Annex 4

Service Schedule

IPVPN at Airports

1 Service overview

1.1 General Service definition

SITA's IPVPN Network Services is a managed IP network service that provides IP VPN connectivity between customer premises. For airport-based IPVPN customers, SITA is offering IP VPN at Airports, an IP-based access method to IP VPN, providing flexibility and cost savings compared with the traditional circuit-based access.

SITA's IPVPN at Airports access is delivered by SITA in airports equipped with SITA Airport Hubs infrastructure, in the context of the SITA Airport Hubs programme. This provides customers with a flexible IP platform for new services and applications, cost savings and service availability improvement.

SITA's IPVPN at Airports will provide the same internetworking service, the main difference being that the WAN access is delivered from a pair of Airport Hub WAN routers, located in a communications room in the airport, and shared by all IPVPN customers.

1.2 Service scope and purpose

Compared to the traditional SITA IPVPN service, IPVPN at Airports aims to deliver cost savings and improved service availability, due to the economy of scale achieved though the aggregation of multiple individual accesses and to the WAN Mission Critical Site infrastructure.

The advantages of IPVPN at Airports are:

- Same IP VPN charge for the dedicated bandwidth and Class of Service
- No dedicated leased line(s) and associated Link Service Charges; instead a simple IP

Port charge with pricing per airport

- Mission Critical Sites ready WAN infrastructure
- Reliable in-airport connectivity

1.3 Architecture overview

The standard VPN topology supported by IPVPN at Airports is the "any-to-any" topology, which allows any customer router and/or virtual routers within the VPN to communicate with any other customer routers or virtual router in the same VPN. Unless otherwise specified and configured, the IPVPN at Airports network does not allow customer routers or virtual routers in different VPNs to communicate with one another. IPVPN at Airports also supports the access to ServiceNet services, similarly to the usual IPVPN service.
A typical IPVPN at Airports service to a customer consists of:

- An IP VPN bandwidth (redundant or not)
- One (or several) IP ports per IP VPN bandwidth

IP VPN bandwidth on Airport Hubs consists of one (1) or two (2) configurations, referred to as virtual routers, on the airport hub routers. The virtual router configuration includes a VLAN sub-interface, a virtual routing table (VRF), and a Frame Relay PVC (up to an IGN PE router, in the same way as the traditional IPVPN service). From the PE router and forward, the service and the customer VPN is normal IPVPN.

The Airport Hubs routers being Mission Critical Site ready by default, a redundant configuration can be implemented shall the customer have a need for it.

Customers using different VPNs at a given airport should use one (1) IP VPN bandwidth per VPN. As an integral part of the service, each customer is provided with a VLAN connectivity service (Ethernet) between the Airport Hub routers and its offices. This service component is referred to as IP port.

Each such VLAN connection to a customer office is delivered as:

- A customer dedicated VLAN configuration on the Airport Hubs infrastructure
- A LAN plug that connects to a physical port of a Airport Hubs infrastructure switch or a (small) Long Reach Ethernet (LRE) CPE where the customer office is far away from the closest airport hub infrastructure LAN switch (generally over 100 meters).

Customers having multiple offices using the same VPN in the airport can order multiple IP ports (i.e. multiple LAN connections) for the same IP VPN bandwidth.
When customers have a need for a full Mission Critical Site implementation, with the IP VPN bandwidth MCS configuration they can also order two (2) IP ports in the same office, for redundancy purposes. However, the exact level of resiliency (path diversity) will be checked on a case-by-case basis, due to the variety of local airport conditions.

2 Service features

- VPN access from the airport via a dedicated VLAN and shared WAN infrastructure
- WAN resiliency option (shared infrastructure is MCS ready)
- LAN resiliency option (customer option to order a redundant IP port)
- CPE options
- Multiple IP ports (i.e. multiple LAN connections from different offices) on same IP VPN bandwidth
- IP-only features of IP VPN except dynamic IP routing on customer LAN.
- Class of Service (Silver, Gold, Gold Flexible, and Platinum in case of customer voice RT traffic)
- Access to ServiceNet services
- Airport Hub node availability reports and related Service Level
- Standard Fault Management (reactive),
- QOS/performance reporting and Service Level reporting (upon availability).
- Electronic commercial ordering

3 Technical design

The Airport Hub routers are IPVPN CE routers deployed in SITA core rooms at airports, or in space rented by SITA in airport telco rooms. The Airport Hub site is Mission Critical site (MCS) ready based on a square architecture (2 x CE, 2 x PE), for resiliency, and with as diverse as possible paths from the airport up to the two (2) different PE locations. The customers' offices in the airport are connected to the Airport Hubs through a Campus VLAN infrastructure.

3.1 Router & WAN design

The physical routers and models are an infrastructure feature, not a customer feature.
The VRF-lite (or Multi-VRF) Cisco feature configured on the Airport hub routers, allows the creation of multiple separate VPNs belonging to distinct customers on that same physical routers.

Each customer is configured with a virtual router and VRF on the physical routers. For MCS implementation, IP rerouting in case of failure of the primary router is ensured due to HSRP protocol (Hot standby routing protocol) and iBGP routing protocol sessions between each pair of customer VRFs.

Each virtual router connects to a PE via a Frame Relay PVC, with CIR only. Access link capacity is managed by SITA.

3.2 VLAN design

Depending on the distances between the customer equipments and the access switches, standard switched Ethernet (over Category 5 cables) or Long Reach Ethernet (over Category 1/2/3 telephone cables) is used. SITA may elect to use alternate available technologies.

4 Service security

In order to guarantee the customer VPN privacy, each customer connection is delivered with:

- A dedicated LAN port
- A dedicated VLAN
- A dedicated VLAN sub-interface on each Airport Hub router
- A dedicated routing table (VRF) on each Airport Hub router
- guaranteed bandwidth on the WAN side

All these components are manually configured, so as to prevent any communication and any visibility between the LANs, VLANs, interfaces and VPNs of the different customers.
All SITA switch configurations follow best security practices, including traffic and protocol filters, deactivation of L2 protocols on un-trusted ports, manual configurations of trunks (no VTP), use of dedicated VLAN for management purposes and abstention from using VLAN 1 to carry any data traffic.

Local access to all airport hub infrastructure devices is secured physically (locked rooms / racks, operator access control) and logically (passwords). Remote access to all airport hub infrastructure devices is controlled and permitted only to authorized personnel.