

# Network Extension and VPN Glossary



This thread has been locked by a moderator.



👁 13

Based on popular demand [1], I decided to write up definitions for some of the terms we used in the Network Extension and VPN world.

If you have questions or comments, or suggestions for additional entries, please put them in a new thread here on DevForums. Tag it with *Network Extension* so that I see it.

Share and Enjoy

Quinn “The Eskimo!” @ Developer Technical Support @ Apple  
`let myEmail = "eskimo" + "1" + "@" + "apple.com"`

[1] Well, [one person asked specifically][refPD] (-: but I've seen a lot of confusion about this elsewhere.

[refPD]:

## Network Extension and VPN Glossary

This posts defines some terms used by the Network Extension framework and VPN.

### TN3134

THis section covers some of the terms used in TN3134 [Network Extension provider deployment](#).

Network Extension providers can be packaged in one of two ways:

- *App extension* — This is supported on all platforms. On macOS, which supports multiple users, the VPN interface is available globally but the provider is run in the context of the user who started the VPN. If that user logs out, the VPN interface goes down.
- *System extension* — This is only supported on macOS. The provider is run in a global context, so it's not affected by users logging in or out.

*App Store only* means that this option is only supported in App Store apps. This is relevant on macOS, where developers can distribute products independently using Developer ID signing. So, in the case of a packet tunnel provider on macOS:

- App extension packaging is only supported in App Store apps.
- System extension packaging is supported for both App Store apps and independently distributed apps.

*Managed devices only* means that the option is only supported on managed devices, that is, devices that are enrolled in an organisation's management system (MDM). This typically means that the feature has to be configured via MDM. For example, on iOS per-app VPN support only works on managed devices because your device manager must use MDM to set the `VPNUUID` property that associates the app with the VPN configuration.

*Supervised devices only* mean that the option is only supported on supervised device. A supervised device is a managed device that's owned by the organisation. This is in contrast to a [BYOD device](#), where the user owns the device but its enrolled in the organisation's management system.

### Other

*VPN On Demand* is the ability for a VPN to start automatically when an app connects to a server that's on the ‘far side’ of the VPN. Imagine you're in an organisation, `example.com`, where all your intranet services are within `corp.example.com`. To access those from outside you must go through the VPN. A site admin might configure VPN On Demand such that, when an app connects to anything with `corp.example.com`, the system will automatically start the VPN as part of the connection process.

*Per-app VPN* is a VPN configuration mode where a device manager can associate a set of apps with a specific VPN configuration. To continue the above example, an organisation might deploy a corporate directory app which connects to an directory endpoint within `corp.example.com`. In a BYOD scenario, they don't want other random apps on the user's device to be able to connect to that endpoint, and thus they deploy per-app VPN such that only their directory app can access it.

An app proxy provider always acts as a per-app VPN. A packet tunnel provider can work in one of two modes:

- In the normal mode, aka *destination IP mode*, packets are routed to the provider based on their destination IP address [1].
- In per-app VPN mode, aka *Source-application routing mode*, packets are routed to the provider based on their source application.

*Always-on VPN* is a feature of Apple's IKEv2 VPN transport such that the VPN is... well... always on. If the VPN can't come up, the device appears to have no network connectivity.

[1] Well, it's not quite that sample. I discuss this in more detail in the various subposts of [Extra-ordinary Networking](#).

Network Extension

Reply

Posted 4 days ago by eskimo

[Add a Comment](#)

This site contains user submitted content, comments and opinions and is for informational purposes only. Apple disclaims any and all liability for the acts, omissions and conduct of any third parties in connection with or related to your use of the site. All postings and use of the content on this site are subject to the [Apple Developer Forums Participation Agreement](#).

Platforms

iOS

iPadOS

macOS

tvOS

watchOS

visionOS

Tools

Swift

SwiftUI

SF Symbols

Swift Playgrounds

TestFlight

Xcode

Xcode Cloud

Topics & Technologies

Accessibility

Accessories

App Extensions

App Store

Audio & Video

Augmented Reality

Business

Design

Distribution

Education

Fonts

Games

Health & Fitness

In-App Purchase

Localization

Maps & Location

Machine Learning

Security

Safari & Web

Resources

Documentation

Curriculum

Downloads

Forums

Videos

Support

Support Articles

Contact Us

Bug Reporting

System Status

Account

Apple Developer

App Store Connect

Certificates, IDs, & Profiles

Feedback Assistant

Programs

Apple Developer Program

Apple Developer Enterprise Program

App Store Small Business Program

MFi Program

News Partner Program

Video Partner Program

Security Bounty Program

Security Research Device Program

Events

App Accelerators

App Store Awards

Apple Design Awards

Apple Developer Academies

Entrepreneur Camp

Tech Talks

WWDC