UNIFIED COMMUNICATIONS AND COLLABORATION AS A SERVICE

How the right cloud architecture can provide a dependable enterprise communications and collaboration solution

For mission-critical, real-time applications like unified communications and collaboration, businesses need a cloud solution that's highly reliable, available, and resilient.

As opposed to public cloud, private cloud infrastructure is operated solely for one organization, so it can adhere to higher levels of security required for mission-critical applications.

OVERVIEW

Private, hosted, and managed cloud services provide IT resources and services based on infrastructure that physically resides at the cloud service provider's data center. These services are available on demand from virtualized and highly scalable data center environments. Such features can help control the cost of cloud services as compared to traditional managed network services, where networking and compute infrastructure are installed and maintained on customer premises. Other benefits of cloud services include the ability to outsource nearly all operational services related to applications, network, and storage infrastructure to the cloud provider, which contributes to faster activation, scalability, and modification of services.

When it comes to mission-critical, real-time applications like unified communications and collaboration, however, organizations need assurances that a cloud solution is highly reliable, available, and resilient, because when communications go down or quality is subpar, business can be significantly impacted. These services therefore require a different cloud architecture than the public cloud, which has a shared operating environment for provisioning and applications. By contrast, a private cloud features infrastructure operated solely for one organization that adheres to high levels of security, availability, and reliability.

This white paper explains the infrastructure and features necessary for secure, reliable delivery of carrier-class, cloud-based unified communications and collaboration services based on a private cloud service.

BENEFITS OF CLOUD SERVICES

- **Greater flexibility** in adding, subtracting, or changing services or service requirements in response to seasonal dynamics or business expansions or contractions.
- **Easier, faster scalability,** enabling organizations to grow without time-intensive and resource-intensive IT build-outs.
- **A more agile IT infrastructure** that enables organizations to rapidly transform ideas into marketable products and services and new business models. Access to services spans users in different geographies.
- **Cost-effectiveness** due to the transformation of capital-intensive investments to pay-as-you-go pricing where costs are tiered and metered to accurately reflect an organization's requirements and usage. Cost management also comes from reduction or elimination of operational costs for maintenance of on-premises equipment and software.

CHOOSING THE RIGHT TYPE OF CLOUD

There are several varieties of cloud services. Public clouds, open to the general public, store your applications and data together with others', which means that cloud may not include the security features you require. Also, the public cloud often does not provide the service levels that organizations require for their real-time communications applications.

Private clouds are recommended for services such as communications and collaboration, which today are mission critical. The private cloud provides dedicated resources to each separate organization. Verizon offers private cloud services; infrastructure for the network, applications, and storage is hosted in Verizon data centers and managed by Verizon professionals.

KEY CONSIDERATIONS FOR AN ON-DEMAND SOLUTION

Communications and collaboration services are considered mission critical in organizations today. Therefore, those services must be as available, reliable, and resilient as services where the infrastructure is deployed and maintained on the customer's premises behind a firewall. Availability

The right network architecture requires three components: the customer network, and the cloud provider's IP Multiprotocol Label Switching (MPLS) network and data center.

of services around the clock seven days a week; reliability of services based on user accessibility from different locations, devices, and quality of the connection; and resiliency of services in the event of a failure or disaster are all dependent upon the platforms, architectural choices, and best practices of the cloud provider.

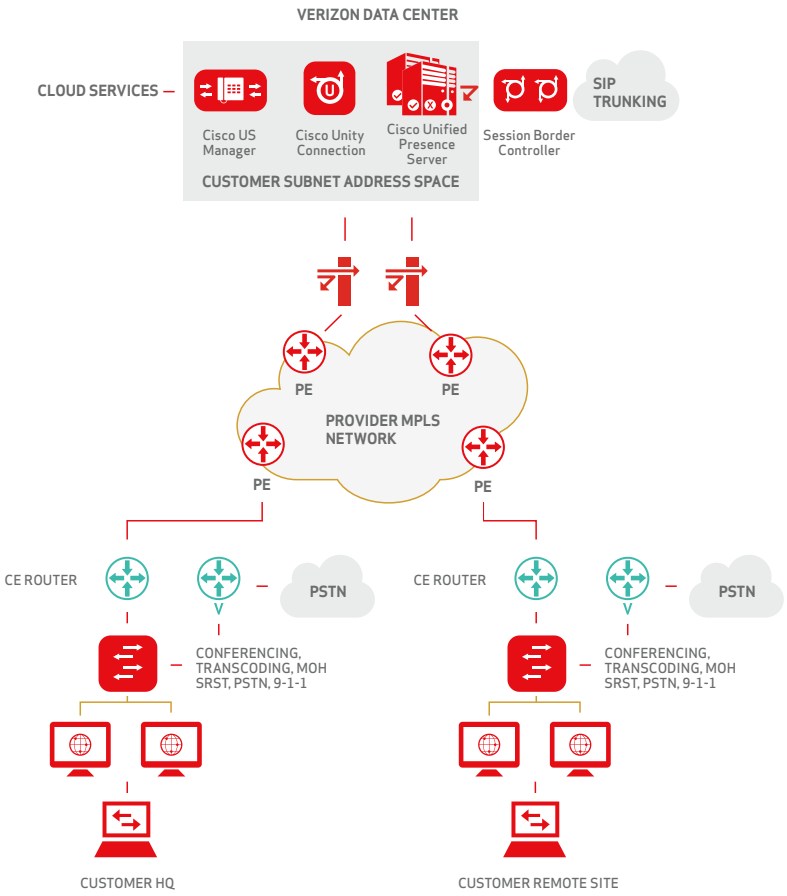
The optimal network architecture for private, hosted, and managed cloud infrastructures that provide unified communications and collaboration services includes three network components: the customer network, the cloud provider's IP Multiprotocol Label Switching (MPLS) network, and the cloud provider's data center. A variety of technologies, platforms, and architectures in these network segments combine to give cloud providers the infrastructure necessary to meet customer requirements.

THE CUSTOMER NETWORK

With private, hosted, and managed cloud services, the infrastructure for communications and collaboration services (which include services such as telephony, call control, voicemail, presence, instant messaging, and integration with collaboration applications like conferencing) moves from the customer network to the cloud provider's data center. The customer-premises equipment (CPE) layer connects customer endpoints (such as phones, mobile devices, and local gateways) to the cloud service provider's network and provides end-user interfaces to network management software.

Each customer connects directly to the provider's Voice over IP (VoIP) network or Public Switched Telephone Network (PSTN) (Figure 1). Organizations with single and multiple sites can be supported. Customer premises have switches and media routers that should be deployed with Cisco Unified Survivable Remote Site Telephony (SRST). In customer networks using the Cisco Unified Communications Manager (CUCM) solution, SRST is embedded within Cisco IOS Software to help provide high-availability IP telephony to branch offices. When access to CUCM from the branch office is impeded (e.g., as a result of a WAN link failure), SRST provides telephony backup services to help maintain service over the private cloud network infrastructure to the branch location. In Figure 1, the architecture illustrates use of an optional second media resources router to support complex or resource-intensive capacity requirements.

Figure 1. Customer Connection to a Private Cloud Service



With private cloud and MPLS, quality of service (QoS) can be engineered into services based on the use of multiple traffic queues and classes.

The CPE media router should also provide a connection to the PSTN as a backup to the provider's VoIP network, 9-1-1 U.S. and Canada emergency agencies dialing, and digital signal processor (DSP) resources for conferencing, Media Termination Points (MTP), and transcoding services in addition to serving as a PSTN gateway. In the diagram above, the architecture illustrates use of an optional second router to support larger location capacity requirements. The CPE switches could be equipped with an application that tracks the movement of IP phones for 9-1-1 emergency dialing. In a customer network with Cisco routing and switching infrastructure, CPE switches are configured to assist Cisco Emergency Responder, which can be used to track the movement of IP phones for 9-1-1 emergency dialing.

For critical sites such as headquarters, customers can request a redundant connection to the provider network, using separate cables coming into each building that connect to different provider edge routers in different parts of the country. This will help maintain a high level of performance for communications and collaboration services.

There are many other features between customer and service provider networks that provide for dependable and resilient unified communications and collaboration cloud services, including the following:

Quality of service (QoS) can be engineered into services based on the use of multiple traffic queues and classes. This is a key point of differentiation between private cloud services such as Verizon Unified Communications and Collaboration as a Service (UCCaaS)—provided over a private MPLS network—and services provided over the public Internet. MPLS gives network administrators more control over traffic in a Private IP (PIP) network. Among other benefits, the technology enables IP packets—the building blocks of data, voice, and video traffic in an IP network—to carry detailed information about what routes to traverse. This can be used to provide QoS for latency-sensitive traffic such as voice and video and for mission-critical data applications, and is not available to customers via the public Internet via a cloud or other managed network service infrastructure. The UCCaaS service architecture is designed with hardware and software that provide the capability for end-to-end QoS. QoS considerations start in the data center where the virtual switch, physical switch, and routing platforms support differentiated services (DiffServ) markings to provide the highest priority to the application traffic that needs it. QoS markings are set at the customer premises, based on the priority needed for various application types. QoS markings are honored as they traverse the Verizon Private IP MPLS backbone into the data center from the customer-premises environment.

DiffServ is a model in which traffic is treated by intermediate systems with relative priorities based on a type of services (ToS) field. It increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. The six most significant bits of the DiffServ field are called the differentiated services code point (DSCP). The last two currently unused (CU) bits in the DiffServ field are used as Explicit Congestion Notification (ECN) bits. Routers at the edge of the network classify packets and mark them with either the IP precedence or DSCP value in a DiffServ network. Other network devices in the core that support DiffServ use the DSCP value in the IP header to select a per-hop behavior (PHB) for the packet and to provide the appropriate QoS treatment. Traffic classes can be defined by a combination of factors, including protocol, port numbers, and DSCP values. Thus, these technologies in the private, hosted, and managed cloud environment allow providers to prioritize voice and video communications, which are less tolerant of delay. As a result of this design, Verizon is able to offer a UCCaaS application availability service level agreement (SLA) of 100% (applications with geographic redundancy).

Per-customer virtual private network (VPN), VPN routing and forwarding (VRF) instances, and virtual local area network (VLAN) connections are used by individual users and from customer premises respectively to the unified communications and collaboration applications in a multitenant data center, providing customer segregation for added security.

THE CLOUD SERVICE PROVIDER'S NETWORK

Carrier-grade or carrier-class networks—which are defined as having extremely reliable, well-tested and proven capabilities and which are tested and engineered to be highly available and to provide fast, efficient fault recovery—allow customers to share information between their sites

Private cloud data centers offer pre-engineered, pre-integrated, and validated hardware configurations for computing resources based on sizing requirements.

across an Internet protocol (IP) network backbone in a secured environment. These networks provide highly scalable any-to-any, hub-and-spoke, or regional connectivity for voice, video, and data network convergence. Using MPLS technology and virtual private network (VPN) connections, services may be engineered for different levels of priority (e.g., higher priority for voice and video with low latency and jitter) and a high degree of security.

Verizon takes advantage of its global IP network, which is highly reliable and secure. For example, the UCCaaS platform is constructed so that Session Initiation Protocol (SIP) trunks for voice calls are built on two different nodes on different sides of the United States. If one node goes down, call traffic can be quickly routed to the other node. Other services that travel over the data network (e.g., conferencing, video, presence applications) also have redundancy features at the application, virtual machine, component, link, and signaling aggregation levels. And Verizon data centers offer a number of other features to promote availability, reliability, and resiliency within its MPLS network, including:

- **Quarterly vulnerability scans,** which assess network infrastructure vulnerabilities to identify malware and failures before they can occur.
- **Security controls,** which are aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 2. These standards define the required security controls in support of information security programs and an organization's overall approach to managing risk.
- **Best practices for authentication and password management** which are followed to make sure that access is limited to authorized users.
- **Access lists** that limit access to trusted hosts and help prevent jump connections.
- **Extensive event logging and alarming** that quickly catch problems or intrusion attempts before they cause any serious damage.
- **Automated provisioning systems** that help protect against any human errors.

THE PROVIDER'S DATA CENTER

In the data center, each cloud services customer is served by dedicated, virtual applications. Virtualization has made it increasingly viable and cost-effective to consolidate network, computing, storage, and management resources in the data center. This in turn has made cloud services less capital intensive, as providers can use data center resources more flexibly and across multiple data centers.

The data center architecture for private, hosted, and managed unified communications and collaboration services can scale too many physical or virtual servers. Network virtualization enables the separation of different customers. Virtual firewalls provide security and reliability for each customer. Each application is fine-tuned within a virtual environment to help control costs and increase operational productivity. This includes the ability to use virtual computing resources to adjust for customer size and usage to support many customers on a shared hardware platform. High-availability features promote customer service uptime, taking advantage of the already-robust, redundancy capabilities of the applications themselves. Installation and upgrades can be handled smoothly using templates and clones of virtual machines. Customization, data security, and end-user application access is still possible because each customer is hosted through private virtual machines.

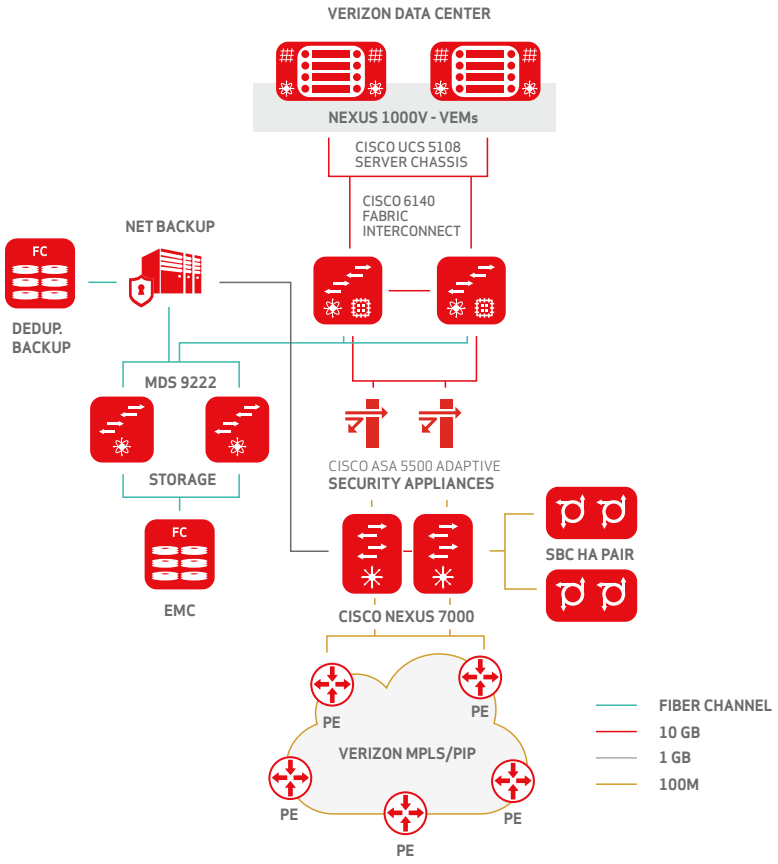
The private cloud provider's data center offers pre-engineered, pre-integrated and validated hardware configurations for computing resources based on sizing requirements. Customers are deployed and scaled easily and provide consistent performance and capacity profiles. The right data center design should include integrated network, storage, compute, and virtualization resources that are aggregated into the data center core and aggregation switches. This design provides a layered approach to maintain scalability, performance, flexibility, resiliency, and maintenance.

Verizon's data center design shown in Figure 2 utilizes the Cisco Unified Computing System™ (UCS™) platform that integrates network, storage, compute, and virtualization resources and is aggregated into the data center core and aggregation switches.

In this architecture, the Cisco UCS infrastructure components are deployed as a single tenant (dedicated per customer) in the cloud. Dedicated components, along with the service management engine (SME) and other management components, run over virtual machines (VMs) on the Cisco UCS. The hardware leverages virtualization technology to enable multiple instances of the communications and collaboration applications to run on the same hardware. The ability to create new VMs supports the ability to scale existing applications or add new customers.

Our data centers feature 24x7 monitoring and redundancy down to the device level for high levels of security.

Figure 2. Data Center Network



Other features that promote availability, reliability, and resiliency within a cloud provider's data center include:

- **Redundancy down to the device level,** including power feeds, switches, routers, supervisor engines and fabrics for the storage area network (SAN). Redundancy features in the components in Verizon's architecture shown in Figure 2 include the following:
  - Cisco UCS virtual server clusters are spread across chassis to help maintain server uptime in case of blade failure, and all chassis use VMware High Availability to recover in case of blade failures. All server hardware has redundant CPU and redundant power for in-chassis redundancy, and every chassis has a duplicate backup for chassis redundancy.
  - Dual Cisco UCS 6200 Fabric Extenders for high availability. The Fabric Extenders help create a lossless fabric from the adapter to the Fabric Interconnect by dynamically throttling the flow of traffic from network adapters into the network.
  - Dual Cisco Nexus 1000V Series Virtual Ethernet Switches for redundancy.
  - Dual Cisco ASA 5500 Security Appliances provide redundant firewalls at the aggregation layer.
  - Dual Cisco Nexus 7000 Series Switches that are fully redundant and help provide status monitoring, power and environmental management, and other functions. The architecture supports lossless fabric based on multiple switch fabric modules.
  - Dual Cisco MDS 9222 Multilayer Fabric Switches and EMC Fibre Channel storage arrays with dual service processors working in active/active redundancy mode.

24x7 monitoring of the data center environment, including physical security with tiered access and entry points secured by key cards and biometric scanners, surveillance with fixed and roving security guards, and bunker-style construction.

Management and Security

In order to provide a reliable, available, and secure enterprise communications solution from end to end, the provider should also excel in three areas: managed services, security services, and professional services to complement the services offered from the data center.

The infrastructure required for offerings such as UCCaaS is complex and multi-layered to meet the needs of the most demanding organizations and industry standards.

The provider should have the ability to manage your network services as they move back and forth to a WAN, LAN, or wireless LAN (WLAN), making sure that data, voice, and video services adhere to published service level agreements. For hybrid deployments with on-premises equipment as well as cloud-based infrastructure, the provider must have a dependable management platform to enable end-to-end troubleshooting, providing fast, efficient problem resolution.

Additionally, the provider should have sufficient expertise and services to address the multitude of security risks that could threaten your network, detect any risks from beyond your network and provide guidance on securing your existing infrastructure to mitigate those risks. The cloud platform must also be flexible enough to incorporate your unique security policies.

It is also important to find a provider that has the deep knowledge, technical experience, and personnel required to understand your current infrastructure, evaluate and incorporate your future requirements, and leverage existing investments in a design and migration plan that best positions your organization to take advantage of advanced collaboration services in the future.

UCCAAS FROM VERIZON

Unified Communications and Collaboration as a Service (UCCaaS) is delivered over Verizon's global IP network and private, hosted, and managed cloud services data centers. The service delivers high uptime (with an application availability SLA of 100%), fault tolerant reliability, and scalability to meet the needs of the largest enterprises. UCCaaS can provide an array of measurable benefits that can impact individual productivity and an organization's bottom line.

CONCLUSION

The private, hosted, and managed cloud services model was designed to emulate the high degree of availability, reliability, resiliency, and security found in the most sophisticated enterprise and carrier-class networks. As a platform for delivery of mission-critical communications and collaboration services to organizations, the private cloud has evolved to become a trusted option backed by infrastructure, architectures, and technologies.

There are many aspects of the network architecture to consider before you decide on a cloud-based solution for your communications and collaboration needs. The infrastructure required for offerings such as UCCaaS is complex and multi-layered to meet the needs of the most demanding organizations and industry standards. Aside from the array of strategic and cost benefits available with private cloud services, customers particularly enjoy the ease and speed with which they can connect to these services.

FOR MORE INFORMATION

Verizon UCCaaS Fact Sheet
verizonenterprise.com/resources/factsheet/fs_unified-communications-and-collaboration-services_en_xg.pdf

Verizon Private IP Service
verizonenterprise.com/resources/factsheet/fs_private-ip-securely-connect-and-communicate-around-the-world_en_xg.pdf

Cisco Unified Communications Manager Security Guide
cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_1_1/secugd/CUCM_BK_C0395F44_00_cucm-security-guide-91.html

Cisco Unified Communications System Solution Reference Network Design
cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09.html

For more information, please contact your account representative or visit
verizonenterprise.com/products/advanced-communications/unified-communications-collaboration/
or verizonciscocollaboration.com

verizonenterprise.com

SLA available to customers implementing both Verizon-approved UCCaaS architectures and Verizon Private IP within the United States. Terms & conditions apply; see your Verizon account manager for details.