Isode

XMPP for Constrained Link Environments

Setting up M-Link for Constrained Networks for use over SatCom (IP) and HF (STANAG 5066) links.

Isode

Contents

Introduction

This guide details the process for setting up a link between two M-Link servers over two different constrained network links:

1. Using IP, such as might be used by a SatCom link.

2. Using STANAG 5066, for use over a HF Radio link.

M-Link is the generic name for a family of XMPP server and gateway products:

- M-Link User Server (XMPP Server)

- M-Link Edge (XMPP Boundary Guard)

- M-Link IRC Gateway (XMPP/IRC Gateway)

- M-Link Constrained Networks (XMPP Messaging for low-bandwidth and/or high-latency networks)

The M-Link product used in this evaluation is "M-Link for Constrained Networks".

> *Use of TLS: Due to UK Export Controls we are unable to provide Evaluation Licenses to certain Geographic regions that would allow the use of TLS so this guide will not configure any TLS. Should you wish to use TLS please contact your Account Manager and if you are located in an approved region we can provide a license (MAC Address of Server required) and additional instructions for configuring TLS.*

Objectives

By the end of this guide you will have:

1. Set up a peer to peer link over an IP network between two M-Link servers

2. Set up a peer- to peer link over a HF Radio (STANAG 5066) networks between two M-Link servers.

3. Set up Federated Multi-User Chat (FMUC) to ensure stable operation of multi-user chat over a constrained link.

4. Learned how to filter out some types of traffic between servers in order to improve performance of both 1:1 and Multi-User Chat.

You'll use the M-Link Console (MLC) management GUI to set up your system. MLC is Isode's central tool for XMPP system Configuration and Operational management for all products in the M-Link family.

The diagram which follows shows the main elements of the system.
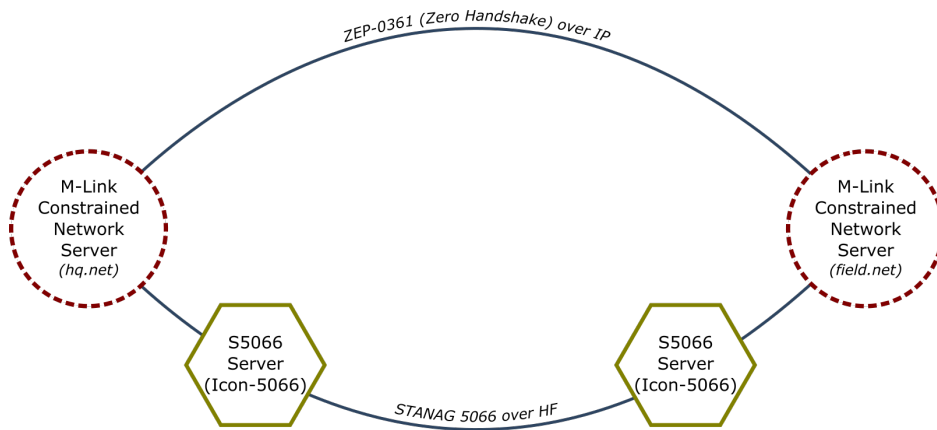
For the purposes of this evaluation we have assumed that the two M-Link servers (*headquarters.net* and *field.net*) have already been set up, together with their associated MUC domains. If you do not know how to set up M-Link servers, please complete the "Setting up an XMPP System for 1:1 and Multi-User Chat" first.

Using Isode Support

You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to *support@isode.com*. Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

Preparation

You should visit *www.isode.com/products/supported-platforms.html* to discover which operating systems are supported for Isode evaluations. Please note that in addition to the server platforms listed, we support the use of Isode servers on Windows 8, Windows 8.1 and Windows 10 for simple evaluations and demonstrations.

Isode Products

Product downloads are held in a password-protected section of the Isode website. If you have not already done so you should apply for a username/password by filling in the form located at *www.isode.com/evaluate/evalrequest.html*.

Products can be obtained by clicking on the links in the "Download Links" section of the Evaluation page (*www.isode.com/evaluate/evaluate-xmpp.html*). The downloads page will give installation instructions specific to your platform.

Product Activation Key

Isode server products require a valid Product Activation Key from Isode before they will run correctly. Keys are issued by Isode Customer Services. If you haven't already been sent a Key when requesting access to the evaluation files, please send a message to request one to *support@isode.com* remembering to specify which Isode server products you need a Key for.

By default, the file you receive needs to be placed in *\Isode\etc* (Windows) or */etc/isode/* (Linux), renamed as 'license.dat'. You may have chosen an alternative installation directory when installing the software, in which case you will have to place the license file there.

Product Activation Key Restrictions
All products in the M-Link family are distributed as part of the M-Link packages you will download and install. The Product Activation Key controls which M-Link product (and what functionality) you have access to.

The Product Activation Key sent to evaluators allows access to all M-Link products for a limited time. If you are an M-Link customer you should be aware that the permanent Product Activation Key you have for your M-Link installation may not include the Constrained Bandwidth features necessary to complete this evaluation. Contact your account manager for more information.

Windows Users: Visual C++ Redistributable Packages

On Windows, R17.0 is built with Visual Studio 2015 which means you must install the Visual C++ Redistributable Packages in order to run the Isode products. You need to download these from Microsoft: *https://www.microsoft.com/en-us/download/details.aspx?id=48145*. Make sure that your Windows server is fully patched with the latest Windows Updates before you install the Visual C++ Packages.

Operation over IP Networks

Isode constrained network protocols can operate over any IP network. They will typically be deployed where network performance is poor (low reliability or high latency or low throughout). As there are no specific IP requirements, initial testing may be done over a fast LAN.

Firewall Settings

On server systems, firewalls should be turned off or TCP Port 65510 enabled (or other port if you choose, we've used 65510 in this guide) for the XMPP Optimized Server-to-Server (S2S) connection

Link Setup for IP Networks

In section we're going to set up an Optimized S2S link between the two nodes in the system. We are doing this from the perspective of headquarters.net. You will need to repeat this step for the field.net node. Within MLC connect to headquarters.net, expand "Service Configuration" and select "Peers and Links" (Image 1).
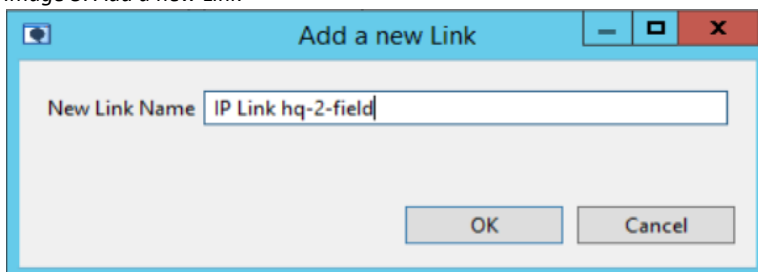
Image 1: Peers and Links
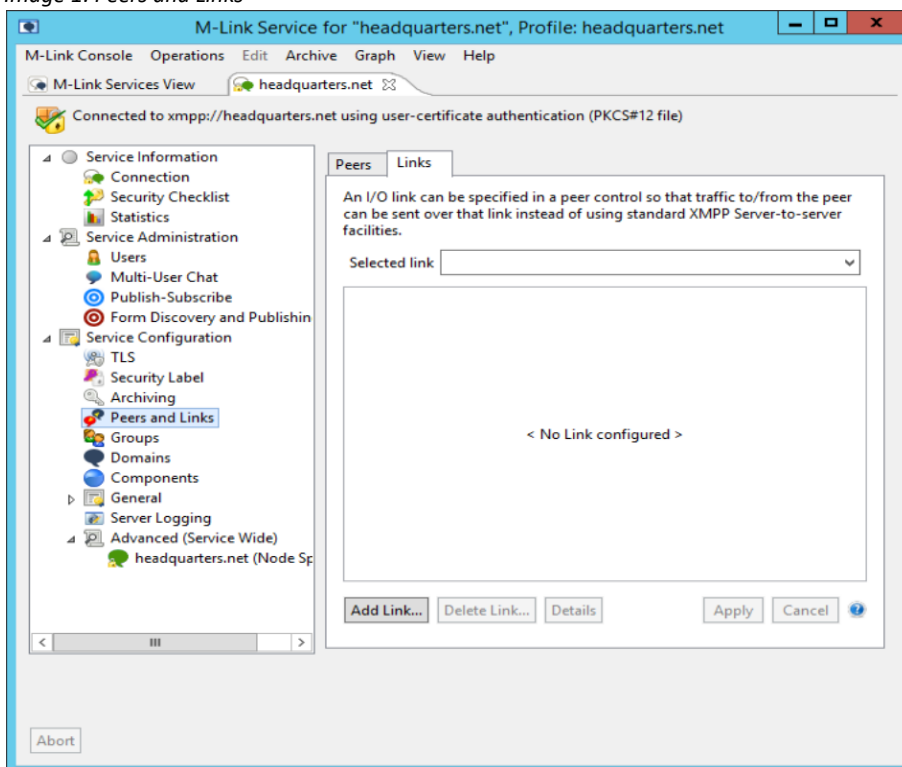
On the "Links" tab, click on [**Add Link**] and, in the pop-up select the "XEP-0361 Zero Handshake Link" option and click [**OK**].

*Image 2: Select a Link Type*
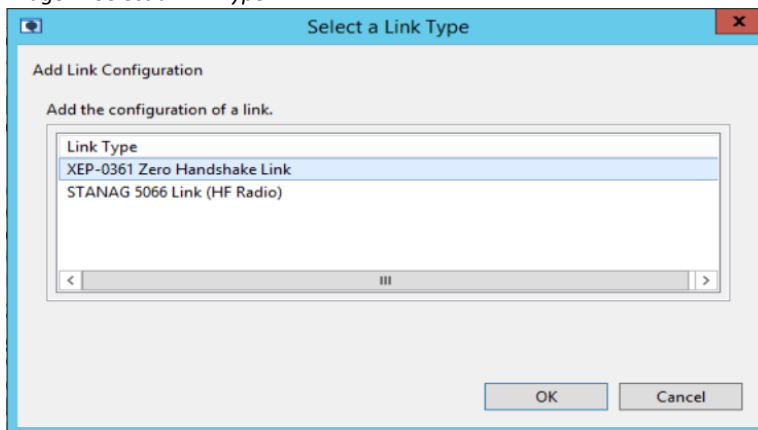
Give the new link a name and click [**OK**] to return to the main MLC interface.

Image 3: Add a new Link

The link parameters in MLC (Image 4) should be completed as follows:

- Remote IP: The IP address of the peer server (field.net in this case)

- Remote Port & Local Port: Both should be set to 65510 or to another value that will not be otherwise used. Firewalls should be configured to open this port

- Compress Traffic & Stream Management: Both of these options should be selected
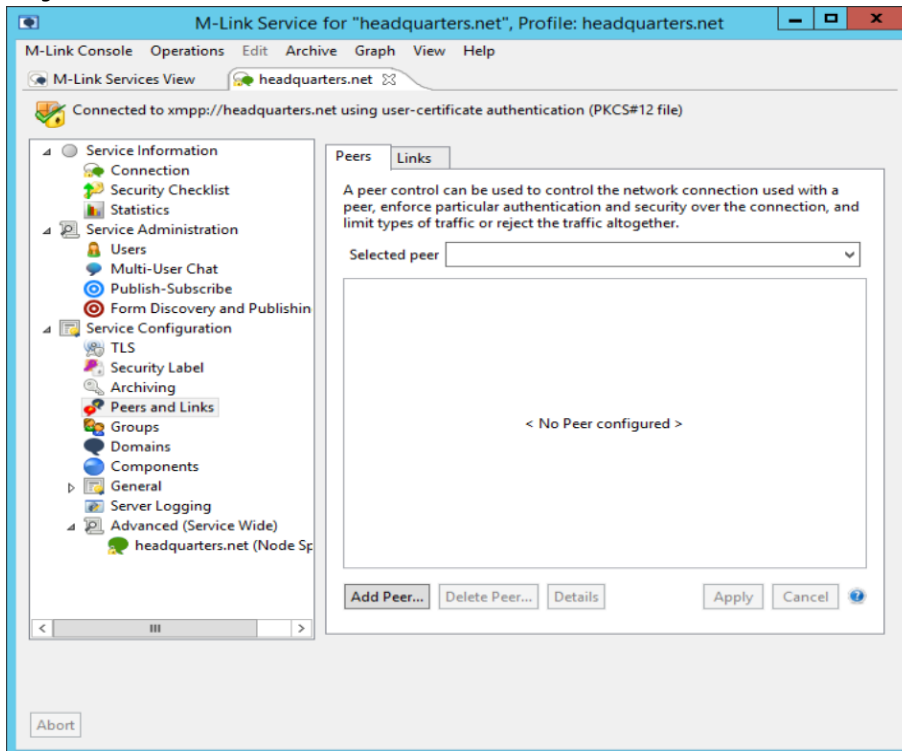
Image 4: Link Parameters
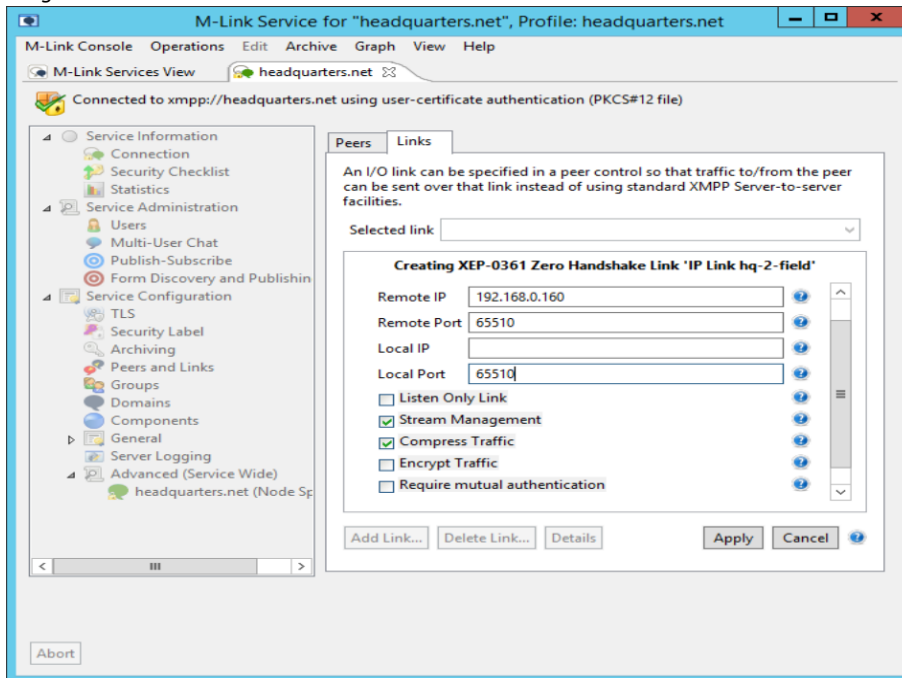
Click on [**Apply**] to commit these changes.

Peer Configuration for IP Networks

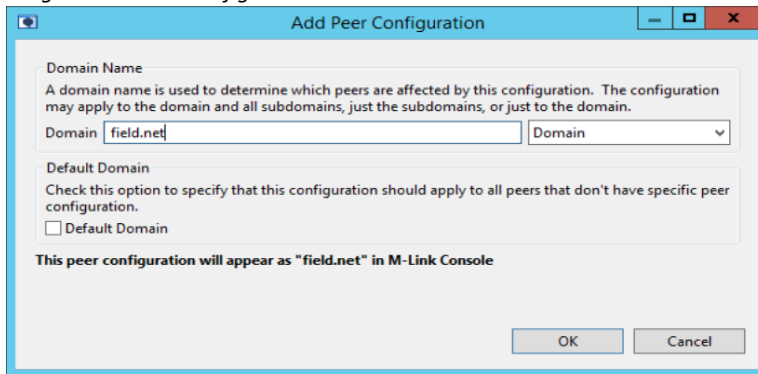Now select the "Peers" tab in MLC.

Image 5: Peers tab

Click on [**Add Peer**] and in the pop-up (Image 6) type in the domain for the system we are peering to "field.net" and then click [**OK**].
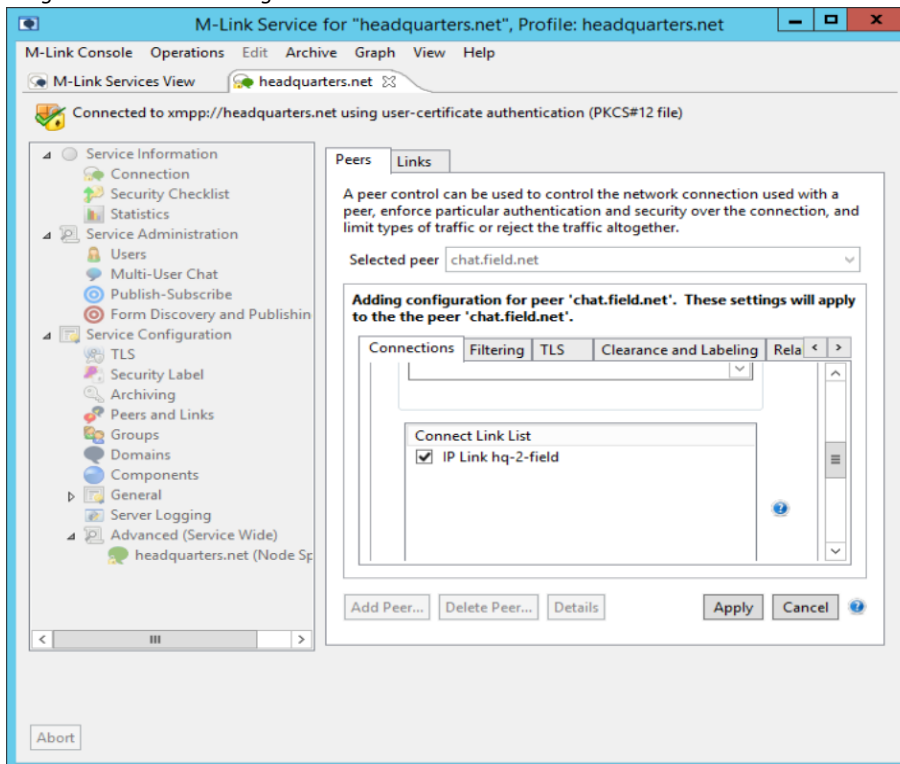
Image 6: Add Peer Configuration

Back in the main MLC interface, select "IP Link hq-2 field" from the list of available links (Image 7) to indicate that we wish to use the link set up in the previous section to connect to this peer. Click [**Apply**] to commit these changes.

Image 7: Commit the changes

We will now repeat this process for the chat domain "chat.field.net".

Click on [**Add Peer**] and this time, the pop-up type in the chat domain for the system "chat.field.net" and click [**OK**]. Back in the main MLC interface, select "IP Link hq-2 field" from the list of available links, Click [**Apply**] to commit these changes.

The M-Link services will need to be re-started to recognize this new configuration. To do this, click on the M-Link Services tab in MLC and, from the "Operations" menu select "Restart local MLink Server".

Image 8: Restart Server
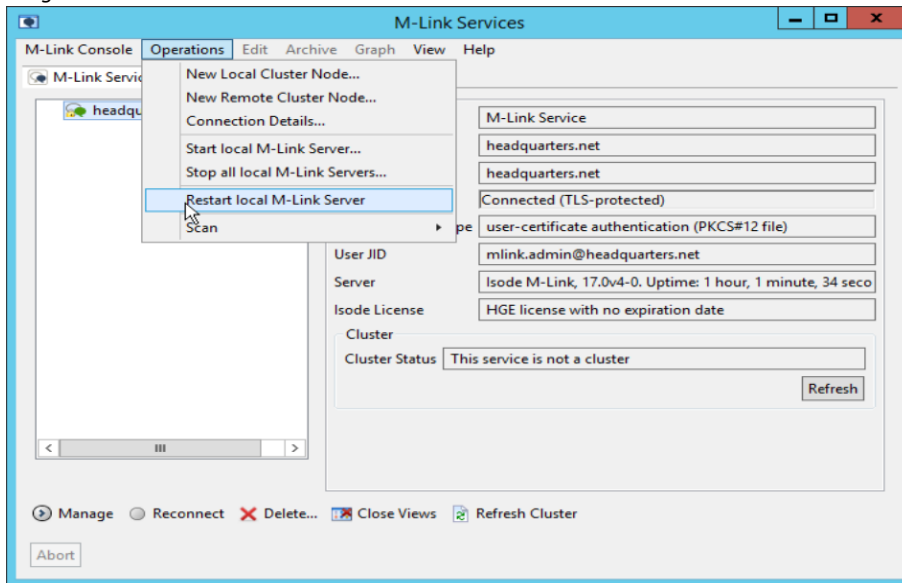
You should now configure the remote XMPP server (*field.net*) in the same way, using the values for *headquarters.net* where appropriate. After configuration of the remote server is completed, XMPP clients connected to the two servers will be able to talk to each other over the IP link.

Operation over HF Radio (STANAG 5066)

STANAG 5066 provides a link level protocol that is optimized for HF Radio. It also defines an access protocol (the SIS Protocol) that enables applications to use STANAG 5066 Link protocols and other HF link protocols (e.g. STANAG 4538). Direct use of STANAG 5066 via the SIS protocol provides for optimum application utilization of HF Radio, and Isode strongly recommends this approach.

This section assumes that you have access to a STANAG 5066 server. Isode's own "Icon-5066" product is available for this purpose and an evaluation guide for Icon-5066 is available from www.isode.com/evaluate/evaluate-network.html.

To configure Isode applications to use STANAG 5066, two parameters are needed:

- The domain (or IP address) of the STANAG 5066 server
- The TCP ports of the STANAG 5066 server (port 5066 is commonly used)

Prior to running Isode applications over an S5066 link, we recommend testing the STANAG 5066 subsystem, using Isode's 'STANAG 5066 Console' tool.

Testing the 5066 Subsystem using S5066 Console

Isode's STANAG 5066 Console is intended to help set up, test, and monitor STANAG 5066 infrastructure. In Windows click Start, and from the Programs menu, select "Isode 17.0 > S5066 Console". In Linux execute the following command:

```
% /opt/isode/bin/s5066console
```

Within the S5066 Console tool, select "View > S5066Console" followed by "S5066 Server>Add". S5066 server parameters screen should be completed as follows:

- Friendly Name: Give the S5006 server an identifying name
- Hostname/Port: Fill in the Host and Port of the S5066 server
- Auto-discover: select this option
- Transmission Mode: Set to ARQ
- Broadcast Address: Configure the broadcast address, which will be set by the server

Link Setup for STANAG 5066

Within MLC, and connected to the *headquarters.net* M-Link server, expand "Service Configuration" and select "Peer and Link". On the "Links" tab, click on [Add Link] and, in the pop-up select the "STANAG 5066 Link (HF Radio)" option and click [**OK**].

Image 9: Select Link Type
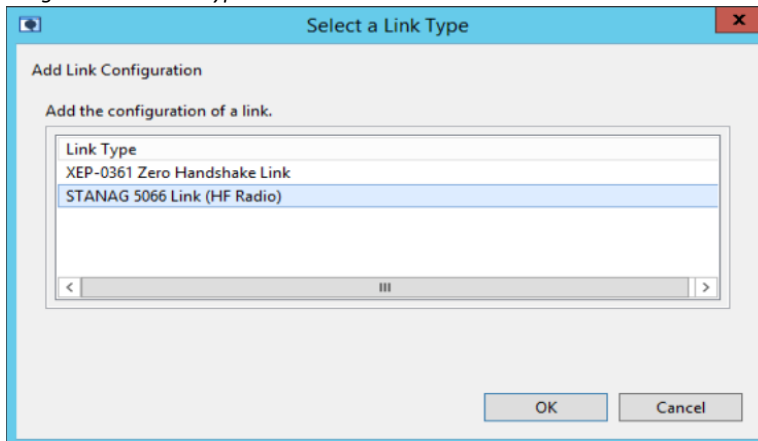
Give the new link a name and click [**OK**] to return to the main MLC interface.

Image 10: Add a new Link
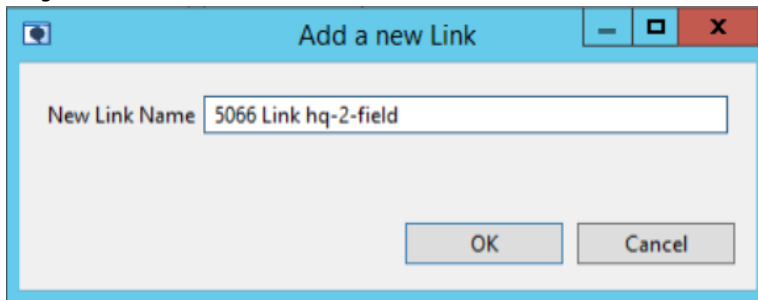
The link parameters in MLC (Image 11) should be completed as follows:

- The link parameters in MLC should be completed as follows:

- SAP ID: Should be set to 6

- Listen On Host: The IP address of the local STANAG 5066 server

- Local Port: The port of the local STANAG 5066 server (typically "5066")

- Local S5066 Address: The address of the local STANAG 5066 server

- Compress Traffic: Compression should be selected
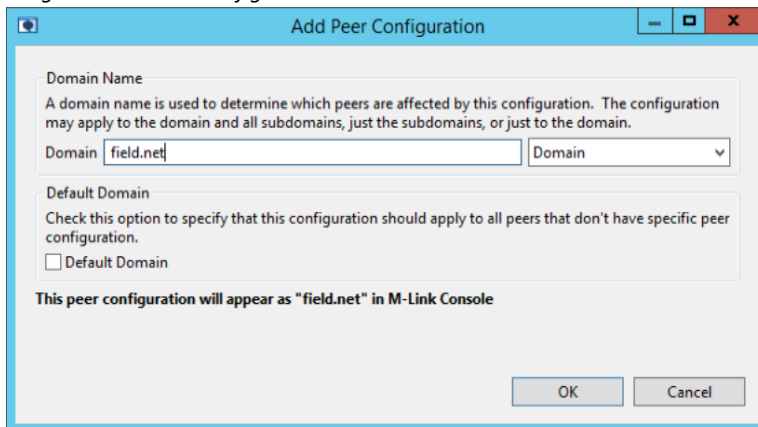
Click [**Apply**] to commit these changes.

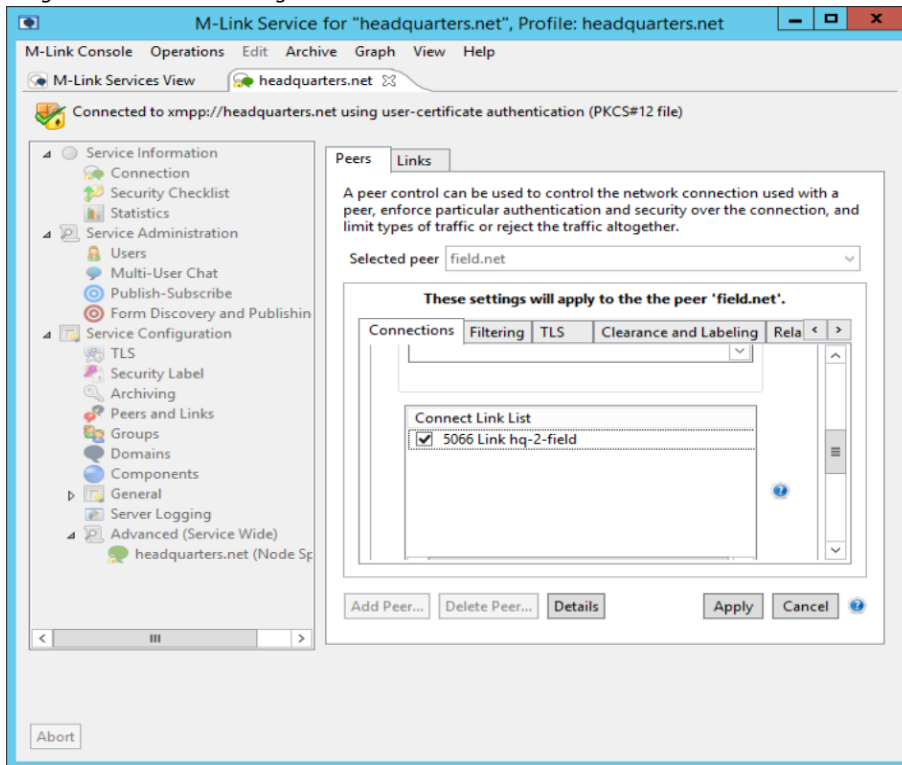*Image 11: Link parameters*
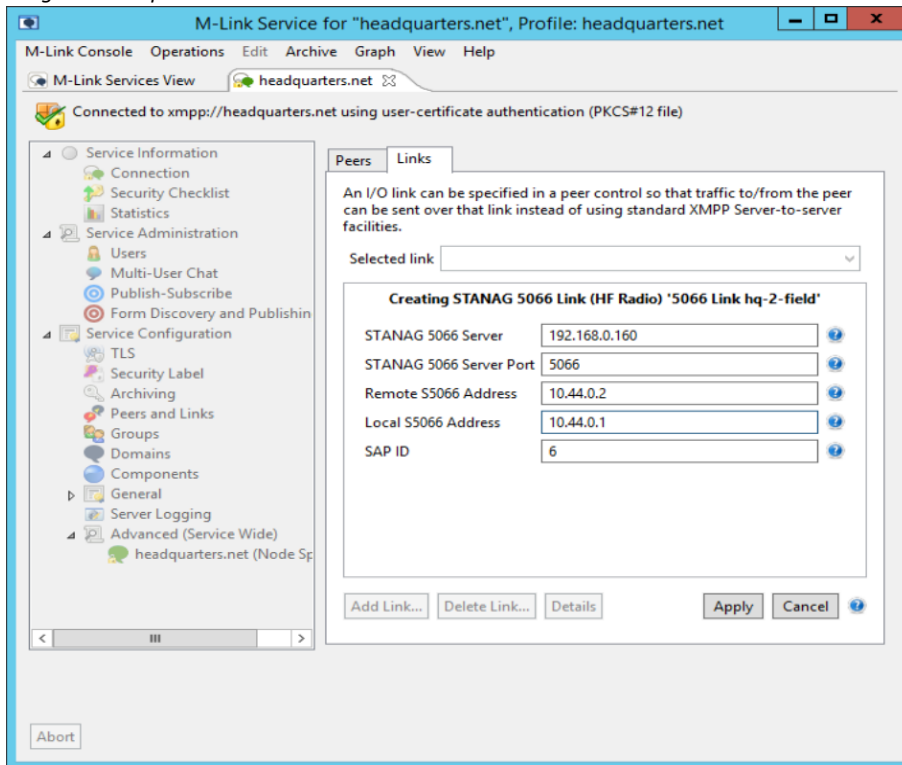
Peer Configuration

Expand Service Configuration and click on Peer and Link then click on the Peers tab Click [**Add Peer**]. Type in the IM domain for the field.net M-Link server, Click [**OK**].

Image 12: Add Peer Configuration

Tick the "5066 Link hq-2-field" from the Connect Link list, click [**Apply**].

*Image 13: Commit the Changes*

We will now repeat this process for the chat domain "*chat.field.net*".

Click on [**Add Peer**] and this time, the pop-up type in the chat domain for the system "chat.field.net" and click [**OK**]. Back in the main MLC interface, select "IP Link hq-2 field" from the list of available links. Click [**Apply**] to commit these changes.

The M-Link services will need to be re-started to recognize this new configuration. To do this, click on the M-Link Services tab in MLC and, from the "Operations" menu select "Restart local M-Link Server" (Image 14).

Image 14: Restart Server
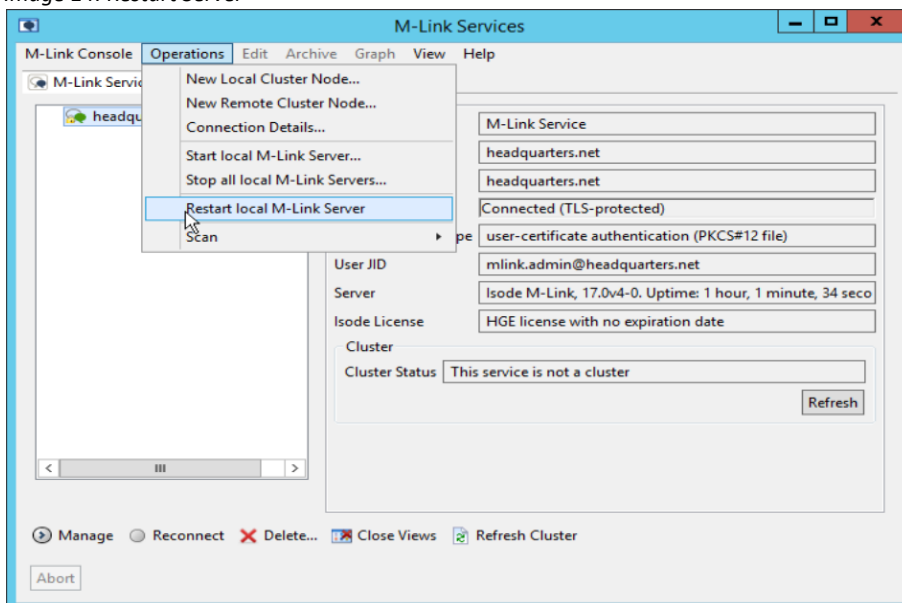
You should now configure the remote XMPP server (*field.net*) in the same way, using the values

for *headquarters.net* where appropriate. After configuration of the remote server is completed, XMPP clients connected to the two servers will be able to talk to each other over the S5066 link.

Traffic Filtering

For slow links it will often be useful to filter out some types of traffic.

In the following example we're using element folding to cut out chat state notifications (e.g. information such a "user is typing") which are normally not desirable on a slow link.

*An extensive set of traffic rules can be set for peer links, some of these are illustrated in this section. For more information, please see the M-Link Administration Guide available from [*www.isode.com/support/docs.html*].*

Click on the "Peers" tab and select the Filtering tab, click on the "Message Folding" radio button, click [**Configure**].

Select the "Advanced Configuration" tab, select "Strip all elements in the rules set" from the "Message Fold" drop-down box (Image 15).
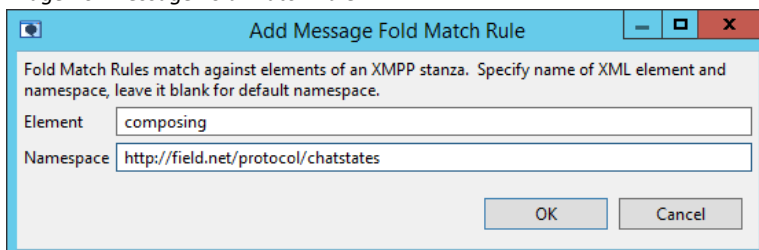
Image 15: Configure Message Folding
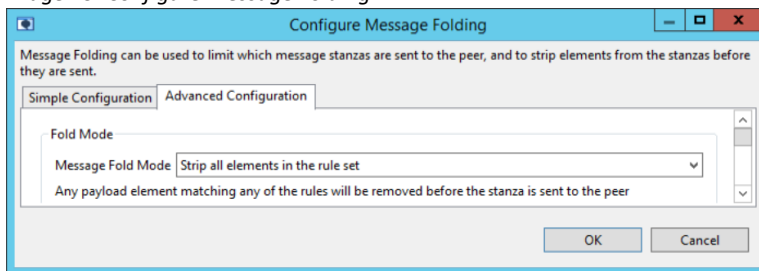
In Element Folding, click on [**Add**], where we will input each element you want to be stripped. We're going to use this to strip the following chat state notification elements for the namespace *http://field.net/protocol/chatstates*:

- composing
- active
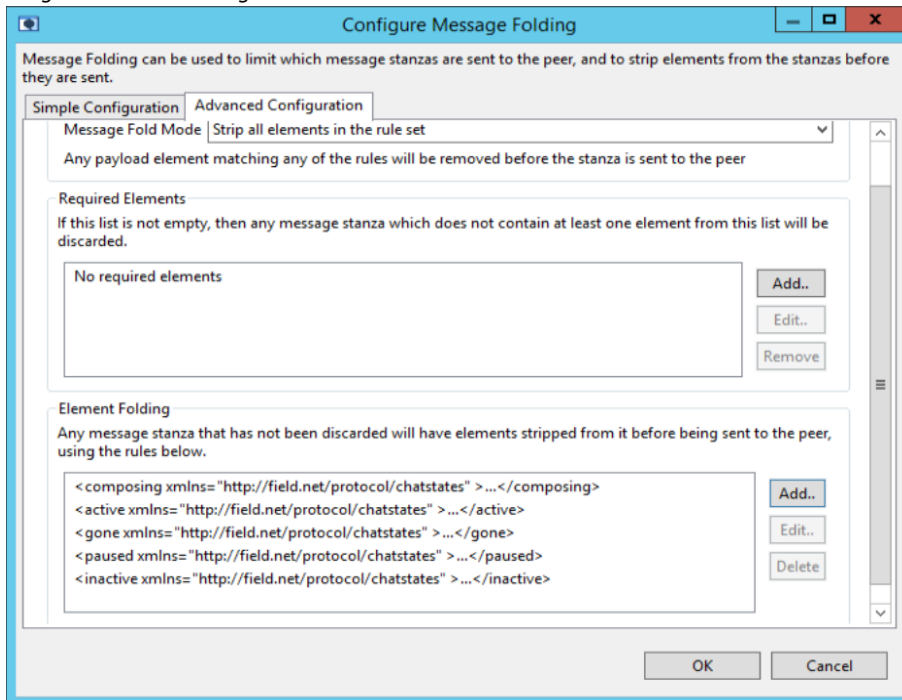- gone
- paused
- inactive

Image 16: Message Fold Match Rule

Once you have added all the elements to be stripped click [**OK**] then [**Apply**] to commit the changes.

Image 17: Commit Changes

You might also want to add the following match rule:

- Element: Html

- Namespace: *http://field.net/protocol.xhtml-im*

This will strip HTML messages, leaving only the text version. Click [**OK**] to Commit the changes.

On extremely slow links (such as a slow HF link with large numbers of users at each end), it may be desirable to strip all presence information. This can be done by setting the Presence Fold mode to "The server will not pass the matched elements to the peer". If this value is set and no rules are specified, this will cause the special action of stripping all presence information. This will only work for 1:1 chat and should not be used in conjunction with Federated MUC.

Federated Multi-User Chat

Federated Multi-User Chat (FMUC) is where a Multi-User Chat room is federated across multiple servers.

In this section we show how to federate two MUC rooms (one hosted by each M-Link server) so that they act as a single coherent MUC room. Local messages will always be delivered rapidly locally and the two MUC rooms will continue to operate if the link goes down. Each MUC room needs to be federated with the other one, so the following steps need to be repeated for both sides of the link.

FMUC needs to be configured, expand "Advanced (Service Wide)", click on "headquarters.net (Node Specific)". Scroll down to "Enable XEP-0289 FMUC" and tick the box.

Click on [**Apply**] to commit the change.

Image 18: Configuring FMUC
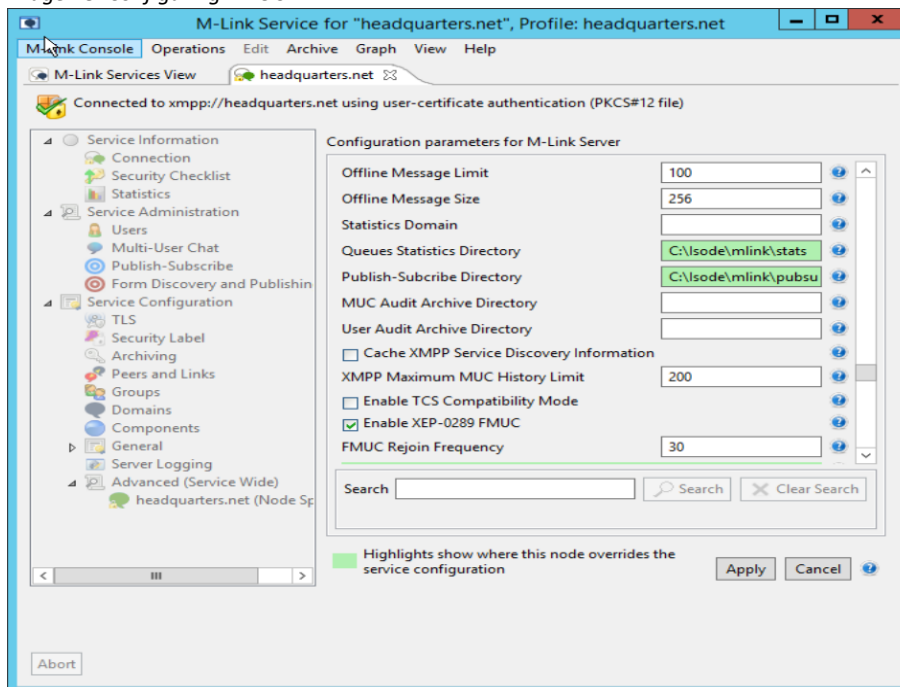
These changes need to be applied to both servers, and both servers restarted, after FMUC is first configured. Once FMUC has been configured, additional options relating to FMUC will appear in the MUC room configuration screen, click on "Service Administration" and select "Multi-User Chat" option in MLC. Select "hqroom1@chat.headquarters.net" and click on [**Configure Room**].

Image 19: Selecting the Room for Configuration
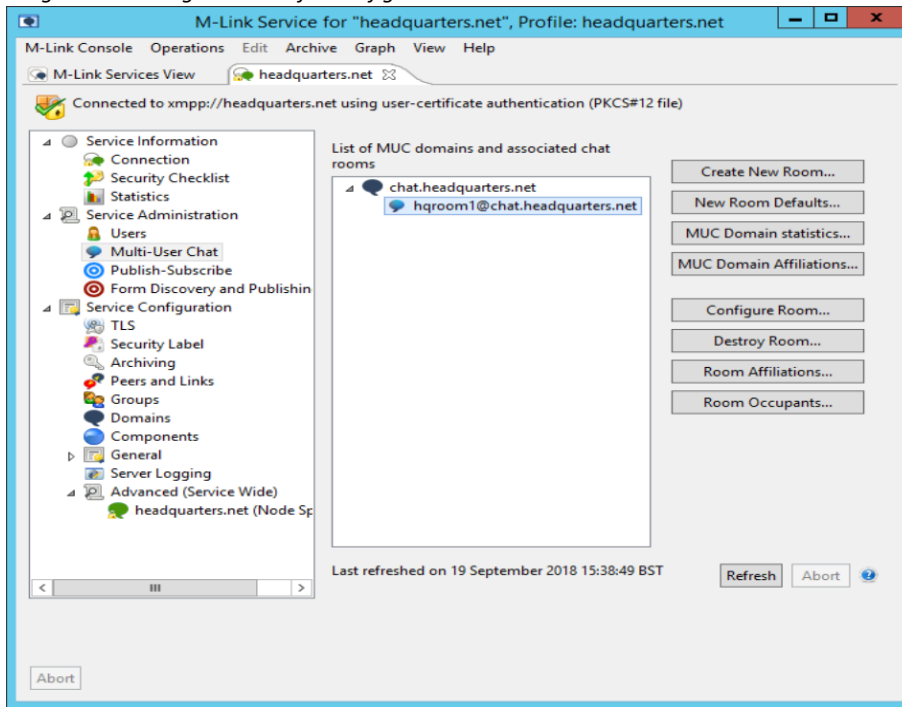
Click on the FMUC tab, to configure FMUC simply add the name of the remote MUC room you are federating with in the MUC configuration screen of your local MUC room. In the example that follows our local MUC room *hqroom1@chat.headquarters.net* is federating with *fieldroom1@chat.field.net* in a master/master configuration.

Image 20: Configure Room
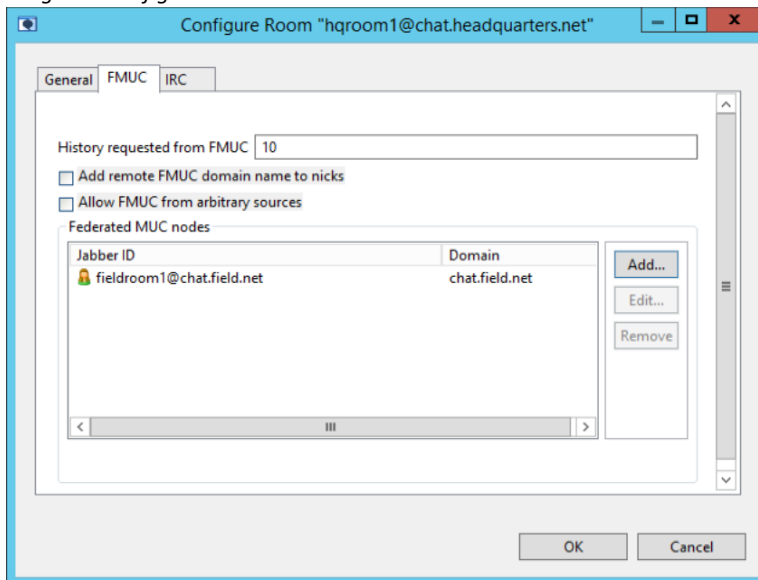
The mirror of this configuration will need to be done for the MUC room on the remote domain. Once completed, the two MUCs will be federated and MUC users will see a single MUC room populated with users connected locally to both servers.

Telemetry Logging

Resolving any issues with constrained link communications can often be assisted by examination of the telemetry.

In this section we show how to set up Telemetry logging. Expand "Advanced (Service Wide)", click on "headquarters.net (Node Specific)" scroll down to Telemetry Log Directory, type in a suitable location for telemetry log storage. (The directory must exist for telemetry logs to be generated).

Image 21: Setting Telemetry Logging Location
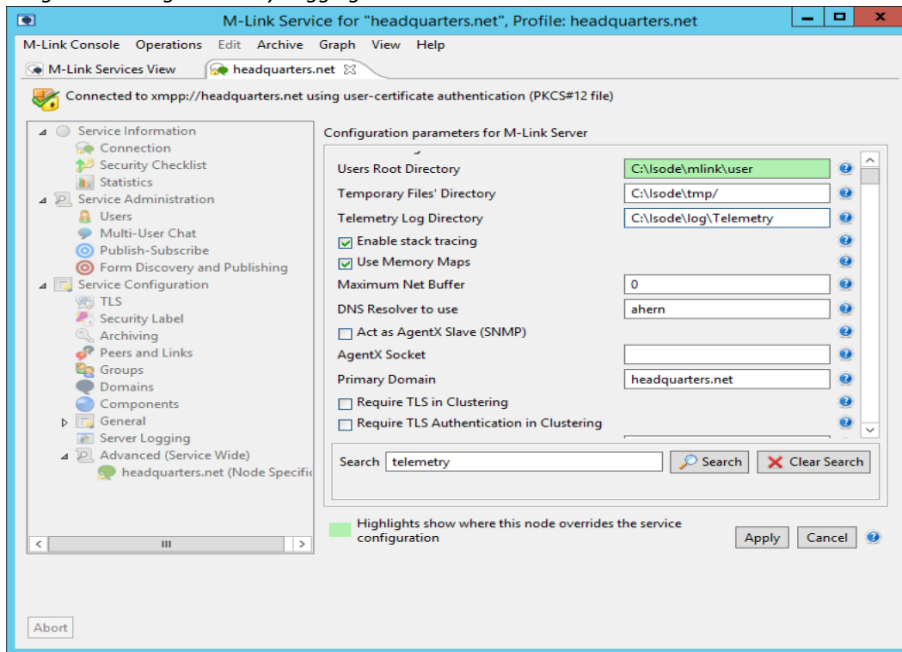
Now create a sub-directory within that directory named after the IP or STANAG 5066 address of the remote XMPP Server (field.net), e.g. C:\Isode\telemetry\192.168.0.160.

After restarting the server you'll be able to view telemetry logs by browsing to the C:\Isode\log\telemetry directory.

Isode

What Next?

More information on the M-Link for Constrained Networks can be found on the Isode website at *www.isode.com/products/m-link-constrained-networks.html*.

Detailed configuration and operational information on all variations of M-Link can be found in the M-Link Administration Guide available from the Isode website at *www.isode.com/support/help.html*.

Other Evaluations

This guide is one of three relating to Isode's XMPP products:

- Setting up an XMPP System for 1:1 and Multi-User Chat
- Connecting XMPP and IRC Chat Services
- XMPP for Constrained Network Environments (this guide)

Information on all of these evaluations can be found *at www.isode.com/evaluate/evaluate-xmpp.html*. For XMPP evaluations outside of the scope of these guides, please contact us.

Whitepapers

Isode regularly publishes whitepapers on technical and market topics related to its products. A full list of these can be found at *www.isode.com/whitepapers/*.

Copyright