The bridge to possible

Defining the Network for You

There are times when it can be fun to share things. Sharing a laugh with a co-worker will bring you closer together. Sharing a late night pizza with a friend is a cliché for a reason—because it's fun. Sharing the password to your favorite streaming service with a friend is a great way to keep up with bingeable content.

But connecting all of your devices on a shared network—like the ones found in college dormitories or long-term hospital rooms-isn't fun at all. Why? How many people are in the building? Two hundred? Two thousand? The onboarding of devices isn't secure and the shared network can be really large. Not only that, but there is limited user control over who can and can't be on the network. This means that if you can see all of their devices on the network, they can see all of yours. And if they can see yours, they may try to access them without your knowledge.

Cisco® User Defined Network (UDN) is about to change the shared network experience. A solution available from Cisco DNA Center (Available second half of calendar year 2020.), Cisco User Defined Network allows network administrators IT to give users control of their very own network partition. They can then remotely and securely register their wireless devices on their network, while at the same time getting access to everything they need outside the building or anywhere on the internet. Perfect for university dormitories or extended hospital stays, User Defined Network grants both device security and control, allowing users the ability to choose who can connect to their network.

How does User Defined Network work? After receiving an invitation, usually via an email, the user is able to register his or her wireless devices while at home or on campus through the Cisco User Defined Network app. None of our competitors offer the ability to personally register the devices from any location; instead, the user needs to physically be on campus. This benefit is because device registration is coordinated with the university network via the Cisco User Defined Network Cloud Service. This service is part of the licensing required for UDN. From there, the UDN cloud service communicates with Cisco DNA Center, the Cisco Identity Services Engine (ISE), and Cisco Catalyst® hardware at the university, which each individual's network as they desire.

What are the key features and benefits of the User Defined Network?

- A homelike user experience in a shared network environment
- Secure on boarding of personal wireless devices
- Ability to register wireless devices from the home network or anywhere
- Ability to limit access to personal devices
- Ability to invite trusted users to join the personal network
- Works on all kinds of authentication mechanisms, including PSK, 802.1X, and more
- Works on both existing and new deployments, meaning that a customer does not need to do significant work to enable the solution as long as they have all the components
- Protocol agnostic and works for mDNS (Bonjour), Universal Plug and Play (UPnP), broadcast, link local multicast, etc. and unicast traffic types

The bridge to possible

User Defined Network requirements

- User Defined Network app
- Catalyst 9800 Wireless Controller
- Identity Services Engine
- Cisco DNA Center
- Cisco Identity Services Engine (ISE)
- Cisco Aironet 802.11ac Wave 2 or higher access points

User Defined Network use cases

- Universities – specifically dormitories
- Hospitals
- Senior Living Facilities
- Hotels (long-term)
- Convention Centers
- Multi-tenant use cases

Being able to register wireless devices from anywhere allows for a simplified day-one experience that lets users start to enable their devices even before all of their devices are connected to the shared network environment, such as a dorm room network.

User Defined Network sounds great for the user, but what about the IT administrator? After the IT administrator deploys the User Defined Network to the network, they simply need to send the users instructions about installing the mobile app and registering their wireless devices at home. Once they head to campus the devices are available to use on day one.

That means fewer streams of support tickets and no mile-long queues filled with people with devices that can't connect to the network or can't be identified after they are on the network. In other words, IT administrators are able to get their big projects done without spending valuable office hours troubleshooting simple connection and visibility issues.

The security for IT admins is improved too, since UDN is paired with Cisco Identity Services Engine (ISE), the provisioning of policy is automated with all users' devices visible to the IT admin, with access to network resources controlled by IT too. UDN isolates a user's group of devices into their partition to effectively segment each users' devices from others within the same domain. In the event of a security incident, this shrinks the attack surface, limits the lateral spread of ransomware, and enables rapid threat containment. Now if a user clicks on the wrong phishing email, malicious traffic is no longer spread throughout the entire dorm and is contained within a single device or UDN.

Unlike similar solutions from competitors, User Defined Network users are able to see dashboards through the mobile app that displays detailed information about their private network. Not only that, but the mobile app allows the user to invite friends to the network with the flick of a finger—and also lets them remove people from their network with the same ease. The User Defined Network mobile app can be found in either the Apple App Store or Google Play.

What is sharing wireless devices like in a residential living environment? Sharing is fun, it's easy, you control who you are sharing with, and you don't have to reach out to campus IT to make it work.

C45-743573-00 06/20