White Paper

Discover Unified Communications and Collaboration as a Service.

Maintaining security, availability, and reliability in the private cloud.

The proven power of private and dedicated cloud services.

More and more, enterprise organizations around the world are turning to managed network and cloud services. They can reduce capital expenses and control operational expenses (CAPEX and OPEX), enhance workforce productivity, increase agility, make costs more predictable, and simplify operations throughout the application life-cycle. Today's managed cloud-based services deliver high reliability, availability, and security —which are all traditional, core attributes of carrier-class service provider infrastructures. But not all cloud services are alike. Public cloud services can be vulnerable to Internet intrusions.

Private and dedicated cloud services are available from service providers to individual organizations, and they provide a secure and reliable foundation through:

- A defense-in-depth security strategy with overlapping layers of protection.
- The use of a customer-specific virtual routing and forwarding (VRF) environment, allowing each customer to have their own dedicated instance of an application that is not shared.
- Firewalls to control traffic as it travels - to and from private cloud services to help protect against threats from inside and outside an enterprise.
- Use of purpose-built management systems, as well as syslogs for system monitoring and management, security auditing, and generalized analysis, debugging, and troubleshooting, to remediate failures quickly, helping reduce downtime.
- The ability for customers to assign addresses utilized behind the cloud-based firewall to extend their private addressing into the service making it appear like a customer-owned and operated service.

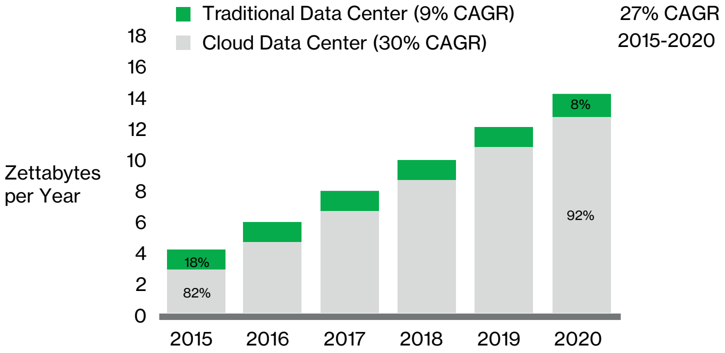
More businesses are using cloud services.

The popularity of cloud services is driving massive increases in data center and network traffic, with global data center traffic expected to more than triple from 2015 to 2020. It will reach 15.3 zettabytes per year by the end of 2020 according to the Cisco® Global Cloud Index: Forecast and Methodology, 2015–2020.

The same study predicts that by 2020, 92% of workloads will be processed by cloud data centers.

This underscores the confidence most organizations now have in the integrity of cloud services.

IDC estimates that $204.5 billion will be spent on cloud services in 2020 (compared to $77.3 billion in 2015)[1].



Source: Cisco Global Cloud Index, 2015–2020.

The combination of private, hosted, and managed cloud services with unified communications and collaboration services can reduce or eliminate the need to install, maintain, and upgrade on-site PBX equipment and applications. Each customer is provided with dedicated, virtual instances of each application, including software and hardware redundancy and availability.

[1] IDC, Worldwide and Regional Public IT Cloud Services Forecast, 2016-2020, Doc #US40739016, December, 2016

Beyond the cost and operational benefits, private, hosted, and managed unified communications help organizations increase teamwork and productivity, improve speed to market, enhance business process flexibility, increase customer satisfaction, and reduce travel expenses. The overall value is further increased by the ability to deliver unified communications and collaboration applications (including presence, IP voice, instant messaging, desktop and web conferencing, and collaboration workspaces) to both fixed and mobile clients.

When it comes to private, hosted, and managed cloud environments, there are various approaches to security, reliability, and availability – some far superior to others. This is especially true for unified communications, where information confidentiality may be required and where the absence of reliable, available services may negatively affect business operations.

Challenges in maintaining security, availability, and reliability.

In an era when business happens in an instant, the confidentiality of trade secrets, sales, and customer information is especially vital – as are communications between employees, customers, partners, and suppliers. Strategic advantage can be won or lost based on the availability and security of information. And reliable unified communications and collaboration services and information can often form the basis of entirely new business models.

Services provided over the Internet and public clouds, moving from large colocation data centers to insecure fixed and mobile devices, generally lack the rigid security and reliability of enterprise network and private cloud services. For enterprise unified communications and collaboration, these shortcomings are simply unacceptable.

By contrast, world-class, private, hosted, and managed cloud services incorporate proven industry best practices, architectures platforms, and technologies – and they adhere to enterprise data center standards. These services also enable many new features based on virtualization and other more recent innovations.

Private IP and UCCaaS.

Verizon's Global Private IP Service infrastructure is a private network that can grow with the enterprise business. Customers obtain services via a Layer 3 MultiProtocol Label Switching (MPLS) VPN. They get the security and quality of service (QoS) that they have come to expect from MPLS , the flexibility and scalability of IP, and the convergence of voice, data, and video applications over an integrated network infrastructure (See Figure 2).

Verizon Unified Communications and Collaboration as a Service (UCCaaS) provides an extensive roster of unified communications and collaboration applications to users in varied work environments and scenarios, packaging the entire suite of Cisco Hosted Collaboration Solution applications into a single user license. The package includes client and server software access rights, service and support, and software upgrades. The solution is based on Cisco Unified Communications Manager and VMware vSphere Hypervisor for virtualization.

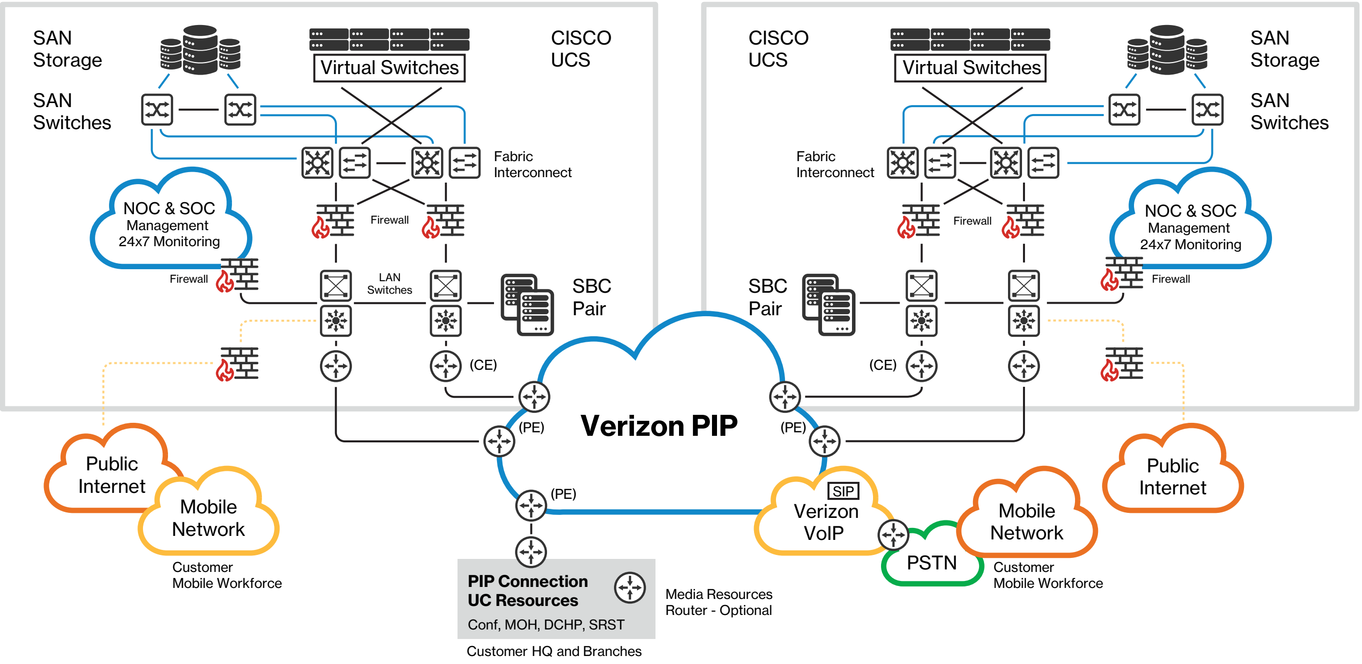


Figure 2. Verizon Private IP service: converged services over IP

Applications.

Cisco Unified Communications Manager:

Delivers call control, voice services, and plug-and-play provisioning of IP phone features.

Cisco Unity Connection:

Provides voice messaging features and services. These include web voicemail and Internet Message Access Protocol (IMAP) integration for Microsoft® Outlook® and Cisco Jabber. Cisco Jabber provides a single interface across presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing.

Cisco Jabber Desktop Client:

Allows customers to bring together all their communication applications in a single, easy-to-use interface for PC or Apple Mac. Users can stay connected virtually anywhere they are and can quickly find people they need to reach. Jabber brings secure soft-phone capabilities, presence, IM, visual voicemail, video, and web conferencing to the desktop.

Cisco Jabber Mobile Client:

Extends communication and collaboration capabilities to the smartphone or tablet, providing remote or mobile workers the ability to connect and collaborate across any network and via preferred devices.

Cisco WebEx, Cloud Connected Audio (CCA) and Spark:

Customers can optionally deploy Cisco Expressway and connect to WebEx and Cloud Connected Audio or Spark, allowing them to collaborate instantly or schedule events in advance.

Key differentiators.

Multi-customer versus multi-tenant computing infrastructure:

Multi-tenant computing infrastructures feature a single set of applications in one IP address space on a server, which then supports multiple customers. By contrast, the multi-customer infrastructure behind UCCaaS provides each customer with dedicated, virtual instances of each individual application through the use of virtualization technology.

This completely isolates each instance of software from every other instance. Applications run in their own address spaces, with dedicated server processing provided to each customer. There is no routing between VRFs and individual instances of firewalls at the edge of the network, which enables customers to set up their own filter rules. Data stores on the storage area network (SAN) feature a logical unit number (LUN) dedicated to each separate customer. The multi-customer environment allows customers to enjoy the benefits of dedicated software while taking advantage of shared hardware, with carrier- class security, flexibility, and resiliency.

Defense-in-depth security model:

This industry-proven best practice features multiple layers of security and different techniques that provide overlap protection (Figure 3). UCCaaS utilizes a variety of technologies and techniques to protect the core network and customer networks. This includes the use of stateful and redundant firewalls, Deep Packet Inspection (DPI), individual server and component hardening, and physical security at Verizon and third-party data [Equinix] data centers.

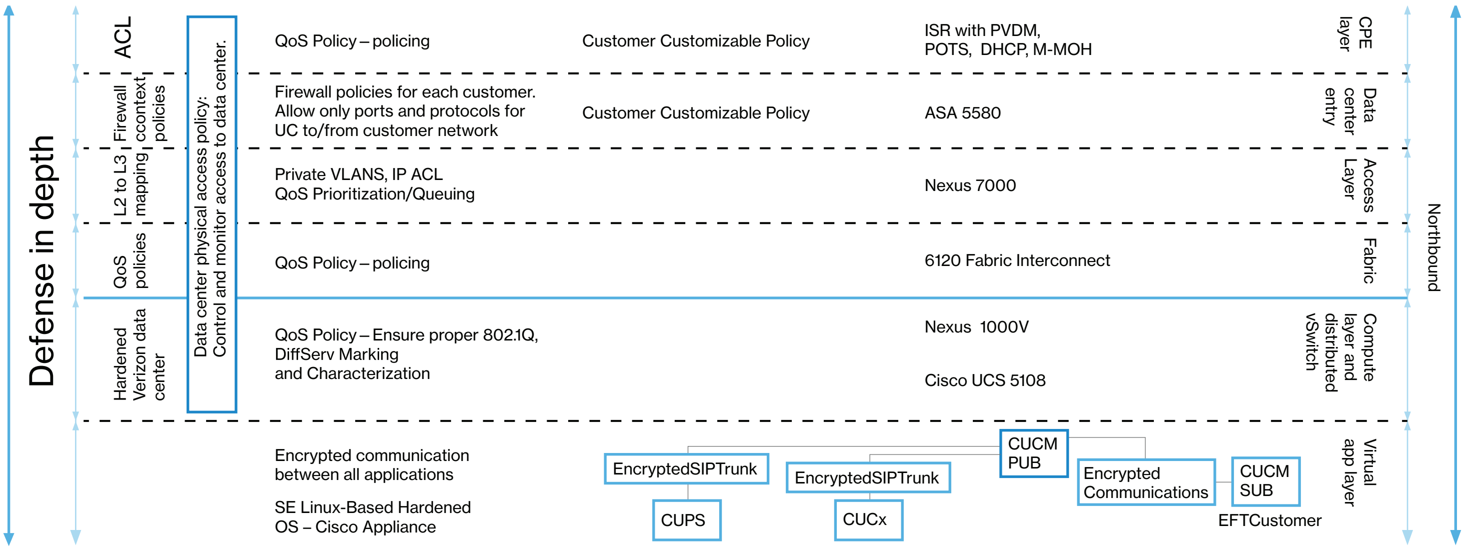

Defense in depth
ACL
Firewall ccontext policies
L2 to L3 mapping
QoS policies
Hardened Verizon data center
Data center physical access policy: Control and monitor access to data center.
QoS Policy – policing
Customer Customizable Policy
ISR with PVDM, POTS, DHCP, M-MOH
CPE layer
Firewall policies for each customer. Allow only ports and protocols for UC to/from customer network
Customer Customizable Policy
ASA 5580
Data center entry
Private VLANS, IP ACL QoS Prioritization/Queuing
Nexus 7000
Access Layer
QoS Policy – policing
6120 Fabric Interconnect
Fabric
QoS Policy – Ensure proper 802.1Q, DiffServ Marking and Characterization
Nexus 1000V
Cisco UCS 5108
Compute layer and distributed vSwitch
Northbound
Encrypted communication between all applications
SE Linux-Based Hardened OS – Cisco Appliance
EncryptedSIPTrunk
EncryptedSIPTrunk
CUCM PUB
Encrypted Communications
CUCM SUB
CUPS
CUCx
EFTCustomer
Virtual app layer

Figure 3. Defense-in-depth security layers and corresponding Cisco platforms.

Security, availability, and reliability features at each network layer.

Customers expect cloud services to provide the security, availability and reliability of on premises applications but with the ease of use and flexibility of a subscription service model.

Verizon and third-party data [Equinix] data centers house the infrastructure in a secure, fully redundant architecture. Customer separation within the datacenter begins at the edge where the Verizon MPLS network ingresses and terminates on fully managed Cisco Nexus 7000 switches. Customer traffic is then segregated into dedicated virtual LANs (VLANs) within the Nexus and switched into a Cisco ASA firewall where a customer-specific firewall context will permit only traffic destined for the UCCaaS platform. Development of the customer-specific rules begins in the low level design process and is developed in conjunction with the customer and with the customer's feedback. (Note: Customers may customize their firewall policies for firewalls that extend and further harden their security posture but Verizon's baseline security policy cannot be modified.)

Traffic allowed to pass through the firewall is then switched into new, separate VLANs for voice and data with QoS to prioritize signaling and voice traffic end-to-end. This holistic approach to QoS allows Verizon to provide a higher quality end user experience than UC providers who deliver their service over the internet, where the traffic must compete with other non-time-sensitive applications such as streaming video and email, for example. Additionally, the Session Border Controller (SBC) included as part of the service provides added topology hiding and security features help protect Voice over IP (VoIP) devices that must interconnect with the public switched telephone network (PSTN).

Finally, the UC applications for a customer are deployed in customer-dedicated instances and provisioned into a customer-owned IP Address space. Since the UCCaaS instances are provisioned only over MPLS, the data centers look and feel like an integral part of the customer's private network. This deployment model is identical to what customers have historically deployed in their own compute space except that the service is delivered out of Verizon and third-party data [Equinix] data centers V instead. This deployment model offers customers the best of both worlds; the traditional, robust architecture they are accustomed to having but priced in a consumption model.

Additional levels of security for network protection.

Verizon has taken great care to provide a robust, secure and flexible architecture for our UCCaaS platform.

The fabric interconnect to the storage array network (SAN):

The ports and backplane used to communicate between VM instances and the SAN is segmented like the virtual LANs that carry voice and data, and distributed switching further isolates customer traffic. While more traditional cloud services that provide infrastructure-as-a-service (IaaS) are transactional, bursty services, UCCaaS carries voice and video traffic and is sensitive to latency, packet loss and jitter and implements full end-to-end QoS features to provide a quality end user experience.

Distributed switching architecture:

Verizon employs a redundant switching infrastructure that helps reduce single points of failure from disrupting service. VLANS created within this switching infrastructure isolate customer data in the data centers, with each customer VRF extended through the switched architecture. Verizon uses extended features within the Cisco Nexus 1000V virtual switches to extend QoS features inside the virtual distributed switch environment to correctly prioritize signaling and media from end to end.

Server Hardware and Application layer:

At the compute layer, systems resources such as memory and CPU cores are dedicated to specific customer instances of the applications. A single customer logical cluster of applications is divided into two and the use of clustering over the WAN distributes the two halves of the cluster between Verizon datacenters to help prevent a catastrophic event at one location from impacting the entire platform. In addition, within each data center the virtual applications are distributed over multiple physical servers to avoid the risk of one device loss bringing down that data center. All customers are provisioned in this geo-redundant mode.

Server OS hardening:

The underlying virtual Linux OS environment has been hardened by the manufacturer to disable all unnecessary services and ports. This appliance model restricts direct access to the OS, instead forcing administration through the management portal. The entire application environment is also monitored and logged using SNMP and syslog logging. In addition, Cisco adheres to industry standard development best practices for the applications and follows all PSIRT guidelines for known security vulnerabilities and remediation.

Physical security:

For the UCCaaS environment at Tier 4 Verizon and third-party data [Equinix] data centers, physical security includes multiple layers of physical isolation, requiring a combination of biometric scans, an ID card, and ticket/ notification to enable access and work on data center infrastructure. All servers and network components are protected by a two-form-factor access method to restrict and actively control access to components.

Platform Access:

Furthermore, the UCCaaS platform is not provisioned to be reached via direct Internet access, requiring the use of dedicated MPLS interconnects to the individual customers' private networks. This provides additional security to the UCCaaS core by isolating the platform from the Internet. This helps protect the platform and customer environment by not introducing backdoor access into the customer's MPLS network.

For customers that would like to take advantage of mobility features by enabling Jabber on mobile devices, Verizon offers the use of Cisco Expressway built into the customer's UCCaaS environment. Cisco Expressway is a secure firewall traversal solution that allows fully encrypted communication between remote Jabber devices and the platform. Expressway works by leveraging two separate devices, Expressway C (Core - inside the network) and Expressway E (Edge – in the DMZ). The Expressway devices maintain a secure tunnel between them and force all traffic to pass between them via this secure, encrypted tunnel. DNS is used to direct Jabber devices that are mobile-- that is, outside the customer's private network-- to establish communications with the Expressway E server. The Expressway E and the remote Jabber client then set up a secure, encrypted communication channel and all traffic, signaling and RTP is encrypted between both endpoints. UCCaaS does offer internet connectivity solely for the purpose of using Expressway and we do not allow non-Expressway traffic to use this for any other purposes.

The UCCaaS architecture provides scalability for even the largest enterprises by utilizing a multi-customer computing infrastructure and defense-in-depth security with geo-redundancy, robust fault-tolerance features, a service provisioning methodology and an application availability SLA of 100 percent[2].

Phone authentication and encryption:

Cisco Unified Communications Manager can be configured to provide multiple levels of security to phones within a voice system, including device authentication plus media and signaling encryption. IP Phone level encryption has implications for the larger platform design not only in terms of the additional overhead for bandwidth but also for other systems that might be deployed in the solution as well such as voicemail and survivability (Cisco Unified Survivable Remote Site Telephony [SRST]). Encryption of the signaling and RTP streams would be limited to internal, customer site-to-site calling and would not extend to PSTN calls as Verizon does not currently support encryption over IP Trunking. For these reasons, Verizon recommends that careful consideration be given by the customer to determine the need and implications to the overall solution during the design phase.

A customer-specific firewall context:

Deployed between the customer's VRF instance of their applications and the applications themselves, this provides an access control and monitoring point to the unified communications and collaboration applications. This firewall also helps identify and mitigate denial-of-service (DoS) attacks against the platform and polices access from the voice and data VLANs based on the customer's application environment and policies.

Reporting (Syslog and SNMP):

Verizon uses advanced management tools that allow us to capture and report on all critical system events. Our managed service NOC leverages SNMP and syslog logging to monitor the customer instance and properly address any issues which may arise.

Recommendations for Customer Owned Equipment (CPE).

Verizon recommends that the customer investigate and employ other security mechanisms on their LAN in accordance with Cisco published best practices for Unified Communications, some of these access security measures may include:

Access Security:

Dedicated Voice and Data VLANs:

Before the phone has its IP address, the phone determines which VLAN it should be in by means of the Cisco Discovery Protocol (CDP) negotiation that takes place between the phone and the switch. This negotiation allows the phone to send packets with 802.1q tags to the switch in a "voice VLAN" so that the voice data and

[2] UCCaaS geographic redundancy design required. Terms & conditions apply. See your Verizon account manager for details.

all other data coming from the PC behind the phone are separated from each other at Layer 2. Voice VLANs are not required for the phones to operate, but they provide additional separation from other data on the network.

Voice VLANs can be assigned automatically from the switch to the phone, thus allowing for Layer 2 and Layer 3 separations between voice data and all other data on a network. A voice VLAN also allows for a different IP addressing scheme because the separate VLAN can have a separate IP scope at the Dynamic Host Configuration Protocol (DHCP) server.

Customers not using Cisco IP Phones should be aware that third-party endpoints do not support Cisco Discovery Protocol (CDP) or 802.1Q VLAN ID tagging. To allow device discovery when third-party devices are involved, use the Link Layer Discovery Protocol (LLDP). LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that enhances support for voice endpoints. LLDP-MED defines how a switch port transitions from LLDP to LLDP-MED if it detects an LLDP-MED-capable endpoint. Support for both LLDP and LLDP-MED on IP phones and LAN switches depends on the firmware and device models. To determine if LLDP-MED is supported on particular phone or switch models, check the specific product release notes or bulletins for that switch model available at www.cisco.com

Switch Level Security Features:

Port Security: A classic attack on a switched network is a MAC content-addressable memory (CAM) flooding attack. This type of attack floods the switch with so many MAC addresses that the switch does not know which port an end station or device is attached to. When the switch does not know which port a device is attached to, it broadcasts the traffic destined for that device to the entire VLAN. In this way, the attacker is able to see all traffic that is coming to all the users in a VLAN.
.
To help protect against malicious MAC flooding attacks from hacker tools such as macof, limit the number of MAC addresses allowed to access individual ports based on the connectivity requirements for those ports. Malicious end-user stations can use macof to originate MAC flooding from random-source to random-destination MAC addresses, both directly connected to the switch port or through the IP phone. The macof tool is very aggressive and typically can fill a Cisco Catalyst switch content-addressable memory (CAM) table in less than ten seconds. The flooding of subsequent packets that remain unlearned because the CAM table is filled, is as disruptive and unsecure as packets on a shared Ethernet hub for the VLAN that is being attacked.

Either port security or dynamic port security can be used to help inhibit a MAC flooding attack. A customer with no requirement to use port security as an authorization mechanism would want to use dynamic port security with the number of MAC addresses appropriate to the function attached to a particular port. For example, a port with only a workstation attached to it would want to limit the number of learned MAC addresses to one. A port with a Cisco Unified IP Phone and a workstation behind it would want to set the number of learned MAC addresses to two (one for the IP phone itself and one for the workstation behind the phone) if a workstation is going to plug into the PC port on the phone.

In addition to helping protect against an attacker from flooding the CAM table of a switch, it also helps prevent unapproved extensions of the network by adding hubs or switches into the network. Because it limits the number of MAC addresses to a port, port security can also be used as a mechanism to inhibit user extension to the IT-created network. For example, if a user plugs a wireless access point (AP) into a user-facing port or data port on a phone with port security defined for a single MAC address, the wireless AP itself would occupy that MAC address and not allow any devices behind it to access the network. Generally, a configuration appropriate to stop MAC flooding is also appropriate to inhibit rogue access.

Dynamic Host Configuration Protocol (DHCP) snooping:

When enabled, this feature treats all ports in a VLAN as untrusted by default and prevents a non-approved DHCP or rogue DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request unless that port is allowed to reply.

Dynamic ARP Inspection (DAI):

Phones on the network are also vulnerable to data attacks. Gratuitous Address Resolution Protocol (GARP) on the phones helps to prevent man-in-the-middle (MITM) attacks involving an attacker who tricks an end station into believing that he or she is the router and tricks the router into believing that he or she is the end station. This attack makes all the traffic between the router and the end station travel through the attacker's machine, thus enabling them to log all of the traffic or inject new traffic into the data conversation. GARP on an IP phone protects against an attacker's ability to capture the signaling and RTP voice streams from the phone. This feature is used on the switch to help prevent GARP attacks on the devices plugged into the switch and on the router. Here the GARP feature protects all devices on the LAN, not just IP phones.

IEEE 802.1X port-based authentication:

Used to identify and validate the device credentials of an IP phone before granting it access to the network, the 802.1X feature is a MAC-layer protocol that interacts between an end device and a RADIUS server. It encapsulates the Extensible Authentication Protocol (EAP) over LAN to transport the authentication messages between the end devices and the switch.

UCCaaS business benefits.

Solutions such as UCCaaS provide an array of measurable benefits for the enterprise user, impacting individual productivity and the organization's bottom line. These include:

Fast time-to-value through rapid deployment:

UCCaaS is ready for adoption quickly, enabling collaboration in real time with a broad set of individuals across multiple locations. UCCaaS can save time over do-it-yourself PBX deployments. The service is customizable for employees and does not require a large capital investment, making it an excellent low-risk alternative to rolling out new technology solutions. Easy integration of existing services reduces the complexity and time frame required for deploying a hybrid model.

Extensibility:

UCCaaS integrates into enterprise software fabric – enterprise resource planning (ERP), customer relationship management (CRM), and custom applications. It integrates with and delivers desktop and immersive video, and is able to grow to meet your organization's changing needs.

Better cost control with no high up-front equipment charges for your communications solutions:

With UCCaaS, companies can move to a predictable monthly cost that can be scaled up or down based on business cycles. As a service instead of a product, UCCaaS helps protect companies from technology obsolescence and allows IT to focus their resources on more strategic projects.

High reliability:

For more predictable business operations, based on carrier-class availability, management, monitoring, and multi-layered security.

A clear value for today's enterprises.

Service providers who use the private, hosted, and managed network cloud for their offerings are including additional benefits. They're incorporating stringent security, availability, and reliability features developed over decades in the most sophisticated enterprise environments and Tier 4 data centers.

Computing architectures utilizing virtualization and based on multi-customer instead of multi-tenant infrastructure provide software and information isolation for each enterprise deployment. The defense-in-depth security strategy protects bare metal and virtualized assets, embedding security throughout all layers of the network to maintain the confidentiality, integrity, and availability of data, applications, endpoints, and the network itself.

UCCaaS is a carrier-class offering that provides these features to enterprises through numerous individual technologies, platforms, and devices delivered through Private IP network connectivity. Beyond providing an array of CAPEX and OPEX benefits, it is easily and flexibly deployed and swiftly brings demonstrable benefits from the use of unified communications and collaboration services by fixed and mobile assets in today's enterprises.

verizon✓