority of the expenditure is on initial training of staff to establish and maintain the facility, it meets the objective many donors have for local capacity building.

General Summary and Conclusions

The primary role of an IXP is to keep local traffic local and reduce the costs associated with traffic exchange between Internet providers. The case for IXPs is compelling and the obstacles relatively clear and well-understood.

To achieve wider IXP deployment in developing countries, the following key requirements must be addressed:

- Regulatory reform and liberalisation. Regulators and competitors must be convinced of the overwhelming benefits of domestic Internet traffic exchange and of the broader proposition that lower costs for competitors can lead to greater revenues for existing operators.
- Overcoming resistance and lack of understanding from potential members, especially monopoly telecom operators and those with market dominance
- The organisation of competitive ISPs into associations capable of neutrally administering shared facilities on behalf of their members

Governments should neither require IXPs to be licensed nor mandate peering and other policies concerning IXP operations. Governments can play a positive role to encourage networks to keep domestic traffic local. In particular, policies aimed at encouraging competitive access to leased lines and wireless connections will help lower costs associated with connecting to an IXP. Governments can also play a positive role by restraining anti-competitive behaviour of incumbents, including attempts by large carriers to block the development of IXPs.

Some IXP Examples

The selected IXPs described below illustrate the variety of approaches to IXP establishment and operations. The examples draw on information from the IXP web sites and, in some cases, case-studies (see end of section for further resources). The first example, KIXP in Kenya, is presented in more detail than others due to the greater availability of case study information.

The Kenya IXP (KIXP)

KIXP in Nairobi is operated by the Telecommunication Service Providers Association of Kenya (TESPOK), a professional, nonprofit organisation representing the interests of ISPs and other telecommunication service providers in Kenya. After attending the Networking Workshop for Developing Countries hosted by the Internet Society in California in 1999, one of Kenya's Internet engineers obtained the knowledge to design, set up, and maintain an IXP. He shared this information with other Kenyan network operators eager to establish a local IXP. After approximately a year of preparatory work, including the design and implementation of the technical operation, funding model, and legal framework, KIXP was launched in November 2000. KIXP does not have a separate governance structure and policies are established through committees of TESPOK.

Almost immediately following its launch, the incumbent telecom operator, Telkom Kenya, filed a complaint with the national regulator, the Communications Commission of Kenya (CCK). They argued that the KIXP violated Telkom Kenya's exclusive monopoly on the carriage of international traffic. Within two weeks, the CCK concluded that the KIXP required a license and ordered that it be shut down as an illegal telecommunications facility.

In response to the CCK's closure order, a case was then presented to the Communications Appeals Tribunal with a strong technical argument showing that KIXP was merely a standard, off-the-shelf Ethernet switch. If the KIXP were to be shut down, then the CCK would need to shut down every computer network in the country since the technical architecture and components were equivalent. Telkom Kenya's opposition to KIXP was fierce, fed by the fear of losing a significant portion of its international leased line revenues, but the Kenyan Internet providers also argued that the KIXP was a closed-user group and, therefore, would be legal under the Kenyan Telecommunications Act. In addition, it was also pointed out that the local exchange of domestic Internet traffic does not contravene Telkom Kenya's international monopoly, as all international traffic would continue to flow over its international links.

After nearly a year of intensive efforts, including public pressure, threats of litigation, and private diplomacy, TESPOK received the approval of CCK in the form of a license, granted in November 2001. Industry observers said that Telkom Kenya had misrepresented the situation and, because the matter was made public and had received a significant amount of attention and coverage in the local and international media, it was necessary to find a face-saving solution. The approach eventually adopted was the establishment of a company called KIXP Limited, which then applied for an IXP licence that CCK duly granted. This made Kenya the first country in the world to have an IXP licence.

KIXP went live again in mid-February 2002 having interconnected five Kenyan ISPs. In the course of 2004, it was decided by TESPOK members that the policies governing membership and use of KIXP were restrictive, since they allowed only licensed ISPs to be members and to connect to the IXP. This prompted a policy review which lifted all restrictions on membership and substantially lowered joining fees. Membership costs KSH 20,000 (approximately USD 330) per month and there are now 25 members peering at KIXP: 16 ISPs, one government network (Kenya Revenue Authority), one education network operator, one ccTLD Operator, three Internet backbone gateway operators, one value-added telecommunication services provider, and two GSM operators.

One of the biggest issues in establishing KIXP related to deciding where it would be hosted. A number of options were evaluated.

- Telkom Kenya was ostensibly the most suitable option since it was the incumbent public national telecoms operator. Some of the reasons cited in favour of Telkom Kenya included the fact that as national operator, all Internet providers had existing links to its data network. Additionally, due to its central location, it would be much easier for the members to gain physical access to the IXP, regardless of their location. However, this option proved to be unworkable because, as described above, Telkom Kenya saw the IXP as a threat to its business and declined the ISPs' request to host KIXP.
- The University of Nairobi was considered as an alternative host for KIXP, mainly due to its dynamic computer studies faculty and its central location. The biggest concern about using the university was the frequency of student riots. Since the KIXP was expected to serve a mission-critical purpose, this concern eliminated the university as a viable option.
- A couple of Internet providers that had their offices conveniently based in the Nairobi central business district offered to host the IXP. The challenges here were (1) how to choose between the two ISPs and (2) the high levels of dissatisfaction expressed by the other ISPs about having to trust a competitor to handle the IXP without seeking for itself an undue advantage.

In order to ensure the acceptability of the IXP concept in Kenya, it was essential to emphasise the neutrality of the facility and obtain consent from prospective members on its location. After an evaluation of all the various existing options without finding one that satisfied all the potential members, the idea of leasing space in a provider neutral, conveniently located building was posed. This option allayed most of the fears and concerns expressed and a lease was taken up for 1,500 square feet on the top floor of a strategically located office building in the Nairobi city centre.

The main operational consideration was cost. As with any other type of data networking or communications infrastructure, costs fell into two broad categories: set-up and operating costs. Set-up costs included the cost of equipment for the core of the IXP and furnishing the room where the IXP was to be located with backup power, air-conditioning, equipment cabinets, and relevant security fixtures. The initial equipment was funded both by a donation from Cisco Systems as well as a small grant from the U.K. Department for International Development. Other set-up expenses were covered by funds from TESPOK. Since the space where KIXP was located was not free, it was necessary to find a way of covering the operating costs, such as rent, electricity, and insurance costs. A monthly subscription fee for all members connecting to KIXP was introduced to cater for these.

It was agreed that KIXP would be based on the same model as the Hong Kong Internet Exchange—a Layer 2 Route Reflector IXP. As a result, the KIXP facility consists of two high-speed Ethernet switches and each KIXP member has the option of connecting their routing equipment to both switches. If one switch should fail, the other will take over automatically. The core is supplemented by two router reflectorss, specially configured routers that bounce routing logic to all members at the KIXP until all the routers have the same view of the network. This design aspect allows for quick and easy policy implementation at the exchange point, which is capable of supporting up to 48 networks. Capacity can be extended to support up to 200 networks.

Until KIXP, all Internet traffic was exchanged internationally, although roughly 30 percent of upstream traffic was to a domestic destination. International bandwidth costs approximately USD 5,000 per megabyte; the local price is about USD 500–1,000. During the first two weeks of KIXP's operation, measurements indicated that latency was reduced from an average of 1,200–2,000 milliseconds (via satellite) to 60–80 milliseconds (via KIXP).

Local traffic has also improved, thanks to a rise in local content facilitatied by digitisation of some government services and the arrival of international companies, such as Google, locally hosting their services. All Google traffic (searches, mail, maps, applications, and documents) goes through KIXP. ISPs pay for the local traffic and Google pays for the capacity from Kenya to their network in the United States.

Due to the limited capacity on the incumbent telecom operator's leased lines, most Internet service providers have moved to terrestrial fibre to connect to KIXP—meaning they now have links of multiple megabits per second into the exchanges.

KIXP has implemented local instances of the Internet's F and J root servers, in addition to local .com and .net resolution services. As a result, locally originated lookup requests for these services no longer need to transit international links for a response.

In 2005, the Kenya Network Information Centre (KENIC), in line with its mandate to promote access to the Internet in Kenya, set up a GPS-enabled NTP Server at KIXP to provide date and time integrity for computers. Most service providers had implemented time synchronisation on their systems using network time servers located in foreign countries. However, these services were not extended to their clients due to the unreliable connectivity and prohibitive costs associated with international links. Some of the organisations using the local NTP services include government bodies, ISPs, banks, companies, and some educational institutions which are able to save on organisational expenses resulting from operational failures and data losses due to time inconsistencies.

KIXP operates an MLPA by which each member must have a peering session with every other member.

Traffic hits 44Mbps during peak time and is expected to reach 50Mbps. KIXP publishes information on Internet usage patterns to illuminate potential market opportunities. The data reveals that traffic flows are highest during weekday business hours, indicating that ISP services are concentrated on corporate users and highlighting an opportunity to maximise off-peak use via products and content attractive to home Internet users.

For more information, see: http://www.kixp.or.ke

The Internet Exchange of Nigeria (IXPN)

In Nigeria, IXP activity began outside the capital in 2003 in the city of Ibadan, when two members connected to a 10/100Mbit/s Ethernet switch and a route server. The maximum recorded traffic between the two ISPs was 102Kbit/s. In early 2005, the ISP Association of Nigeria (ISPAN) began discussions on setting up an exchange in Lagos, which was expected to be managed by an independent entity to be set up by ISPAN. In November 2005, President Olusegun Obasanjo directed the national regulator, the Nigerian Communications Commission (NCC), to ensure that a national IXP be established as soon as possible. An Interim Board was inaugurated in March 2007 and IXPN was established with 15 initial members.

Since then, 14 members have begun the process of joining and IXPN has established three operating sites in Lagos in partnership with two co-location operators connected by fibre switch fabric. Each location has two Foundry switches connecting separate peering LANs to ensure reliability. The primary peering LAN is interconnected on a 1Gbps circuit (fibre); the secondary peering LAN is interconnected on a 450 megabit wireless backhaul. Two of the three operating locations have route servers in place. All the switches provide 10/100BaseTX switched Ethernet and 1000BaseSX Gigabit Ethernet over multi-mode fibre connections. IXPN plans to expand to six other cities in the near future.

IXPN is overseen by a board comprising the CEO and six directors. A technical committee assists the staff and advises the Board on technical matters relating to IXPN's operations.

For more information, see: http://www.nixp.net

The London Internet Exchange (LINX)

LINX is one of the world's largest and oldest Internet exchanges. It is a mutually owned membership association for Internet operators that also represents the interests of its members on public policy matters.

LINX has more than 280 members in 40 countries with 47 new members in 2007. While most of the members are from Europe, nearly a quarter are based outside, with those in North America comprising 15 percent and a further 7.5 percent coming from Africa, the Middle East, Asia, and Oceania.

Initially LINX membership was restricted to operators of traditional ISPs. In 2000 this restriction was relaxed and today a wide variety of networks peer at LINX exchanges, including Google, Akamai, Yahoo, and the BBC. The diversity of service providers peering at LINX is increasing and comprises gaming and gambling specialists, media streaming providers, DDoS mitigation specialists, software-as-a-service providers, and advertising networks.

The LINX network consists of two Ethernet switching platforms installed across seven United Kingdom locations. LINX facilities have more than 575 connected member ports with 100 10GigE ports and over 256Gb/sec of peak traffic. To provide fault tolerance, at least two switches from different vendors are installed in every LINX location and locations are connected by multiple 10 Gigabit Ethernet circuits linked via optic fibre to form two physically separate backbone rings. Physical protection of the dark fibre network is achieved by using diverse paths where available.

Management of the logical redundancy of the network is carried out using rapid-failover protection mechanisms (EAPS or MRP). In the event of the loss of a network segment, these activate the redundant links within tenths of a second to restore connectivity.

LINX offers dual route servers (running Quagga) on each of the two peering LANs. These servers have sessions with approximately 120 members and offer nearly 20,000 routes. This is an optional, free service. Members that prefer bilateral agreements may continue to use them.

For more information, see: http://www.linx.net

The Johannesburg Internet Exchange (JINX)

South Africa's largest city hosts the Johannesburg Internet Exchange, operated by the Internet Service Providers' Association (ISPA), a nonprofit Internet industry body. ISPA has more than 145 members, comprised of large, medium, and small Internet service and access providers. ISPA also facilitates dialogue between independent Internet service providers, the South African Government Department of Communications, the national regulator (ICASA), telecommunication operators, and other service providers.

All members of ISPA may connect to JINX, with medium-sized members being restricted to connections of up to 512 kbps and small members being restricted to connections of up to 128 kbps. ISPA does not require JINX users to interconnect with all other JINX users. Each organisation connecting to JINX is expected to establish its own policy for interconnection. It is up to each new participant to negotiate interconnection agreements with the other members, preferably before installing a physical connection to JINX. Members not publishing a specific interconnection policy of their own agree to exchange traffic with all other participants on a no-charge basis. JINX members may also offer transit services to other members. Members must let ISPA know with which other members they have established an interconnection agreement, but they do not have to disclose the exact nature of that agreement. ISPA reserves the right to disconnect the lines of any JINX participant who fails to reach an interconnection agreement with at least two other JINX participants.

Content-server hosting is not available at the exchange. ISPA's policy is to not compete with its own members, which provide hosting services. While it may seem appealing to host a server at a central location, ISPA points out there is a negligible difference in performance if the server is hosted on the network of an ISPA member with a high-speed connection to JINX.

An exchange was also briefly operated in Cape Town but was closed due to lack of support. For the same reason, efforts to establish an exchange in Durban have not yet been successful.

JINX users must pay the appropriate ISPA membership fees and a one-off JINX joining fee, ranging between ZAR 25,000 (about USD 3,000) for large members to ZAR 2,500 (USD 300) for small members (members elect which category they fall into).

JINX users connecting to JINX via means other than circuits leased from a licensed telecommunications operator may be liable for equivalent line charges. The equivalent line charge model was the result of more than a year of discussion and negotiation between ISPA members. Prior to the introduction of the equivalent line charges, some companies connecting to JINX enjoyed an unfair advantage over others. While most participants must lease data lines to connect to JINX, ISPA members located in the same building can connect to JINX at minimal cost. The equivalent line charges are intended to ensure that JINX participants enjoy equitable and fair access. The equivalent line charge is based on the traffic measured on the switch port(s) of any ISPA member that does not lease a circuit from a licensed telecom operator to connect to the exchange. Traffic exchanged directly between JINX participants (via a direct cable instead of via the switch) is not subject to a charge. This means that ISPA members are free to negotiate alternative settlements with other peers to bypass the equivalent line charges. Fees are loosely based on estimated data-line costs for lines capable of carrying monitored traffic levels.

An example statement of an ISP's interconnection policy is provided by the Internet access provider Storm, which states that it will exchange traffic with all other participants on a no-charge basis, provided that they:

- are in the business of providing Internet access to more than one organisation or group of companies with common shareholding;
- act in good faith and in a co-operative manner on issues relating to the interconnection;
- respect Storm's acceptable-use policy and the generally accepted Internet etiquette;
- use the interconnection in such a manner as to reduce the costs of exchanging traffic between the parties and improve connectivity between the parties;
- take all reasonable measures to ensure that they do not compromise the integrity or stability of Storm's network; and
- comply with the technical requirements required to facilitate the interconnection, including ensuring that sufficient bandwidth is always available on interconnection links.

For more information, see: http://www.ispa.org.za/jinx

The Rwanda Internet Exchange (RINEX)

RINEX has been operational since mid-2004. In October 2003, SIDA (the Swedish International Development and cooperation Agency) in collaboration with the Swedish Royal Technical Institute (KTH) began an initiative to assist Rwanda in establishing a national IXP. Prior to this, Internet providers in Rwanda had been discussing the need for an IXP, but the question of funding remained an issue. For SIDA, Rwanda fulfilled the prerequisites needed for assistance, including the presence of a neutral body to host the peering point, the existence of at least two independent ISPs in the country, and a team of technicians from the various Internet providers trained in the techniques of setting up and maintaining a peering point. The Government's Rwanda Information Technology Authority (RITA) took responsibility for the project with assistance from four people drawn from the two main educational institutions (also commercial ISPs): the National University of Rwanda (NUR) and the Kigali Institute of Science and Technology (KIST).

A major problem in establishing RINEX was that the country did not have an industry association that could oversee its management. As a result, RITA is continuing to manage the exchange until its members are able to establish an appropriate management structure and nonprofit institution to host it. In the interim, a simple administrative model has been adopted where all members are equal, independent of size. The management structure consists of two entities: the RINEX Council and the Executive Committee. The RINEX Council is a formal managerial unit which is responsible for making decisions regarding RINEX, having one representative from each connected organisation or member, and a president. The president for the initial six months is RITA.

After this initial trial period, RITA will transfer the presidency to the RINEX Council. This will be continued on a rotational basis among all the members.

Finding the appropriate host for the IXP was also an issue in setting up RINEX. Finding independent premises with electricity, a backup power generator, security, telephones, office space, and an air conditioner proved impossible. The academic entities in Rwanda lack physical facilities and the private ISPs had limited capacity. So it was decided to host the IXP at the premises of the incumbent telecom operator, Rwandatel, which already had existing connections to most of the Internet providers.

The stakeholders agreed to a Layer-2 based IXP model because of its simplicity to set up and administer, its reliability, and its independence. Each network operator provides a circuit from its backbone and a router which connects to the IXP switch. As shown in Figure 4, the inner box represents the equipment that is located in the IXP premises. This consists of the IXP core and member routers and communications equipment.

The Mongolian IXP (MIX)

The case of Mongolia demonstrates that a combination of ISP cooperation and tacit support from governmental authorities can lead to the rapid and successful establishment of an IXP in a developing country. In January 2001, a group of leading Mongolian network operators met in Ulaanbaatar to explore the creation of a national IXP. At the time, all Mongolian ISPs were interconnected via providers in the United States or Hong Kong. Satellite latencies amounted to a minimum of 650 milliseconds (over half a second) for each packet of data in each direction. Costs were high and very few Mongolian Internet business services were hosted within Mongolia.

Without interference from the Mongolian government, Mongolia's three leading Internet providers completed planning for an independent exchange within three months. MIX was launched in April 2001 with three ISP members. By March 2002, MIX had six ISP members and steadily increasing traffic between them. Today,

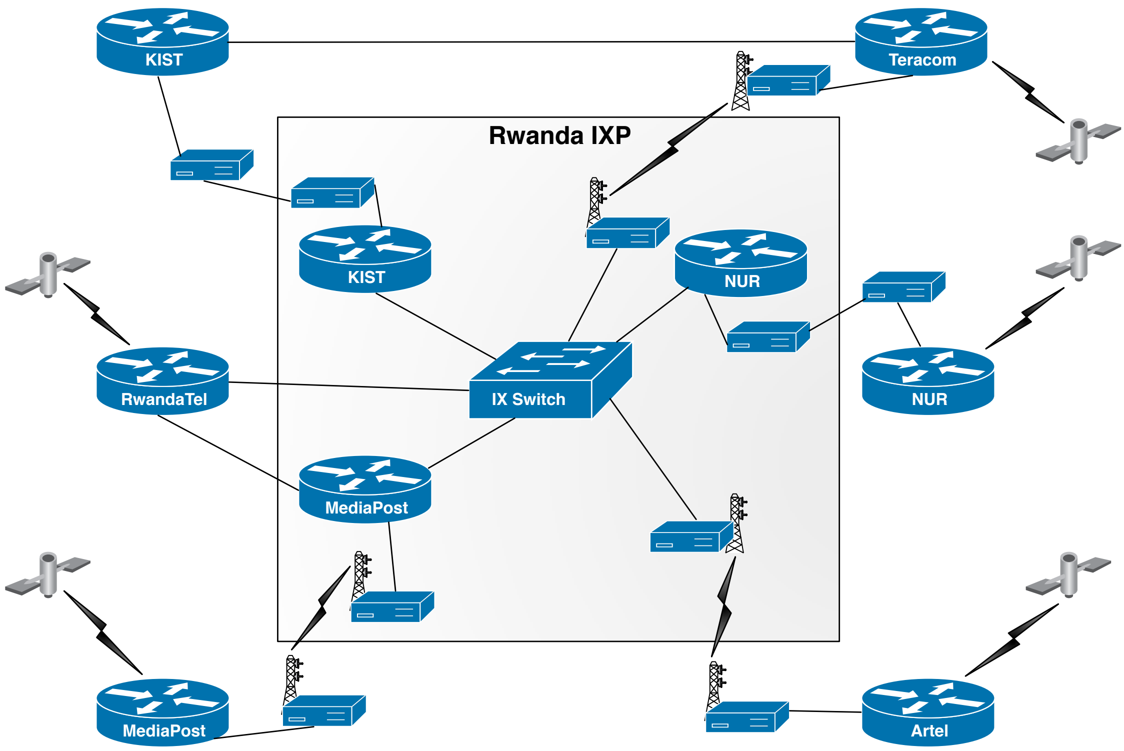

Figure 4.

local latency is less than 10 milliseconds per transaction and an average of 377 gigabytes of data are transferred domestically each day among MIX's members. Moreover, each domestically exchanged transaction frees up an equal amount of international bandwidth, thereby improving connection speeds and reducing latency over Mongolia's international links.

References

1. See https://prefix.pch.net/applications/ixpdir/summary for a list of countries without IXPs

2. Quagga is a routing software package that provides TCP/IP based routing services with routing protocols support such as RIP, OSPF, and BGP for Unix platforms. It also supports special BGP Route Reflector and Route Server behaviour in IPv4 and IPv6 routing protocols. For more information see http://www.quagga.net

For More Information

AFIX Decision-makers' Workshop: Session 1, African Internet Exchange Point, http://afix.afrispa.org/decision-makers/D1/D1_handout.doc

Huston, G, *Interconnection, Peering and Settlements,* Internet Society, http://www.isoc.org/inet99/proceedings/1e/1e_1.htm

Internet Traffic Exchange in Less Developed Internet Markets and the Role of Internet Exchange Points (IXPs), 2008, report from the IGF Rio - Best Practices Session, The Internet Society, http://www.isoc.org/educpillar/resources/igf-ixp-report-2007.shtml

McLaughlin, A, May 2004, *Internet Exchange Points: Their Importance to Development of the Internet and Strategies for their Deployment – The African Example,* Global Internet Policy Initiative, http://www.gigiproject.org/practices/ixp.pdf

McLaughlin, A & Zuckerman, E, *Introduction to Internet Architecture and Institutions,* Berkman Center for Internet and Society, http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html#Notes

Walubengo, J, Msiska, K, & Kasonde Kasolo, T, *Internet eXchange Points (IXPs) and Continental Backbone for Africa: Means to an End?* Internet Governance Research Project, DiploFoundation, http://www.diplomacy.edu/poolbin.asp?IDPool=127

Glossary

ASN	Autonomous system number. Unique ASNs are allocated to Internet operators by the regional internet registries (RIRs) for use in multipath routing. An ASN is only issued when an institution demonstrates the means to maintain an independent routing policy. This entails having direct interconnections with at least two other, similarly independent external network entities. In the widest sense, an autonomous system is a connected group of one or more IP prefixes run by one or more network operators, with a single and clearly defined routing policy.
Backbone	The trunk routes of a network used as the path for transporting traffic between different networks. Backbones can be the physical telecommunication infrastructure or the Internet circuits established over them by a particular Internet operator.
Bandwidth	The size or capacity of a communications channel to transfer data, usually measured in the speed of data transfer in bits per second (bps), although also often stated in the frequency range assigned to the channel and measured in Hertz (Hz).
BGP	Border gateway protocol. The protocol standard used to ensure that there is more than one route to an Internet provider's network. Supports both route aggregation and classless interdomain routing (CIDR).

BLPA	Bilateral peering arrangement. An agreement between two networks to exchange traffic.
bps	Bits per second. The number of bits passing a point every second. The transmission rate for digital information, that is, a measure of how fast data can be sent or received. Often expressed for broadband links as Megabits per second (Mbps).
Broadband	A high-speed (multimegabit) data connection.
ccTLD	Country code top-level domain. The two-letter codes which signify the origin of Internet traffic in a human readable form. E.g., .es for Spain and .br for Brazil.
Connection redundancy	Two or more physically separate connections via different network providers. Redundancy ensures continued links to the Internet in the event of one connection going down.
DNS	Domain name system. Matches human-readable names with IP addresses. A tree structure divides the Internet into a hierarchical structure of domains and subdomains: top-level domains (TLDs) include generic domains such as .com, .edu, and .org and country code domains (ccTLDs), such as .uk, .za, .gh, and .ke. Administrators of a TLD may create as many subdomains as they wish. An international network of DNS servers maintains data on which domain name goes with which IP address. Changes can be made on any server and are propagated through the network.
Fibre optic cable	A technology using glass fibre for the transmission of data. A signal is imposed on the fibre via pulses (modulation) of light from a laser or light-emitting diode (LED). Because of its high bandwidth and lack of susceptibility to interference, fibre optic cable is used in long-haul or noisy applications. With advances in modulation technology, international fibre cables are now usually deployed with terrabit capacities.
Gbps	Gigabits per second.
Gigabit	One billion bits.
Interconnection	Any direct connection between two networks—private or commercially operated Internet-based networks or telecom networks of fixed or mobile operators. Cost of interconnection is usually incurred by the parties on either end of the connection.
International gateway	Technically, a facility to consolidate and share the cost of international links and termination points. In practice a licensing term used by many developing-country governments, which may allow only the state-owned monopoly operator and perhaps a small number of other licensed telecom operators to carry international traffic. Most often these are the licensed mobile operators.
Internet	A global mesh of computer networks using TCP/IP. The Internet's national and international backbones are high-speed, fibre trunk lines owned by telecommunication companies. National Tier-1 service providers aggregate data traffic and pass it over the backbones and work with local service providers, who connect to customers via digital links or modems.
IRR	Internet routing registry. A globally distributed routing information database that ensures stability and consistency of Internet-wide routing by sharing information between network operators. The IRR comprises several databases in which network operators publish their routing policies and announcements. In addition to making Internet topology visible, the IRR is used by network operators to look up peering agreements, determine optimal policies, and configure their routers.

ISP	Internet service provider. A generic term for organisations that provide Internet services such as web site hosting and Internet access. ISPs purchase bandwidth from companies, which have direct links to the Internet and then sell that bandwidth to consumers and businesses in smaller chunks. E.g., an ISP may take the bandwidth of a 45Mbps connection to the Internet and sell it to thousands of 56Kbps dial-up modem users.
IXP	Internet exchange point. Also called IX, EP, NAP, or peering point. Both a physical networking location and a logical networking strategy, which facilitates interconnection between Internet-based networks.
Leased line	A telecommunications circuit usually rented from a telecom operator to connect two or more locations. Where regulations allow and the physical location of the two points to be connected makes it feasible, Internet providers may establish their own wireless, cable, or fibre link, thereby eliminating the need to lease a circuit from a third party.
Looking glass	A web-based connection to a router that enables administrators of other networks to see a network's routing information. Looking-glass information may or may not be made available to the broader public.
MAN	Metropolitan area network. Usually a fibre-optic ring spanning a large city.
Mbps	Megabits per second. A unit of traffic measurement.
Megabit	One million bits.
MLPA	Multilateral peering agreement. An agreement by networks connecting to an IXP to exchange data with all other networks connected to the peering point. Often mandatory when joining an IXP.
Network	A collection of devices interconnected via TCP/IP. Networks may be commercially run by an ISP or run by an organisations for internal purposes, such as company-wide and academic networks. May also refer to the underlying telecommunication infrastructure, but this use is less common in the Internet arena.
Peering	A zero-compensation arrangement in which network operators agree to exchange traffic at no charge. Common practice where the networks in question have roughly the same characteristics and traffic volumes, meaning a net financial burden from traffic flow between them is likely to be small. In a peering agreement, there is no obligation for the peer to carry traffic to third parties. The process by which a network qualifies for peering is usually privately negotiated based on market position, network coverage, volume of traffic, range of services provided, and network reliability. In general, peering only takes place when one of the two networks would not be significantly disadvantaged by termination of the link between them.
Petabit	One thousand terabits.
PSTN	Public switched-telephone network. Traditional voice telephone system, based on switched (rather than packet) networking protocols, usually based on TDMA.
PTO	Public telecom operator. The incumbent, state-owned monopoly operator. Technically, the distinction between fixed line, cellular operators, and ISPs is becoming increasingly blurred.
RIR	Regional internet registry. The five organisations responsible for allocating IP addresses and related numeric resources to network operators in their respective re-

	gions: AfriNIC – Africa; ARIN – Canada, many Caribbean and North Atlantic islands, and the United States; APNIC – Asia Pacific; LACNIC – South America and the Caribbean; RIPE NCC – Europe, Central Asia and the Middle East.
Route server	One or more IXP BGP route server peers that collect and redistribute IXP member routes
TCP/IP	Transmission control protocol and Internet protocol. The two protocols, which form the basis of communication across the Internet. Currently most of the Internet is based on version 4 of the IP protocol, but as the free pool of IPv4 addresses approaches capacity, there are growing calls to accelerate IPv6 deployment.
Terrabit	One thousand Gigabits.
Transit	An arrangement in which a network sells access to another network to enable its connection to a third party network. Transit charges are set by negotiation and often are not disclosed publicly. Transit arrangements typically provide access to an array of networks not limited to one country. In many cases one Internet transit arrangement with a large network can provide a small, remote network with access to the rest of the world.
TDMA	Time division multiple access. A commonly used communications protocol used on traditional switched telecommunication networks.
VoIP	Voice over Internet protocol. A method to use TCP/IP to carry voice calls.
VPN	Virtual private network. An encrypted channel between two end points on the Internet that provides secure communications.
WiFi	Wireless fidelity. A commonly used set of standards for wireless networking.
WiMax	World interoperability for microwave access. A wireless technology for last mile broadband access.

Further Resources

A session at the forthcoming Internet Governance Forum (IGF) 2008 in India is being planned to focus on strategies for encouraging the emergence of more IXPs. *http://www.intgovforum.org*

A variety of organisations around the world are making efforts to support the establishment of new IXPs and to help ISPs and existing IXPs improve access, functionality, and costs. These include:

The Asia Pacific Operators' Forum (APOPS), *http://www.apops.net*

APRICOT (Asia Pacific Regional Internet Conference on Operational Technology), *http://www.apricot.net*

The African Internet Exchange Point Task Force (AFIX-TF), *http://afix.afrispa.org*

The African ISP Association (AfrISPA), *http://www.afrispa.org*

The Association for Progressive Communications (APC), *http://www.apc.org*

EP.NET, LLC, *http://www.ep.net*

The European Internet Exchange Association (Euro-IX), *http://www.euro-ix.net*

The European Internet Services Providers Association (EuroISPA), *http://www.euroispa.org*

The European Operators Forum WG (EOF), *http://www.ripe.net/ripe/wg/eof*

The International Telecommunication Union (ITU), *http://www.itu.int*

The Internet Society (ISOC), *http://www.isoc.org*

The Latin American and Caribbean Region Network Operators' Group (LACNOG), *https://mail.lacnic.net/mailman/listinfo/lacnog*

The London Internet Exchange (LINX), *http://www.linx.net*

The Middle East Network Operators' Group (MENOG), *http://www.menog.net*

The Network Startup Resource Centre (NSRC), *http://www.nsrc.org*

The North American Network Operators' Group (NANOG), *http://www.nanog.net*

The Organisation for Economic Co-operation and Development (OECD), *http://www.oecd.org*

The Packet Clearing House (PCH), *http://www.pch.net;* PCH Directory of IXPs, *http://www.pch.net/ixpdir*

The South Asian Network Operators' Group (SANOG), *http://www.sanog.org*

The World Bank's InfoDev unit's ICT Toolkit, *http://icttoolkit.infodev.org*

The World Information Technology and Services Alliance (WITSA), *http://www.witsa.org*