# Cloud onRamp for Office 365

## Optimizing SaaS connectivity using Cisco SD-WAN

As more applications move to the cloud, the traditional approach of backhauling traffic over expensive WAN circuits to the data center or a centralized Internet gateway via a hub-and-spoke architecture is no longer relevant. Traditional WAN infrastructure was not designed for accessing applications in the cloud. It is expensive and introduces unnecessary latency that degrades the user experience. The scale-up effect of the centralized network egress model, coupled with perimeter stacks optimized to handle conventional Internet browsing, often poses bottlenecks and capacity ceilings, which can hinder or bring to a stall a customer's transition to the SaaS cloud.

As enterprises aggressively adopt SaaS applications such as Office 365, the legacy network architecture poses major problems related to complexity and user experience. In many cases, network administrators have limited or even no visibility into the network performance characteristics between the end user and Software-as-a-Service (SaaS) applications. A "one size fits all" approach focusing on perimeter security without application awareness, which legacy network architectures often use, does not allow enterprises to differentiate and optimize sanctioned and more trusted cloud business applications from recreational Internet use. This results in the former being subject to expensive and intrusive security scanning, which further slows down the user experience.

Massive transformations are occurring in enterprise networking as network architects reevaluate the design of their WANs to support a cloud transition, reduce network costs, and increase the visibility and manageability of their cloud traffic while ensuring an excellent user experience. These architects are turning to Software-Defined WAN (SD-WAN) to take advantage of inexpensive broadband Internet services and to find ways to intelligently route trusted SaaS cloud-bound traffic directly from remote branches. Cisco® SD-WAN fabric is an industry-leading platform that delivers an elegant, simplified, secure, end-to-end hybrid WAN solution that can facilitate policy-based, local, and direct connectivity from users to your trusted, mission-critical SaaS applications, such as Office 365, straight from your branch office. Enterprises can use this fabric to build large-scale SD-WAN networks that have advanced routing, segmentation, and security capabilities with zero-touch bring-up, centralized orchestration, visibility, and policy control. The result is a SaaS cloud-ready network that is easy to manage and more cost-efficient to operationalize and that empowers enterprises to deliver on their business objectives.

A fundamental tenet of the Cisco SD-WAN fabric is connecting users at the branch to applications in the cloud in a seamless, secure, and reliable fashion. Cisco delivers this comprehensive capability for SaaS applications with the Cloud onRamp for SaaS solution, in alignment with Microsoft's connectivity principles for Office 365 (aka.ms/pnc).

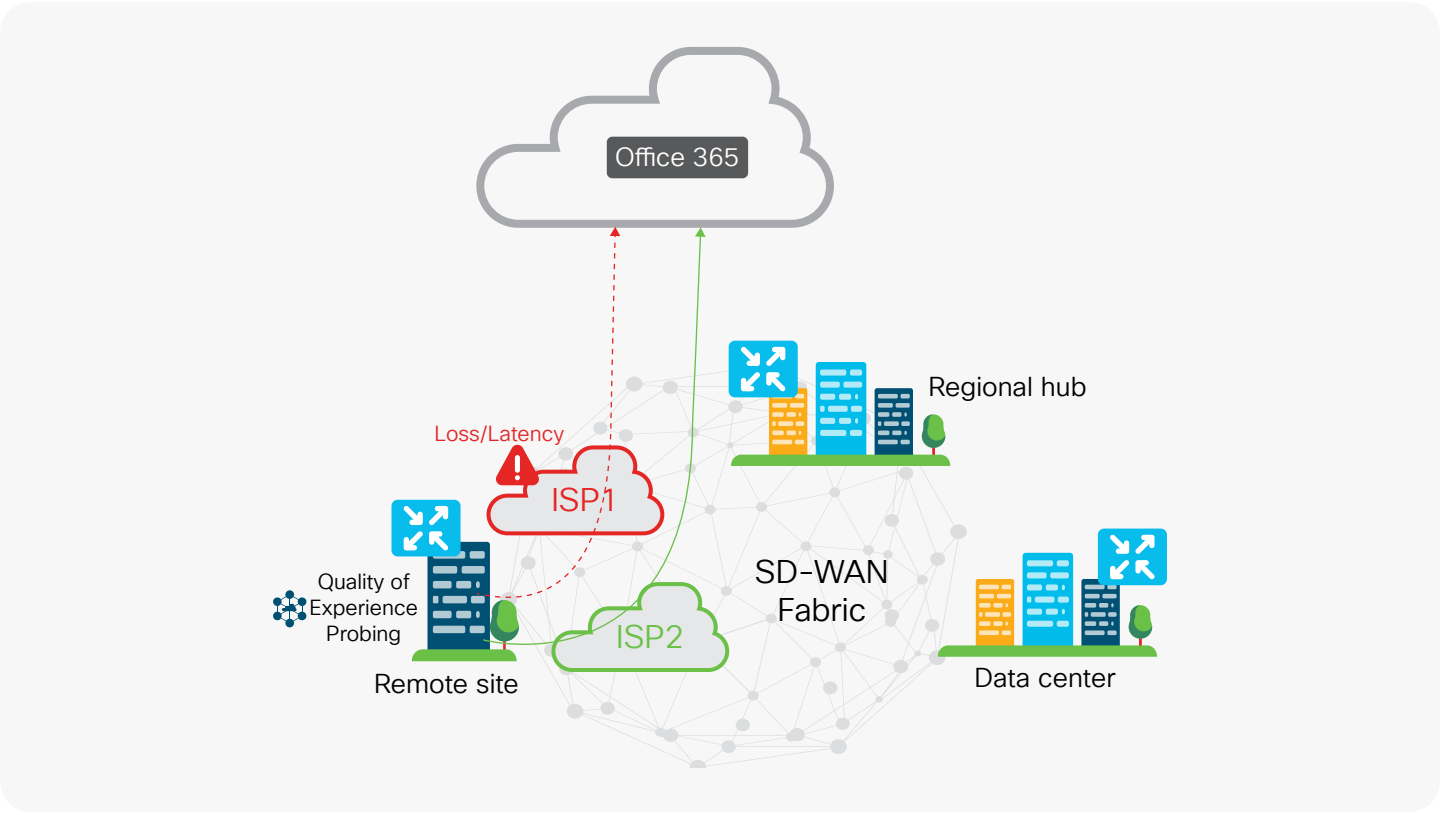
With Cloud OnRamp for SaaS, the SD-WAN fabric continuously measures the performance of a designated SaaS application through all permissible paths from a branch. For each path, the fabric computes a quality-of-experience score ranging from 0 to 10, with 10 being the best performance. This score gives network administrators visibility into application performance that has never before been available. Most importantly, the fabric automatically makes real-time decisions to choose the best-performing path between the end users at a remote branch and the cloud SaaS application. Enterprises have the flexibility to deploy this capability in multiple ways, according to their business needs and security requirements.

# Use case 1: Direct cloud access from a remote branch

Enterprises using a single or multiple inexpensive broadband Internet circuits at remote sites can enable Cloud onRamp on the branch router to permit traffic to Office 365 to break out directly to the Internet. Only trusted and critical traffic to Office 365 will be allowed a secure local breakout, while all other Internet-bound traffic will follow its usual path. For example, a customer can specify a policy in which the most performance-demanding and trusted Office 365 applications, such as Exchange Online, SharePoint Online, Skype for Business Online, and Teams, are permitted to take advantage of local and direct Internet connection, while the rest of user network communication outside of the customer network will be routed through the customer data center. Office 365 network traffic will be recognized and categorized by leveraging Microsoft Office 365 IP and URL web services. See details at aka.ms/IPURLBlog.

Cloud onRamp can also enable customers to achieve higher availability and better Office 365 experience by intelligently switching between several network paths based on measured availability and performance characteristics – for example, switching between two Internet egress links from different ISPs or providing a fallback path through an alternative network egress in the regional hub or remote data center (Figure 1).

Figure 1. Direct cloud access from a remote branch

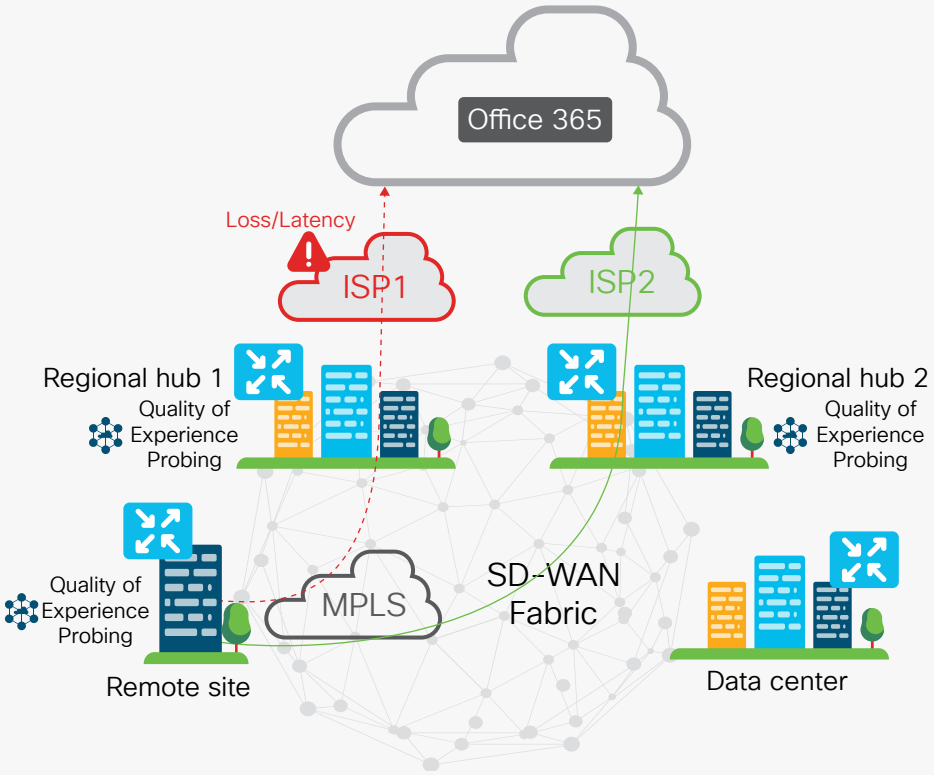


# Use case 2: Cloud access through the most optimal regional hub or carrier-neutral facility

For some enterprises it may not be practical to get Internet connectivity directly to every branch, and as an intermediate step they may want to use a regional hub egress architecture for their Office 365 traffic. While such architecture may not offer the same performance level and cost-effectiveness as local and direct Internet exit, Cisco SD-WAN can help ensure the best possible path through the available regional hub infrastructure.

In such deployments, Cloud onRamp can be deployed in a gateway mode, helping ensure that the optimal regional gateway is dynamically chosen for the customer's Office 365 application traffic (Figure 2).

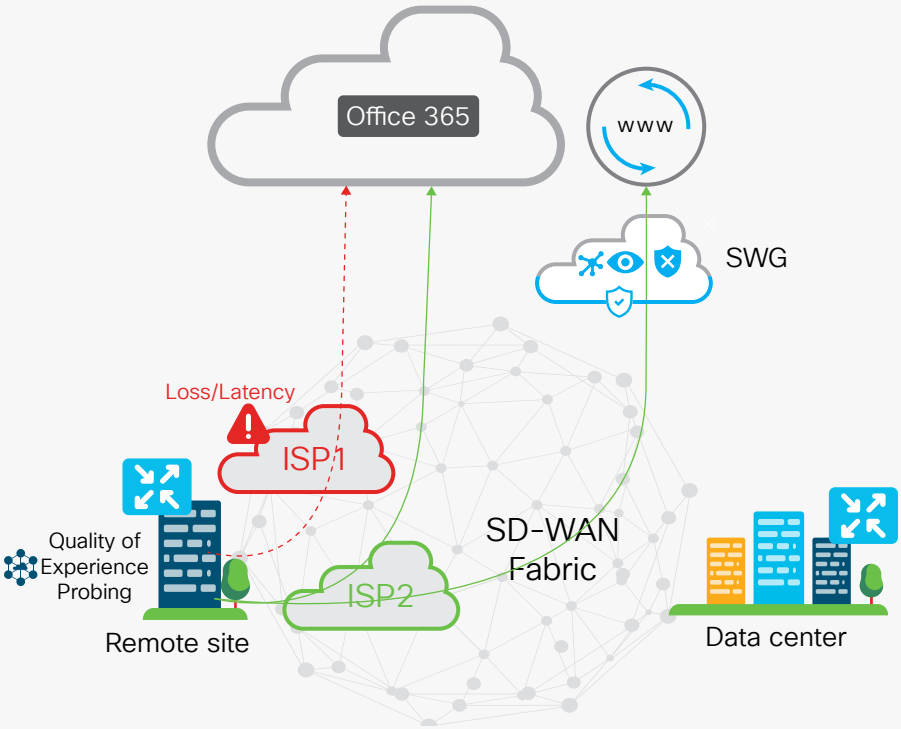
**Figure 2.** Cloud access through the most optimal regional hub



# Use case 3: Local Internet access through secure web gateways

In some deployments, enterprises connect remote branches to the SD-WAN fabric using inexpensive broadband Internet circuits, and they want to apply differentiated security policies depending on the types of services users are connecting to. For example, instead of sending all branch traffic to a Secure Web Gateway (SWG) or Cloud Access Security Broker (CASB), an enterprise may wish to enforce its IT security policies in a targeted manner by routing regular Internet traffic through an SWG, while allowing performance-optimal direct connectivity for a limited set of sanctioned and trusted SaaS applications, such as Office 365. In such scenarios, Cloud onRamp for SaaS can be set up to dynamically choose the optimal path among multiple ISPs, both for applications permitted to go directly and for applications that are routable through the SWG per enterprise policy (Figure 3).

Figure 3. Local Internet access via secure web gateways



# Summary

- Cisco SD-WAN technology enables enterprises to build a scalable and carrier-neutral WAN infrastructure, allowing them to reduce WAN transport costs and network operational expenses.
- Cisco SD-WAN enables customers to apply business-centric, application-aware, and differentiated routing policies – providing end users at the branch direct connectivity to performance-intensive trusted applications, such as Office 365, while routing generic Internet traffic via SWGs, CASBs, or the customer's data center.
- Enterprises can leverage Cisco's Cloud onRamp for SaaS capabilities to intelligently route Office 365 traffic, providing a fast, secure, and reliable end-user experience.
- All paths to Office 365 from each circuit at the branch, regional hub, and data center will be monitored continuously for performance, and the application traffic will be dynamically routed to the best-performing path without requiring human intervention.
- Cloud onRamp for SaaS provides network administrators superior real-time and historical visibility into application performance through a quality-of-experience metric.



C11-741353-00 09/18