WHITEPAPER

128 TECHNOLOGY

OPTIMIZING O365

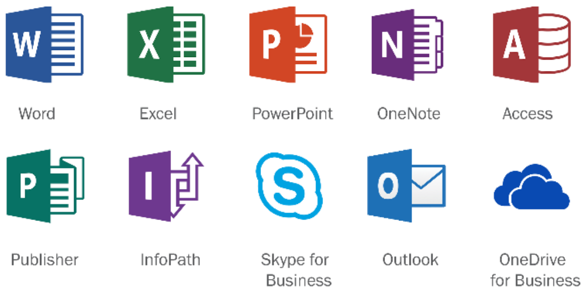
CONTENTS

INTRODUCTION

Software as a service (SaaS) allows users to connect to and use cloud-based applications over the network. Examples of SaaS solutions are Office 365, SharePoint, Salesforce, Box, ServiceNow, Workday, and others. As organizations move away from using on-premises predecessors to increasingly using SaaS solutions – the user experience can be severely impacted with traditional Software defined Wide Area Network (SD-WAN) and WAN Optimizer solutions. Network congestion is a huge cause for poor application performance and end user experience. Virtually all traffic today is SSL/TLS encrypted from the workstation to the cloud using keys that aren't readily accessible. This makes it impossible for traditional WAN Optimizers and legacy solutions to identify traffic and provide adequate Service Level Agreements (SLAs).

Gartner states that 78% of organizations are using or plan to use Office 365 and by 2019 half of those global deployments will face network related problems[1]. 20% of all organizations using Office 365 report service performance challenges today.

Each application in the Office 365 suite is deployed slightly differently; however, the major applications — Exchange Online, SharePoint Online/OneDrive and Skype for Business Online — are all implemented as a single active instance globally, per enterprise client, with failover instances at other data centers in the same Microsoft Region. Traffic to the Exchange Online traffic mailbox server is directed via client access servers, which are globally distributed, and each client's traffic can be directed to the most appropriate server. Yammer is only delivered from a limited number of U.S. data centers, regardless of the client's location.



Enterprises may deploy hybrid combinations of Office 365 together with some components, such as Skype for Business or SharePoint hosted in their own data centers or with third-party providers.

Office 365 is reliant on the underlying network transport, and will suffer service performance degradation issues if the underlying network is inadequately designed, provisioned, or implemented.

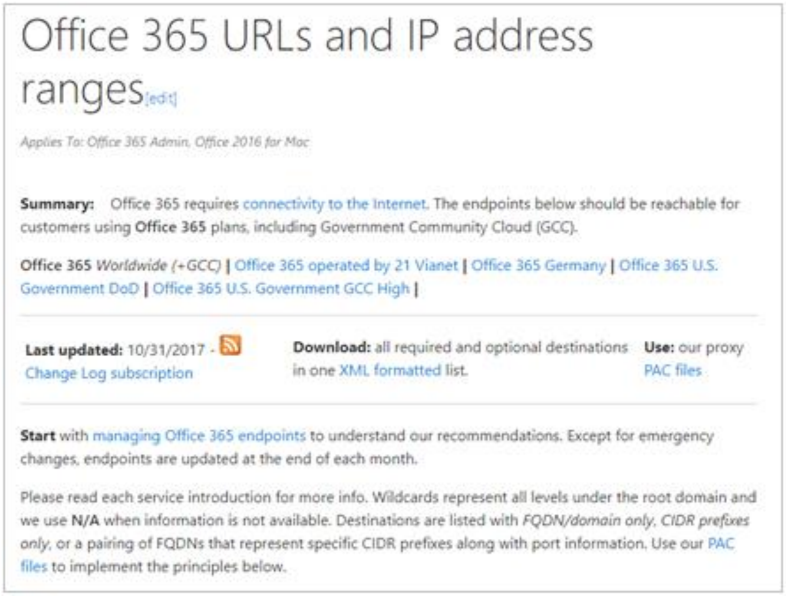
With low cost high speed Internet links and variety of direct connection techniques it is possible for an intelligent network solution to constantly monitor network paths and dynamically guarantee SLAs to Office 365 traffic. The 128 Technology solution can monitor different paths and ensure that Office 365 sessions are always kept on a path that provides the desired performance. Automatic detection of Office 365 applications enables to classify traffic and guarantee performance.

[1] Neil Rickard, Andrew Lerner, Bjarne Munch (2017). Network Design Best Practices for Office 365. Gartner.

IDENTIFY AND DIFFERENTIATE OFFICE 365 TRAFFIC

As customers migrate to Office 365 – there is a need to allow and provide special consideration to various workloads in the Office 365 product sets, such as Skype for Business, OneNote, Exchange Online, and so on. Microsoft publishes Office 365 over a huge range of URLs, and IP addresses. Microsoft dynamically publishes a fully up-to-date list of all IPs, URLs and ports used by each of the components of Office 365.

To classify Office 365 traffic, the 128T Session Smart router obtains IP addresses and FQDNs from the Microsoft site for the purpose of classifying Office 365 traffic. A network administrator can assign actions to take for such traffic depending on the needs of the organization. Identifying Office 365 network traffic is the first step in being able to differentiate that traffic from generic Internet-bound network traffic.



Office 365 URLs and IP address ranges[edit]

Applies To: Office 365 Admin, Office 2016 for Mac

Summary: Office 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using **Office 365** plans, including Government Community Cloud (GCC).

Office 365 *Worldwide (+GCC)* | Office 365 operated by 21 Vianet | Office 365 Germany | Office 365 U.S. Government DoD | Office 365 U.S. Government GCC High |

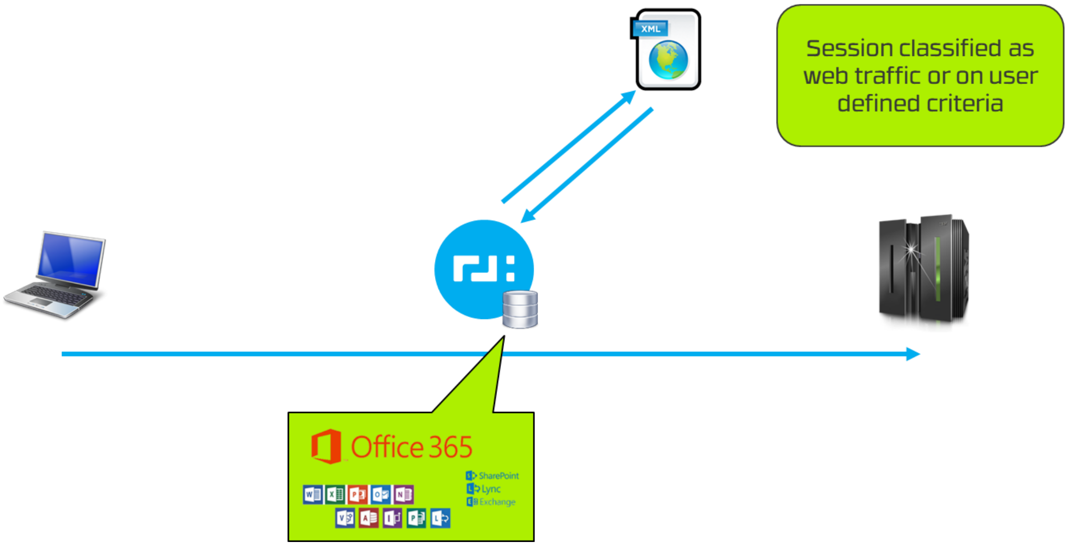
Last updated: 10/31/2017 - Change Log subscription

Download: all required and optional destinations in one XML formatted list.

Use: our proxy PAC files

Start with managing Office 365 endpoints to understand our recommendations. Except for emergency changes, endpoints are updated at the end of each month.

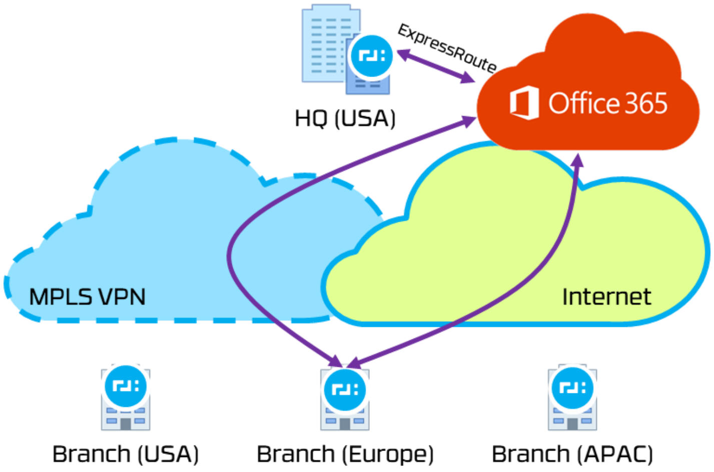
Please read each service introduction for more info. Wildcards represent all levels under the root domain and we use **N/A** when information is not available. Destinations are listed with *FQDN/domain only*, *CIDR prefixes only*, or a pairing of FQDNs that represent specific CIDR prefixes along with port information. Use our PAC files to implement the principles below.


XML
Session classified as web traffic or on user defined criteria
Office 365
SharePoint
Lync
Exchange

For example, if Skype for Business is being used for company meetings then the 128T router can dynamically detect those sessions and give it higher priority over low priority file transfers or other traffic. When bandwidth is constrained, using 128T router's Quality of Service (QOS) and traffic engineering capabilities can dramatically improve Office 365 performance.

An organization may have multiple connections to Office 365 via:

- Distributed Internet access
- Extending the enterprise WAN to the Microsoft Network Edge location or direct connectivity to ExpressRoute, using a dedicated or cloud exchange connection
- ExpressRoute directly to the enterprise's WAN provider

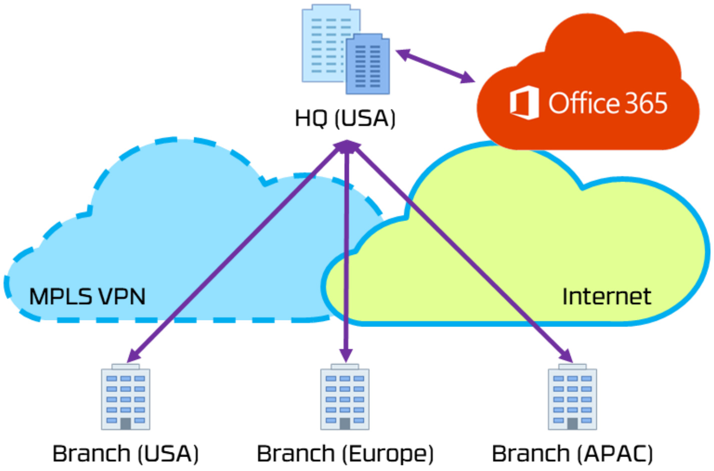


The 128T router can monitor latency, jitter, loss, and loads over these different paths and choose the optimal path for sending Office 365 traffic thereby guaranteeing performance for those sessions as needed. Choosing the optimal path will help minimize and stabilize latency between users and the Office 365 application. For Exchange Online deployments where latencies significantly exceed 50ms and SharePoint Online/OneDrive deployments where latencies significantly exceed 25ms, choosing an alternative path can mitigate the effects of latency and dramatically improve performance.

Enterprises can deploy the 128T router in Azure. This enables the enterprise to monitor paths to Microsoft's Azure Infrastructure as a Service (IaaS) before passing the traffic over an ExpressRoute connection reaching the Microsoft Network Edge. If multiple connections are available then the 128T router can monitor SLAs over these different paths and direct Office 365 traffic accordingly.

AVOID BACKHAUL AND NETWORK HAIRPIN

Most enterprise WANs are designed to backhaul network traffic to a central company head office or to a cloud security provider for processing before network egress to the Internet. Backhauling adds latency and directs traffic to distant Office 365 front end servers rather than those that are close to the user. Unfortunately, most SD-WAN solutions available today follow a hub-and-spoke model that backhauls traffic to a central location. This can lead to "tromboning" or needlessly long paths between the user and Office 365.



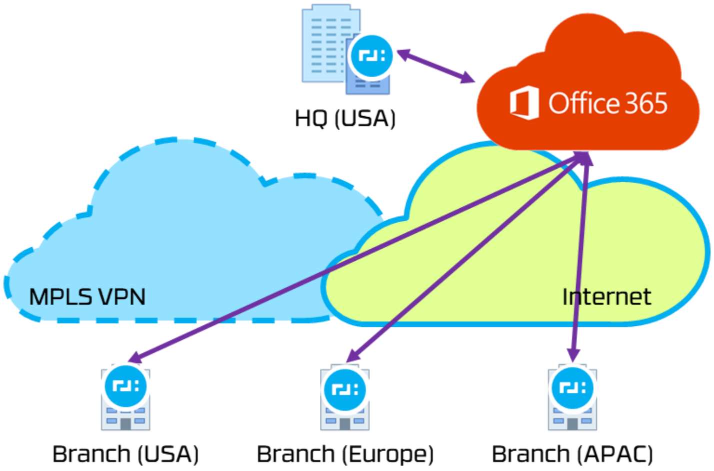
Many SD-WAN providers also have integrations with third party cloud security providers that backhauls traffic away from the user. Many of these cloud-based network security vendors have limited hosting locations and directs a user to a site that is distant from them. This may create a hairpin route where network traffic goes from the user to the distant network device and back to an Office 365 front end server that is near the user.

Many Office 365 applications use Domain Name System (DNS) requests to determine the user's geographic location. If the users DNS lookups are not done at the same point as the network egress the user may be directed to a distant Office 365 front end server.

Microsoft operates a large global network that includes many front-end servers around the world. In most cases there will often be a network connection and front-end server close to the user's location. The 128T solution does not require VPNs or tunnels to a central location. The tunnel free solution with no encapsulation ensures that Office 365 traffic can be easily identified.

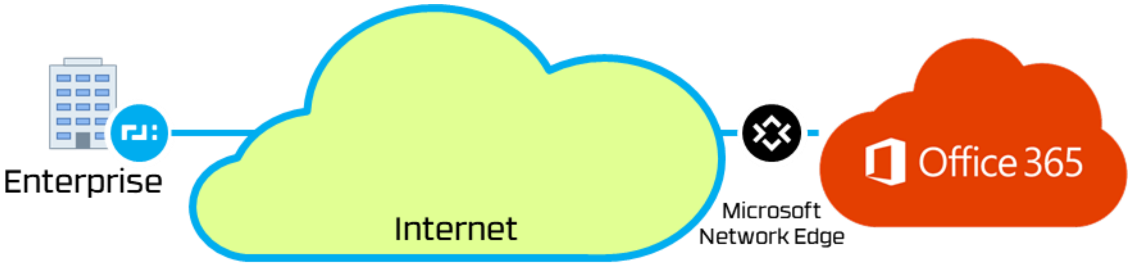
The 128T router follows a zero-trust security model without requiring backhauling traffic to a cloud security provider. Office 365 has many built-in security features such as Data Loss Prevention, Anti-Virus, Multi-Factor Authentication, Customer Lock Box, Advanced Threat Protection, Office 365 Threat Intelligence, Office 365 Secure Score, Exchange Online Protection, Network DDOS Security, and many other security features.

The 128T router provides users with local Internet egress and local DNS resolution. This ensures the traffic destined for Office 365 can connect to Microsoft's global network and Office 365 front end servers as close as possible to the user. Shortening the network path reduces latency to improve Office 365 performance.



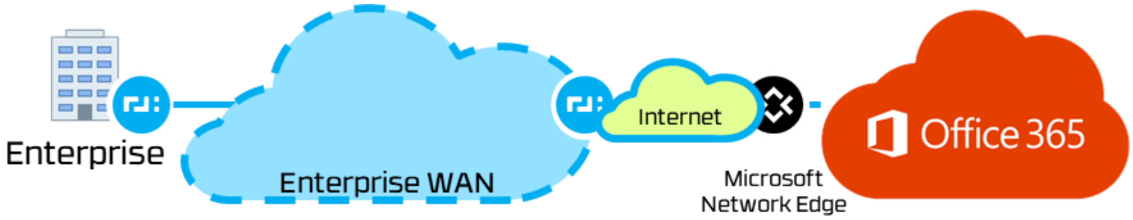
CHOOSE THE RIGHT CONNECTIVITY

Microsoft recommends round-trip latency below 275ms and ideally below 50ms for Exchange Online Traffic. Skype for Business is not latency sensitive when used for instant messaging. However, when it is used for voice and video like for conference calls when user traffic is sent via Skype for Business Online servers, Microsoft recommends that round trip latency not exceed 100ms.

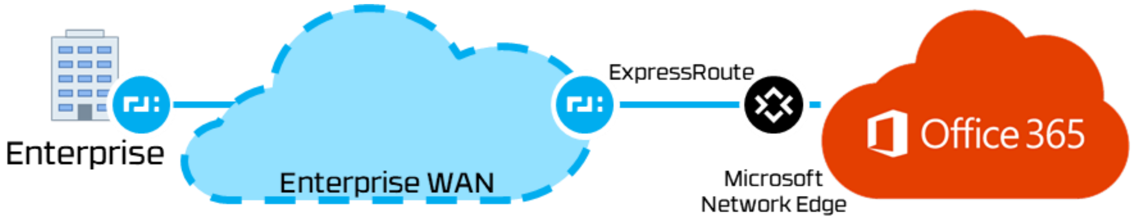


Distributed Internet access is the most popular method for enterprises to connect to Office 365 whose sites are geographically close to a Microsoft Network Edge location. 128T routers deployed in branch locations will enable improved performance and eliminate "tromboning" from any location.

Another option to improve performance and take out the uncertainty of traffic connections over the Internet is to utilize a provider to extend the enterprise WAN to connect to the Microsoft Network Edge locations. Placing the 128T routers at the edges of the enterprise WAN will ensure guaranteed SLAs for office 365 applications.



Direct WAN connectivity to Office 365 using Microsoft ExpressRoute is another option to improve performance. There are three variants of this approach, including a dedicated enterprise connection, connection via a cloud exchange (e.g., the Equinix Cloud Exchange) or a connection via the WAN providers cloud interconnect service (e.g., AT&T NetBond, Verizon Secure Cloud Interconnect, BT Cloud Connect).



Usually enterprises will combine multiple Office 365 connectivity options with some locations having ExpressRoute connections while others using distributed Internet access. The 128T routers are an ideal solution in this case as it can intelligently route Office 365 traffic over the most efficient connection depending on the location and the connectivity options available. Another option is to deploy the 128T router in Azure and pass the Office 365 traffic over an ExpressRoute connection. The 128T routers can prioritize Office 365 traffic over lower priority Internet traffic during congestion to ensure end user experience.

SUMMARY

The 128T Session Smart router can automatically identify Office 365 traffic. Based on the policies set by the network administrator and the connectivity options available the 128T Session Smart router can ensure that Office 365 traffic is sent over the best possible paths, has higher priority over competing low value traffic, and ensures end user experience. Networks can get congested and Internet links can suffer. It matters what the router does during those critical periods to provide a pleasant experience to the end user. 128T Session Smart routers are built to deliver exceptional SaaS and Office 365 experiences.

128 TECHNOLOGY

www.128technology.com | info@128technology.com