Hosting Service Networking

The **UIS Hosting Service** allows institutions to have their servers hosted in UIS-managed Data Centre facilities, either physically or virtually. This page describes the networking available with this service.

More general information about the physical hosting service is available on the Data Centre Colocation Service (https://help.uis.cam.ac.uk/about-us/data-centre/services) pages

Contents

Options

There are several different options available. The networking depends on which option is taken:

- **Physical hosting** (also known as "*colocation*") — an institution's own hardware is physically housed in one of the UIS-managed Data Centre facilities. The institution is responsible for the maintenance, replacement and upgrades of the hardware and physical connectivity.
- **Virtual hosting** — the UIS provides virtual machines which share the same physical hardware as other virtual machines. The UIS will provide and maintain the physical hardware and connectivity and handles maintenance, replacement and upgrades.

For **physical hosting**, the networking can done in two different ways, depending on whether a dedicated rack is taken or not:

- **Dedicated rack** — here the institution has an entire rack in which to locate their equipment: the rack has only dark fibre connections and it is the responsibility of the institution to organise networking to it, using GBN circuits (https://help.uis.cam.ac.uk/service/network-services/fibre/gbn) and internal Data Centre dark fibres, or take a UDN PoP switch (https://help.uis.cam.ac.uk/service/network-services/datanetwork/pop-equipment). This will be discussed no further on this page.
- **Shared rack** — the institution is allocated space in a rack which is shared between themselves and other institutions: the UIS provides network equipment at the top of the rack which has connectivity to the UIS Data Centre Network (DCN).

The following table summarises the responsibilities with the different options:

	Physical w/ Dedicated rack	Physical w/ Shared rack	Virtual
Network equipment	Institution	UIS	UIS
Physical connections	Institution	Institution	UIS
IP/VLANs	Institution	Institution	UIS and Institution

Physical connectivity in shared racks

This section applies only to physical hosting in a shared rack.

There are two main options for physically connecting a host to the DCN, differing by the number and type of Top-of-Rack (ToR) network devices it is plugged into.

	Single 1GE	Dual 10GE
Physical connectivity	Copper 100M/1G ethernet connection to a single ToR networking device (e.g. switch).	Pair of SFP+ 10G ethernet connections to two ToR networking devices. Connection should typically be made through Direct Attach Cables (DACs).
Redundancy	Single ToR device provides a single point of failure. If it is unavailable, connectivity will not be restored until it is repaired/replaced.	Dual ToR devices provide redundancy in the event of a single unit failing.
Link configuration	Simple, standalone port.	Ports configured in a *Link Aggregation Group (LAG)* — sometimes called a 'port-channel' (Cisco) or 'trunk' (HP). It is strongly recommended LACP is used to manage this. Hosts must not use 'host-based' or standby link redundancy.

Availability during software upgrades	The single ToR device will go offline for 5-10 minutes during a software upgrade. Institutions will be notified of this work in advance but cannot ask for it to be rescheduled.	One ToR device will go offline and return before the other is similarly upgraded. Connectivity should be maintained throughout. Institutions will be notified of this work in advance. They cannot ask for it to be rescheduled but should ensure that maintenance on their hosts is not taking place during this time, degrading redundancy.
Expansion options	Can have more than one 1G connection to increase bandwidth in multiples of 1Gbit/s.	Can have multiple pairs but must always be connected to both ToR devices.
Out-of-band management connection	Through another 100M/1G copper ethernet port to the same ToR device.	Through a 100M/1G copper ethernet connection to a 1G ToR device (separate from the in-band 10G ToR devices).

IP/VLANs

This section applies to both physical connections in a shared rack and virtual hosting.

Once physical connectivity has been established, one or more VLANs, with IP subnets, will need to be presented on the links to make them useful.

In all cases, the VLAN/subnet provided to a host will be one specific to the client institution (or group within an institution, if appropriate). Further hosts will be added to the same VLAN/subnet.

The VLAN/subnet must be separate from the ones provided to an institution elsewhere on the UDN — for example, they cannot be the same VLAN fed to an institution's PoP switch and, as such, will require that any hosted equipment uses IP addresses in a distinct subnet.

The subnet will be sized appropriately for the hosting needs of the client institution. When a new VLAN/subnet is set up, the UIS will discuss with the client institution what their future requirements are likely to be. In the event that a subnet is filled and a new, larger subnet is allocated, the institution will be expected to renumber their hosts into the new range, over an appropriate period of time.

There are two choices for how the subnet is routed:

- **Directly into the data centre** — traffic entering and exiting the VLAN will be routed from the UDN into the DCN, typically through a firewall. Traffic between the institution's connection to the UDN and DCN will route through the institutional network onto the UDN (including any border firewall) and enter the DCN through the firewall there.

- **Inside an MPLS VPN** — here, traffic between the institution and the DCN crosses the UDN inside a private network provided by the MPLS Virtual Private Network (VPN) Service (https://help.uis.cam.ac.uk/service/network-services/datanetwork/mpls-vpn), potentially bypassing the firewall at each end. Traffic destined for other institutions or internet can exit onto the UDN backbone from neither, one or both ends. This option tends to be more useful where an institution requires a high-speed backend connection between hosts located in the Data Center and their own network that does not need to pass through a firewall as it is considered "secure" (e.g. backup data).

In most cases, the first option is the most suitable. A need for the second option, must be discussed with the UIS first, to explain the use case.

Last modified: 20th May 2019