Disaster Recovery essensys Connect

Overview

This paper describes how essensys Connect services continue to be delivered in the event of a disaster. The paper covers platform resiliency and business continuity.

Platform Redundancy and Resiliency

This best way to handle a disaster is to avoid it in the first place. That's why the Connect product is built on a fully resilient architecture to ensure that if the worst happens, services continue.

essensys' underlying platform strategy is to provide multiple layers of both redundancy and resiliency.

Redundancy is built into each platform element – this includes physical redundancy on the platform element itself, including dual processor and interface cards, dual and redundant power hardware, and redundant network connectivity interfaces. This ensures localised issues on an individual platform element will result in full service continuity. In the event of any localised equipment failure, redundant capabilities ensure service continuity, and essensys operations will automatically be alerted of hardware failures to ensure rapid full element repair, and a return to full redundancy.

In addition to individual platform element redundancy, essensys have implemented a multi-site resiliency architecture, which allows for full service continuity in the event of any catastrophic single-site failures. This is achieved through utilisation of full replication of all systems in two world-class data centres, using both load balancing and active/standby resiliency strategies.

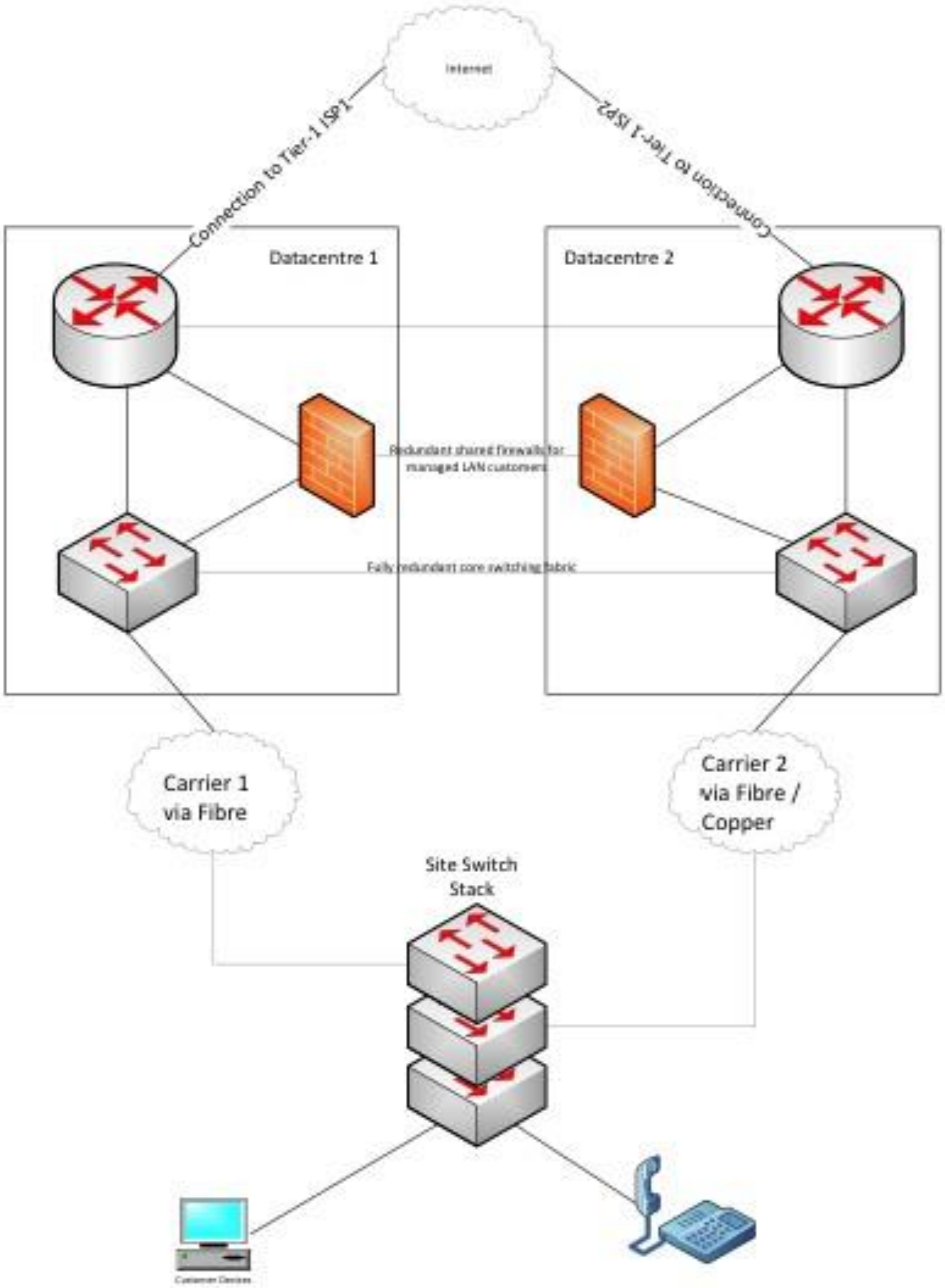
To ensure continuity of service, essensys conducts full resiliency solution verification at least four times per year during pre-arranged maintenance windows.

Operator Site Network Connectivity Resiliency

It is standard essensys practice to deliver resilient connectivity to each end customer site, through both primary and secondary data circuits, which are used for both network and voice traffic. Both primary and secondary circuits are delivered via two different tier-1 providers. essensys works with our carrier partners to maximise full path diversity for primary and secondary connections.

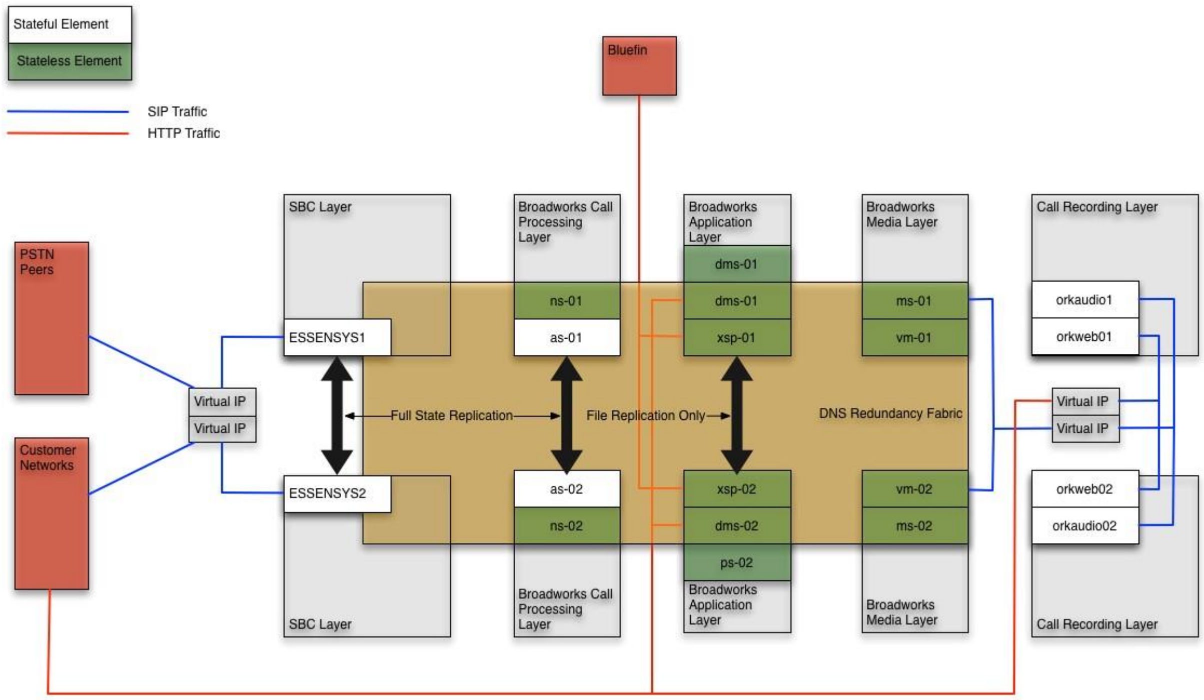
Network Resiliency

These primary and secondary circuits terminate in geographically redundant data centres. All platforms have resilient mirror copies in each of these two data centres. In the very unlikely event of a full failure of one data centre, services automatically survive due to resilient network design. The diagram below shows how essensys implements network connectivity from an individual customer site via primary and secondary network circuits, into a diverse and resilient dual data centre solution.


Internet
Connection to Tier-1 ISP1
Connection to Tier-1 ISP2
Datacentre 1
Datacentre 2
Redundant shared firewalls for managed LAN customers
Fully redundant core switching fabric
Carrier 1 via Fibre
Carrier 2 via Fibre / Copper
Site Switch Stack
Customer Devices

essensys Voice Application Resiliency

essensys operate several applications in its data centres, with voice being a mission critical service for our customers, and theirs. All individual voice platform elements follow the standard essensys model of having full localised redundancy. In addition, the voice platforms are resiliently mirrored across both essensys data centres to ensure full service continuity in event of catastrophic data centre failure. This mirroring across data centres is shown in the diagram below.



essensys Connect Application

The essensys Connect SaaS application is another mission critical application for both operators and their tenants. The application platform, including Software and Hardware elements, has been designed from the ground-up to ensure both localised redundancy for individual components in a single data centre, as well as resilient mirroring across both essensys data centres to ensure full service continuity in event of catastrophic data centre failure.

essensys Business Continuity

In addition to maintaining technology and platform operating capability when faults or disasters hit, our business needs to continue to function to ensure our customers' businesses continue to run.

essensys has separated its delivery and support operating capability (including our Network Operations Centres (NOC)) from our underlying technology stack. To enable global business continuity, essensys NOCs are based in two separate locations (in London and New York City), operating in a 1+1 configuration, while our technology platforms are distributed across for separate data centres globally (East London, West London, Manhattan, and New Jersey).

Our NOC sites are provisioned with redundant power, power backup solutions, and redundant network connections. In the event of an issue (power, site closure, etc) that removes one NOC from service, essensys can provide global service from our other NOC. essensys has automated our incoming communications to immediately transfer activity to the other NOC. In addition, essensys utilise contingency plans for operations staff to have secondary work locations throughout the UK and metropolitan New York areas should a NOC not be in-service or accessible. Essensys test these business continuity procedures quarterly.