Redesigning network topology for modern app architecture

Microsoft IT is evaluating and implementing fundamental changes to the corporate network design and topology. Legacy network zones aren’t suited to support modern apps—so we’ve implemented solutions for these challenging scenarios, and we have a vision for Microsoft network connectivity and security.

Understanding networking for modern app architecture

Our vision for the cloud is that all of Microsoft runs in the cloud. In the end state, a vast majority of applications will be completely in the cloud, designed using modern engineering principles. This new modern app environment removes dependency on the server/client and multi-tier application scenarios. It uses modern platform-as-a-service (PaaS) components as the default building blocks for a business-focused app environment. Connecting users to modern cloud-based apps and services requires a different type of connectivity from what we’re accustomed to providing with our legacy network architecture. Modern apps built in the cloud don’t rely heavily on on-premises network connectivity, isolated components, and robust internal bandwidth. Instead, the modern app architecture favors Internet presence and defined connectivity models between app components. The user experience is based on highly available, robust Internet connectivity. As apps are transitioned from our internal corporate network to the cloud, the way our workers interact with the corporate network topology is changing, and they’re finding it difficult to effectively connect to different apps while they’re still connected to our corporate intranet.

We recognized that we needed to assess, redesign, and re-architect our network infrastructure to support the modern app environment and enable our workers to truly be mobile-first, cloud-first.

Implementing networking for modern app architecture

We’re implementing this networking transition for all non-domain-based corporate devices and functions that use our network or modify traffic behavior. This includes branch offices, clouds, datacenters, labs, offsite facilities, and edge networks. The primary vision for these objectives is to offer connectivity services that provide a great experience and maximum productivity, while enabling network policies that allow businesses to protect their services and data from misuse.

Our implementation is intended to establish a software-defined networking model that provides a common taxonomy, standard configuration, relevant monitoring, analysis of the environment, automation of services and a self-healing, policy-based virtual network infrastructure. We’re moving from a reactive network environment to a proactive model, in which we’re planning for the desired state of our network and managing it accordingly using standardized templates and a consistent taxonomy. In the future, we want to take this approach further to be predictive—using policy-based optimization, automated self-healing, and zero-touch provisioning.
The pillars of modern networking

We’ve created three pillars of modern networking that keep our networking team focused on supporting company objectives of being mobile-first, cloud-first and working toward building a network environment that enables the modern app environment. These pillars help support the creation of a network that provides the same type of experience regardless of global location or presence on the Microsoft corporate network.

**Internet first**

The Internet is the greatest enabler of mobile-first, cloud-first technology. We want our applications to be Internet-facing as much as possible and in turn, our workers. We want to remove the dependency of our apps on the corporate network, and have Azure as the default access point. The corporate network serves a significantly reduced role in the modern app infrastructure and a reduction in our corporate network saves costs, so we’re transitioning our networks accordingly. With so much of our app infrastructure in Microsoft Azure, we want our workers to be connected to the first and best network choice for Azure, the public Internet.

**Wireless first**

Wireless is the default network connectivity mechanism for the vast majority of the devices that our workers are connecting to our network, which has been driven by worker behavior and needs. As such, we want our wireless networks to be available everywhere and we want them to be the first choice for our workers to connect to. Wired network infrastructure for worker connectivity is used only for specialized scenarios that are unsuitable for wireless.

**Automation**

We want to manage and control the network with as little human interaction as possible. Automation is a critical part of moving our network toward the goal of being predictive.
Considerations for automation
There are several considerations for implementing automation within our network topology:

- There’s potential for conflict with existing network access strategies.
- There may be a lack of adherence to common software deployment models.
- There might be a conflict between the standardization that’s required for automation and flexibility for emerging business requirements.
- Processes need to change. We need to focus on business service functionality instead of the technology that supports it. Our network configuration standards need to be implemented organization-wide.

Establishing network access future state
Design and functionality changes to our networking service lines represent a fundamental shift in our approach to networking team structure. Previously, teams were aligned based on the technology they supported. This resulted in a lack of continuity and experience between different connectivity types. In our network access future state, establishing the network service lines illustrated in Figure 2 ensures that our networking teams are aligned with our business. They’re set up to serve business needs first, in much the same way that the software engineering teams have been aligned. With this realignment, our networking and software engineering teams are working within a common structure toward a common goal.

![Figure 2. Microsoft IT network access future state](image)

Access
The primary design for access is to create a wired and wireless layer that enables connectivity to the network. This layer provides client authentication and authorization, whether on-premises or off-premises. Our access objectives are to:

- Enable wireless-first connectivity scenarios.
- Provide a secure guest access model.
- Ensure robust remote access connectivity.
• Clearly define access segmentation models, separating managed and unmanaged devices and accounting for scenarios such as Internet of Things and Bring Your Own Device (BYOD).
• Drive Internet-first connectivity.
• Make optimized network access investments, focusing on capability, cost and non-complexity.

Considerations for access
To achieve these objectives, we have to consider several factors in the implementation and management of access within our network environment. These include:
• PC refresh cycles and retiring legacy systems.
• Partnership with product groups in domain join scenarios and to enable seamless connectivity over Wi-Fi.
• Network address translation placement and scaling for IPv6 first.
• Quality of services in an Internet-first environment.

Core
The core contains services for providing global connectivity between our campuses, remote offices, datacenters, Microsoft Azure, and the Internet. We’re implementing advanced transport and routing along with network virtualization to this core structure, which will be designed to:
• Transition to a transport network using service chaining.
• Logically separate traffic dependent on destination network.
• Provide segment routing.
• Use emerging overlay standards to simplify the routing plane.
• Use fault domains to provide resiliency.

Considerations for the core
There are several considerations for the core component that will affect design and deployment. These include:
• Availability or lack of availability of services in certain regions.
• Budgeting for new hardware and additional capacity to support core upgrades.
• Support for multicast in a virtualized network.
• Organizational support model for virtualized devices or virtual machines.
• Staff training to deploy and support the virtualized network.
• Implementation and engineering resource availability to perform the required work.

Services
There are several services that are provided to network clients that aren’t part of a specific app or business group—based function. These services are treated outside of the scope of separate app network architecture, but they’re still a critical part of network functionality. These include:
• Addressing and assignment, such as DHCP and IP address management.
• Name registration and resolution, and traffic management.
• Policy enforcement at locations, such as at edge firewalls.
• Several small, miscellaneous services, including acceleration, caching, site location, and time.

The services service is designed to enable revised placement of network services traditionally delivered from on-premises datacenters or branch offices. Primarily, we’ll leverage existing IP and networking services from trusted providers. We’ll investigate and evaluate appliances and modular platforms that could provide such services, thereby creating optimized connectivity to the Internet and public cloud.
Considerations for services
One of the most important aspects of services is the always-available nature that our workers expect. Our services, when deployed into a network environment that supports the modern app architecture, warrant some considerations:

- What does the support model look like for services outside of staffed locations?
- How do we manage new relationships with external service providers?
- How do we verify the authenticity and integrity of services delivered by partners and external service providers?

With these focus areas and the team structures in place, our overall vision and strategy is to move the topology of networking up the application stack. In the past, our network segmentation and topology could be easily drawn out with logical boundaries. The new structure will be determined by the applications and their connections to our workers and between applications, relying on the underlying network services. The design of this network will require far less human intervention for additions and changes, while allowing applications to scale up and down as needed. In addition to changes to the physical network, it also requires changes to the applications to ensure security and performance is inherent to their modern design.

Creating a service-oriented hybrid access service

The Enterprise Hybrid Connectivity (EHC) service is an example of how we’re moving our networking model toward better support for the modern app environment. While we’re moving toward a cloud-first networking environment, we must enable secure models to support the realities of traditional architectures now. EHC provides the framework for connectivity between Azure and our Microsoft domain networks, specifically to expose APIs or other app components that are currently being hosted on-premises to Azure resources as native Azure PaaS HTTPS REST services. EHC helps our software engineers gain access to APIs that might not be available in Azure or the public and use them in their Azure PaaS solutions. This makes it easier for our software engineers to develop in Azure PaaS and still have access to APIs that they require for their solutions. EHC is intended to further promote development in Azure PaaS and move our app portfolio toward cloud-first.

Design goals

We knew that enabling connectivity in the hybrid cloud needed to meet enterprise security and durability needs, and to adhere to our modern networking model. EHC takes on-premises APIs that can’t be re-architected for the cloud and makes them available for consumption in cloud apps that support modern engineering principles. With EHC, our development teams can pursue modern engineering in their solutions and still use APIs that would have been unavailable if not for EHC. EHC was designed using the pillars for modern networking and was aligned to the following goals:

- **Meet security control and compliance policy.** We needed to make sure that EHC would fulfill all standards for security, auditing, and compliance standards that affect our business.
- **Meet enterprise durability requirements.** We had to ensure that the solution was durable and scalable in an enterprise context, including high availability and disaster recovery requirements.
- **Minimize or eliminate impact to the legacy corporate network.** As much as possible, we wanted to simplify EHC offerings and reduce or eliminate the requirement for investment of capital or infrastructure on the corporate network.
- **Provide effective and efficient access.** We made sure that the EHC model was constructed to accommodate the scalable and elastic nature of Azure PaaS solutions.

Implementation and architecture

The EHC architecture incorporates Azure PaaS and networking components to ensure robust, controlled, and elastic connectivity between on-premises APIs and the Azure PaaS solution. EHC is deployed by a set of scripts that create
the platform components in an Azure subscription and configure telemetry and security for the platform. The key components include App Service Environment, Traffic Manager, Azure API Management, virtual networks, Azure Key Vault, and ExpressRoute.

We implemented two versions of EHC:

- **EHC Basic.** This version is focused on integration with compute instances hosted on Azure infrastructure as a service (IaaS). It takes on-premises APIs and exposes them to Azure by using Azure Active Directory or certificate-based authentication and Azure ExpressRoute to connect existing on-premises (or domain-attached IaaS) web services.

- **EHC Premium.** This version is focused on integration with compute instances hosted on Azure PaaS. It also uses Azure Active Directory and certificate-based authentication, along with Windows authentication using NTLM (via Azure Key Vault) for impersonation, or alternatively using Azure Active Directory or certificate-based authentication. It provides direct availability of on-premises APIs for consumption by Azure PaaS services that can interact with the APIs. The connection between Azure and the on-premises network is also established using ExpressRoute.

![EHC architecture](Image)

**Figure 3. EHC architecture**

**Conclusion**

Our fundamental changes to our network design and topology to better support the modern app environment will continue to grow and mature. As dependence on legacy network zones decreases and we implement solutions like EHC, we’re moving closer to a more efficient and predictive networking model. The alignment of our network teams has enabled us to adopt modern networking from the technology standpoint, and to move toward a culture of modern networking throughout our organization.

**For more information**

**Microsoft IT**


©2017 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.