

Title:	GCSx Pre-Connection Take-On Guide
Version:	1.7
Date:	16 May 2008
Author:	Government Connect (Colin Wisby)
Owner:	Government Connect (Anna Smith)
Client:	Government Connect

Table of Contents

1 Welcome to Government Connect (GC) 4

 1.1 Document Updates..... 5

Intended Audience and Scope of this Document..... 6

2 Connecting to GCSx 10

 2.1 Overview 10

 2.2 C&W’s Role in the Installation 16

 2.3 The Customer’s Role in the Installation 17

3 Where is the GCSx Service Available? 18

 3.1 Background 18

 3.2 Fixed Access Lines 19

4 Further Details on Things You Need to Do 20

 4.1 Connectivity 20

 4.2 Routed IP Network 21

5 GCSx Connection Initiation (Setup and Configuration)..... 22

 5.1 IP Addressing 22

 5.2 IP Routing..... 24

 5.3 DNS Resolution..... 24

 5.4 Web Proxies 27

 5.5 E-mail Servers..... 28

 5.6 Definition of Local Aliases 33

 5.7 User Details GC Directory..... 35

 5.8 Network Time Service 35

 5.9 Firewall 37

 5.10 Schematic Diagram..... 39

6 GCSx Connection Validation (Multi-Layer Testing) 39

7 GCSx Service Desk and Support 40

8 Appendix A – Testing 41

 8.1 Test Objectives and Strategy 41

 8.2 Limits of Testing Scope 41

 8.3 Useful Test Resources 41

 8.4 Test Prerequisites 43

 8.5 Connectivity Testing..... 44

 8.6 Mail Exchange Testing..... 45

9 Appendix B – Environmental Information 48

 9.1 Introduction..... 48

 9.2 Wall-mounted NTP 48

 9.3 Rack-mounted NTP..... 49

 9.4 NTE Specifications 50

 9.5 Customer Edge Router Specifications 52

10 Appendix C – Example Communication to Customer from C&W 61

11 Appendix D - C&W Government Connect Circuit Delivery 64

12 Appendix E – Connection Checklist 66

13 Appendix F – Aggregate Gateway Connections..... 68

 13.1 Overview 68

 13.2 Relationships..... 68

 13.3 Network Access Control 69

 13.4 Architecture 70

 13.5 Detailed Technical Options 71

14 Appendix G – Glossary of Terms 73

1 Welcome to Government Connect (GC)

The Government Connect Secure eXtranet (GCSx) is a secure, digital communication network that links local authorities with each other, the NHS, criminal justice agencies and central government departments. Effectively it completes a single secure intranet for government of all forms, enabling trusted individuals to exchange information that may be sensitive for personal, legal or financial reasons.

GCSx is a private, and therefore inherently secure, national IT infrastructure that will provide significant value to the UK Government 'back office', enabling products and services to be delivered securely. To-date, Central Government Departments, their Agencies and Scottish Local Authorities (LAs) have had access to a private and secure national infrastructure called the Government Secure Intranet (GSI). The GSI is a Managed Service operated by OGCbuying.solutions currently delivered through a partnership with Cable & Wireless Communications Ltd (C&W).

Government Connect (GC) is enabling LAs in England and Wales to share sensitive information between themselves, central Government Departments and Agencies. GC has implemented the Government Connect Secure eXtranet (GCSx) to enable the establishment of a trusted network for this purpose. This will be achieved in full cognisance of the importance of trust and secure handling of personal information in order to develop confidence in online services.

GC is an enabler to Transformational Government and will, in due course, require the connected organisations to develop appropriate processes and software applications to make use of the technical capability being provided by GC.

GC is a programme delivering incremental technological enhancements, which are being rolled out in tranches. The Tranche being delivered at this time provides:

- A secure network which bridges the existing gap between Local and Central Government secure networks (aka GCSx), and
- A secure messaging relay for the ad-hoc distribution of e-mails (i.e. unstructured data and information), known as GC Mail.
- A directory and e-mail distribution list system, known as GC Directory.

The GC programme is connecting organisations across England and Wales and as the roll-out phases progress, the number of organisations and, as a consequence, the total number of addressable Users, are increasing dramatically.

1.1 Document Updates

At the time of writing, the Government Connect programme and GCSx network are at a maturing of rollout. Lessons identified as a result of rollout experiences may affect the content of this document, and what an LA may be required to do to gain full access to all services. Please ensure you have the latest copy of this document by downloading it from www.govconnect.gov.uk or by contacting Government Connect.

Intended Audience and Scope of this Document

This document is intended for technically skilled people responsible for the control and management of Customer IT systems. This document contains technical information and procedural guidance intended to provide those tasked with establishing the connection of a Customer to GCSx with sufficient knowledge to prepare for successful connection. Generically, this document refers to connecting organisations as the 'Customer'.

Note: This document is UNCLASSIFIED. References to data that is protectively marked RESTRICTED have been avoided (e.g. IP addresses are presented as [TBC]). GC will provide RESTRICTED information (such as IP addresses) to each Customer under separate cover. This RESTRICTED data set will be provided once the Customer's Code of Connection (CoCo) has been approved and the Customer is about to undertake technical integration of GCSx.

This document is the GC "Pre-Connection Take-On Guide"; the first of two documents, which together provide a complete overview of GC Take-On. The second document in the series will be the "GCSx Operational Support Guide". The scope of each of these documents is:

- **GC Pre-Connection Take-On Guide:** this document details the equipment and installation activities involved in connecting to GCSx and the pre-configuration aspects associated with the use of the GC Mail service. It explains who will provision the initial GCSx Services and who will support you through the initial testing process. To complete configuration of Customer equipment, Customers will need access to the RESTRICTED information referenced within this document. This information will be provided by the GC technical team under separate cover.
- **GCSx Operational Support Guide:** this document provides important strategic guidance and background information required for rolling this service out to the Customer's Users. This document also includes information relating to the GC Service Desk.

The Pre-Connection Take-On Guide should be read in the context of (and may make reference to) the following key documents, which are essential to the success of the overall take-on process. Collectively these documents form part of the GC Technical Implementation Pack. The documents of note are:

- **Subscription Process:** to guide the Customer through sign-up into implementation and beyond.
- **Pro-forma:** created for GC to allow LAs to demonstrate their intent to sign up to GCSx. The pro-forma acts as the order form for LAs to provide key ordering information to C&W.
- **Code of Connection (CoCo):** details of the security compliance process as well as the checks and audits that will be carried out in order for a Customer to connect to GCSx. There are related FAQs and guidance on what happens if the Customer does not comply with the CoCo. LAs will also be issued with generic best practice guidance on security including CCTM & IT Health Check advice.
- **Fact Sheets:** Information Sheets to provide a concise, but informative overview of GCSx, GC Mail and GC Exchange.

- **OGCbuying.solutions Terms and Conditions:** the document that all organisations must sign before they are eligible to become a member of the GSi community.
- **Register of Service (RoS):** the formal catalogue entry of exactly what a Customer can order; initially, this only covers service/products supplied solely by Cable & Wireless e.g. GCSx & GC Mail. The RoS is used to select the GC service/configuration required and these details are recorded on a 'pro-forma' which serves as an order form.
- **C&W Service Contract:** the C&W Service Contract will be provided to the Customer by C&W to allow them to formalise the service order. This will be pre-populated as far as possible with Customer-specific information. Each Customer must sign and return a completed C&W Service Contract to C&W.

The above documents are not repeated within this document; however, you will need access to these documents in order to gain a complete understanding of the options selected by your Customer and the specific conditions to which the Customer has agreed. Some of the above documents invoke additional processes, documents and agreements that the Customer must put in place and maintain to enable authorisation of the GCSx connection and in-service operation with the GC community. If you do not have access to these documents please contact GC for advice on accessing them (please contact GCTechTeam@communities.gsi.gov.uk).

Note: For any organisation to connect to the GCSx to use the GC Mail service (and future other services) contractual agreements and commitments are required; contractual arrangements for these must be in place. The technical establishment of a physical connection will, in itself, not be sufficient to join the GC community due to the commercial and security-related criteria that must also be assured (see above). This document assumes that such undertakings have been made and that contractual arrangements are in hand (i.e. these are not the subject of this document).

2 Connecting to GCSx

2.1 Overview

The GCSx installation activities will involve the Customer's Organisation, GC's Programme Team and the GCSx Service provider, C&W. It should be noted that GC is acting on behalf of OCGb.s for the implementation of this programme.

Note: This document provides information aimed primarily at a Customer connecting to GCSx using a dedicated, individual C&W-provided network connection. In some cases, groups of Customers are connecting via existing Wide Area Networks (WANs) through a single aggregated connection. Further information for aggregated network configurations may be found in Appendix F.

For the purposes of this document, a number of pre-requisite activities are assumed to have been completed. For further details of these, please refer to the appropriate documents (Section 2). These pre-requisites are:

	Activity	Detail	Owner
1	Place Order	Place an Order (via the GCSx Order Proforma) for GCSx. The Customer must agree and sign up to the Terms and Conditions with OGCBuying.solutions.	Customer
2	Prepare Service Contract	C&W prepare and agree a GCSx Service Contract (your Contract).	C&W
3	Contract for Service	The Customer signs a Contract from C&W; C&W agrees the Contract (this establishes the formal Contract for the GCSx connection).	Customer / C&W
4	Confirm Delivery	The C&W GCSx Order Desk will confirm the planned delivery date (referred to as the AFRS date) for the GCSx connection.	C&W
5	Confirm Service Details	GC will issue IP addresses & Schema to the Customer. GC will issue DNS domain details to the Customer. The Customer must return technical configuration details to GC to assist C&W to manage the GCSx network.	GC

The following activity details are expressed in a high-level, generic manner. Please bear in mind that your local arrangements / specifics may be slightly different to those listed and adjust for these. The key activities involved are listed in sequence in the table below:

	Activity	Detail	Owner
6	Installation of GCSx Circuit Equipment	<p>C&W will undertake (or arrange with BT) the physical installation of the GCSx equipment.</p> <p>Depending on the site, an Engineer may need to visit the installation site to determine the best method of delivery. You will be contacted in advance and informed when this site survey will take place.</p> <p>The installation of a tail circuit and CE router will not necessarily happen at the same time. There is a chance that there will be two engineering visits required to deliver connectivity to a Customer site: one visit to install the tail circuit, and a second visit to install the CE router. This will be communicated to the customer via C&W.</p> <p>The Customer needs to support C&W and, if appropriate, confirm the installed equipment is deemed electrically safe to operate and conforms to IEE regulations (electrical certification).</p> <p>C&W will confirm downstream connectivity (IP level) from the Customer's new installation to the GCSx network.</p> <p>Once the C&W engineer has tested and confirmed connectivity to the C&W network, the service installation at the Customer will be deemed complete. The customer-facing LAN port on the CE router will be disabled until the Customer has received Authority to Connect from OGCbs.</p> <p>The Customer's installation authority may also need to inspect the installation and confirm he/she is satisfied that the installation work has been completed to his/her satisfaction and is fit to operate.</p>	C&W / Customer
7	Configure Local Equipment	<p>The Customer is to confirm internal routing and connectivity is configured correctly for connection to GCSx. Customer to confirm local equipment (e.g. mail servers, proxies, firewalls) have been pre-configured, or are ready for configuration to enable connectivity to GCSx.</p> <p><i>Further guidance on the above are contained within the body of this document.</i></p>	Customer
8	Test Local Server Equipment	<p>The Customer will conduct internal testing to ensure that their server equipment is configured correctly to communicate with the GCSx network, and that GCSx connectivity (IP and MTA (GC Mail)) has been successful.</p> <p>A test plan has been included later in this document which will assist Customers to confirm that connectivity has been established. This will include tests to confirm connectivity to the mail and DNS servers within the GCSx network. These tests assume the Customer has connectivity to the GCSx network, and have configured their internal network infrastructure/servers correctly.</p>	Customer / C&W

	Activity	Detail	Owner
9	Service Desk First Contact	The 'demarcation point' for the service delivered into the Customer site by C&W is the LAN port on the CE router. GC will provide the GCSx Helpdesk contact details and hours of work, and what to do 'out of hours'. This information will be supplied in the GCSx Operational Support Guide.	GC
10	Authority to go Live	GC (acting on behalf of the GSi Accreditor) will seek appropriate assurance that security-related functions and procedures are in place (in accordance with the CoCo). By default, C&W will disable installed connections until the Customer has gained CoCo Approval and Authority to go Live has been received from OGCbs.	GC / CESG / OGCbs

Note: All information provided by C&W to the Customer will also be provided to GC to enable GC to maintain control and oversight of the overall GC Programme.

2.2 C&W's Role in the Installation

C&W will be involved in most aspects of the GCSx installation as detailed in the overview above.

Once you have placed your order for your new service, a member of the C&W team will contact you to provide you with details of the timescale for the delivery of your service. An e-mail communication will be sent to the nominated contact (taken from the GCSx Order Proforma) and will contain information as highlighted in Appendix C.

Upon receipt of an order, C&W will arrange and manage the delivery of the access connectivity between GCSx and the Customer site. Once the tail circuit is installed, C&W will arrange a time for a second Engineer to visit your site. The C&W Engineer will install the new GCSx CE router and ensure that the physical connection to GCSx network has been achieved. The Engineer's scope of work is limited to the C&W network, up to and including the LAN interface(s) on the C&W-provided and managed Customer Edge (CE) router.

Note: The C&W Engineer performing the installation will have a minimum of BS clearance, which should be sufficient for the majority of installations. If, for your particular site, SC cleared staff are required, you must inform the C&W Project Manager at least four weeks prior to the installation.

Note: The connection from the LAN interface(s) on the C&W-provided and managed Customer Edge (CE) router to your local (Customer-owned and managed) equipment (e.g. router) will need to be arranged by yourselves (the Customer). Generally this will involve a LAN cable connecting the GCSx CE router to the Customer LAN equipment (and configuration of the Customer LAN equipment).

2.3 The Customer's Role in the Installation

You, the Customer, will be actively involved in most aspects of the GCSx installation as detailed in the overview above. Although C&W are providing the core service and will install and maintain the new equipment, there are local aspects of the service configuration and management that will not happen unless you, the Customer, do something (or arrange for it to be done on your behalf).

The most important things to do are the pre-connection paperwork and preparation, including agreeing to the Terms and Conditions and placing the Service Contract on C&W.

The diagram in Appendix D summarises the C&W order process for GC orders.

You must provision sufficient space and power for the new equipment (refer to section 10.4 NTE Specifications, and section 10.5 CE Router Specifications), support C&W when they are on-site installing their equipment and make provision for physical connection from their newly installed router to your network (e.g. router / EAL4 Firewall).

You must arrange for your system to be configured to work correctly with the GCSx service, and be prepared to manage this connection into the future.

Before you will be allowed to connect, you will have to demonstrate to GC that your Customer has an agreed level of compliance with the Code of Connection (CoCo). The Code of Connection must be signed and returned to GC so that it can be assessed by CESG before Authority to Connect will be awarded. Once the Authority to Connect (aka 'go Live') has been issued by OGCbs, C&W will enable the LAN port on the CE router which will provide network connectivity to the GC network.

3 Where is the GCSx Service Available?

3.1 Background

The GCSx solution is based on the C&W MPLS IP VPN¹ Service which is an integrated portfolio of IP services providing a managed IP networking environment for customers to link their sites, people and information with other customers within the same communications infrastructure.

C&W will select the delivery technology (copper or fibre) and supplier for the tail circuit delivered to your site.

Note: Should the customer wish to specify a particular supplier or delivery technology (copper or fibre), C&W reserves the right to pass on any additional delivery costs to the customer.

If you have no existing Private Circuit type services from any supplier, or where a service is currently delivered via radio, C&W will quote for additional ductwork and circuit delivery charges if/as appropriate.

Where circuit / network separation is required and your site does not have suitable ducting entering the premises, C&W reserves the right to pass on additional ductwork and circuit delivery charges as appropriate for provision of alternate duct route.

3.2 Fixed Access Lines

C&W fixed line services normally utilise C&W or BT private circuits as the access method. C&W fixed line services are available in England, Scotland, Wales and Northern Ireland including all islands served by BT (e.g. Hebrides, Isle of Wight).

¹ Multi Protocol Label Switching, Internet Protocol, Virtual Private Network

10Mbps and 100Mbps services are based on BT LES (LAN Extension Services) for delivery of the access tail. Consequently, 10Mbps and 100Mbps services cannot usually be deployed more than 25km from the nearest C&W Network Access Point. If your site (service delivery address) is more than 25km from the nearest C&W Network Access Point, C&W will determine the best access method available and communicate this to you.

Provision of all services at 10Mbps and above are subject to a C&W feasibility study.

4 Further Details on Things You Need to Do

4.1 Connectivity

As part of the managed service, C&W will provide managed equipment to connect your site to GCSx.

The Customer must provide a suitable location for C&W's equipment (e.g. on an equipment shelf or within an equipment rack). This information must be provided by the customer at the time of placing the order for the GCSx service (this must be added to the GCSx Order Proforma). The space and power requirements for a given tail circuit size (e.g. 2Mbps) can be found attached in Appendix B.

Note: The actual equipment installed by C&W in the first instance will be scaled to meet your declared needs. Appendix B provides details of the equipment types that can be installed and provides specific examples of the environment required for these equipment types (e.g. power required, physical size required). The installation of GCSx equipment in totality may include additional hardware, dependent on which GC Services are procured and should be able to cater for increased capacity without impact on the reserved installation provision. Should your organisation have a specific problem in this regard please contact GCTechTeam@communities.gsi.gov.uk to discuss the potential agreement of a waiver.

The equipments that will be supplied by C&W are:

- C&W Managed Router(s) (see Appendix B)
- Network Terminating Unit(s) (see Appendix B)

Additional equipment may be required to complete this installation (which may also have been procured from C&W) such as:

- Any additional Customer Premise Equipment (CPE) ordered (e.g. managed firewall)

The physical presentation of all routers supports 10/100Mbps Ethernet as the standard Local Area Network (LAN) Interface. These interfaces are IEEE 802 conformant LAN technologies, which define the rules employed by devices (such as personal computers and file servers) attached to them within the same LAN.

Note: The standard presentation is 100Mbps Full Duplex. If you require alternative presentation (e.g. 10Mbps Half Duplex) please notify C&W when placing your order.

The C&W Service Termination Point (STP) is the physical connector at the customer facing LAN port on the C&W-provided CPE. C&W provides services to the STP, but has no responsibility for any of the equipment on the Customer's side of the STP.

4.2 Routed IP Network

GCSx is an IP service; therefore, each connecting customer requires an IP routing infrastructure to interface with the C&W STP.

To use the GCSx services, customers will require suitable infrastructure (e.g. firewalls, mail servers, DNS servers, proxy servers) capable of connecting to the C&W GCSx System. Whilst the exact choice of this equipment is a matter for the Customer, the generic configuration of them is mandated; details required for these configurations are provided in the following sections.

5 GCSx Connection Initiation (Setup and Configuration)

5.1 IP Addressing

C&W will, by default, allocate each Customer connection (and other connected organisations) a /28 IP Subnet from the GCSx address space (RIPE Registered). Within this IP Address block, fourteen addresses are useable. Of these fourteen addresses, three are reserved for the managed C&W router (which will allow for upgrades to resilient connectivity) and three are provided for the firewall or whatever device you use to provide Network Address Translation (NAT) at your boundary. C&W will only route to addresses in the range allocated and where Network Address Translation (NAT) is required to fit within this range it must be applied by the customer; C&W will not implement any NAT on the CE router.

You must use the standard schema below when allocating IP addresses. The IP Schema includes room for expansion and includes sufficient space for you to write in the actual IP addresses allocated to you.

Note: Please be aware that, once completed, these details will be sensitive information representing a potential vulnerability to the service. Accordingly, these details must be securely protected.

Subnet Allocation	Subnet Mask
	255.255.255.240 (/28)

IP Address	IP Address	Your Device/Hostname	GCSx Default for all Sites
Subnet +1			Firewall (real/VRRP)
Subnet +2			Firewall (real)
Subnet +3			Firewall (real)
Subnet +4			Mail Server NAT
Subnet +5			Proxy Server PAT
Subnet +6			DNS Server PAT
Subnet +7			Edge Server NAT
Subnet +8			Other
Subnet +9			Other
Subnet +10			Other
Subnet +11			Other
Subnet +12		Reserved for C&W	C&W Reserved
Subnet +13		Reserved for C&W	C&W Reserved
Subnet +14		Reserved for C&W	C&W Router (Next hop address for GCSx routes)

Note: GCSx IP Subnet allocation or larger subnets (/27 or greater) Subnet+1 through Subnet+7 should be used as shown above and the C&W Router IP addresses will be moved to the top of the allocation by C&W.

Note: For standard subnet allocations the customer should use Subnet+14 as the next hop address for all routes in to the GCSX network. HSRP (group 1) will be configured on the C&W CE router(s) using the Subnet+14 address, even in single router deployments. This will negate the need for next hop routing changes on the customer hand off equipment when migrating to a dual router/circuit scenario.

Note: The CE router HSRP address (Subnet +14) will respond to ICMP ping requests.

5.2 IP Routing

Prior to testing any of the applications associated with GCSx, you must configure suitable IP routing within your environment.

The new GCSx is summarised by the address block **[TBC]** (community) and **[TBC]** (hosting).

All GSi communities are summarised by the address blocks **[TBC]** and **[TBC]** and should route traffic destined for these address blocks via the C&W GCSx router (i.e. Subnet +14).

Note: [TBC] will be provided to you through secure means on a verified need-to-know basis.

5.3 DNS Resolution

The GCSx service uses DNS to enable easy access to resources around the community and to provide resilience and to enable routine maintenance. Within the DNS service the active hosted systems for all of the central systems are defined, as well as information supplied by you concerning the naming / addressing of your own servers and services.

For resilience to be provided, it is important that your environment is correctly configured. To achieve resilience, you should use either the GCSx DNS to connect to the C&W platforms or configure your environment to handle planned or un-planned outages of the IP addresses that provide the services. If you don't configure your environment correctly, maintenance or failure could result in a loss of service for the Users within your organisation.

The IP addresses of the GCSx DNS resolvers that you should configure on your DNS resolvers are **[TBC]** and **[TBC]**, both accessible using DNS on **UDP Port 53**. For optimal performance across the whole GCSx community, you should randomise the order in which you enter these IP addresses onto your systems.

The C&W GCSx DNS resolvers also provide recursive resolution to the Internet.

You should configure your environment to forward requests for DNS name resolution of GCSx-related systems names to the GCSx DNS resolvers (this is often referred to as 'conditional forwarding' or 'forward zones').

The following domain names are available for forwarding to the GCSx DNS resolver, these have been prioritised into groups as detailed below:

Generic GSi Domains (all LAs without conditions)

- *.gcsx.gov.uk
- *.gsi.gov.uk
- *.gsx.gov.uk
- *.gse.gov.uk
- *.gsisup.co.uk

Police Domains (all LAs – refer to CJSM Domain)

- *.pnn.gov.uk
- *.pnn.police.uk

Ministry of Justice Domains

- *.cjsm.net
- *.cjsm.gov.uk

If the Customer already has a CJSM MTA on site or already routes any of these domains to a CJSM DNS resolver, do NOT configure the above routes without seeking further advice from GC – please contact GCTechTeam@communities.gsi.gov.uk.

National Health Service Domains

- *.nhs.net
- *.nhs.uk

To maximise efficiency and performance within your estate, DNS should be directed to a local DNS server, and this server should be configured to forward onto GCSx.

In order to use the DNS service, you must provide the following information:

- GCSx domain name (assigned by GC).
- Mail server GCSx IP address(s) & MX records (using the standard addressing schema shown in section 5.1).

For information, the DNS Start of Authority information used on all DNS Zones is as follows:

10800	; refresh ² (3 hours)
3600	; retry ³ (1 hour)
604800	; expire ⁴ (1 week)
86400	; minimum ⁵ (1 day)

5.4 Web Proxies

The LA's Web Proxy Server must be configured to enable GCSx Users secure web access to GSi-hosted services. Generic routing through to *.**gsi.gov.uk** should be enabled as well as to specific domains as detailed to the LA within the RESTRICTED data sets (provided at time of connection). The specifics of which websites will be accessible to GCSx Users via the GSi

² Interval before the zone should be refreshed

³ Interval that should elapse before a failed refresh should be retried

⁴ Upper limit on the time interval that can elapse before the zone is no longer authoritative

⁵ Number of seconds that the records in the zone are valid for

will be updated as the use of GCSx matures; examples of these being the DWP’s Customer Information Services (CIS) and the Joint Asset Recovery Database (JARD).

It is important that the need for the reconfiguration of the Web Proxy Server based on the GCSx User Group be considered when planning how GCSx Users are to be identified within the LA (e.g. within Active Directory). LA Users who are not registered as GCSx Users must not be allowed to access GSi-hosted services.

5.5 E-mail Servers

GC recommends the use of a dedicated secure mailbox for GCSx Users (e.g. username@la.gcsx.gov.uk) in addition to their extant LA Mailbox. The primary reason for this is as risk mitigation to avoid sensitive e-mails inadvertently being transmitted to insecure networks (e.g. the internet). Accordingly, GC recommends that e-mails sent from a User’s GCSx Mailbox be sent ONLY to the secure e-mail domains listed below. E-mails sent to all other domains should be rejected to prevent inadvertent release to other networks. E-mails destined for insecure networks should be sent from the LA’s existing mailbox (e.g. username@la.gov.uk).

A few LAs may choose to ignore this recommendation as they have sufficient trust in their GCSx Users to operate securely with a single Mailbox for both secure and insecure e-mail. Please contact GC GCTechTeam@communities.gsi.gov.uk to discuss further if this is the case.

The following options illustrate how a new GCSx Mailbox could be configured on either a single server or on two separate servers.

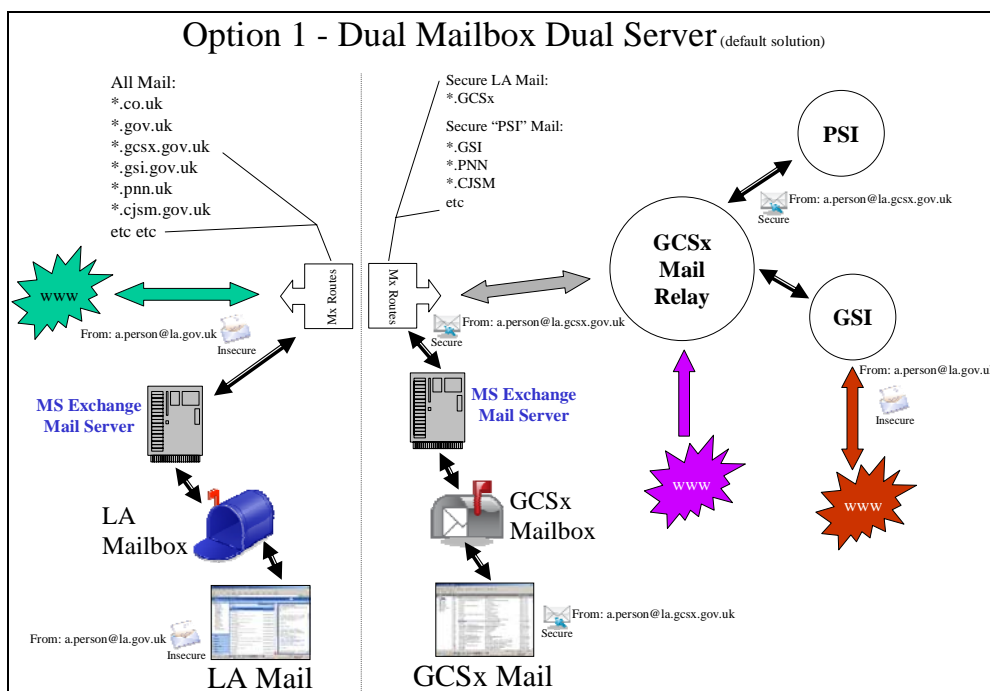


Figure 1 – GC Mail Configuration – Dual Server Option

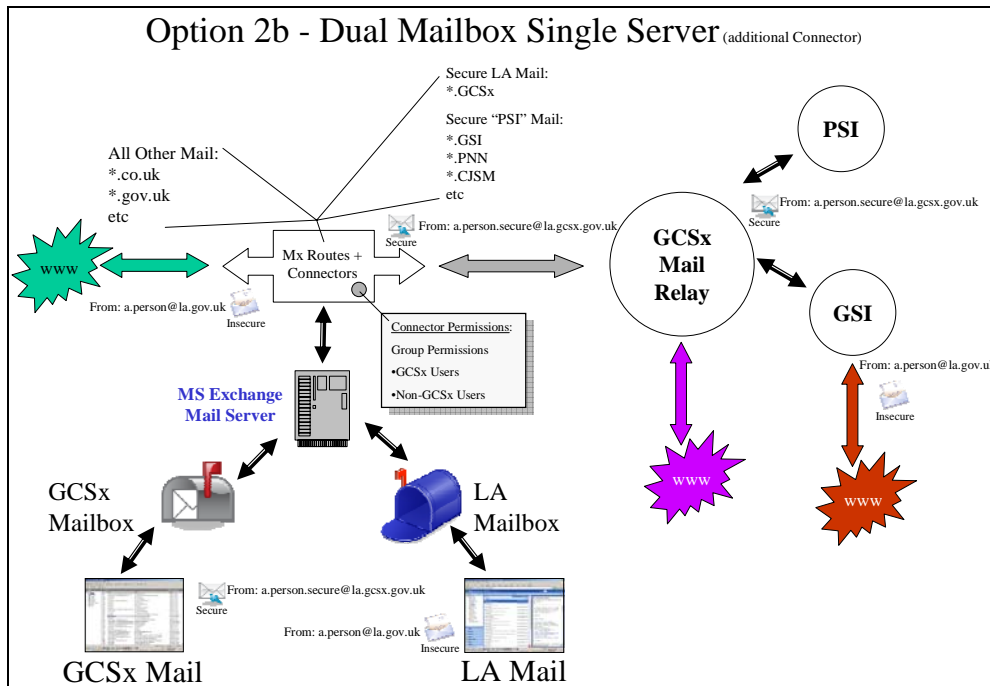


Figure 2 – GC Mail Configuration – Single Server Option

For the GCSx User Group all secure e-mail destined for the secure communities (e.g. GCSx, GSi) must be sent through the GCSx e-mail relay service. Secure e-mail destined for these communities must NOT be sent directly from Customer mail servers to any other mail servers.

The e-mail platform will need to interact with the GCSx internal DNS system to determine the destination for your mail, so it is critical that the DNS information you provide for the mail platform is correct and kept up-to-date.

The hostname for the GCSx mail system is **smtp.gcsx.gov.uk** and the service is available via **SMTP** on **TCP Port 25**.

The following domain names are available for forwarding secure e-mails via the GCSx e-mail relay, these have been prioritised into groups as detailed below:

Generic GSi Domains (all LAs without conditions)

- *.gcsx.gov.uk
- *.gsi.gov.uk
- *.gsx.gov.uk
- *.gse.gov.uk
- *.gsisup.co.uk

Police Domains (all LAs – refer to CJSJ Domain)

- *.pnn.gov.uk
- *.pnn.police.uk

Ministry of Justice Domains

- *.cjsm.net
- *.cjsm.gov.uk

If the Customer already has a CJSM MTA on site and already routes e-mails to these domains via this MTA, do NOT configure the above e-mail routes without seeking further advice from GC – please contact GCTechTeam@communities.gsi.gov.uk.

National Health Service Domains

- *.nhs.net
- *.nhs.uk

You will receive e-mail from the GCSx inbound mail servers. To receive mail you must accept inbound e-mail from [TBC] (GCSx Hosting). These servers will contact your e-mail servers using **SMTP** on **TCP Port 25**.

You must provide your e-mail server name and IP address, both for forward and reverse name resolution in the DNS section. It should be noted that some e-mail servers need to be able to verify their own name and IP address in DNS before the application can start handling mail, so correct DNS configuration is key to your e-mail server's availability and performance.

In the event of a receiving e-mail server being unavailable, the GCSx Mail Servers will attempt to deliver the e-mail for up to 72 hours. The service will attempt deliveries every 10 minutes for 1-hour, then every 30 minutes until 24-hours then every 1 hour until 72-hours. If a mail has not been delivered after 72 hours a failure notice will be sent to the sender.

Further information with respect to the administration of each Customer's GC Directory will be provided within specific GC Directory documents and the GCSx Operational Support Guide.

5.5.1 E-mail Anti-Virus (AV)

All e-mail passing through the GCSx e-mail relay will be scanned for viruses by the GC Mail service. Any mail believed to contain viruses will be deleted, and a message returned to the sender with an appropriate warning message.

5.5.2 E-mail Footers

Footers will be added to e-mail as it passes via the GCSx e-mail relay and AV.

5.6 Definition of Local Aliases

In order for the GCSx Service to function effectively, it will be necessary to define aliases so that key roles within organisations are addressable without specific reference to named individuals. Maintaining an up-to-date contact list can be difficult, due to moves and changes. To ensure accurate rapid communication, generic e-mail addresses are used across the whole GSi community in the format gsi@xyz.gsi.gov.uk, gsi@xyz.gsx.gov.uk & gsi@zyx.gcsx.gov.uk.

Within GCSx, you should create an e-mail address in the style of gsi@xyz.gcsx.gov.uk. This address should be monitored by your organisation (possibly by being forwarded to those responsible for running the GCSx for your organisation).

The generic mailboxes will be used by all of the GCSx management organisations (e.g. OGCbs, NISCC, C&W, GC) to communicate information such as notifications of changes and invitations to GC and GSi Customer Forums.

Additionally, the generic mailboxes also enable GCSx users to communicate with one another where the contact details are not already known (e.g. to request access to an application).

GSI administration requires the ad-hoc 'broadcasting' of information to local site administrators. Occasional, e-mails will be sent from OGCbs and C&W to all connected organisations informing all of GSI-related updates. The GCSx GC Mail Service also provides a 'list server' to facilitate the distribution of communications such as these. Your organisation is required to provide the following local alias:

Required Alias	Alias Resolved To
gsi@xyz.gcsx.gov.uk	a.person@xyz.gcsx.gov.uk ano.person@xyz.gcsx.gov.uk

Security administration will also require the ad-hoc 'broadcasting' of information to local site system security officers and Section 151 officers; for this purpose your organisation is required to provide the following alias:

Required Alias	Alias Resolved To
security_officer@xyz.gcsx.gov.uk	a.person@xyz.gcsx.gov.uk ano.person@xyz.gcsx.gov.uk
section_151_officer@xyz.gcsx.gov.uk	a.person@xyz.gcsx.gov.uk

System policy makers and directors will also require the ad-hoc 'broadcasting' of information to local CEOs; for this purpose your organisation is required to provide the following alias:

Required Alias	Alias Resolved To
CEO@xyz.gcsx.gov.uk	a.person@xyz.gcsx.gov.uk ano.person@xyz.gcsx.gov.uk

In the above, xyz will need to be replaced with your organisation's domain and the 'person names' will need to be defined properly and maintained should these people change roles.

5.7 User Details GC Directory

Each Customer should supply details of GCSx Users in accordance with the GC Directory User Template for initial population of the GC Directory. The template will be accompanied by appropriate guidance notes.

GC will provide an Administrator's Guide and User Guide for GC Directory.

GC anticipates that LAs may also wish to extract current User details from their existing Mail Servers (where appropriate).

5.8 Network Time Service

GCSx provides a Network Time Service, which is the same as that used by the GSI network. The central GSI time servers take the time signal from GPS. The GCSx time source is a Stratum-4 time service.

The use of the GCSx Network Time Service is recommended, but not mandated (please refer to the CoCo). In all cases, connecting systems are required to provide accurate system time to enable consistent, auditable timestamps.

The GCSx Time Service is available using SNTP V3 (RFC1769), SNTP V4 (RFC2030), NTP V3 (RFC1305) and NTP V4 (no RFC). Department NTP clients should request time on a unicast (point-to-point) basis.

You should configure your NTP clients to use the following server name for NTP updates: **ntp.gcsx.gov.uk**. The service is available using **NTP** on **UDP Port 123**.

The maximum recommended update frequency for departmental servers is hourly.

Note: You may wish to establish your own time service taking a Stratum-4 time signal from the central GCSx time service and providing a Stratum-4+1 time signal within your organisation.

5.9 Firewall

5.9.1 Summary Rulebase

The protocols detailed above can be summarised as follows for GCSx:

From	To	Protocol	Action	Comment
Your Proxy/NAT	[TBC]	HTTP (TCP/80) HTTP (TCP/8080) HTTPS (TCP/443)	Allow	Enable outbound access to applications in GCSx & GSi on HTTP & HTTPS (add other protocols as required)
[TBC]	<i>Your Applications/ Web Servers</i>	HTTP (TCP/80) HTTPS (TCP/443)	Allow	Enable inbound requests from GCSx to your web servers/applications (if applicable, add other protocols as required)
[TBC]	<i>Your Mail Server(s)</i>	SMTP (TCP/25)	Allow	Enable inbound e-mail from GCSx mail relays
<i>Your Mail Server(s)</i>	[TBC]	SMTP (TCP/25)	Allow	Enable outbound e-mail to the GCSx mail relays
<i>Your DNS Server(s)</i>	[TBC]	DNS (UDP/53) DNS (TCP/53)	Allow	Allow queries to GCSx DNS servers
<i>Your NTP Server(s)</i>	[TBC]	NTP (UDP/123)	Allow	Access to GCSx NTP Server
<i>Your Mail Client(s)</i>	[TBC]	LDAP	Allow	Access to GCSx LDAP (GC Directory)
Any	Any	ICMP	Allow	Temporarily Allow ICMP for connectivity testing
Any	Any	Any	Block	Clean-up Rule

Note: [TBC] will be provided to you through secure means on a verified need-to-know basis.

5.9.2 Summary Routing

Route	Entity	Suggested next hop
[TBC]	C&W GCSx & GSi Communities	C&W GCSx Router Port (Subnet + 14)

Note: [TBC] will be provided to you through secure means on a verified need-to-know basis.

5.10 Schematic Diagram

The diagram below shows the main protocols that pass between the customer estate and GCSx:

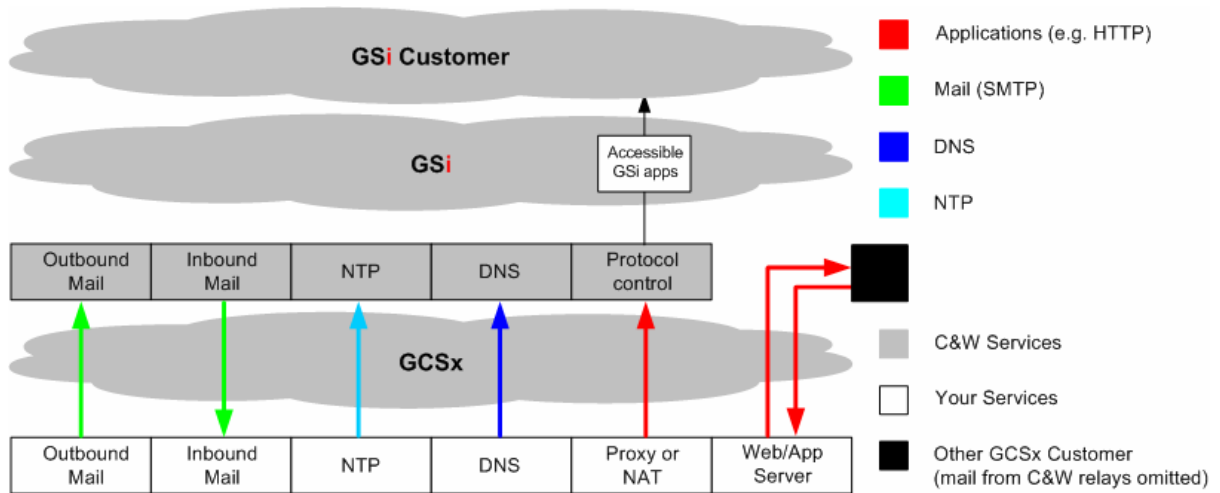


Figure 3: GCSx Network Schematic

6 GCSx Connection Validation (Multi-Layer Testing)

C&W will test the basic connectivity of a GCSx connection during the installation of the router and any other C&W managed equipment.

To validate the GCSx connection from a functional and security perspective a series of tests is recommended, evidence from some of which will be mandatory for subsequent Permission to Go Live.

Tests are layered to prove Server configuration validity and functionality before Client functionality. Testing is an essential element of GCSx Connection proving and you are encouraged to supplement/amend these to suit your specific installations and requirements.

7 GCSx Service Desk and Support

GC provides the first-line Helpdesk, which is in place to offer a Single-Point-of-Contact to all Customer Administrators. Initially, the GC Helpdesk will be provided by Tameside, who are assisting in capturing operational metrics for use in the longer-term procurement of a full Helpdesk. Contact details will be provided for the GC Helpdesk. Following installation of GCSx, any support issues should be raised through the GC Helpdesk.

Additional information with respect to the GCSx Service Desk and Support is contained in the GCSx Operational Support Guide.

C&W operate a dedicated GCSx Service Desk to provide a single point of contact for *all C&W managed Services on the GCSx*. The C&W Service Desk is available 24x7. No 'first contact' details will be provided for the C&W GCSx Service Desk; only the GC Helpdesk is authorised to receive incident reports.

8 Appendix A – Testing

8.1 Test Objectives and Strategy

Basic connectivity (e.g. IP) will be proven during the installation of the router (and any other C&W managed CPE) by the C&W representative. The purpose of the tests listed below is to verify you can connect to the services located at the C&W Data Centres. The tests cover the basic functionality of the core application components (e.g. DNS, NTP). You are encouraged to supplement/amend these tests to suit their specific installations and requirements.

8.2 Limits of Testing Scope

The following are out of scope of testing:

- Volume / load testing.
- Penetration testing.
- Resolution of any internal ICT issues you may encounter during these tests (however Consultancy can be purchased if required).

8.3 Useful Test Resources

In addition to the specific tests detailed below there are a number of GCSx resources that can be used as part of installation testing and for ongoing functional testing.

The GCSx community contains a number of e-mail auto responders that can be used to test e-mail connectivity. You can use these by sending an e-mail to the e-mail address listed below whereupon the echo responder will automatically reply to the senders mail address.

Resource	Address
GSI E-mail Echo Responder 1	responder@hosting-w.gsi.gov.uk
GSI E-mail Echo Responder 2	responder@hosting-e.gsi.gov.uk
GSX E-mail Echo Responder 1	echo@hosting-e.gsx.gov.uk
GSX E-mail Echo Responder 2	echo@hosting-w.gsx.gov.uk
GCSx E-mail Echo Responder 1	responder@hosting-w.gcsx.gov.uk
GCSx E-mail Echo Responder 2	responder@hosting-s.gcsx.gov.uk
Addresses in East & West data centres that can be pinged from GCSx	Watford - [TBC] Swindon – [TBC]

8.4 Test Prerequisites

The table below lists the items (plus responsibility) that are required to be in place before commencing the tests.

Item	Owner
1	Customer
2	C&W
3	GC
4	Customer
5	Customer
6	Customer
7	Customer

8.5 Connectivity Testing

The following tests can be used to assist in proving that connectivity from a Customer site has been established with the core GCSx network. The word “server” refers to the appliance which will be used by the Customer during the testing process.

	Objective	Approach	Expected Results
1	PING your gateway from the Test PC connected to your internal LAN.	PING <C&W Router LAN IP Address> - [TBC]	Ping reply
2	PING a test address at the 1 st C&W Data Centre	PING Watford - [TBC]	Ping reply
3	PING a test address at the 2 nd C&W Data Centre	PING Swindon - [TBC]	Ping reply
4	Resolve GCSx DNS name space at C&W Data Centre	nslookup smtp.gcsx.gov.uk	Resolves to IP address

	Objective	Approach	Expected Results
5	Resolve GSI DNS name space	nslookup www.gsi.gov.uk	Resolves to IP address
6	Resolve PSI DNS name space	nslookup http://esef.cis.dwp.gsi.gov.uk	Resolves to IP address
7	Synchronise with the GCSx time source	Run NTP client on a server and synchronise with GCSx time source	Time value returned

8.6 Mail Exchange Testing

The following tests can be used to assist in proving that e-mail server functionality has been established using the GCSx network.

	Objective	Approach	Expected Results
8	Exchange e-mail with GCSx	Open server mail application and exchange e-mail from test mailbox with the GCSx echo responders (responder@hosting-w.gcsx.gov.uk , responder@hosting-s.gcsx.gov.uk)	E-mail received from the echo responder
9	Exchange e-mail with GSI	Open server mail application and exchange e-mail from test mailbox with the GSI echo responders (responder@hosting-e.gsi.gov.uk , responder@hosting-w.gsi.gov.uk)	E-mail received from the echo responder
10	Exchange e-mail with GSX	Open server mail application and exchange e-mail from test mailbox with the GSX echo responders (echo@hosting-e.gsx.gov.uk , echo@hosting-w.gsx.gov.uk)	E-mail received from the echo responder

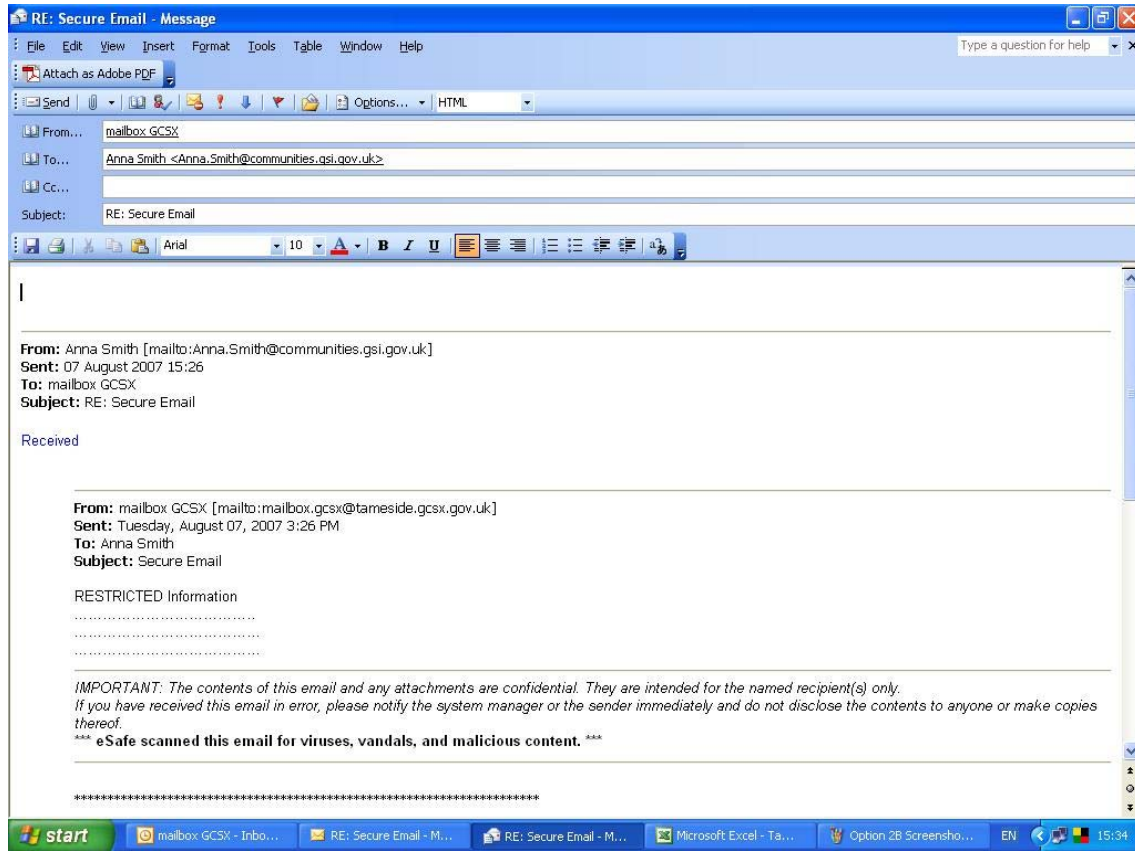


Figure 4 – Example E-mail within GCSx Mailbox

9 Appendix B – Environmental Information

9.1 Introduction

This Appendix provides information on the main types of Network Terminating Equipment (NTE) and routers used in the C&W network. This information can be used to understand the specific details of the equipment to be installed with respect to the installation environment (e.g. power required, physical size required).

Note that this information is provided for guidance only as C&W may, from time-to-time, provide alternative equipment. Generally, the provision of alternative equipment may be necessary to overcome obsolescence issues and will, as far as practicable, be replacements in form, fit and function.

The NTE equipment must be located within 3m (cable length) from the GCSx CE router so that C&W SLAs can be assured. The NTE equipment may be wall mounted or rack mounted; dependent on the tail circuit delivery and is not an orderable part of the circuit installation.

The diagrams below show the two methods of service installation (for a typical customer installation).

9.2 Wall-mounted NTTP

The following should be in place at the installation location:

- The NTTP termination equipment will be installed by BT or C&W (subject to survey).
- Total cable distance between the NTTP and the GCSx CE router should be less than 3 metres.
- A dual 13Amp un-switched power supply for each NTTP must be in place prior to circuit delivery.
- Any UPS or power backup is the responsibility of the customer.
- C&W will supply and maintain the GCSx CE router, the cable connecting the router to the NTTP, and the NTTP equipment.

9.3 Rack-mounted NTTP

As per the Wall-mounted NTTP with the additional condition:

- To enable this type of configuration, the full details of the cabinet location, reference and reserved shelf space is required at the point of ordering the GC service.

9.4 NTE Specifications

The table below summarises the NTE which will be installed by BT, given a circuit size.

NTE Options	Power Supply / Consumption	Dimensions	Weight
1 x 2 Mbps NTE 52/53	240v AC or -48v DC, 22.5W ETS 300019-1-3, class 3.2	H 50mm W 260mm D 270mm	1.8 Kg
4 X 2Mbps NTE 4U/7A OR EU FUJITSU ASDH	240v AC or -48v DC, 22.5W ETS 300019-1-3, class 3.2	H 44mm W 440mm D 220mm	<3kg
16 X 2Mbps NTE 4U NTE EU NTE 16U/7A OR 16P/7A FUJITSU ASDH	240v AC or -48v DC, 44W ETS 300 019-1-3, class 3.2	H 114mm W 440mm D 220mm	<16kg
63 X 2Mbps SMA1 SDH	240v AC or -48v DC	H 500mm W 450mm D 280mm	16Kg
1 X 34Mbps or 1 X 45Mbps NTE 16U NTE 34U/7A OR 34P/7A FUJITSU ASDH	240v AC 30W ETS 300 019-1-3, class 3.2	H 44mm W 440mm D 220mm	<3kg
1 x 155Mbps (STM-1)	tbc	Tbc	tbc

Table 1: NTTP detailed information

BT will select the type of NTE equipment based on the access speed procured by the Customer.

9.5 Customer Edge Router Specifications

9.5.1 Introduction

C&W will select the type of Customer Edge (CE) router which will be installed by C&W at the Customer site based on the access speed procured by the Customer, the current equipment options are:

Line Speed	CE router deployed on customer site
2Mbps	Cisco 2801
10Mbps	Cisco 2811
100Mbps	Cisco 3825
155Mbps	Cisco 7304

Table 2: CE Router Types

The environmental information of the routers shown is summarised in the tables below.

9.5.2 2800 Series Technical Specifications

	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Rack Mounting	Yes, 19-inch	Yes, 19- and 23-in. options		
Wall Mounting	No	Yes	No	No
Power Requirements				
AC Input Voltage	100 to 240 VAC, autoranging			
AC Input Frequency	47-63 Hz			
AC Input Current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	
AC Input Surge Current	50A maximum, one cycle (-48V power included)			
AC-IP Maximum In-Line Power Distribution	120W	160W	240W	360W
AC-IP Input Current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
AC-IP Input Surge Current	50A maximum, one cycle (-48V power included)			
DC Input Voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
DC Input Current	No DC Power Option available	<ul style="list-style-type: none"> · 8A (24V) · 3A (60V) · Startup current 50A<10 ms 	<ul style="list-style-type: none"> · 12A (24V) · 5A (60V) · Startup current 50A<10 ms 	
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	280W (955 BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)

	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Power Dissipation-AC with IP Phone Support-IP Phones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
Power Dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
RPS	No	External only, connector for RPS provided by default		
Recommended RPS Unit	No RPS option	Cisco RPS-675 Redundant Power System		
Environmental Specifications				
Operating Temperature	32 to 104°F (0 to 40°C)			
Operating Humidity	10 to 85% non-condensing	5 to 95%, non-condensing		
Non-Operating Temperature	-	4° to 149°F (-20° to 65°C)		
Operation Altitude	<ul style="list-style-type: none"> · 25°C @ 3 km/10 kft · 40°C @ sea level 	<ul style="list-style-type: none"> · 27.5°C @ 15 kft · 35°C @ 3km/10 kft · 40°C @ sea level 		
Dimensions (H x W x D)	<ul style="list-style-type: none"> · 1.72 x 17.5 x 16.5 in. · (43.7 x 445 x 419 mm) 	<ul style="list-style-type: none"> · 1.75 x 17.25 x 16.4 in. · (44.5 x 438.2 x 416.6 mm) 	<ul style="list-style-type: none"> · 3.5 x 17.25 x 16.4 in. · (88.9 x 438.2 x 416.6 mm) 	
Rack Height	1 rack unit (1RU)		2RU	
Weight (Fully Configured)	13.7 lb (6.2 kg)	14 lb (6.4 kg)	25 lb (11.4 kg)	
Noise Level (Min/Max)	<ul style="list-style-type: none"> · 39 dBA for normal operating temperature (<90°F/32.2°C) · 53.5 dBA (@ maximum fan speed) 	<ul style="list-style-type: none"> · 47 dBA for normal operating temperature (<90°F/32.2°C) · 57 dBA (@ maximum fan speed) 	<ul style="list-style-type: none"> · 44 dBA for normal operating temperature (<90°F/32.2°C) · 53 dBA (@ maximum fan speed) 	
Regulatory Compliance				
NEBS	Yes	Yes	Yes	
Safety	<ul style="list-style-type: none"> · UL 60950 · CAN/CSA C22.2 No. 60950 · IEC 60950 · EN 60950-1 · AS/NZS 60950 			
Immunity	<ul style="list-style-type: none"> · EN300386 · EN55024/CISPR24 · EN50082-1 · EN61000-6-2 			
EMC	<ul style="list-style-type: none"> · FCC Part 15 · ICES-003 Class A · EN55022 Class A · CISPR22 Class A · AS/NZS 3548 Class A · VCCI Class A · EN 300386 · EN61000-3-3 · EN61000-3-2 			
FIPS-2	FIPS 140-2 Certification for 2801, 2811, 2821, 2851			

	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
TELCOM**	<p>For all four platforms, Telecom compliance standards depend upon country and interface type. Interfaces comply with FCC Part 68, CS-03, JATE Technical Conditions, European Directive 99/5/EC and relevant TBR's. For specific information see the datasheet for the specific interface card.</p> <p>Homologation requirements vary by country and interface type. For specific country information, see the on-line approvals data base: http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH&module=EXTERNAL_SEARCH</p>			

Table 3: 2800 series router technical specifications

9.5.3 3800 Technical Specifications

	Cisco 3825	Cisco 3845
Physical Specifications		
Dimensions (H x W x D)	· 3.5 x 17.1 x 14.7 in. · 2 Rack Unit (RU)	· 5.25 x 17.25 x 16 in. · 3 Rack Unit (RU)
Weight (minimum)	23 lb	45 lb
Rack-Mounting	Yes, 19-" and 23" options	Yes, 19-" and 23" options
Wall-Mounting	No	No
Power Specifications		
AC-Input Voltage	100-240 VAC, auto-ranging	100-240 VAC, auto-ranging
AC-Input Frequency	47-63 Hz	47-63 Hz
AC-Input Current	· 3A (110V) · 2A (230V) · Startup current 50A maximum (one cycle)	· 4A (110V) · 2A (230V) · Startup current 50A maximum (one cycle)
AC-IP-Input current	· 8A (110V) · 4A (230V) · Startup current 50A maximum (one cycle)	· 8A (110V) · 4A (230V) · Startup current 50A maximum (one cycle)
DC-Input Voltage	24-60 VDC, auto-ranging positive or negative	24-60 VDC, auto-ranging positive or negative
DC-Input Current	· 12A (24V) · 5A (60V) · Startup current 50A<10 ms	· 18A (24V) · 7A (60V) · Startup current 50A<10 ms
Output	· AC or DC power supply: · 210W for system · AC-IP power supply: · 210W for system · 360W for IP phones (-48V)	· AC or DC power supply: · 300W for system · AC-IP power supply: · 300W for system · 360W for IP Phones (-48V)
Redundant Power Supply (RPS)	External only (Cisco RPS 675)	Internal AC, AC-IP, or DC RPS
Recommended RPS Unit	Cisco RPS 675	-
Power Dissipations		
AC Without IP Phone Support	300W (1025 BTU/hr)	435W (1485 BTU/hr)
AC With IP Phone Support-System Only	370W (1262 BTU/hr)	555W (1890 BTU/hr)
AC With IP Phone Support-IP Phones	360W (1128 BTU/hr)	360W (1128 BTU/hr)
DC	325W (1100 BTU/hr)	460W (1570 BTU/hr)
Environmental Specifications		

	Cisco 3825	Cisco 3845
Operating Temperature and Altitude	32° to 104°F (0° to 40°C) up to 6000 feet (1800 m) At 15000 ft (4500 m), max operating temperature is 27.2C. At 13000 ft (4000 m), max operating temperature is 30C. Note: For all other altitudes scale operating temperature by a factor of 1.4C per 1000 ft (300 m) of altitude change.	32° to 104°F (0 to 40°C) up to 6000 feet (1800 m) At 15000 ft (4500 m), max operating temperature is 27.2C. At 13000 ft (4000 m), max operating temperature is 30C. Note: For all other altitudes scale operating temperature by a factor of 1.4C per 1000 ft (300 m) of altitude change.
Non-Operating Temperature	-40° to 185°F (-40° to 85°C)	-40° to 185°F (-40° to 85°C)
Relative Humidity Non-Condensing	5-95% non-condensing	5-95% non-condensing
Noise Level (minimum)	50 dBa typical, 53 dBa maximum	56 dBa typical, 58 dBa maximum
Regulatory Compliance		
Safety	<ul style="list-style-type: none"> · UL 60950 · CAN/CSA C22.2 No. 60950 · EN 60950 · AS/NZS 60950 	<ul style="list-style-type: none"> · UL 60950 · CAN/CSA C22.2 No. 60950 · EN 60950 · AS/NZS 60950
EMC	<ul style="list-style-type: none"> · 47 CFR, Part 15 · ICES-003 Class A · EN55022 Class A · CISPR22 Class A · AS/NZS 3548 Class A · VCCI V-3 · EN 300386 · EN 61000 	<ul style="list-style-type: none"> · 47 CFR, Part 15 · ICES-003 Class A · EN55022 Class A · CISPR22 Class A · AS/NZS 3548 Class A · VCCI V-3 · EN 300386 · EN 61000
TELCOM	<ul style="list-style-type: none"> · 47 CFR, Part 68 · TIA/EIA/IS-968 · CS-03 · RTTE Directive 	<ul style="list-style-type: none"> · 47 CFR, Part 68 · TIA/EIA/IS-968 · CS-03 · RTTE Directive

Table 4: 3800 series router technical specifications

9.5.4 7304 Technical Specifications

	Cisco 7304
Physical Specifications	<ul style="list-style-type: none"> • 4-RU (7-in.) chassis 4 line-card slots per chassis • Dimensions (H x W x D): 7 x 17.2 x 20.5 in. • Weight: 28 lb (without power supply; power supplies 8 lb each)
Power Requirements	AC Input Power Supply/Chassis AC input voltage: 100 to 240 VAC AC Input Current 8A at Vin = 100 VAC and maximum load (540W) 4A at Vin = 200 VAC and maximum load (540W) Mean time between failure (MTBF): 5.5 years for system configuration
Environmental Conditions	Operating Condition Temperature: 32 to 104°F (0 to 40°C) Altitude: 6500ft (2000 m) Humidity: 10 to 85 percent noncondensing Storage Condition Temperature: -4 to 149°F (-20 to 65°C) Humidity: 5 to 95 percent noncondensing

Cisco 7304	
Regulatory Compliance	CE Marking
Safety	UL 60950 CAN/CSA C22.2 No. 950-00 EN 60825-1 Laser Safety (Class 1) 21CFR 1040 Laser Safety EN60950 IEC 60950 TS 001 AS/NZS 60950
EMC	FCC Part 15 (CFR 47) Class A VCCI Class A EN55022 Class A CISPR 22 Class A AS/NZS 3548 Class A EN61000-3-2 EN61000-3-3 EN55024 EN50082-1 ETS300386
NEBS Level 3 Compliance per Telecordia SR-3580	GR-1089-Core-Electromagnetic Compatibility and Electrical Safety, GR-63-CORE-NEBS: Physical Protection ETSI Compliance ETS-300386-2 Switching Equipment ETSI Environmental ETS 300 019 Part 1-1 Class 1.1 ETS 300 019 Part 1-2 Class 2-3 ETS 300 019 Part 1-3 Class 3.1

Table 5: 7304 series router technical specifications

10 Appendix C – Example Communication to Customer from C&W

This shows the type of e-mail communication an Customer can expect to receive from C&W on acceptance of an order for the GCSx service.

C&W UK Order Acceptance and Delivery Information

C&W UK Order Number:

C&W UK Circuit Reference:

BT Circuit Reference:

**Requested Service or SCR
Option:**

Site Location:

Circuit Speed:

Account Manager:

Requested Termination Point:

Agreed Ready for Service Date:

Dear xxxx

Thank you for your recent order for C&W UK services at the above location. I confirm that C&W UK accepts this order in accordance with the contract between us.

The 'Agreed Ready For Service Date' is the date by which we plan to deliver your order. To ensure that the delivery is successful it is very important that the nominated site contacts are fully briefed with the detail below.

What to expect ?

The site where the service is to be delivered will normally have 2 engineer site visits. The first will be a BT engineer and shortly after (usually the ARFS date) will be the C&W UK engineer who brings the circuit into service

If there is equipment that is required for the installation this will arrive by TNT and should be stored close to where the installation is to occur

What you or your nominated site contact need to do ?

The nominated site contact (and secondary contact) need to be fully briefed about the planned installation to avoid engineers being refused access to sites (please advise us if there are additional access restrictions we may need to plan for)

C&W UK will normally require two free 13A sockets immediately adjacent to where C&W UK equipment is to be installed. Please can you arrange for these to be available for your install date

The nominated site contacts need to be aware of the exact location that the circuit should be installed to by the BT engineer.

To eliminate any errors in where the BT engineer terminates the circuit, we have provided a 'Termination Point' Demarcation (see attached). The site contact can print the attachment and stick it on the wall in the precise location (specified by yourself for the order form). The BT engineer will have the same instruction from C&W UK.

Without the above, there is a possibility the job will be aborted, the delivery date will be postponed and/or additional charges incurred.

If you wish to discuss any aspect of this letter, please telephone the COM Centre on 0118 919 3020 quoting your Order No.

11 Appendix D - C&W Government Connect Circuit Delivery

The diagram below shows a summary of the C&W GC Circuit delivery process.

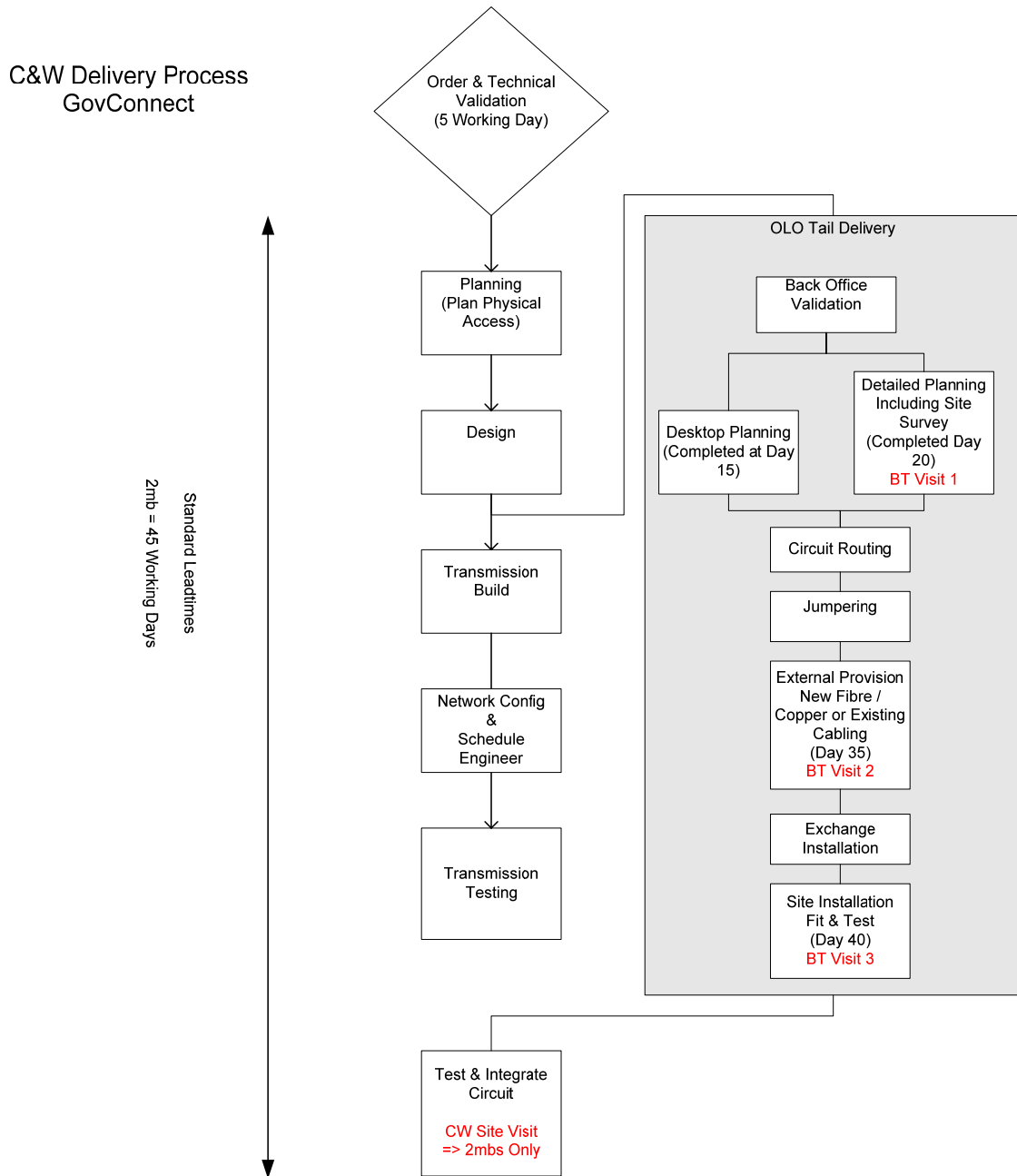



Figure 5: C&W Government Connect Circuit Delivery Process

12 Appendix E – Connection Checklist

The checklist below provides a summary of the major tasks / actions, which must be undertaken to complete the GCSx connection process.

	Task / Action	Description	Complete?
1.	Circuit Installed	BT and/or C&W has installed and tested the CE Router	Yes/No
2.	Firewall Installed and Configured	Customer Firewall and Network equipment installed and configured	Yes/No
3.	Mail Server Configured	Customer Mail Server configured	Yes/No
4.	Web Proxy Server Configured	Customer Web Proxy Server configured	Yes/No
5.	CoCo Compliance Received	CoCo compliance received and GCSx Circuit enabled	Yes/No
6.	GCSx Testing Complete	Network connectivity proven – ping / DNS. GSI Browsing proven – GSI homepage accessed GC Mail proven – Responder echos received GC Directory – homepage accessed	Yes/No Yes/No Yes/No Yes/No
7.	Administration Accounts Complete	Generic GC Mail Accounts created GC Mail aliases created GC Directory Administration Accounts created GC Directory populated (initial entries)	Yes/No Yes/No Yes/No Yes/No
8.	Security-related Procedures / Policies in place and Ready to Use	User Training available User Personal Statements in place Security Reporting mechanisms in place BS Users identified Internal Approval to enable BS Users on GCSx	Yes/No Yes/No Yes/No Yes/No Yes/No
9.	GC Informed 	Confirmation e-mail to be sent to the GC DESK and Gov Connect Team, confirming that the above checks have been completed and the LA is now using GCSx. it-services@tameside.gov.uk GCTechTeam@communities.gsi.gov.uk <i>Note: GC will conduct confirmation checks to verify the key aliases have been configured, so please expect incoming e-mail to these accounts.</i>	

13 Appendix F – Aggregate Gateway Connections

13.1 Overview

In some cases Customers are connecting via an existing Wide Area Network (WAN) with one Customer taking responsibility for the physical connectivity with the C&W GCSx network; such 'shared' connections are referred to as Aggregate Connections.

Note: The term "Partnership" may also in some instances be used by Customers as a Customer membership group may also correspond to a political or contractual partnership. To avoid confusion with political or contractual partnerships, the terms used herein will use the term aggregate instead.

Aggregator – one Customer will act as the Primary Customer and will take control and responsibility for access to the shared services offered through the aggregated connection. The Aggregator may host the physical connection(s), but connection(s) may also be physically located in other locations (e.g. Aggregate Member Customer sites).

Aggregate Member – a Customer who accesses GCSx via the network services provided by the Aggregator with whom there is a formal, if not necessarily contractual, relationship.

13.2 Relationships

The relationship between Aggregator and Aggregate Member should be formalised. Where the Aggregator is a commercial organisation, the relationship should be formalised within a contract agreement. Where the Aggregator is a non-commercial organisation (e.g. a Local Authority) a formal contract may not be appropriate. In such cases, other means (e.g. a Memorandum of Understanding) may be more appropriate.

It is important that Aggregator and Aggregate Member(s) have an agreed, documented definition of the services being provided / consumed. In particular, it is critical that all parties understand who has responsibility for GCSx connectivity and who has to take action if an incident occurs. To illustrate this further, if an Aggregate Member's GCSx connection stops 'working', the first point of support for help and assistance should be the Aggregator (not the GC Helpdesk). Further issues that may require clarification would be the Aggregator's 'time-to-fix' should a fault develop in its infrastructure that affects onward service delivery to Aggregate Members.

The recommendation from GC is that Aggregator and Aggregate Members have an agreed Service Level Agreement (SLA). *An SLA is a formally negotiated agreement between two parties. It is a contract that exists between customers and their service provider, client or between service providers. It records the common understanding about services, priorities, responsibilities, guarantee, and such - collectively, the level of service. For example, it may specify the levels of availability, serviceability, performance, operation, or other attributes of the service like billing and even penalties in the case of violation of the SLA.*

13.3 Network Access Control

Network Access is subject to Code of Connection (CoCo) Approval by OGCbs. In the case of an Aggregate, this applies to all Aggregate Members as well as the Aggregator. Where the Aggregator is a Local Authority, that Local Authority will be subject to CoCo Approval both as an Aggregate Member and, additionally, as an Aggregator. As an Aggregator, the CoCo Submission and Approval will take account of the security measures in place to provide assurance of secure network management and onward network connectivity to each Aggregate Member.

The C&W Aggregator router(s) will be configured with an Aggregate Member Access Control List (ACL) on the CE interface for inbound traffic restrictions. This ACL controls IP traffic routing through the Aggregator on a per-Aggregate Member subnet basis. The GC Aggregator Order Proforma defines the Aggregate Members for this purpose. The ACL will be updated with the relevant IP networks for each Aggregate Member. 'Permit' or 'Deny' statements will be added at the time the Aggregator goes 'live' to reflect those Aggregate Members who have successfully completed the CoCo process (i.e. OGCbs have approved 'Go Live'), and those who have not. Those Aggregate Members who have not successfully completed the CoCo process will not be able to route any traffic via the Aggregator's connection. 'Permit' entries for these Aggregate Members will be added later in response to each gaining CoCo approval via the process agreed with OGCbs.

13.4 Architecture

An Aggregator C&W CE router(s) will route an IP subnet per indirectly connected Aggregate Member via the Aggregate Member's Firewall and/or router. Both Aggregator and Aggregate Member will be assigned a /28 subnet from the GC LAN range for hand off LAN addressing (regardless of whether the Aggregator has local E-mail, HTTP Proxy, Edge Server and DNS resource definitions or not).

Once connected to the GCSx VPN each Aggregator will benefit from the inherent any-to-any connectivity the IP Connect service provides. Aggregate Members routing via the Aggregator will be able to connect to the C&W hosted GCSx services and also allow other Aggregate Members to connect to its own services (e.g. Web servers).

A high-level representation of a typical Aggregate architecture is:

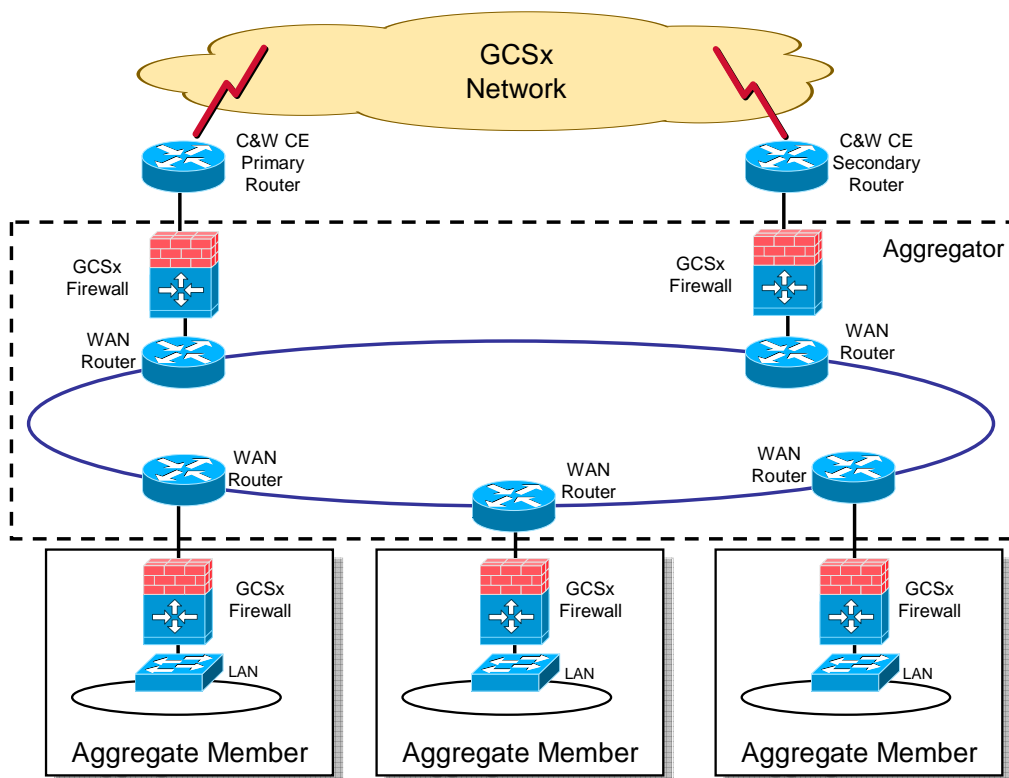


Figure 6 – Typical Aggregate Network

13.5 Detailed Technical Options

There are a number of architectural options available for Aggregate Networks. The number and scale of the communities served by an Aggregator will influence the bandwidth and configuration options. In particular, the options for geographic resilience need further explanation at a level above the information appropriate to this document.

Those requiring further technical information should apply to GC via GCTechTeam@communities.gsi.gov.uk to be provided with the C&W Aggregated Gateway GCSx Connectivity Detailed Design Document.

14 Appendix G – Glossary of Terms

Term	Description
BS	Baseline Standard (aka BPSS – Baseline Personnel Security Standard)
BT	British Telecom plc
C&W	Cable & Wireless plc
CE, PE, P	C&W managed MPLS routers: Customer Edge, Provider Edge, Provider
CJX	Criminal Justice eXtranet
CoCo	Code of Connection - The document describing the security requirements for connection to the GCSx.
CPE	Customer Premises Equipment
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GC	Government Connect
GCSx	Government Connect Secure eXtranet
GPS	Global Positioning System satellite-based navigation system
GSE	Government Supplier Extranet
GSI	Government Secure Intranet framework – includes communities GSI, xGSI, GSX, GSE and GCSx.
GSI	Restricted-High Community
GSU	Secure community for Unrestricted / Not Protectively Marked traffic.
GSX	Restricted Community
IP	Internet Protocol
LES	BT Lan Extension Service
LGOL Net	Local Government OnLine Network
MPLS	Multi Protocol Label Switching
MX	Mail Exchanger DNS Record
NAT	Network Address Translation
NISCC	The National Infrastructure Security Co-ordination Centre. The body responsible for authorizing GSI applications, as well as more generally responsible for ensuring that the critical national infrastructure is protected against electronic attack. (http://www.niscc.gov.uk)
NTE	Network Termination Equipment
NTP	Network Time Protocol
NTTP	Network Test and Termination Point
OGCb.s	Office of Government Commerce buying solutions
PAT	Port Address Translation
PING	Ping is a basic command that lets you verify that a particular IP address exists and can accept requests. The verb ping means the act of using the ping utility or command.
SC	Security Check
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
STP	Service Termination Point
Stratum 1	A time server with a reference clock attached to it
Stratum 2	A time server 1 server away from a Stratum 1 time server
Stratum N	A time server N-1 servers away from a Stratum 1 time server
URL	Uniform Resource Locator. The address of a web page on the world wide web
VPN	Virtual Private Network

Term	Description
xGSI	Confidential-High Community