INTRODUCTION TO BYON (BRING YOUR OWN NETWORK)



Signaling traffic is increasing in corporate IT networks, making it impossible for a single network system to satisfy the unique connectivity service requirements of every user. Cisco predicts that IP traffic will explode to 5 zettabytes (that's 5 followed by 21 zeros!) annually by the year 2022.

Of course, corporate IT network capacity is not growing at the same pace. An emerging and promising solution may be giving end-users the ability to establish alternative networks. This practice is known as Bring Your Own Network (BYON) and follows principles similar to the popular Bring Your Own Device (BYOD) movement.

How does BYON work?

Bring Your Own Network refers to virtualized WiFi networks that are dynamically established around specific devices using dedicated base station resources. BYON is designed to satisfy specific Quality-of-Service (QoS) requirements and are used as a secure gateway to other virtual networks. These base stations can be moved across geographic locations and can follow personalized service configuration policies. As a result, a mobile workforce can operate their own BYON and dynamically configure their virtualized network resources. In principle, additional frequency channels, WiFi, and wired interfaces can be assigned to the BYON network.

Business organization may not have the infrastructure resources to maintain high levels of QoS for a growing communications network. BYON addresses this limitation by allowing employees to set up a mobile hotspot using their own cellular or WiFi service. The network can migrate between

geographic locations following the BYON owner and be channeled as a gateway to the corporate network.

As an example, consider the case of an employee traveling abroad and using expensive roaming cellular service for corporate use. Cellular companies charge significantly more for international data roaming services; instead, employees can use a local cellular service for cost savings. Subscribing to a global wireless network service or creating mobile hotspots using local cellular service providers instead of relying on insecure public WiFi can be a cost-effective and secure BYON practice.

The service resources that constitute a BYON network can be migrated and localized. The devices are dynamically configured to avoid network congestion, maintain appropriate QoS, and enforce security policies. Latency issues are reduced since a local connectivity service is used and shared among a limited number of devices. If densely-located devices connect the network from a specific geographic location, the BYON service can migrate to nearby servers and prioritize the service quality for appropriate devices.

Efficient allocation of network resources requires accurate information regarding the number of devices and their data transmission requirements. However, this information is not always available before devices actively participate in the BYON network traffic. A strategic approach to establishing resource-efficient BYON networks might consider two common strategies:

- **Common slice.** This virtualization strategy makes a BYON network visible to every device within a geographic region surrounding the network base station. Standard authentication, access control, and security mechanisms may be used. The resources are shared among multiple devices. Unique IT service provisioning and management configurations are not applied to common slice networks.
- **Dynamic slice.** This invisible BYON network virtualization is designed to meet the requirements of specific service applications. The network slice can be dynamically configured to transition between different service-specific applications. The network can also be expanded continuously while maintaining a logical connection to the same base station. Configuration changes can depend on the sensitivity of data transmitted from the corporate servers and the number of devices connecting the network.

This resource provides a detailed overview of the Network Slice concept, especially in context of 5G communication systems.

BYON extends enterprise networks

The current state of IT service management and operations strategies for many organizations are often inadequate to extend the boundaries of the corporate IT network across disparate geographic locations. BYON networks effectively operate as virtualized networks that may be procured by the employees themselves, similar to BYOD devices. Multiple localized hosts can connect in a mesh configuration to form a virtual network with gateway connections to the corporate servers to access the necessary business information.

Most organizations experience a dynamic demand for BYOD devices connecting to the corporate network. IT security policies and configurations are traditionally developed for a limited number of managed devices, which leaves unmanaged devices as potentially vulnerable network end-points. With the prevalence of BYOD devices, organizations must incorporate support and prepare for unmanaged devices while mitigating the inherent risks. Instead of relying on static metrics and

controls associated with the infrastructure, external networks and devices must be evaluated dynamically to support BYOD initiatives. Following Mobile Device Management (MDM) can help companies address BYOD-related risks.

With the BYON system, devices can follow a model of stateless mobile architecture system. This approach allows IT to decouple protection from the underlying infrastructure and embed security controls at the application level virtualization. Instead of managing security at the external BYON network or devices connecting to the network, the security controls are applied to the data and traffic requests. For example, a mobile banking app transaction can be performed from any device and network. Security protocols are designed to verify the authentication information, device status such as jailbroken or OS version, banking details, location, and other real-time data to evaluate the trustworthiness of the transaction request. Not every device performing a mobile banking transaction is verified for security, but the associated information is adequately evaluated when the transaction is requested.

Cost benefits of BYON

The mobile, simple, and modular nature of a BYON network allows organizations to shift from a capital expense to an operational expense investment model. Instead of investing in the infrastructure resources, network bandwidth expansion and ongoing IT service costs, BYON resources can be acquired on a subscription basis. The corporate network can be optimized to handle fewer data transfers of large volume and the mobile last mile data communication of low volume characteristics can move to the cloud.

While BYON allows the application of security controls and IT service management policies in a decentralized fashion, using external virtualized networks for sensitive business operations comes with its inherent challenges. A lack of IT security policies designed specifically for unmanaged devices and networks with gateway access to the sensitive business information can lead to data leaks, network exploitation, and limited enforcement of regulatory policies. Effective BYON adoption will therefore require IT service management and security policies that limit risk exposure for data accessed via distributed, decentralized virtual networks.