



Where to Peer

This section of the Toolbox describes the where a network operator would seek peering.

Private Peering

Private peering is where there is a private connection between the two network operators for the purpose of exchanging traffic. The following topics cover the aspects needed in any Private Peering setup.

- [Meaning](#)
- [Location](#)
- [Physical Connection](#)
- [Configuration](#)
- [Private Peering Agreement](#)

Meaning

Private means that the physical link between the two network operators is organised by them (by one operator or by both), is only for their use, and is usually jointly owned (costs are shared) by both operators.

Location

It is up to the two operators who wish to peer privately to agree the location that would suit them best. If they are in the same physical datacentre, a link between their equipment cabinets may be enough. If parts of their respective networks are in the same metropolitan area, perhaps local capacity can be leased from an infrastructure operator. But if they are far apart, or in different countries, a wide area network link will need to be used, chosen according to what makes most economic sense.

Physical Connection

The physical link can take many forms, including:

- copper ethernet or fibre optic cable patching between each operators routers in different equipment racks in the same datacentre
- fibre optic leased from an infrastructure provider between the two operators datacentres
- wireless media (the various 802.11 standards) connecting over the air across distances up to 10km (usually where fibre interconnect is not possible)
- satellite infrastructure (whether low earth orbit, medium earth orbit, geosynchronous or geostationary) connecting over large distances where neither fibre nor wireless can service the need.
- layer-2 infrastructure provided by a layer-2 infrastructure operator (today this is typically using L2VPN services over MPLS; in the past ATM and Frame Relay technologies were used).

Configuration

At a high level, the configuration applied to each network operator's router ensures that each operator only sends the routes (public IP address space) they and their customers use for Internet access, and only accept the routes that their peer (and their customers) use for Internet access. All other routing information is blocked on this private link (a very important requirement for routing security).

The routes that a network operator learns from a private peer must not be passed on to any other autonomous network **unless** and **only** if there is agreement with the private peer that this is desirable.

Detailed configuration examples are covered elsewhere in the Toolbox.

Private Peering Agreement

Operators who enter into a Private Peering usually will exchange documentation which details the peering agreement between them. This agreement usually contains information such as:

- which routes will be exchanged
- the process by which changes to the routes being exchanged will be informed to the peer
- an undertaking to upgrade the interconnect capacity (bandwidth) in a timely manner (timely will be defined at what percentage of capacity is used before an upgrade is needed)
- contact details of the Peering Coordinator (the administrative contact) in each operator
- contact details of the Network Operations Centre at each operator (not customer helpdesk!)
- escalation process in case of faults on the interconnect
- any other relevant information relating to the interconnect to ensure its continuous and reliable operation

Not all operators enter into such an agreement although it is recommended simply so there is a documentation trail and that each operator knows what to do if any issues need to be resolved.

Public Peering / Internet Exchange Point

Public peering is where there is a public interconnect location where network operators can interconnect for the purpose of exchanging traffic. This public interconnect is known as an **Internet**

Exchange Point. The following topics cover the aspects needed in any Public Peering setup.

- [Meaning](#)
- [Location](#)
- [Physical Connection](#)
- [Configuration](#)
- [Agreements](#)

Meaning

Public means that the physical infrastructure provided for interconnecting to other networks is open to all and any network operator to participate in, as they wish. Each network operator is responsible for providing their own connectivity to the public interconnect location.

Location

Public interconnects are located where it is most convenient for the largest number of network operators to access and participate at the most optimum cost to the network operators. (Bearing in mind that peering is designed to minimise the cost of operation for network operators.)

Ideal locations for public interconnects include datacentres and/or locations of concentrations of fibre provided by several infrastructure operators. These locations all have good physical and network access, 24 hour coverage, independent power grid supplies with on-site backup, sufficient cooling, and are well protected from natural disasters (earthquake, tsunami, wildfire, floods, volcanoes, cyclones).

Given the large concentration of network operators present, these public interconnects are often considered critical infrastructure, and their reliable operation is often considered of national importance.

Physical Connection

The physical link each operator has to provide to the public interconnect can take many forms, including:

- copper ethernet or fibre optic cable patching between the operator's routers and the IXP switch in the same datacentre
- fibre optic leased from an infrastructure provider between the operator's datacentre and the IXP location
- wireless media (the various 802.11 standards) connecting over the air across distances up to 10km (usually where fibre interconnect is not possible)
- satellite infrastructure (whether low earth orbit, medium earth orbit, geosynchronous or geostationary) connecting over large distances where neither fibre nor wireless can service the need.
- via a layer-2 infrastructure provider, which means the operator does not need to physically connect to the IXP by any of the above options (this is known as Remote Peering).

Configuration

At a high level, the configuration applied to the network operator's router ensures that the operator only sends the routes (public IP address space) they and their customers use for Internet access, and only accept the routes that their peers (and their customers) use for Internet access. All other routing information is blocked on the public peering links (a very important requirement for routing security).

The routes that a network operator learns from a public peer must not be passed on to any other autonomous network unless and only if there is agreement with the public peer that this is desirable.

Detailed configuration examples are covered elsewhere in the Toolbox.

Agreements

Operators who participate at an IXP usually will sign an agreement with the IXP itself. This agreement usually contains information such as:

- contact details of the Peering Coordinator (the administrative contact) at the operator
- contact details of the Network Operations Centre at the operator (not customer helpdesk!) and the IXP
- escalation process in case of faults on the interconnect
- rules/behaviour at the IXP
- how to use IXP infrastructure to aid with setting up connections with other operators
- any other relevant information relating to the connection at the IXP to ensure its continuous and reliable operation

Not all IXPs require such an agreement although it is recommended simply so there is a documentation trail and that the operator knows what to do if any issues need to be resolved.

[Back to Home page](#)

From:

<https://bgp4all.com/pfs/> - Philip Smith's Internet Development Site

Permanent link:

<https://bgp4all.com/pfs/peering-toolbox/where-to-peer?rev=1660560858>

Last update: **2022/08/15 10:54**

