



# Network connectivity options guide

August 2022

Version	Date issued	Comments
v1.0	March 2008	
v1.1	March 2009	
v1.2	September 2009	
v1.3	November 2010	
v1.4	November 2010	
v1.5	September 2011	Bandwidth Requirement revision
v1.6	December 2013	Updated Server IP details.
v1.7	April 2016	Updated Server IP details
v1.8	January 2019	Removal of FIX MD
v1.9	September 2019	VPN topology addition. Updated leased-line and consolidated providers topologies.
v1.10	July 2022	Updated list of consolidated/network providers Bandwidth requirements updated
V1.11	August 2022	Update to consolidated providers contacts

# Table of Contents

1	Introduction .....	5
1.1	Document purpose.....	5
1.2	Intended audience.....	5
2	Connection policy.....	6
2.1	Bandwidth requirements.....	6
2.2	Datacentre .....	6
2.3	Resilient communication links .....	7
2.4	Firewall policy.....	7
2.5	Monitoring.....	7
2.6	Testing.....	7
3	Connection types.....	8
3.1	Consolidated providers.....	8
3.2	Internet VPN .....	9
3.3	SFTP .....	9
3.4	Fixed link .....	9
3.4.1	Leased line (layer 2) .....	9
3.4.2	Local connect.....	10
3.5	Network address translation (fixed links) .....	10
4	Gateway operation .....	11
4.1	Market Data .....	11
4.1.1	Normal operation .....	11
4.1.2	Gateway failure.....	11
4.2	Trading.....	12
4.2.1	Normal operation .....	12
4.2.2	Gateway failure.....	13
4.3	UAT .....	13
	Appendix A Topologies.....	14
	Appendix A.1 Typical leased-line connectivity topology .....	14

Appendix A.2 Typical consolidated provider connectivity topology..... 15

Appendix A.3 Typical site-to-site VPN topology ..... 16

# 1 Introduction

## 1.1 Document purpose

This document describes the network communication types recommended for connection to Equiduct's suite of financial services.

Equiduct Systems will support customers in selecting the best method for a connection, taking into account the requirements and restrictions of each customer. Only in the event that a service is severely impacted by the chosen connectivity method will Equiduct prescribe an alternative connection type.

In the offered connectivity options, Equiduct has always sought best of breed on suppliers, shortest link in network distance and carriers able to offer diverse routes to ensure an uninterrupted service.

The Connection Policy outlines general assumptions and design considerations common to all connection options and describes the methods of communication supported by Equiduct.

The connection options have been divided into three communication types:

- Internet
- Direct connection
- Consolidated suppliers

Not all communication options listed are appropriate for all Equiduct services.

Equiduct will always endeavour to support any suggested connectivity option so long as the option will perform appropriately, is reliable and cost effective.

Equiduct offers trading and market data services from both production and from a functionally identical User Acceptance Test (UAT) environment.

## 1.2 Intended audience

This document is aimed at all Equiduct market participants and distributors of market information.

This document seeks to provide all alternatives for connectivity, should another connectivity option be required, please contact Equiduct directly at [onboarding@equiduct.com](mailto:onboarding@equiduct.com).

## 2 Connection policy

### 2.1 Bandwidth requirements

Bandwidth requirement is dependent upon the number and type of services required by an individual firm.

See the table below for a guide of the bandwidth requirements for each logical connection for Order Entry and the various Market Data Product offerings.

Equiduct services	Recommended bandwidth
FIX Order Entry	1Mb for an average of 100 messages per seconds
ITCH HybridBook	10 Mb
ITCH VBBO	50 Mb
ITCH Market by Limit	50 Mb
ITCH ALP Orders	10 Mb

For Market Data connections, the recommended bandwidth is sufficient for a single logical connection consuming data for all stocks in the Equiduct universe. Multiple logical connections, e.g. for redundancy/resiliency, will require a corresponding multiple of the recommended bandwidth.

Equiduct monitors activity levels and bandwidth consumed and may review and adjust the bandwidth recommendations from time to time in line with increasing market activity.

### 2.2 Datacentre

Equiduct has selected capacity within Interxion's datacentre at:

Interxion  
 11 Hanbury Street  
 London  
 E1 6QL

The datacentre meets the standard expected of the technology infrastructure of a Regulated Market. The selected datacentre currently provides capacity for other execution venues and the wider financial services community; enabling excellent local connectivity and access to exceptionally low latency, high quality market data information.

## 2.3 Resilient communication links

Equiduct has a policy of using multiple carriers for network connectivity to its clients. In selecting a communication partner, both legs of a resilient circuit are mapped to ensure they do not share any common infrastructure. Where appropriate, we recommend separate carriers are selected to prevent systemic failures affecting service delivery.

## 2.4 Firewall policy

All connections to Equiduct are firewalled providing mutual protection as well as segregating traffic from other Equiduct users. Connectivity is regulated by use of source & destination addresses and TCP ports.

## 2.5 Monitoring

All of Equiduct Systems external links are monitored continuously.

## 2.6 Testing

Equiduct will offer differing levels of test connection:

- Basic connectivity testing to test integrity of the links
- Functionality testing is the available in the UAT system using a basic VPN connection
- Failover testing can be undertaken when the full production network solution is installed

## 3 Connection types

### 3.1 Consolidated providers

Equiduct supports connectivity from many consolidated providers such as BTRadianz, Colt PrizmNet and ICE Data Services as well as serial and Ethernet connectivity from carriers such as Colt, BT, Verizon, IPC and Options.

Consolidated providers provide a single point of contact for access to multiple financial services partners. Equiduct have aligned themselves with several of these providers ensuring that their point of presence is close (in network terms) to the hubs of their networks. Each of the consolidated providers has a highly resilient connection at the Interxion datacentre.

The consolidated provider networks are resilient and well managed with connectivity to most domestic European Stock Exchanges and leading Investment Firms.

Equiduct have connections to BTRadianz, ICE Data Services, VFn, Colt PrizmNet & Pico Global and support for additional providers is in the pipeline.

The consolidated providers will NAT network addresses to maintain IP addressing structure across their network.

Pico Global	ICE Global Network	Verizon Financial Network (VFn)
122 Leadenhall Street, 30th Floor London EC3V 4AB	5th Floor Milton Gate 60 Chiswell Street London EC1Y 4SA	Reading International Business Park Basingstoke Road Reading Berkshire RG2 6DA
Shamir Parmar +44 (0)207 550 0888 <a href="mailto:shamir.parmar@pico.global">shamir.parmar@pico.global</a>	IGN Sales Team +44 (0) 207 429 4610 <a href="mailto:ICEglobalnetwork-info@theice.com">ICEglobalnetwork- info@theice.com</a>	Akdag Sezen <a href="mailto:sezen.akdag@uk.verizon.com">sezen.akdag@uk.verizon.com</a>
BT Radianz	IPC	Colt PrizmNet
BT GFS Kinsfield House 66 Prescott Street London E1 8HG	Tower House 67-73 Worship Street London EC2A 2DZ	Colt House 20 Great Eastern Street London EC2A 3EH
James Barratt +44(0)207 778 4089 <a href="mailto:james.barratt@bt.com">james.barratt@bt.com</a>	John Owens +44 (0)20 7550 8862 <a href="mailto:john.owens@ipc.com">john.owens@ipc.com</a>	Andrew Young +44 (0)7966 967731 <a href="mailto:Andrew.Young@colt.net">Andrew.Young@colt.net</a>

## 3.2 Internet VPN

The Internet is an alternative and convenient method of delivering information. It is not, however, under the control of Equiduct or their clients/vendors. Failures within the Internet can result in traffic being redirected over less than optimum routes. Congestion within the Internet is not uncommon, and this can also impact the transfer of critical financial data.

Therefore, internet VPN connectivity cannot be used for production connections for trading or market data access. However, it is commonly used as a quick enabler of connectivity to our User Acceptance Test (UAT) system.

VPNs are easy to set up and provide a secure method of information delivery. Equiduct will support both point-to-point (for more secure access) and remote access (primarily for testing) type of VPN.

Supported VPN Point-to-Point protocols:

- IPSEC VPN (with Internet key subscription) using pre-shared keys which are exchanged on the phone after the VPN connectivity form has been returned.

## 3.3 SFTP

Equiduct have sftp servers for the delivery of end of day reports and reference data files.

The servers can be accessed from all provided connectivity types: Internet based VPN, direct, or via consolidated providers.

The servers' address and TCP port numbers are provided as part of the onboarding documents.

## 3.4 Fixed link

A fixed link is a layer 2 circuit directly between Equiduct and client/vendor. The two types considered here are the leased line and local direct connection.

### 3.4.1 Leased line (layer 2)

A leased line link is a Point-to-Point layer 2 connection between Equiduct and the client/vendor. This link could be a serial connection but Ethernet is the preferred protocol.

- Ethernet
- Dark (or fractals) fibre

Links should be provided as a resilient pair.

This can be provided by Colt, Verizon, Abovenet, Level 3, Geo net, Hibernia, EUNetworks, Edge Telecom, and Interroute. The client is responsible for the carrier choice, but we typically recommend that the customer go with a carrier that is on-net at Interxion as this will reduce the lead time of the circuit.

### 3.4.2 Local connect

Equiduct's policy of placing systems within datacentres hosting other execution venues, market data providers and clients means that many of Equiduct's client and vendor equipment will be adjacent to Equiduct's. This allows for layer 2 connections with ultra-low latency, maximum security and the lowest cost. Where possible, local connects are the first-choice method of connection.

Please note that there is an associated cross connect charge for the local connection. This is limited to a one-off cost and no monthly charges.

Equiduct uses BGP as the routing protocol over this connection. As standard, these are 1 Gigabit links.

## 3.5 Network address translation (fixed links)

Where Equiduct provides CPE devices on a customer's site Equiduct will take care of all NAT and will present in line with the customers addressing. Where a customer provides CPE equipment, they will be responsible for the NAT boundary. We require the use of a globally unique address space that is allocated to them or, that they NAT to an Equiduct address range which will be provided. Where this is not acceptable to them, they will be required to perform NAT on their own devices.

## 4 Gateway operation

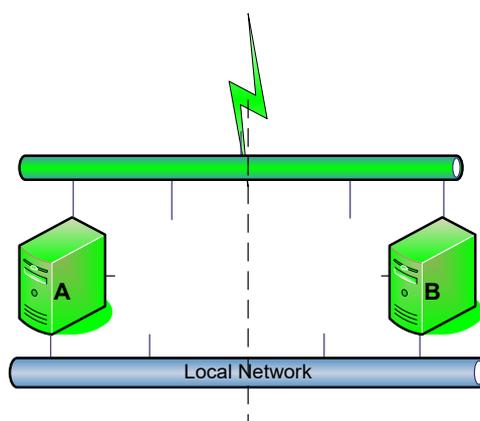
### 4.1 Market Data

Equiduct will always provide at least two resilient gateway addresses for clients to connect to. These gateways run in “hot-hot” mode and to avoid a single point of failure clients are recommended to connect to both at all times.

Market Data is available via Equiduct’sITCHMD protocol over point-to-point TCP connections.

#### 4.1.1 Normal operation

There are two gateways assigned to each client. (i.e. Gateways A and B). Both gateways are live ready to service the client market data requests and will deliver identical streams of data.



*Figure a: live-live scenario for the MD gateways.*

#### 4.1.2 Gateway failure

Should any of the gateways fail then the other gateway will still be available for client connectivity.

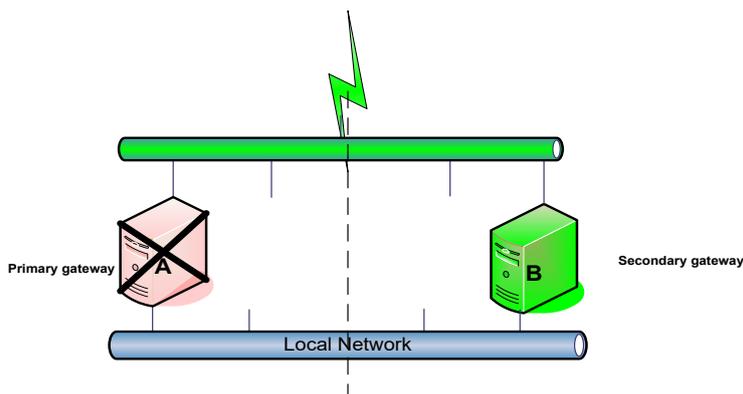


Figure b: failure scenario for the MD gateways.

## 4.2 Trading

For FIX trading gateways (order entry/management and trades flow), there is a primary and secondary gateway for each client session. Gateways operate in “hot standby” mode with the secondary gateway only available in case of a failure of the primary gateway. In case of connection loss or unavailability, client systems should attempt to connect to the secondary gateway and keep trying both primary and secondary until a session is re-established.

### 4.2.1 Normal operation

Client connects to the primary gateway A and gateway B is configured as a hot standby to take over in the event of gateway A failing.

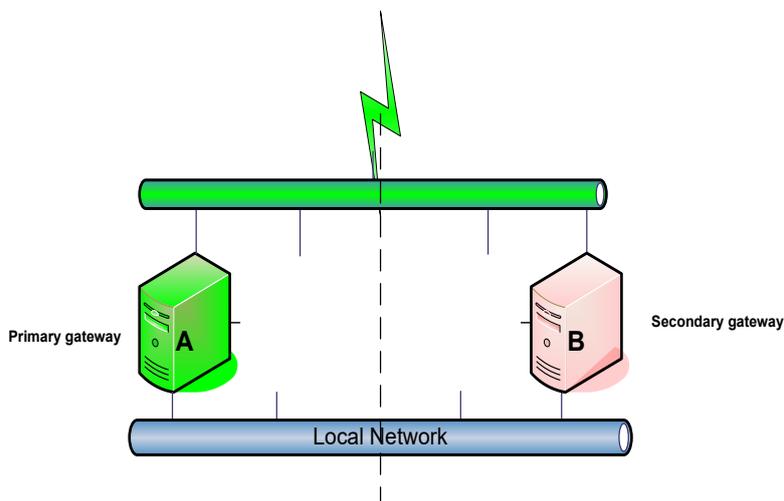


Figure c: hot-standby scenario for the TX gateways.

## 4.2.2 Gateway failure

In the event of a failure of primary gateway A connection is made to gateway B. Note that gateway A and B are synchronised so there is no loss of data after the FIX session resynchronisation.

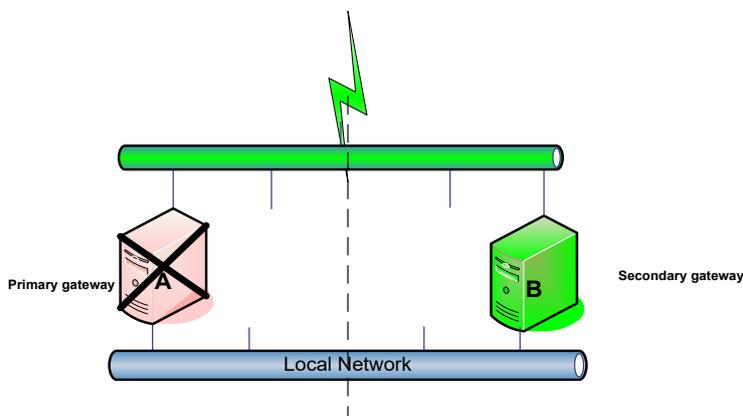


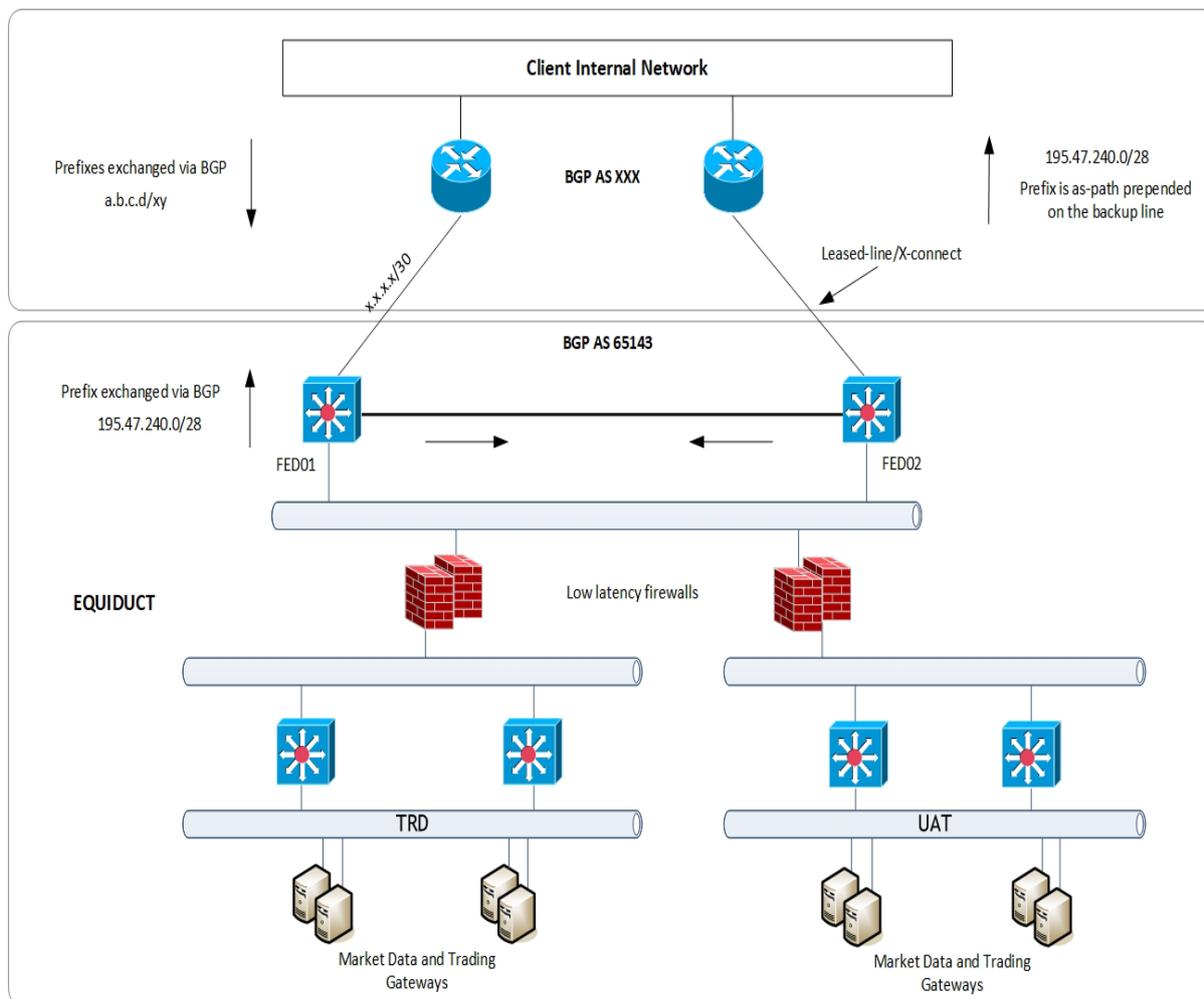
Figure d: failure scenario for hot-standby TX gateways.

## 4.3 UAT

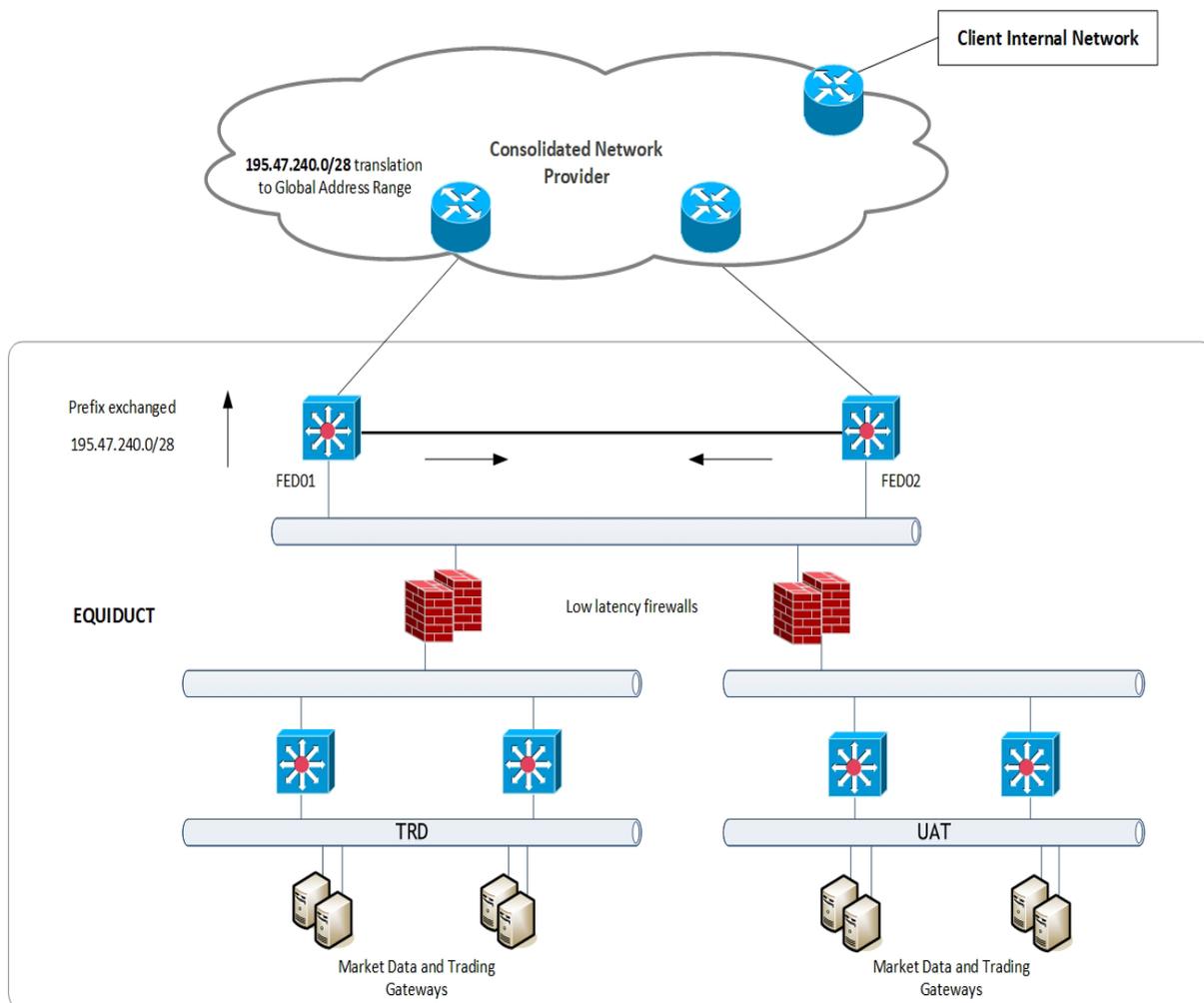
Equiduct offer a single Virtual IP address which provides connectivity two both Market Data and Transactional UAT gateways. Clients will be allocated specific ports, and where applicable usernames and passwords. Equiduct can offer VPN connectivity to provide fast commissioning of a UAT connection. Client host address information will be required for firewall access.

# Appendix A Topologies

## Appendix A.1 Typical leased-line connectivity topology



## Appendix A.2 Typical consolidated provider connectivity topology



## Appendix A.3 Typical site-to-site VPN topology

