WiFi and Network Infrastructure
Best Practices

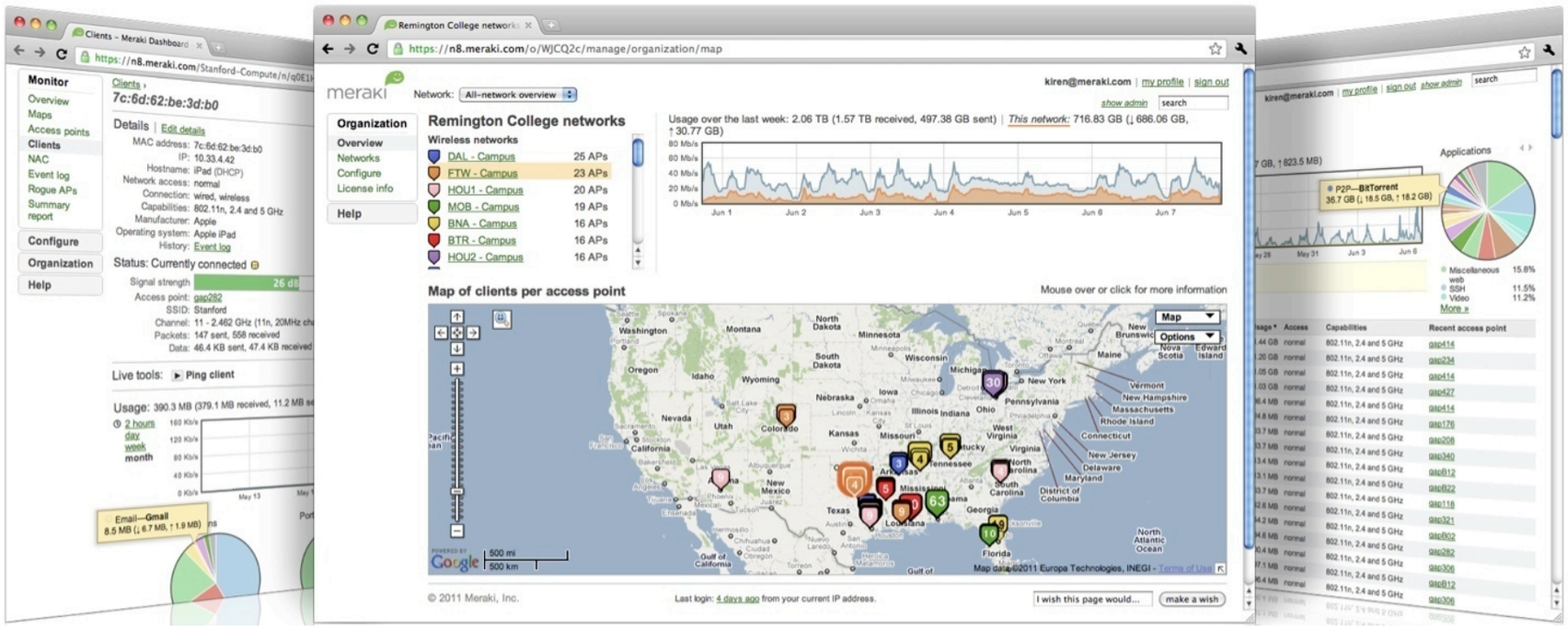
Pablo Estrada
Solution Architect
Meraki, Inc.

Agenda

- Meraki overview
- Wireless security and access
- Role-based policy enforcement
- Remote access
- Resource and application management
- Q&A

Meraki builds cloud-based networks that are easy to manage.

Wireless LAN, WAN and security product family



Cloud Managed Branch Routers and Wireless LAN
With Integrated Application, User, and Content-Aware Security

meraki

18,000 sites and 40 Million Clients Connected

meraki

Wireless security and access

Encryption: protecting data over the air

Admission control: who can join the network?

Admission control: who can join the network?

WPA2-PSK

- Easy to deploy, requires no integration
- Hard to scale, so best for small networks

Admission control: who can join the network?

WPA2-PSK

- Easy to deploy, requires no integration
- Hard to scale, so best for small networks

WPA2-Enterprise / 802.1X

- Scalable and has fine-grained control
- RADIUS integration with Open Directory, LDAP, OpenLDAP, AD

Admission control: who can join the network?

WPA2-PSK

- Easy to deploy, requires no integration
- Hard to scale, so best for small networks

WPA2-Enterprise / 802.1X

- Scalable and has fine-grained control
- RADIUS integration with Open Directory, LDAP, OpenLDAP, AD

Native LDAP / AD

- Scalable, easy to deploy
- No RADIUS configuration necessary
- Requires using splash page

Admission control: who can join the network?

Admission control: who can join the network?

MAC-based authentication

- Easy to deploy for small networks
- Hard to scale
- Not encrypted, MAC can be spoofed

Access control: what can they access?

Access control: what can they access?

NAT mode with LAN isolation: Internet-only access

- Ideal for guest access and unmanaged devices
- Protects internal network and isolates clients from each other

Access control: what can they access?

NAT mode with LAN isolation: Internet-only access

- Ideal for guest access and unmanaged devices
- Protects internal network and isolates clients from each other

Bridge mode: LAN / VLAN access

- VLAN tagging: tie SSID to a VLAN
- Firewall rules: restrict IP ranges, ports
- Policy firewall: user-driven firewall rules

Access control: what can they access?

Access control: what can they access?

Policy firewall example

- Students: Internet-only access, via content filter
- Teachers: Internet-only access, bypass filter
- Staff: internal and external access

Guest access and protecting critical assets

Guest access and protecting critical assets

Separate network, APs, switches, WAN uplink

- Suitable for sites with the highest security concerns

Guest access and protecting critical assets

Separate network, APs, switches, WAN uplink

- Suitable for sites with the highest security concerns

LAN isolation

- Isolates guests from internal network
- Secure (PCI-compliant)

Guest access and protecting critical assets

Separate network, APs, switches, WAN uplink

- Suitable for sites with the highest security concerns

LAN isolation

- Isolates guests from internal network
- Secure (PCI-compliant)

VLAN integration

- Requires some integration work and custom firewall rules
- Flexible and fine-grained access

Guest access and protecting critical assets

Separate network, APs, switches, WAN uplink

- Suitable for sites with the highest security concerns

LAN isolation

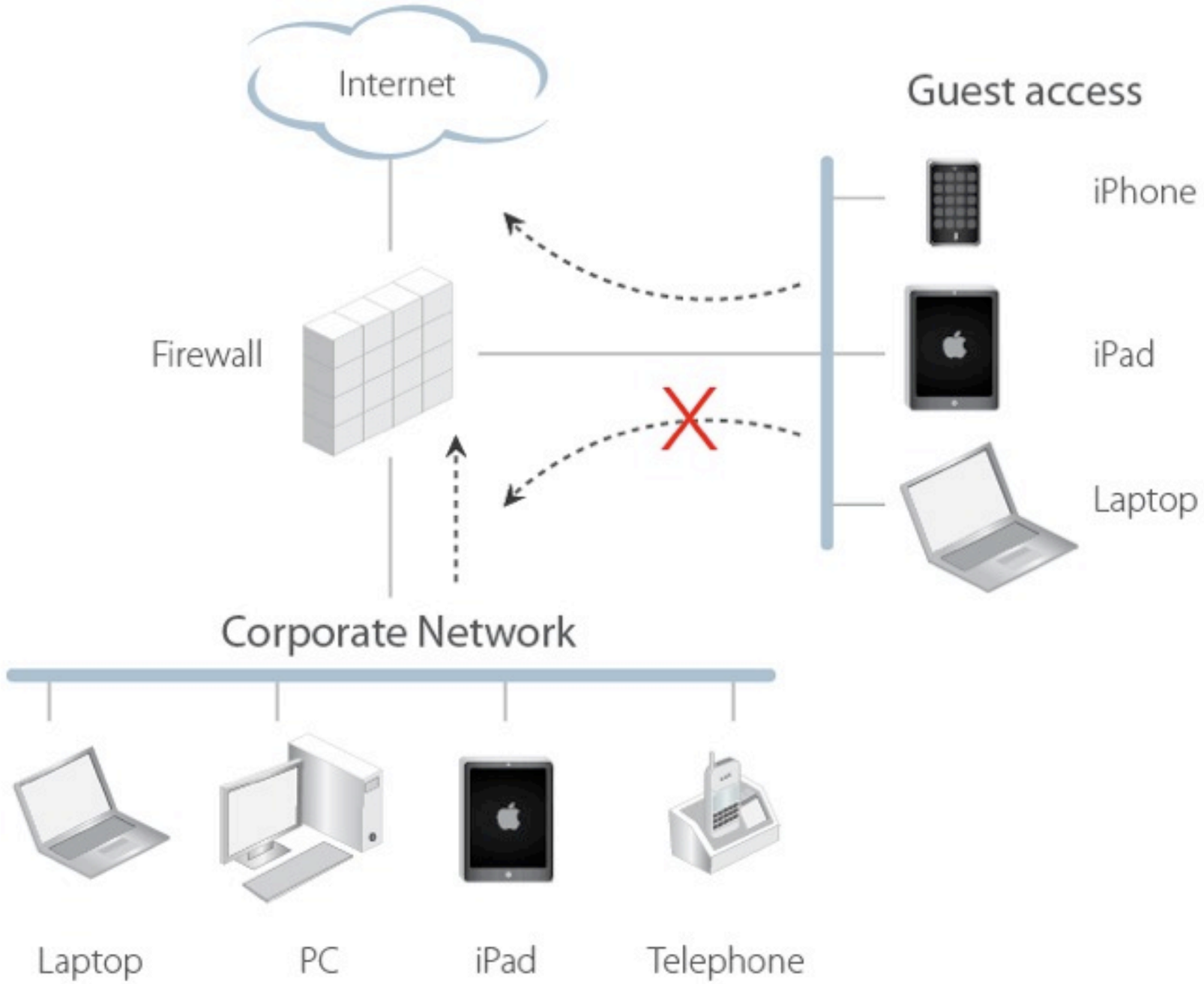
- Isolates guests from internal network
- Secure (PCI-compliant)

VLAN integration

- Requires some integration work and custom firewall rules
- Flexible and fine-grained access

Block access to LAN resources
(file share servers, etc.)

Secure Guest Access



Guest access: other considerations

Guest access: other considerations

Admission control

- Open network, WPA2-PSK, Lobby Ambassador

Guest access: other considerations

Admission control

- Open network, WPA2-PSK, Lobby Ambassador

Splash page

- Click to accept terms of service
- Show branding, advertisements, coupons

Guest access: other considerations

Admission control

- Open network, WPA2-PSK, Lobby Ambassador

Splash page

- Click to accept terms of service
- Show branding, advertisements, coupons

Restrictions

- Bandwidth
- Applications
- Content (sites)

Role-based policy enforcement

Role-based policy enforcement

Role-based policy enforcement

Access policies applied based on role / group

- Based on 802.1X / RADIUS
- Allows for fine-grained policy enforcement

Role-based policy enforcement

Access policies applied based on role / group

- Based on 802.1X / RADIUS
- Allows for fine-grained policy enforcement

Implementation

- Create groups for different employee types
- Upon authentication, policies applied based on RADIUS response

Role-based policy enforcement

Access policies applied based on role / group

- Based on 802.1X / RADIUS
- Allows for fine-grained policy enforcement

Implementation

- Create groups for different employee types
- Upon authentication, policies applied based on RADIUS response

Restrictions

- IP ranges, ports
- Bandwidth limits
- Content (sites)

Role-based content filtering

Role-based content filtering

Ensures compliance

- Especially important in sensitive environments, such as schools

Role-based content filtering

Ensures compliance

- Especially important in sensitive environments, such as schools

Organizational control

- Block adult content
- Block recreational content
- Block potentially illegal activity

Example: policy firewall and content filtering

Remote access

Why offer remote access?

Why offer remote access?

Remote employees

- Permanent staff
- Traveling employees

Why offer remote access?

Remote employees

- Permanent staff
- Traveling employees

IT / admin

- Sometimes useful to “tunnel in”
- Requires leaving a door open

Why offer remote access?

Remote employees

- Permanent staff
- Traveling employees

IT / admin

- Sometimes useful to “tunnel in”
- Requires leaving a door open

May not be desirable based on environment

Restrict based on “need to know”

Remote access

Remote access

Client VPN

- Used for remote employee access
- Requires client-side software agent
- Needs remote termination / configuration

Remote access

Client VPN

- Used for remote employee access
- Requires client-side software agent
- Needs remote termination / configuration

Site to site VPN

- Used to connect multiple offices together
- Transparent to clients
- Normally requires tedious VPN appliance configuration

Remote access

Remote access

Teleworker VPN

- Used for remote employee access
- Doesn’t client-side software agent
- Extends the corporate network to the home via an access point
- Needs remote termination / some configuration

Resource and application management

Resource and application management

Resource and application management

Global settings

- Use for broad policy enforcement
- Choose restrictive settings carefully!

Resource and application management

Global settings

- Use for broad policy enforcement
- Choose restrictive settings carefully!

Application traffic

- What's on your network?
- What are your users doing?

Resource and application management

Global settings

- Use for broad policy enforcement
- Choose restrictive settings carefully!

Application traffic

- What's on your network?
- What are your users doing?

Goal: ensure a proper experience for all wireless users

Resource and application management

Resource and application management

Understand

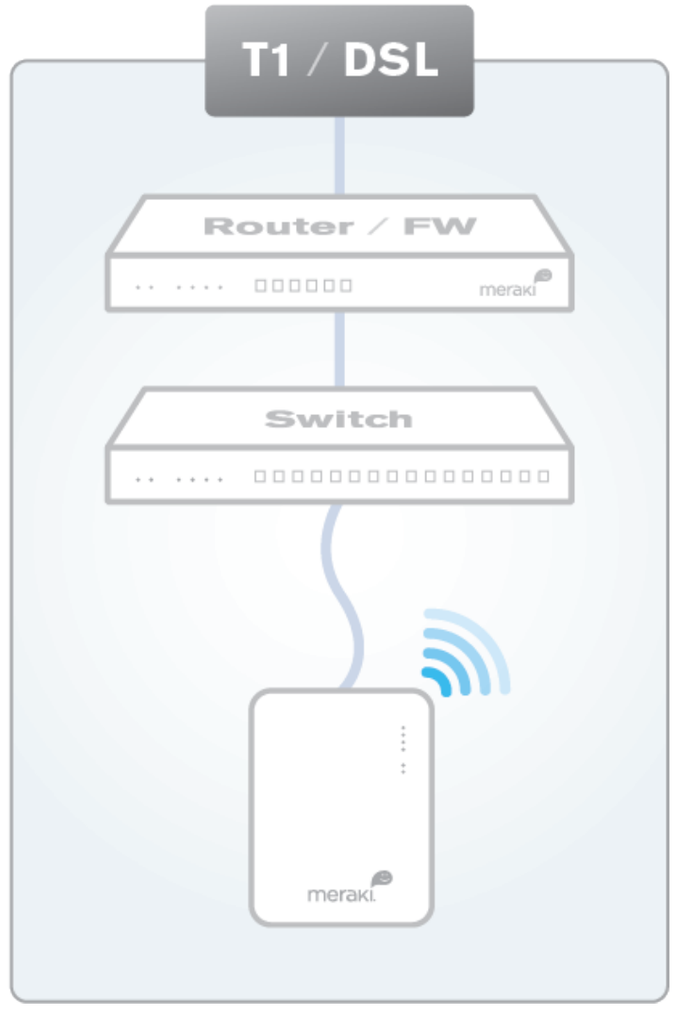
- Visibility into traffic and users is critical
- Enforce policies and deploy services based on needs of the network

Resource and application management

Understand

- Visibility into traffic and users is critical
- Enforce policies and deploy services based on needs of the network

Points of insight



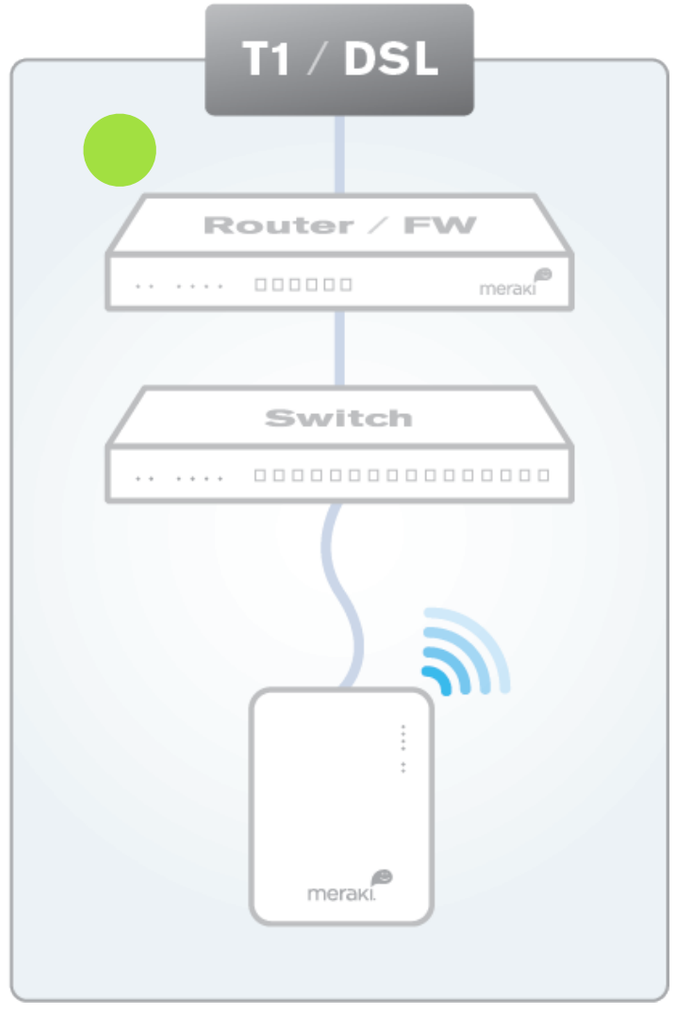
Resource and application management

Understand

- Visibility into traffic and users is critical
- Enforce policies and deploy services based on needs of the network

Points of insight

- Network perimeter



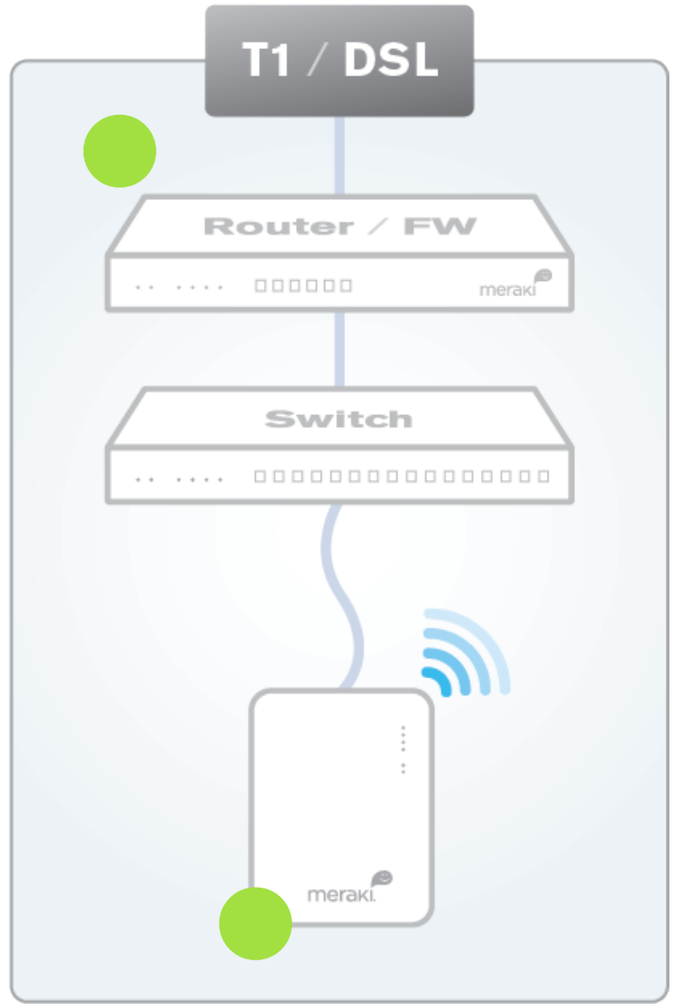
Resource and application management

Understand

- Visibility into traffic and users is critical
- Enforce policies and deploy services based on needs of the network

Points of insight

- Network perimeter
- Network edge



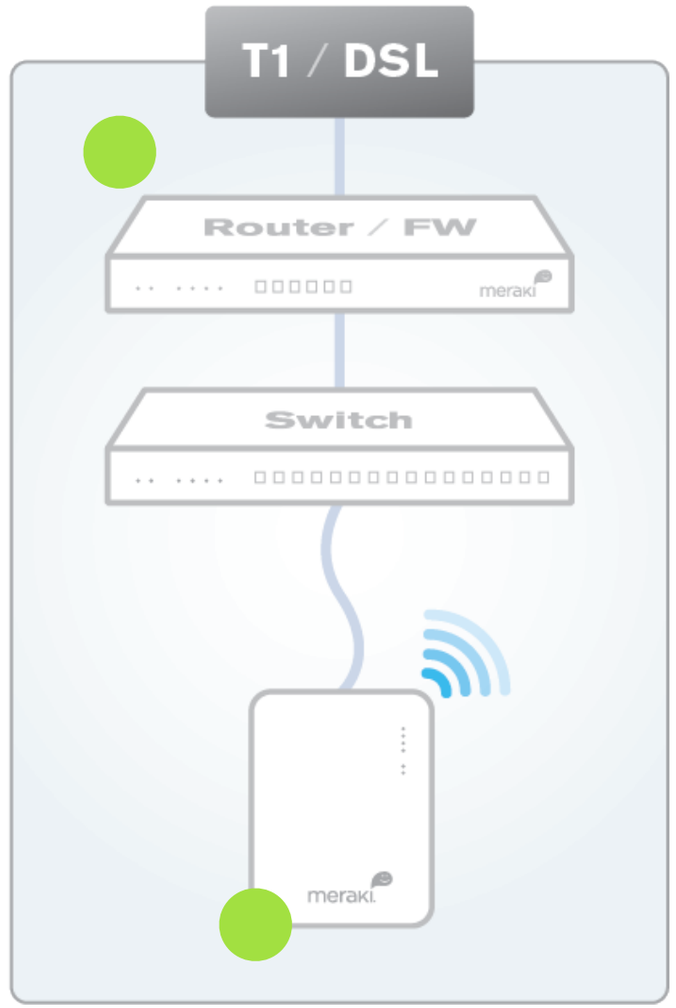
Resource and application management

Understand

- Visibility into traffic and users is critical
- Enforce policies and deploy services based on needs of the network

Points of insight

- Network perimeter
- Network edge
- Requires layer 7 insight



Resource and application management

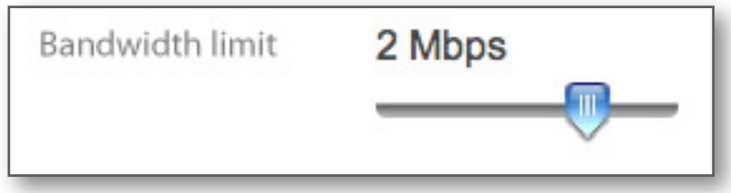
Resource and application management

Restrict recreational traffic

- Throttle undesirable applications
- Throttling still allows access, but creates a less than ideal experience
- Ensures bandwidth isn’t being used primarily for non-critical traffic

Resource and application management

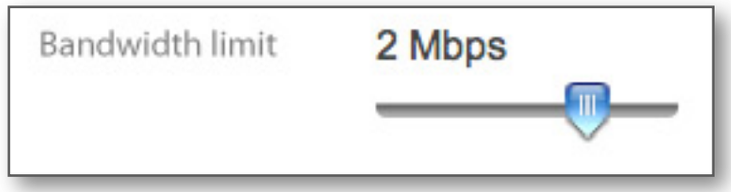
Restrict recreational traffic



- Throttle undesirable applications
- Throttling still allows access, but creates a less than ideal experience
- Ensures bandwidth isn't being used primarily for non-critical traffic

Resource and application management

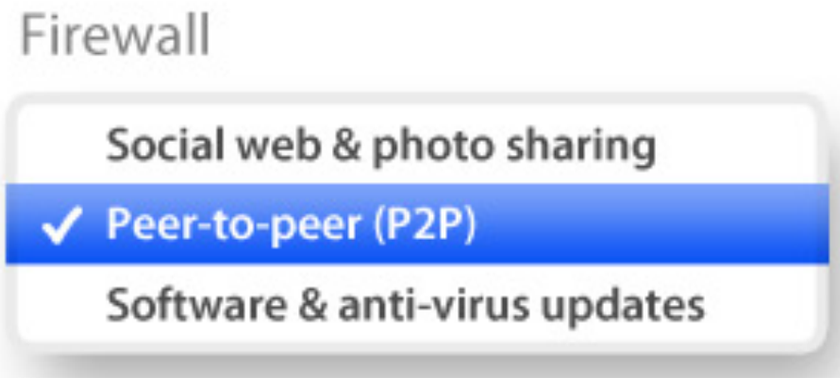
Restrict recreational traffic



- Throttle undesirable applications
- Throttling still allows access, but creates a less than ideal experience
- Ensures bandwidth isn't being used primarily for non-critical traffic

Block unwanted traffic

- Especially important to meet compliance requirements
- Eliminate malicious or destructive applications
- Requires a layer 7 firewall



meraki

Resource and application management

Resource and application management

Prioritize critical traffic

Resource and application management

Prioritize critical traffic

- Services critical to the organization must work!
  - email
  - VoIP / video conferencing
  - CRM, internal apps

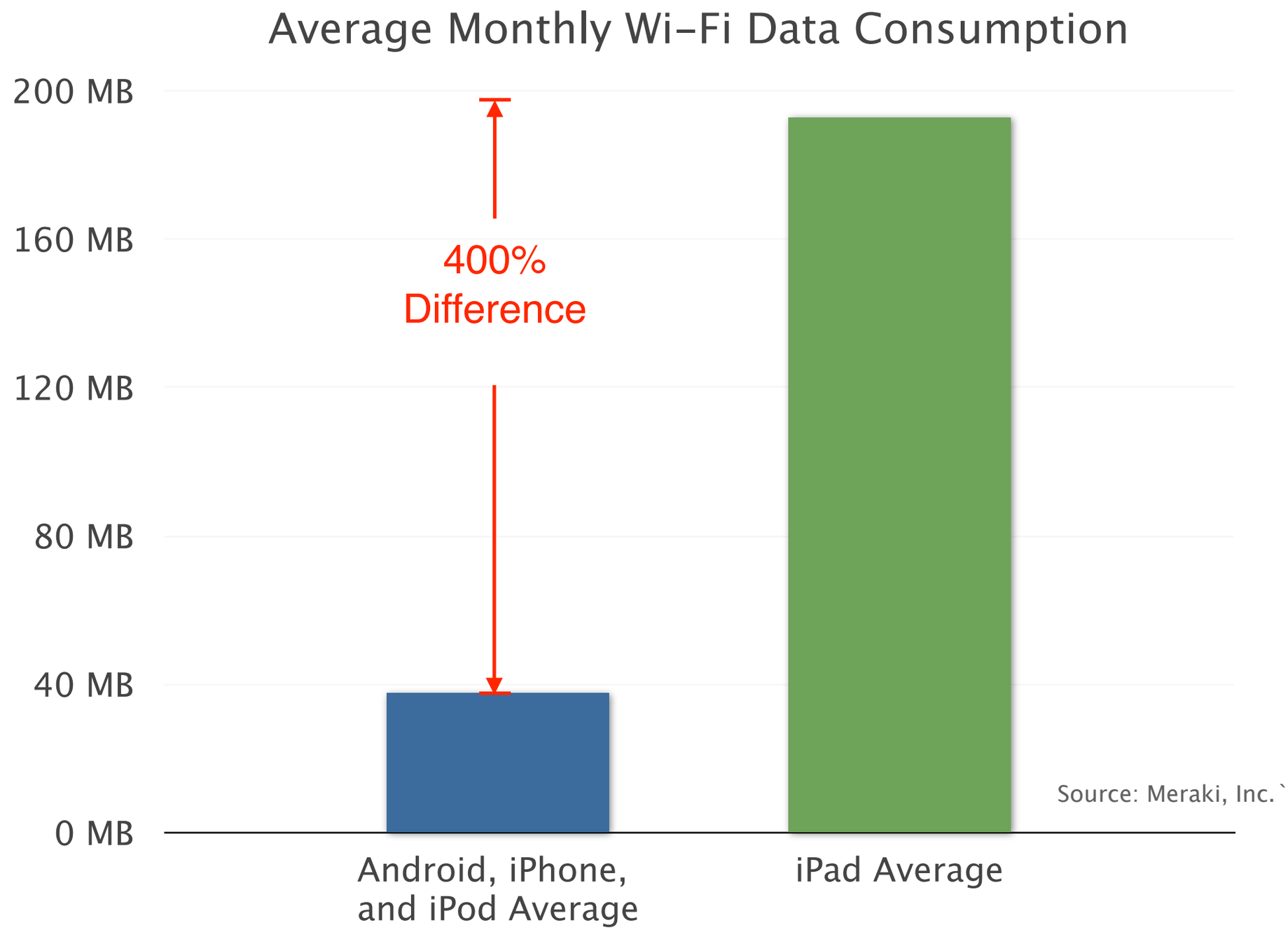
Resource and application management

Prioritize critical traffic

- Services critical to the organization must work!
  - email
  - VoIP / video conferencing
  - CRM, internal apps

Prioritizing critical apps and throttling undesired ones helps ensure IT serves the business needs

iPad Wireless Data Consumption



Q&A

meraki®

Networks that simply work