Powering collaboration: The Cisco WebEx Collaboration Cloud

WebEx Communications, Inc.
3979 Freedom Circle,
Santa Clara, CA 95054 USA

Main: +1.408.435.7000
Sales: +1.877.509.3239

www.webex.com

Table of contents

Introducing the Cisco WebEx Collaboration Cloud

The Cisco WebEx™ Collaboration Cloud is a communications infrastructure purpose-built for real-time web communications, and delivered as software-as-a-service (SaaS). Architected and designed to facilitate large-scale web communications globally, it delivers the very highest meeting performance, including many types of complex media throughout each session.

Cisco® is the global leader in on-demand web conferencing—an achievement made possible only because of the benefits of the Cisco WebEx Collaboration Cloud.

Outlining the strength of the Cisco WebEx Collaboration Cloud

Cisco WebEx™ offers a unique technological advantage that sets it apart from the other SaaS providers –a platform built from the ground up to deliver only Cisco WebEx meeting traffic with the highest reliability, availability, and scalability.

- Intelligent routing based on location, bandwidth, and availability, help to ensure you the best meeting performance every time—with over 99.99% uptime. Over 200,000 WebEx sessions per day flow through the WebEx Collaboration Cloud, adding up to over 785 million people-minutes per month by meeting attendees from over 150 countries.
- All meeting traffic on the WebEx Collaboration Cloud is globally load-balanced at all times so meetings can scale to meet demand, regardless of how many attendees are in your meeting.
- When joining a meeting, the WebEx Collaboration Cloud determines which point of presence has the lowest latency and offers the best performance, providing each meeting with the best possible audio, video, and data experience.
- Seamless and transparent global backup for data, audio, and video, ensure reliability throughout your meeting.
- All meeting data is kept secure through the multi-layered security model and through the enterprise policy controls inherent in the WebEx Collaboration Cloud.

Built to operate at less than half of its full capacity at any given time, the WebEx Collaboration Cloud is monitored constantly. As the usage of WebEx grows, hardware, bandwidth, and data centers are added to maintain idle capacity. Continuous improvements to the architecture help to ensure that every person attending your meeting has the best performance, every time.

Figure 1

Evaluating Cisco WebEx meeting applications

Enterprise-scale collaboration, which spans corporate networks and the Internet, requires a dedicated architecture optimized for on-demand collaboration. The WebEx Collaboration Cloud makes robust web conferencing available to the enterprise by:

- **Building a dedicated network as an overlay to the Internet.** The WebEx Collaboration Cloud links high-bandwidth dedicated lines with substantial, global connectivity to large Internet data centers, as shown in *Figure 1*. By providing ubiquitous access, the WebEx Collaboration Cloud carries both the voice communications and the rich media commonly used in web meetings today. This dedicated network was designed with enterprise-grade security to ensure communications are kept private and secure.
- **Creating a suite of meeting applications that run on the WebEx Collaboration Cloud, interconnected by a private system of distributed multimedia switches.** These collaboration switches carry session traffic generated by the Cisco WebEx application suite, and are managed at the back-end by a dedicated Operational Support System.
- **Populating the Cisco WebEx Collaboration Cloud with patented "Collaboration Switches,"** optimized for routing multimedia traffic between secure web clients. These multimedia switches are specially equipped to carry converged voice, video, and data with a high quality of service and very low end-to-end latency by separating voice and video from data, and prioritizing and routing them over the best possible path between collaboration endpoints.
- **Creating sessions spontaneously or on a pre-planned schedule.** Connections made between hosts and participants distribute live session data among the connections, and provide synchronous, real-time, and very low delay communications. The Cisco WebEx Universal Communications Format (UCF) compresses multimedia documents to reduce payloads over the network. This provides greater efficiencies and smoother flow in the web conference experience.
- **Switching all collaboration traffic over a dedicated infrastructure** with the least number of router hops, never storing data persistently with the capacity to scale to a large number of hosts or participants.
- **Protecting sessions with multiple forms of encryption**, over-provisioned capacity, real-time failover, and hardware redundancy.

Why not just use the Internet?

Giving everyone the potential to connect to anyone else on demand is one of the great benefits of the Internet. Unfortunately, this on-demand connectivity also creates the potential for significant, unpredictable Internet congestion. Working around predictable congestions during peak-time usage is sometimes possible, but frequent business users who depend on the Internet for some or all of their communications need reliable, *anytime*, on-demand access.

Traffic handled using a "best effort" method is the cause of public Internet congestion. Traffic doesn't take a defined or direct path from one point to another. There are no service-level guarantees that packets will reach their destination by a specific time—or ever reach their intended destinations at all. This "best effort" method is especially problematic when using the web for real-time communications—resulting in significant delays of audio, video, and presentations, and compromising the smooth flow of the online meeting session.

The only solution is to bypass much of the public Internet using a dedicated network that peers with the highest-capacity peering points when accessing the Internet, as shown in *Figure 1*.

Examining the Cisco WebEx Collaboration Cloud

The Cisco WebEx Collaboration Cloud is a global network, created with a carrier-class information-switching architecture. Only WebEx® traffic flows over the WebEx Collaboration Cloud as shown in *Figure 2*.

This network consists of application-specific multimedia switches at key peering points to handle rapid session traffic and guarantee a high quality of service for WebEx meetings. These switches are housed in highly secure Cisco data centers interconnected via dedicated lines that circumvent the public Internet. The network is purpose-built for real-time communications and has been specially formulated to minimize latency associated with TCP-layer flows. In addition, Cisco maintains global, high-bandwidth peering arrangements with telecom carriers for Internet access to provide web points of presence on a global scale.

Figure 2

Cisco locates data centers strategically near major internet access points to route meeting traffic around the globe, securely and reliably. In addition to these large data centers housing major meeting nodes, Cisco deploys nodes around the world. The network is built on fully-redundant clusters with Global Site Backup and an Enterprise Backup Solution. These services, and other facilities, form part of the Cisco WebEx Collaboration Cloud Operational Support System.

Defining the architecture

The WebEx Collaboration Cloud architecture protects all WebEx meeting applications including:

- Cisco WebEx Meeting Center.
- Cisco WebEx Training Center.
- Cisco WebEx Event Center.
- Cisco WebEx Support Center.

Every time you connect to a WebEx meeting, the Internet provides only the "first mile or last mile" of the connection. Once the connection is established, the WebEx Collaboration Cloud architecture manages all synchronous real-time interaction that make up a WebEx meeting, as depicted in *Figure 3*.

Users access WebEx applications through the WebEx Collaboration Cloud, which resides within the Web Zone. The Applications Program Interface ties the WebEx applications to the switching platform in the Meeting Zone within the WebEx Collaboration Cloud core. Numerous clusters of interconnected and distributed collaboration switches, their associated databases, and the logical and physical network infrastructure make up the WebEx Collaboration Cloud core. Multi-layer security components and the WebEx Operational Support System encircle the network with an additional layer of protection.

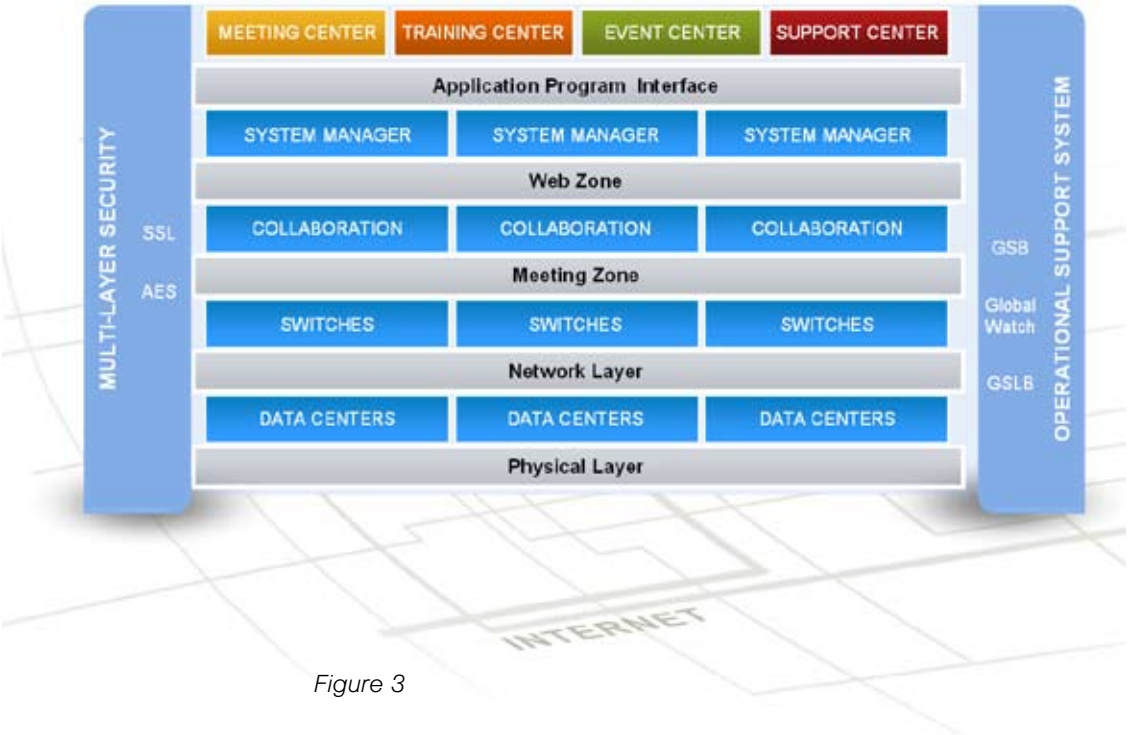

Figure 3

Switching on real-time web collaboration

WebEx meeting applications rely on data being distributed between meeting participants through the WebEx Collaboration Cloud, so no data needs to be stored on intermediate servers or internal hard drives—eliminating significant delays when forwarding data to participants. This switched approach minimizes transport time, reduces latency, enhances interactivity, and lowers the threat of data theft.

To accomplish these goals, SSL encryption protects meeting data, which once in the Collaboration Cloud, is then routed across the private WebEx backbone. The tight coupling of WebEx Collaboration Cloud switches over dedicated fiber lines helps to ensure a higher performance path between presenter and participants in collaboration sessions than the public Internet. In addition, to lower the burden on all networks involved in the transmission, the WebEx Collaboration Cloud evaluates and intelligently compresses multimedia imagery, documents, and screen captures prior to shipment from the host computer into and out of the collaboration network—in real time.

Because the WebEx Collaboration Cloud was designed with the capacity to handle ever-increasing meeting traffic, increasing the number of sessions will not degrade meeting performance.

All of these factors contribute to the high quality experience expected from an enterprise-class, real-time collaboration solution.

Guaranteeing high performance

Minimizing bandwidth, optimizing user experience: Cisco WebEx UCF

Achieving acceptable performance requires minimizing transport time between the meeting presenter and participants by lowering the bandwidth requirements of session data. The patented Cisco WebEx Universal Communications Format (UCF) drastically reduces payloads at critical times during a session by creating a portable document structure that eliminates redundant information.

Sharing presentations, text and graphical documents, video, and other multimedia files are typical activities in meeting sessions. Sent raw and uncompressed, sharing such files would add delay and interrupt the smooth flow of your meeting experience. Instead, UCF analyzes the object structure of each file, and minimizes redundancies. Once the presenter shares the minimized file with participants, the WebEx Collaboration Cloud accepts only major changes made by the presenter, significantly lowering bandwidth requirements for the session. The UCF performs vector conversions on all shared graphics, desktop images, and bitmaps to minimize bandwidth utilization and decrease session response time. The quality of the shared files is comparable to the original in all cases.

The WebEx UCF serves as a multimedia container that both encapsulates the available digital media and acts as a "play back" machine on each participant's computer. The presenter controls what goes into the WebEx UCF play back machine, the WebEx UCF converts the files to minimize bandwidth, the WebEx Collaboration Cloud enables significant changes, and the participants can play back the information without delay, for an optimized experience that facilitates collaboration.

Intelligent routing within the Cisco WebEx Collaboration Cloud

The WebEx Collaboration Cloud delivers real-time traffic reliably, using intelligent routing, Global Site Backup (GSB), and Global Server Load Balancing (GSLB).

First, based on the geographic location of WebEx meeting participants, the WebEx Collaboration Cloud determines the point of presence that offers the lowest latency and best performance.

Second, as a WebEx meeting host, you automatically get a backup site physically located in a geographically-distant Cisco data center. In the unlikely event that your primary customized WebEx site is unavailable, Global Site Backup (GSB) will automatically and transparently switch all meeting activity to the backup site. Meeting hosts and attendees won't even know that they are being redirected to a backup site and the meeting experience never changes. This ensures the highest service availability and enables WebEx to operate continuously without affect meeting activity. GSB provides real-time, two-way database synchronization between the primary site and the backup site, helping to ensure redundancy and disaster recovery both before and during meetings. (Find more information about GSB on p. 11.)

Third, Global Server Load Balancing (GSLB), is a load balancing design that helps traffic sent to the WebEx Collaboration Cloud to find the least congested switch, minimizing delays. So if one meeting switch has congestion, traffic is directed to an alternate switch, resulting in faster screen updates and synchronization among participants, and a better meeting experience.

Synchronizing voice and data

One of the central functions of the WebEx Collaboration Cloud is to synchronize voice and meeting data to all participants while maintaining very high data security and very low transport delay. In the architecture diagram shown in *Figure 4*, the switched services are built over the physical and network layers of the WebEx Collaboration Cloud. Here, meetings and other elements of real-time collaboration such as application, desktop, and multimedia sharing are transported to their destination. Switching and broadcasting also take place at this level, with full meeting authentications maintained throughout. This also coincides with WebEx multi-point audio or third-party voice bridging for both VoIP and POTS/PSTN inbound and outbound calls.

Advanced load balancing algorithms help the network adapt to varying load patterns. A distributed database housing data about your site configuration preferences, corporate brand, pre- and post-session information, and real-time routing data round out the core technologies of this platform.

The Operational Support System monitors and controls all these interoperating modules at all times.

Revealing the anatomy of a WebEx meeting

Outlining the anatomy of a WebEx meeting is a good way to understand the role and purpose of the various components of the WebEx Collaboration Cloud. For this WebEx meeting, let's assume the following criteria:

- A meeting host uses a custom-branded WebEx website to present or share information to participants who are either within an enterprise network, or remotely connected over the Internet.
- Participants may be using Windows, MAC, Linux, or UNIX computers in the meeting.

- This meeting uses either a teleconferencing (audio) bridge or VoIP computer connection.
- The presenter or participants have the option to use live or stored video.
- Security and other settings, as determined by the WebEx Site Administrator in the Site Admin modules, are in place.

Figure 4

Using the custom-branded WebEx site, a host sets up a meeting. The meeting carries on a dialog within the Web Zone of the WebEx Collaboration Cloud. Protected by HTTPS SSL secure communications over the Internet, the host invites participants and begins the meeting, as illustrated in *Figure 4*.

Next, the invited participants join the meeting through the custom-branded WebEx site of the host. After entering the meeting number and password, they are authenticated as live participants of the meeting.

All information and multimedia subsequently shown by the host or any other presenter to the participants is converted to the Cisco WebEx Universal Communications Format, (WebEx UCF). This reduces the payload to manageable levels while maintaining a very low interactive latency or delay. Data is encrypted with SSL and, optionally, with end-to-end AES encryption. When a user enables end-to-end encryptions, the data remains encrypted even while routing through the WebEx data center.

After encoding the multimedia data to WebEx UCF and encrypting it using SSL (and, optionally, with AES) the data transmits securely over the Internet to the WebEx Collaboration Cloud where it enters the Meeting Zone. Here it's switched and replicated in real-time to authenticated meeting participants. The multimedia session data is transmitted in WebEx UCF format using 128-bit SSL encryption and, optionally, 256-bit AES encryption, and delivered to each participant's computer. Once decrypted, and UCF decoded, the multimedia data is presented, virtually simultaneously, on each participant's computer screen. Since the participants are in a voice conference, the presentation time must be synchronous to all. The use of both the WebEx Collaboration Cloud infrastructure and WebEx UCF compression results in a smooth and immediate user experience with very low latency for all media.

Ensuring secure and reliable collaboration

Incorporating multilayer security

At every layer of its architecture, Cisco has incorporated the best possible security standards, relying on industry-standard technologies, best practices, robust third-party audits, and transparency with customers. All these measures provide the best, most secure and reliable web collaboration experience.

Figure 5 shows the interrelated elements of the WebEx security model for each functional level. At the Physical Security level, Cisco personnal provide required logistical, security, operational, and change management support to each WebEx data center worldwide—24 x 7. The Network Security Level helps to ensure secure meetings using encryption technologies such as SSL and AES. At the Meeting Security level, WebEx offers an array of permissions that the host can set, such as requiring passwords or making a meeting private rather than displaying a public listing. At the Site Security level, the WebEx Site Administration module provides many security options that Site Administrators can set through the Account Management module, including the creation of and criteria for passwords.

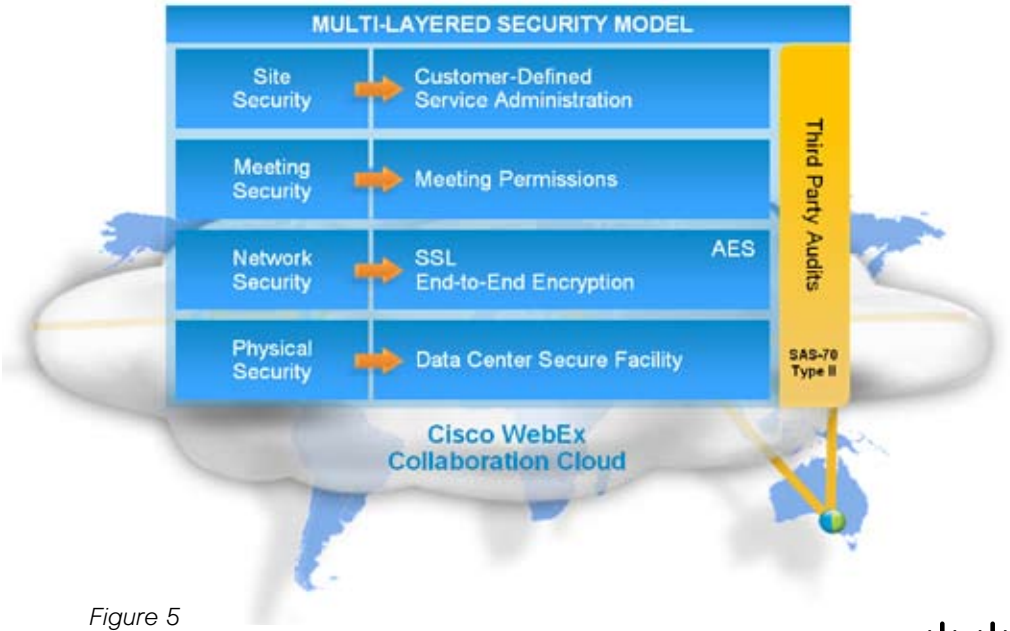

Figure 5

Beyond its own stringent internal procedures, the WebEx Office of Security engages multiple independent third-parties to conduct rigorous audits against internal policies, procedures and applications every year. These audits validate mission critical security requirements for both commercial and government deployments. Find more information on Cisco WebEx security, third-party accreditations, and independent audits in the *Security overview of Cisco WebEx solutions white paper.*

Managing enterprise policy

The Cisco WebEx Site Administration module gives WebEx Site Administrators the ability to set and enforce security policies across WebEx meetings at the enterprise, group, or individual levels, as illustrated in *Figure 6*.

Figure 6

For example, the presenter's ability to share their desktop or transfer files can be disabled on a per-site basis by customizing session configurations.

Each WebEx Site Administrator can use Site Security to delegate a level of policy management to meeting hosts, who can select which privileges to assign to participants. Each host can set passwords, access, and sign-in requirements, as well as choose to list meetings publicly, or keep them unlisted for privacy.

The Site Administrator has numerous options for controlling security. For example, the Site Administrator can restrict site access, requiring authentication for all users—hosts and participants. Enabling this setting requires authentication even to access site information (for example, listed meetings), as well as to gain access to meeting on the site.

Your enterprise can further protect its data by using a branded portal that contains a unique URL and provides the ability to set companywide security parameters, preferences, and other attributes.

While there is a minimum baseline security setting for all WebEx meetings, your Site Administrator can enact a variety of more stringent, security policy options, based on the policy preferences of your enterprise.

Supporting firewall and desktop lockdown

Most enterprises use firewalls, through which all traffic requesting to enter the corporate domain must pass. Each enterprise determines its own firewall policies and procedures. To account for these firewall policies and minimize the need for administrator attention, the Cisco WebEx client communicates through standard ports; HTTP on Port 80, or HTTPS signed by VeriSign, and encrypted with 128 bit SSL on Port 443. Additionally, WebEx may encrypt documents with Advanced Encryption Standard, or AES.

IT organizations in many enterprises now assign PowerUser rights rather than Administrator-privilege levels to the general user population. The result is that many users may no longer receive and install web client components distributed by third-parties. WebEx solutions fully support locked-down desktops, with client-side deployment fully controlled by the IT department using software distribution automation. Using the WebEx client download mechanism, participants don't need Administrator rights to their computers to participate in a WebEx meeting. WebEx auto-detects the privilege level, creates temporary user folders, and downloads clients securely for users without the ability to install applications.

Delivering availability and reliability: Global Site Backup

The Cisco WebEx Collaboration Cloud is designed for continuous service, 100% uptime, and very robust cutover to redundant meeting nodes during outages. If a customer's primary site is unavailable, GSB will automatically and transparently move all meeting activity to the backup site. A customer's site is physically located on switches at a specific WebEx data center. WebEx tracks session information such as scheduled start time, the session name, and the invitees on these switches. This data center is considered the customer's primary site location.

Every customer also has a backup site physically located in a geographically-distant WebEx data center. If a customer's primary site is unavailable, GSB will automatically and transparently move all meeting activity to the backup site. Neither hosts or participants know that they are being redirected to a backup site and the meeting meeting experience never changes.

As shown in *Figure 7,* the Global Site Backup (GSB) system facilitates continuous accessibility to WebEx meetings worldwide, and retains all attributes, address book, preferences, and meeting schedules for each branded WebEx site by:

- Ensuring the primary site and the GSB site use the same site URL and site ID.
- Proving two-way, real-time data replication between the primary and GSB sites.
- Scheduling one-way incremental file/branding backup from the primary site to GSB daily.

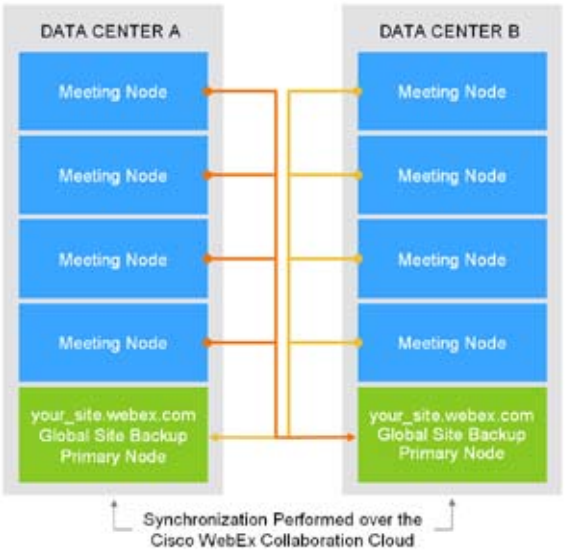

Figure 7

GSB provides for real-time, two-way database synchronization between the primary site and the backup site. Because of this synchronization, GSB provides redundancy and disaster recovery both before and during meetings. Additionally, because WebEx stores all usage information in a centralized meeting and scheduling database, all usage and billing reports will contain activity on both the primary and backup sites.

Managing capacity

Since there's no need to store meeting content, the main priority is the availability of WebEx Collaboration Cloud switching capacity. Switching capacity directly governs the total number of available sessions and potential participants. The WebEx Collaboration Cloud employs a mechanism called Global Switch Load Balancing (GSLB) that helps to ensure expedited meeting switching by accessing the least-used modules in the network. GSLB also handles SSL acceleration.

Facilitating high quality service

The Cisco WebEx Collaboration Cloud is a large, scalable, real-time communications platform designed to stay online perpetually. The platform delivers real-time transactions, process monitoring, fault tolerance, global backup, and load balancing. The Operational Support System (OSS), an integrated suite of back-end software, manages these functions.

The OSS reconciles services delivered to customers and handles firmware upgrades, network provisioning, system transaction monitoring, and performance data. The OSS facilitates a quick resolution to any service problems by making performance data easily available to customer service representatives, ensuring a high quality of service.

Gaining visibility into network usage

Global Watch, a part of the WebEx Collaboration Cloud OSS, is a browser-based remote monitoring application designed to probe the WebEx Collaboration Cloud during live operation. It can profile single or multiple host activity down to very fine granularity of function and offers visibility into performance and service. The rich function set of Global Watch displays data points such as network latency, and statistics of active and past WebEx sessions and provides advanced reporting.

Summarizing the benefits

The Cisco WebEx Collaboration Cloud is more than a network—it's a stable, secure platform for conducting real-time, on-demand web communications and collaboration. As a mission-critical platform, the dedicated WebEx Collaboration Cloud scales to meet increasing capabity, uphold rigid security policies, enforce stringent performance requirements, and maintain continuous availability and reliability. It's the WebEx Collaboration Cloud that helps to ensure that WebEx solutions delivers a ubiquitous and perpetual enterprise-class experience for you.