



MIF in Android 5.0

Pre-Lollipop MIF support

- One network at a time
 - Wifi, cell, BT, Ethernet
 - TYPE_MOBILE = 0, TYPE_WIFI = 1, ...
- One routing table, one default route
 - MMS / carrier app support via host routes
 - requestRouteToHost(**int**, **int**)
- Per-interface DNS using host routes
- Per-user VPN using iptables rules and local NAT44

Pre-Lollipop limitations

- Captive portal captivates entire device
- Very hard for app to select network
 - `startUsingNetworkFeature`, DNS, `requestRouteToHost` to each IP, ...
 - Host routes affect all apps on device
- VPN using NAT44 breaks end-to-end
 - Particularly bad for IPv6
- Hardcoded transport types
 - “Am I on wifi?” vs. “Is network unmetered?”

New APIs in Lollipop

- Maintain multiple networks at the same time
 - Based on [NetworkCapabilities](#): transport, resources, speed, ...
- [Network](#) object loosely equivalent to PVD
 - Currently, interfaces N:1 with [Networks](#)
- Apps can select network for:
 - Whole process: [ConnectivityManager.setProcessDefaultNetwork](#)
 - DNS lookup: [Network#getByName\(String host\)](#)
 - Socket: [Network#bindSocket\(Socket socket\)](#)
 - HTTP request: [Network#openConnection\(URL url\)](#)

VPN support in Lollipop

- Two modes
 - Secure: disallow traffic on other networks
 - Blocks MMS, link-local communication (e.g., MDNS, casting, ...)
 - Bypassable
- VPN apps can choose to offer service to specific apps
- The above in addition to existing split tunnel support
- IPv6 support

Current implementation

- Based on available Linux network primitives
 - Linux is based on the weak host model
- One routing table per interface
 - Routes from different interfaces don't stomp on each other
- Routing rules select networks
 - Switch between networks = change default rule
 - Select network = match rule
 - `SO_MARK` / `SO_BINDTODEVICE` / `in6_pktinfo` / permissions
- VPN using kernel per-UID routing

Initial use cases

- Graceful network transitions
 - LTE kept up for 30s after switch to wifi
 - Connections established on LTE stay on LTE
- Captive portal detection/login in background
 - You can still read email while you log in
- Avoid disconnected networks
 - Won't automatically connect to wifi AP that has no Internet connection
- Better application-facing API

Questions?