AUTOMATA

Technology Services

Optimizing Enterprise Networks

Enabling Apple Device Support
802.1X Enterprise Networks
Cisco Fast Lane
Content Caching

Apple Device Support

Lecture

Built-In Network Services

- VPN Support

  - IKEv2

  - Cisco IPsec

  - L2TP over IPsec

- Content Filtering through MDM restrictions and proxies

- Cisco Support

Apple Push Notifications

- Your network must support APNs

    - Proxies are okay as long as they don't inspect network traffic to APNs.

- Ports and Hosts

    - TCP port 5223 to communicate with APNs

    - TCP port 443 or 2197 to send notifications from MDMs to APNs.

    - Whitelist 17.0.0.0/8 address block.

Bonjour

- Apple's name for the zero-configuration network standard.

- Allows devices to automatically find each other on a network.

- Bonjour-enabled services include…

  - AirPlay

  - AirPrint

  - AirDrop

Enterprise Networks

Enterprise Networks

- Apple products require access to a variety of Internet hosts for many services.

- HTTPS Interception

- See the link in Resources for an exhaustive list of network configuration requirements for enterprise networks.

Optimizing Network Traffic

- Content Caching

- Filtering Content

- Managing DNS Traffic

- Proxies and Network Relay

- App Prioritization

802.1X WiFi Networks

Lecture

Wi-Fi Access

- Apple products support a host of authentication and encryption methods including…

  - Open, Captive, WPA2/3 Personal and WPA2/3 Enterprise

  - PSK, 802.1x and AES

  - RADIUS authentication

  - TTLS and PEAP

- Support wireless roaming via PMKID (Intel) and 802.11k,r,v in Apple Silicon Macs and iOS devices.

Wi-Fi Protocols

- 802.11ax (Wi-Fi 6, 6E)

- 802.11ac (Wi-Fi 5)

- 802.11n (Wi-Fi 4)

- 802.11g, 802.11b (Legacy)

WPA2/3 Enterprise

* WPA2/3 Enterprise authentication uses a RADIUS server for authentication.

* 802.1X Supported authentication protocols:

    * EAP-TLS

    * EAP-TTLS (MSCHAPv2)

    * EAP-FAST

    * EAP-AKA

    * EAP-SIM (carrier only)

    * PEAPv0 (EAP-MSCHAPv2)

    * PEAPV1 (EAP-GTC)

Connection Options

- Manually

- Via MDM Configuration Profile

  - Ensure the certificate from the RADIUS server is from a CA trusted by Apple's OSes, or…

  - Use a configuration profile to provide a certificate to establish trust of the RADIUS server cert.

  - Recommended to put these into separate configuration profiles.

Wi-Fi Connectivity Using SCEP

- Allows for automatic connectivity of devices to Wi-Fi networks using Simple Certificate Enrollment Protocol (SCEP).

- The SCEP payload allows an organization to support certificate identity authentication.

- Configuring SCEP allows devices to connect to the SCEP server to retrieve the required certificate(s).

Configuring 802.1X Wi-Fi
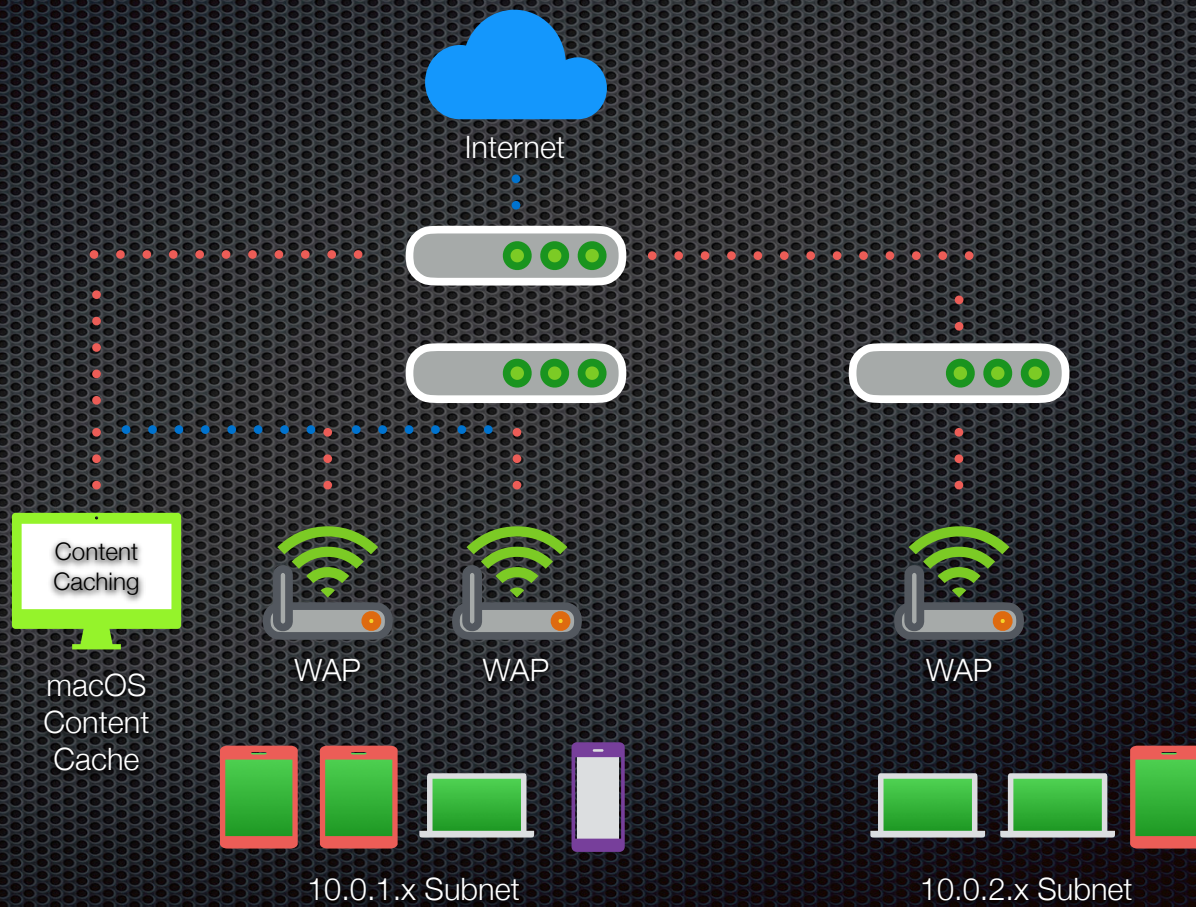
Practical Exercise

Content Caching

Lecture

Introduction to Caching

- Service that you can enable on any Mac.

- Benefits…

  - Reduce Bandwidth demands.

  - Faster Content downloads.

  - iCloud Caching

Types of Cached Content

* Apple Books content

* Apps and app updates from the App Store

* GarageBand downloadable content

* iCloud data (photos and documents)

* OS installers, updates, and Internet Recovery images

* Xcode downloads (simulators, SDKs)

* Rosetta 2 Executable for macOS

* Screensavers for AppleTV

* Schoolwork content (Apple Classroom)

Illustration

Internet

Content
Caching

macOS
Content
Cache

WAP   WAP   WAP

10.0.1.x Subnet   10.0.2.x Subnet

Configure a Caching Server

Practical Exercise