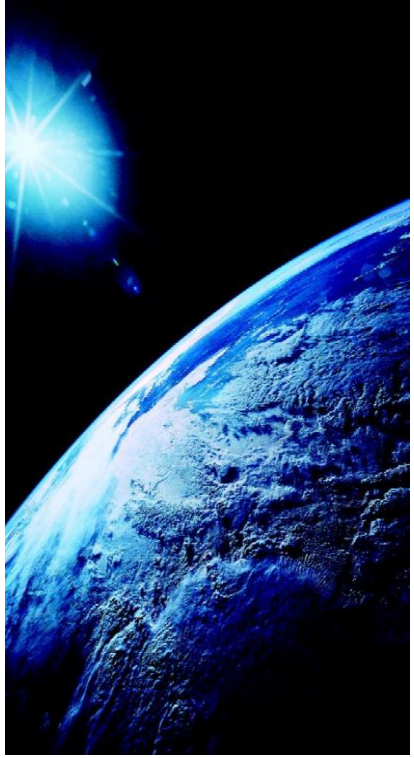
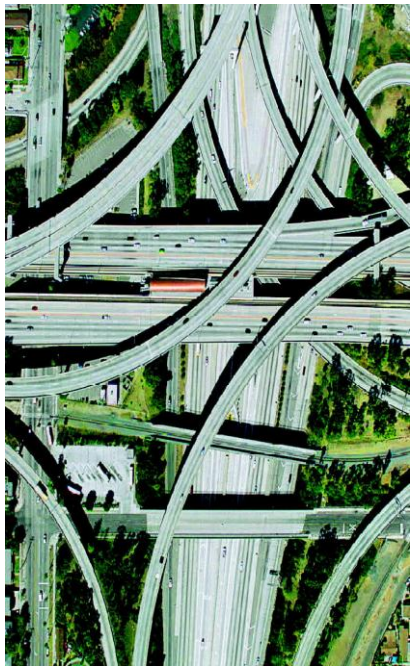
Cisco Connect

Praha, hotel Clarion
10. – 11. dubna 2013





Sjednocení různých typů přístupů k síti

přístup pod kontrolou snadno a rychle

ARCH1 / L2

Radek Boch, CCIE # 7096, Cisco
Adam Horník, Dimension Data

Úloha sítě?

- … Top Level Management má v oblibě …
- … IT Operations Team využije …
- … Pro Security Team je to „noční můra“…

Prostě se připojit!

Rozuměj: „bez námahy ale kontrolovaně připoj jakékoli zařízení, včetně tradičních“

Megatrends: Evolving User Workspace

BYOD
- Secure access
- Customized experience
- Guest access

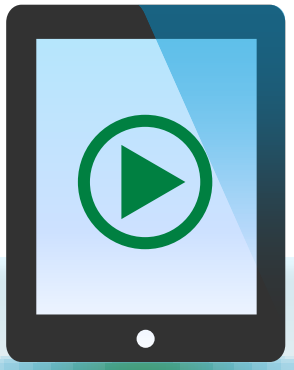
Mobility
- Seamless roaming
- Optimal client performance
- Cloud access/VXI

Video
- Multicast streaming
- Video conferencing
- Reliable performance

IT Requirement

Deliver an Uncompromised User Experience on Any Workspace

Uncompromised User Experience - Challenges

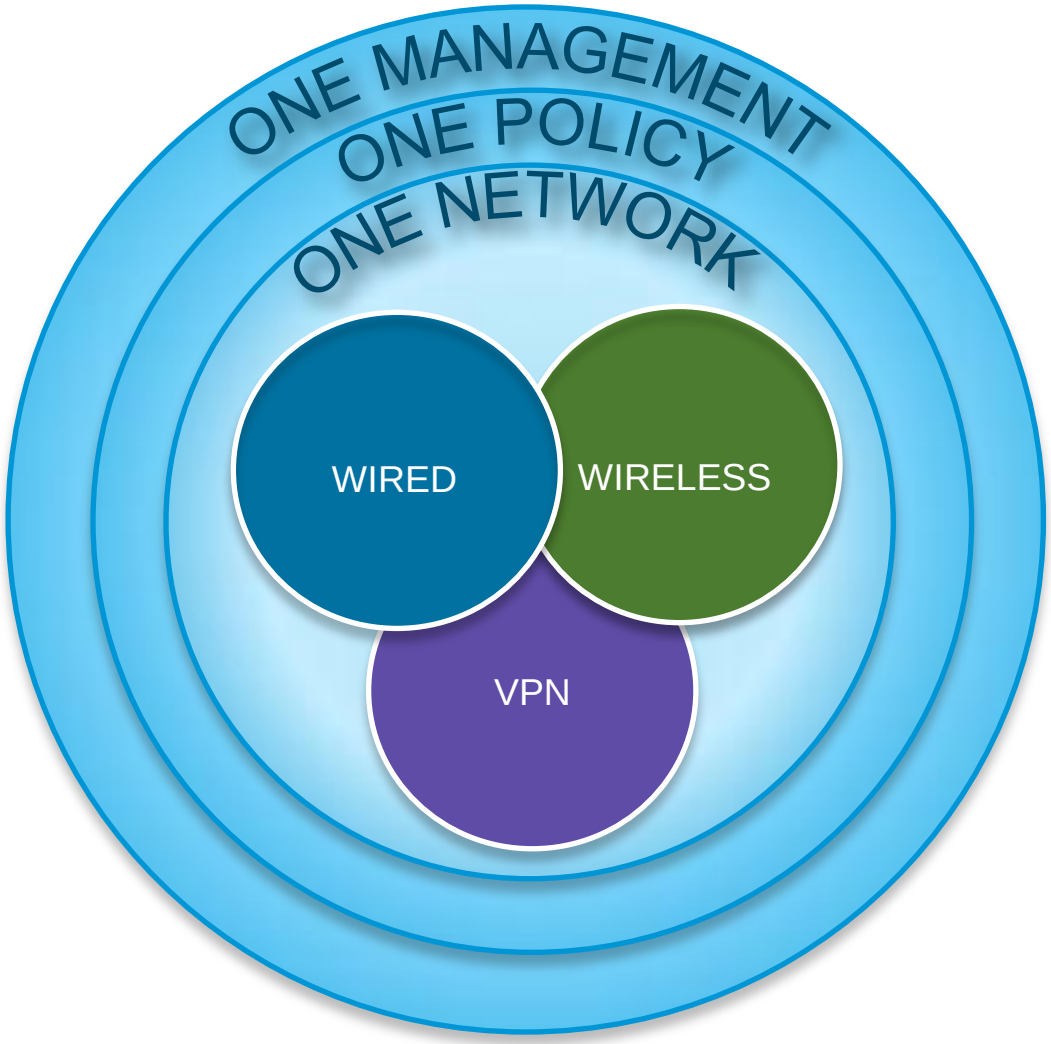


Securing Any Access

Managing Complexity And Scale

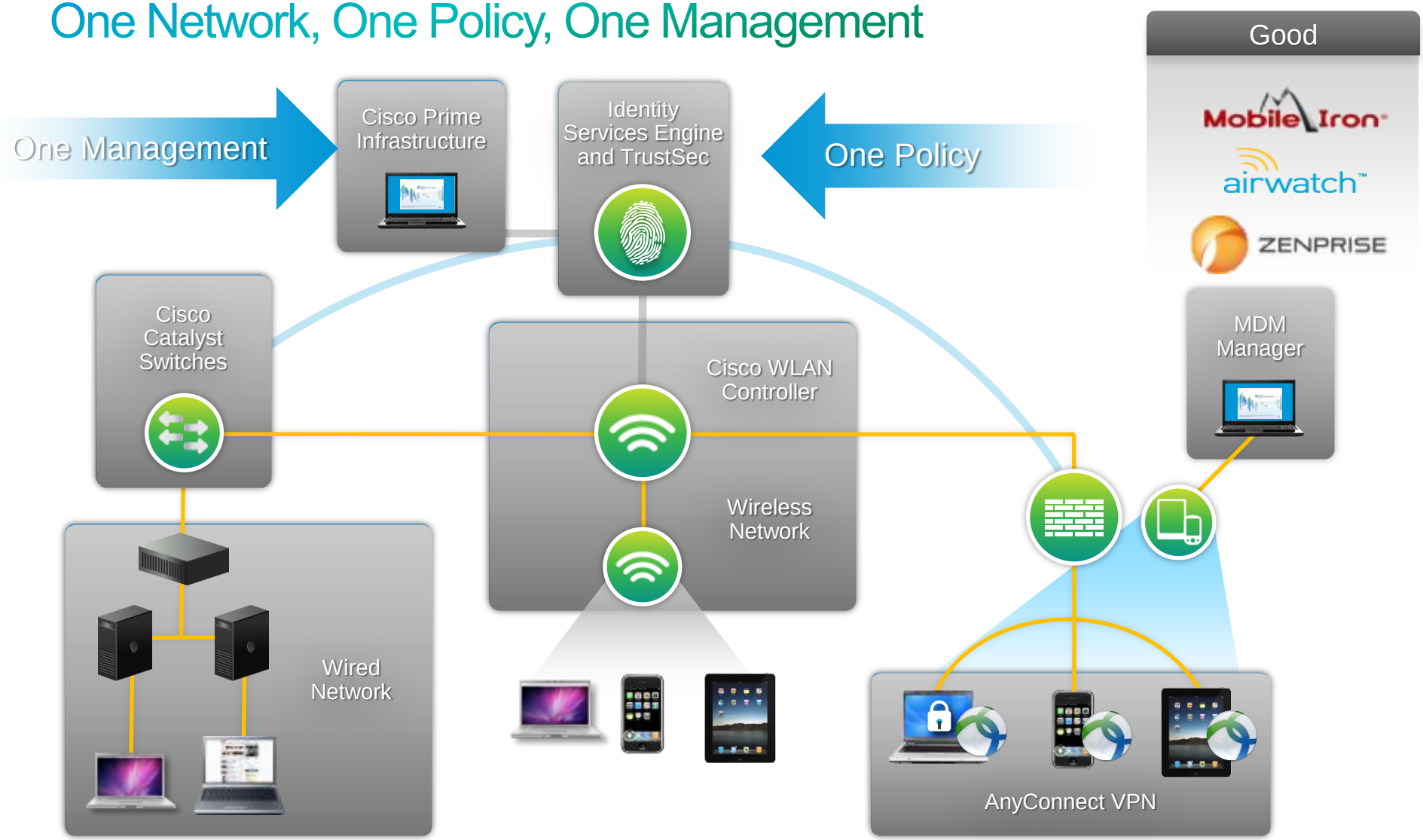
Delivering High-Quality Experience

Cisco Response: Unified Access



Unified Access Architecture

One Network, One Policy, One Management



Single Platform for Wired and Wireless

20+ Years of IOS Richness – Now on Wireless

WIRELESS

Features:

- 802.11n
- CleanAir
- VideoStream
- Radio Resource Management (RRM)
- Wireless Intrusion Prevention System (WiPS)
- 802.11ac Ready

WIRED

Features:

- Stacking
- Stackpower
- Flexible Netflow
- Granular QoS
- Trustsec*/Identity
- AVC/Medianet*
- Smart Operations*
- EnergyWise*

Benefits

- Built on **UADP ASIC** – Cisco's Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

Unified Access: The Cisco Advantage

One Policy

- Single Business Policy
  - **Wired, Wireless, and VPN**
  - Managed & BYOD assets
- Context-based Control
  - **Who, what, when, where**
  - **Application** visibility/control
  - Advanced segmentation
- User-Specific Services
  - **Self-service on-boarding**
  - Lifecycle **Guest** handling
  - Location-based services

One Management

- Comprehensive Visibility
  - **Single Pane of Glass**
  - **User/device centric**
  - Users, devices, location, posture
- Operational Efficiency
  - Virtual switching
  - Auto provisioning
  - Programmable network
- Lower TCO
  - Intuitive troubleshooting
  - Service assurance
  - Energy management

One Network

- Uncompromised Experience
  - **Best in class RF: ClientLink, CleanAir VideoStream**
  - **Always-on VPN**
  - **Wired/Wireless convergence**
- Resiliency and Scale
  - Services at scale
  - Reduced downtime
  - Secure infrastructure
- Deployment Flexibility
  - Campus/branch/home
  - Architectural options
  - Virtualization

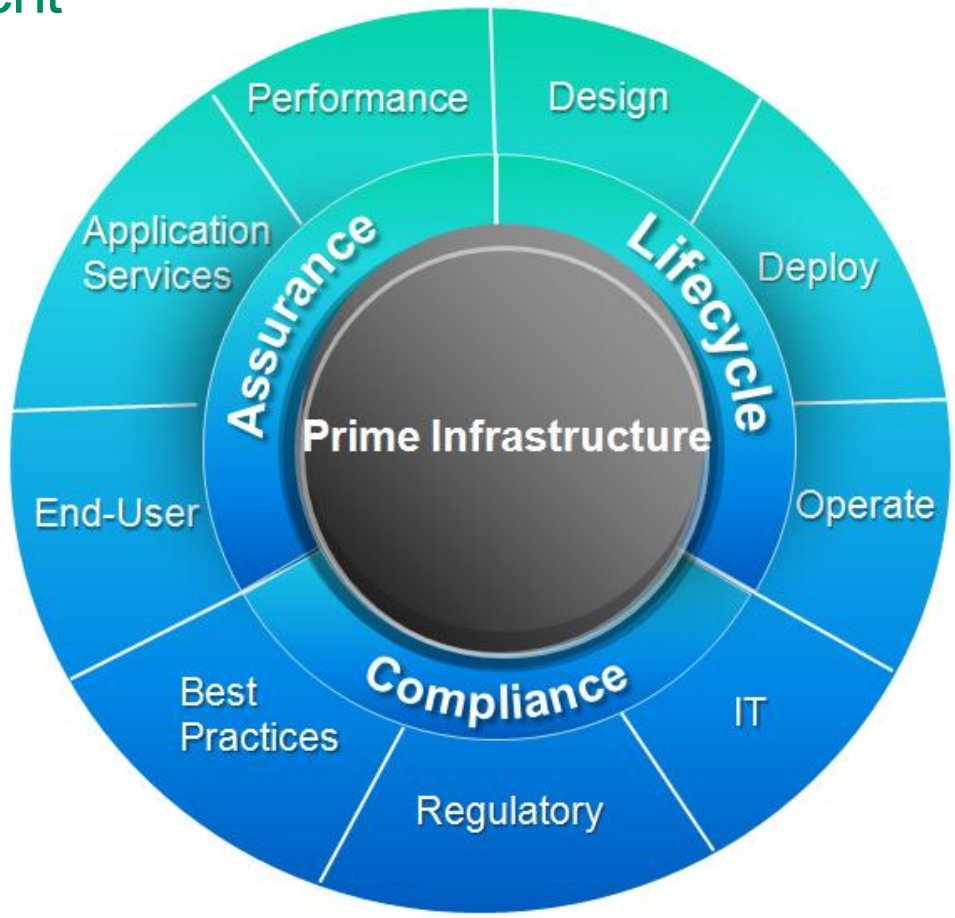
One Management

Cisco Prime Infrastructure

Single Pane of Glass Management

A Single Solution for Converged **Wired and Wireless** Management

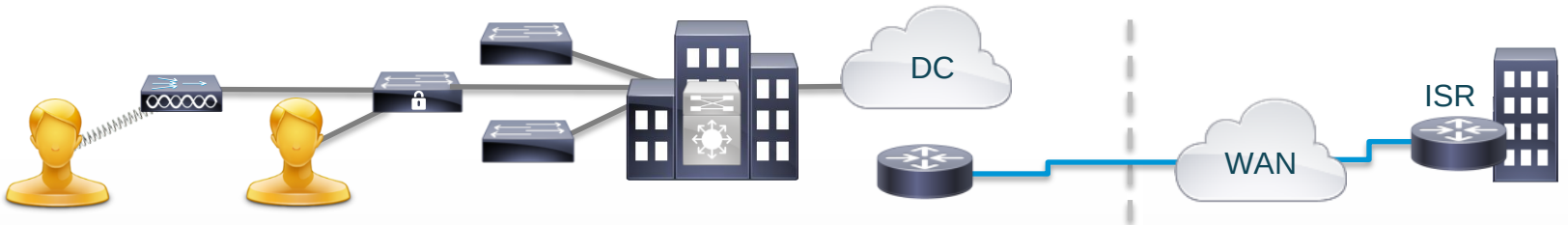
- Lifecycle
  - Discovery, inventory, configuration, fault, troubleshooting, remediation
- Assurance
  - Application performance visibility
  - End-user experience
- Compliance
  - Regulatory compliance and best practices
- End User centric
- Centralized policy integration (Cisco Prime and ISE)
- ISE/MSE/NAM/NGA integration



Simplified Ordering | Speed Troubleshooting |
Lower TCO with Intuitive User Experience

Converged Wired/Wireless, Campus, and Branch Network Management

Spanning the Entire Enterprise



- Discovery, inventory, SWIM, config archive support for wireless controllers, and access, core and distribution switches
- Centralized visibility and control in a single platform
  - Security alerts — Adaptive wIPS
  - Alarms — Cisco CleanAir technology
- Rich-client visibility with user 360
- Unified wired and wireless security through Cisco Self-Defending network and NAC
- WLC support
- Troubleshooting: AP, RF, location API, mobility
- Deployment templates for: Spanning Tree, VLANs, EtherChannel, etc.
- Third-party support

Wired/Wireless Access and Campus

- Security templates
  - DMVPN
  - GET-VPN
  - ScanSafe Connector
- Device-level support (Device Work Center) for:
  - ZBFW rules
  - NAT rules
- Plug and play for automated deployments
  - Securely provision devices in remote branches once connected to the network

Branch

Assurance
Improve Application Visibility and End-User Experience

End User Experience

- ✓ Wired/wireless user experience: top applications based on endpoint type, BW utilization, etc.
- ✓ Voice quality experience
- ✓ Path trace (for voice/medianet applications)

Visibility

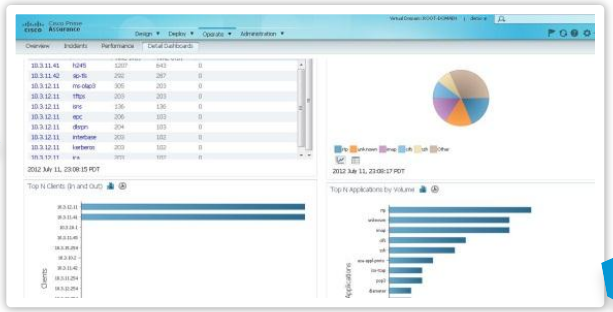
- ✓ Traffic analysis and reporting
- ✓ End-to-end application performance
- ✓ Multi-NAM: packet level debugging and troubleshooting
- ✓ WAN optimization visibility

Network Performance

- ✓ Availability and performance polling with event/alarm generation
- ✓ Custom MIB poller
- ✓ Configuration of devices for data and flow collection: NetFlow, medianet, PA, NBAR

How Is Assurance Achieved?

Cisco Prime Infrastructure



Cisco ISR
NBAR2, PA, Medianet

NAM Module/Appliance

Cisco ASR
NBAR2, AVC, Medianet

NetFlow Generation Appliance (NGA) 3140

Wireless Controller
NBAR2

Cisco Catalyst 3750-X with 3K-X 10G NetFlow, Medianet

Cisco 6509
NetFlow, Medianet

SNMP/ CLI Polling | SPAN/ ERSPAN | NetFlow | WAAS | PA | MEDIANET | NBAR | NBAR2

By Normalizing and Correlating Data Across Multiple Sources:
Leverage the Power of Embedded Cisco Instrumentation

Use Case Example
BYOD: Client Troubleshooting with Cisco Prime

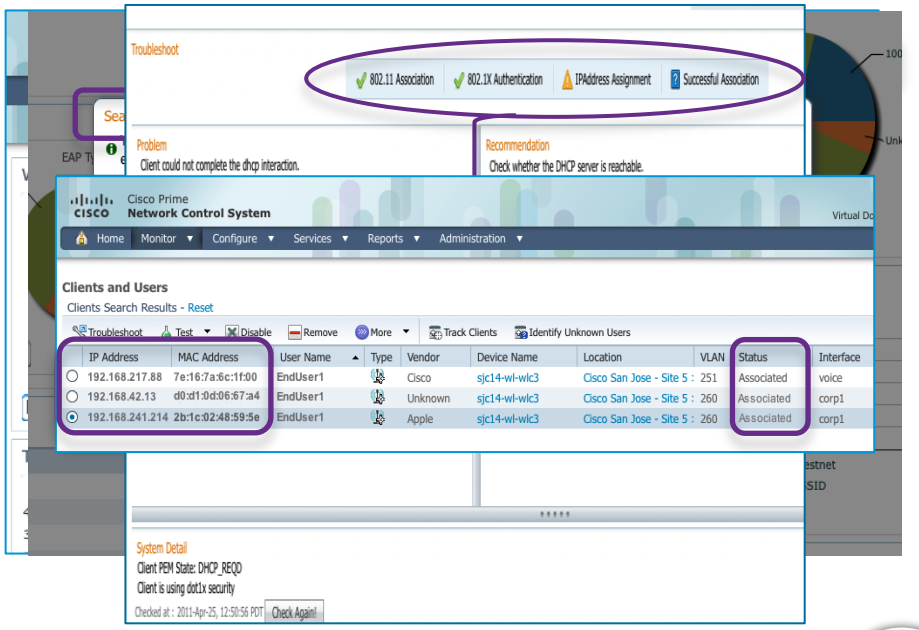
Once BYOD Works, Cisco Prime Can Show the User Experience of the Collaboration and Video Services in a Converged Wired/Wireless Network

Troubleshoot Wired and Wireless Access

Using Cisco Prime Infrastructure to Quickly Resolve Client Access Problems

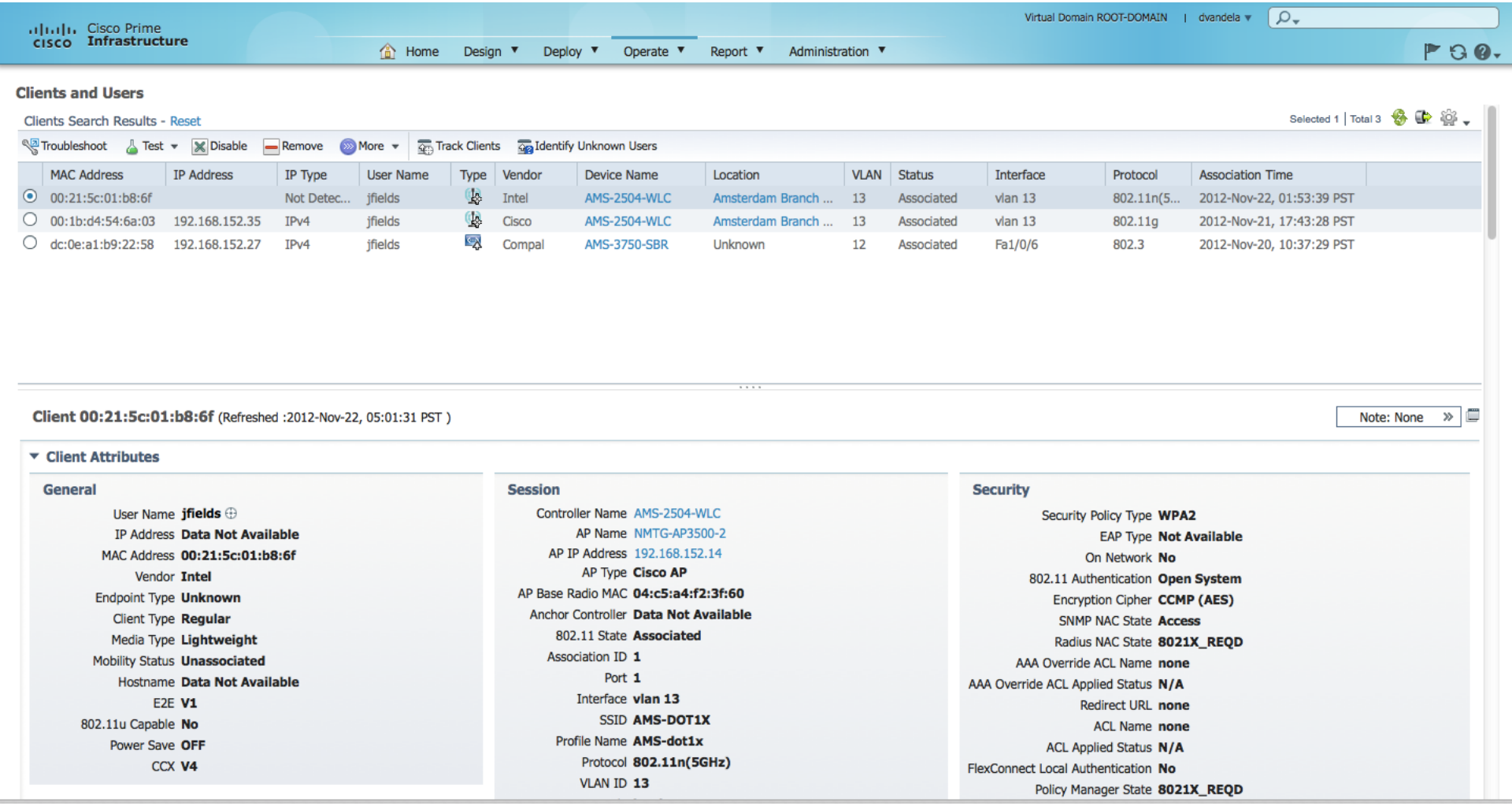
USE CASE: User Calls into Help Center Because They Cannot Get Access to the Network from Their iPad

1. Search on user name
2. Identify wired and wireless devices associated with the user
3. Display associated and disassociated devices
4. Use automated client troubleshooting workflow to resolve the issue
5. Pull up policy details for user from ISE; note authentication issues
6. User takes corrective action

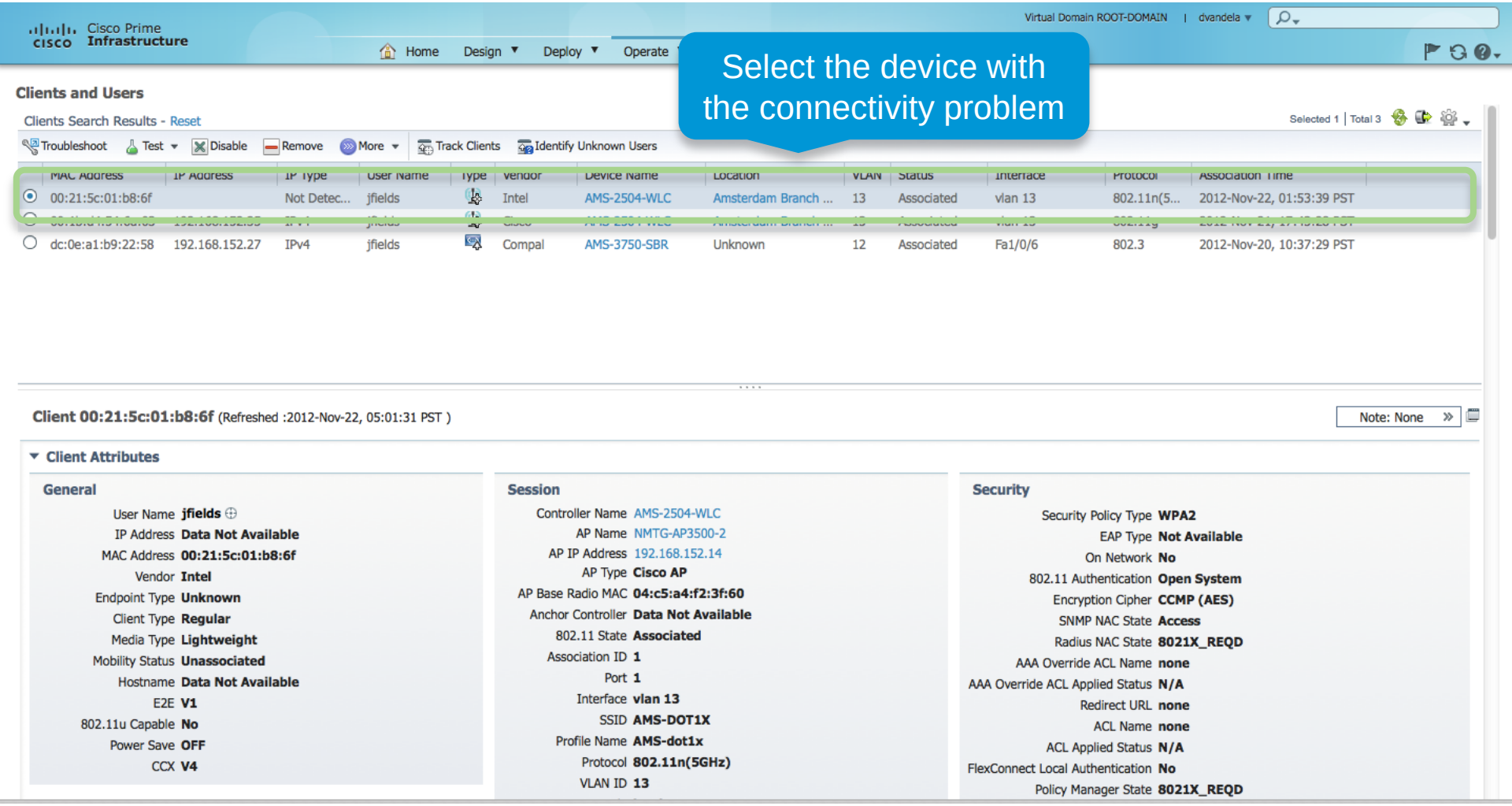


- Troubleshoot User and Access Issues Based on Identity
- Speed Resolution with Intuitive Guided Workflows

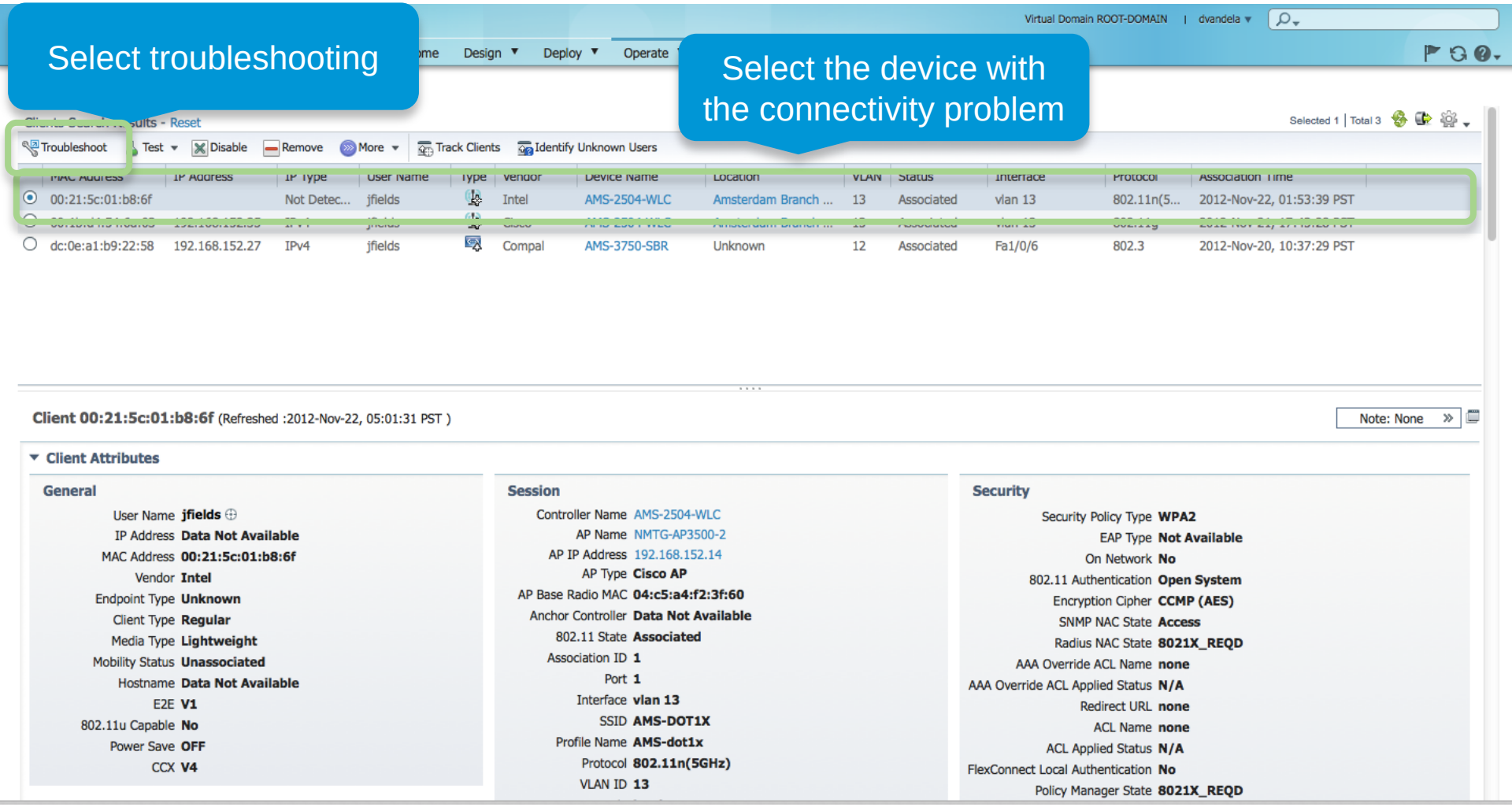
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



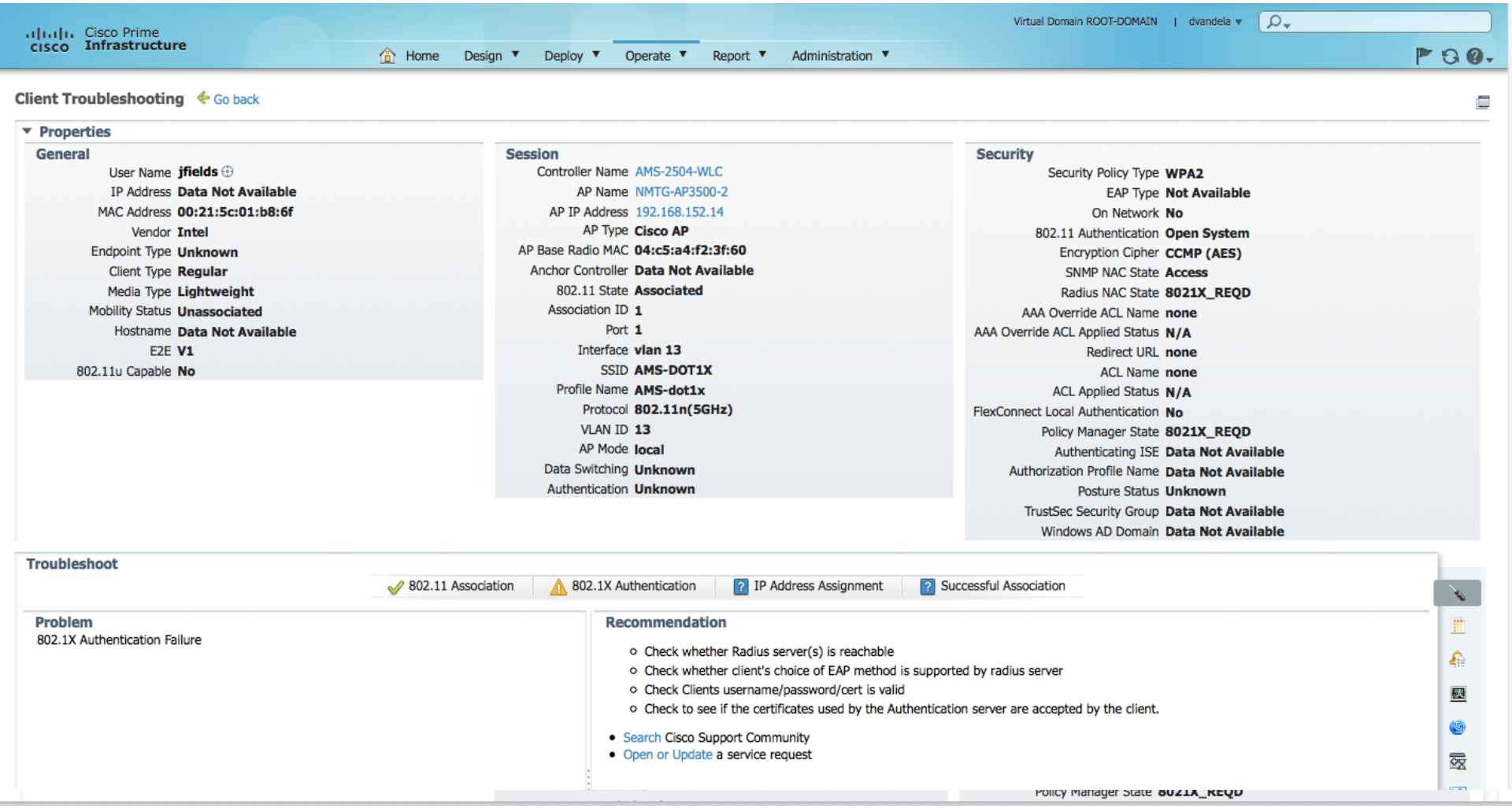
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



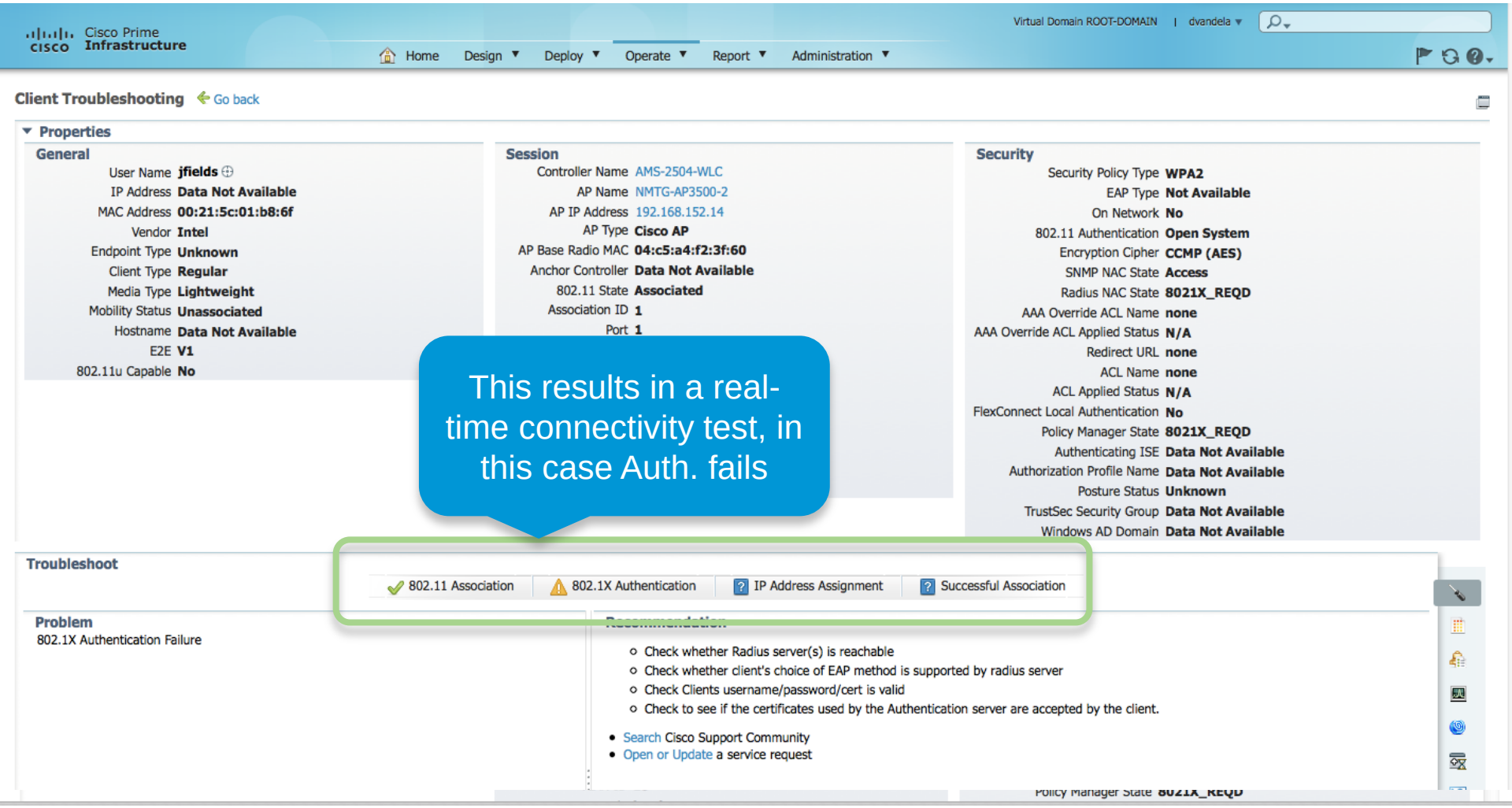
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



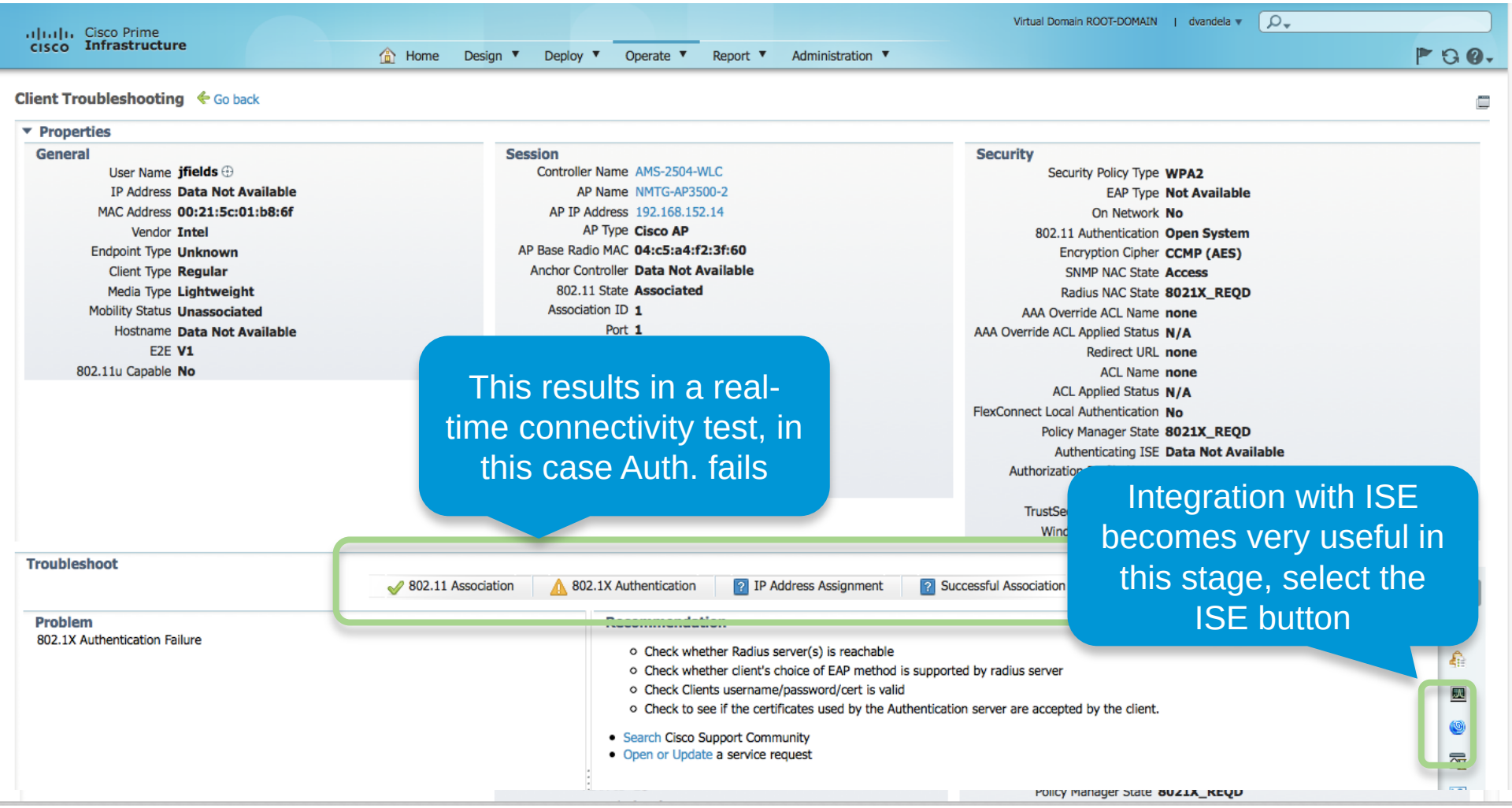
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



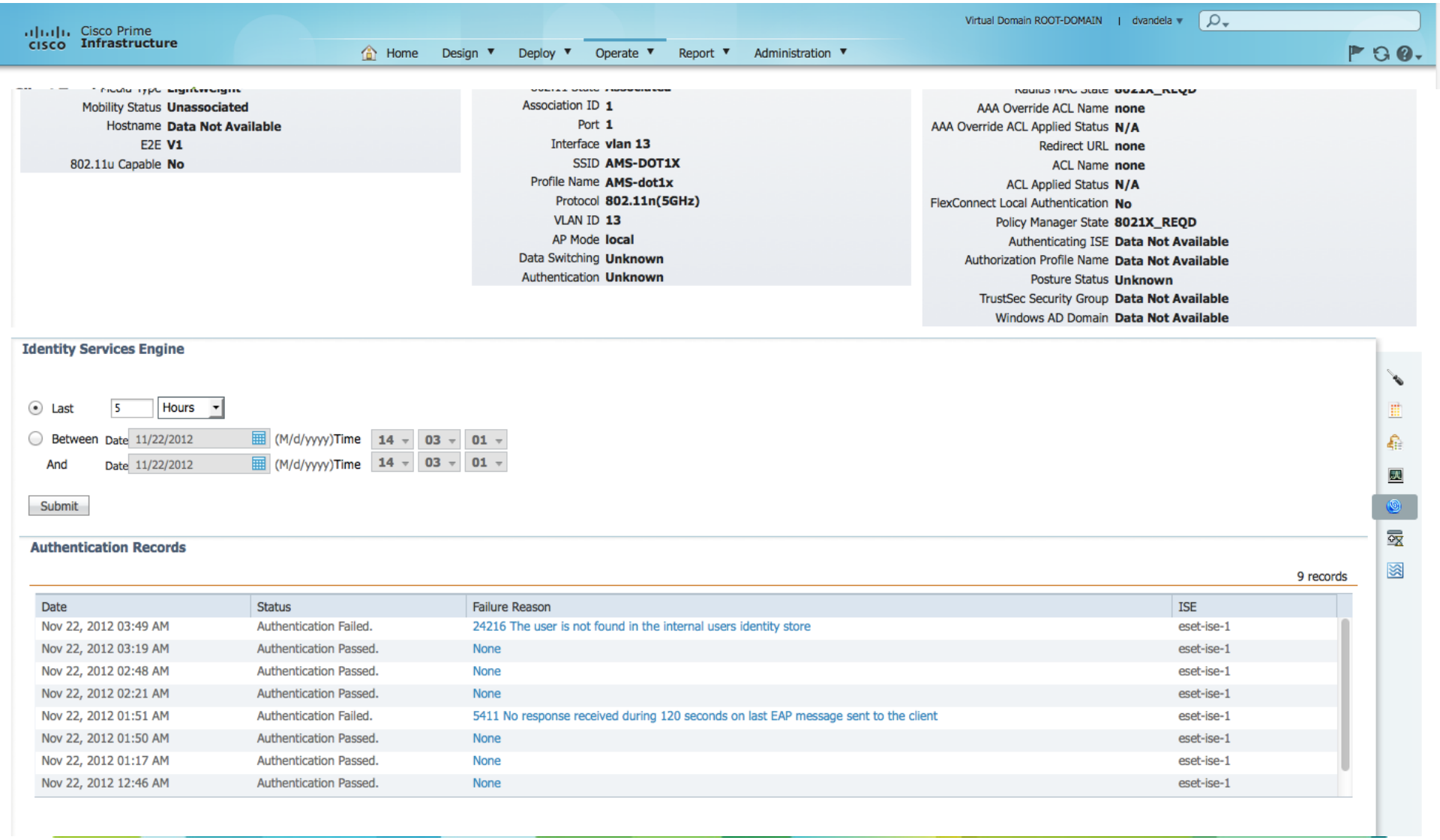
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



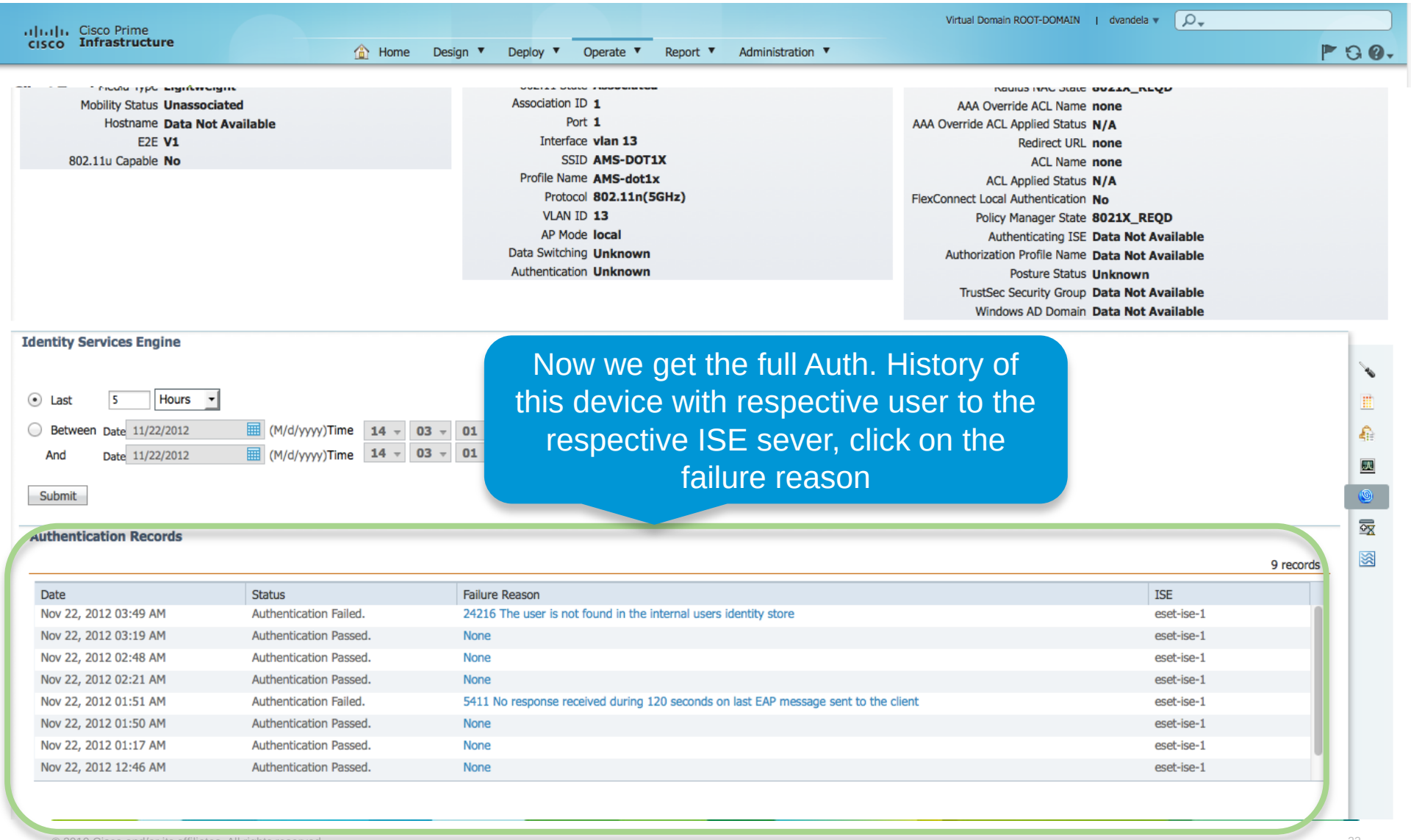
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



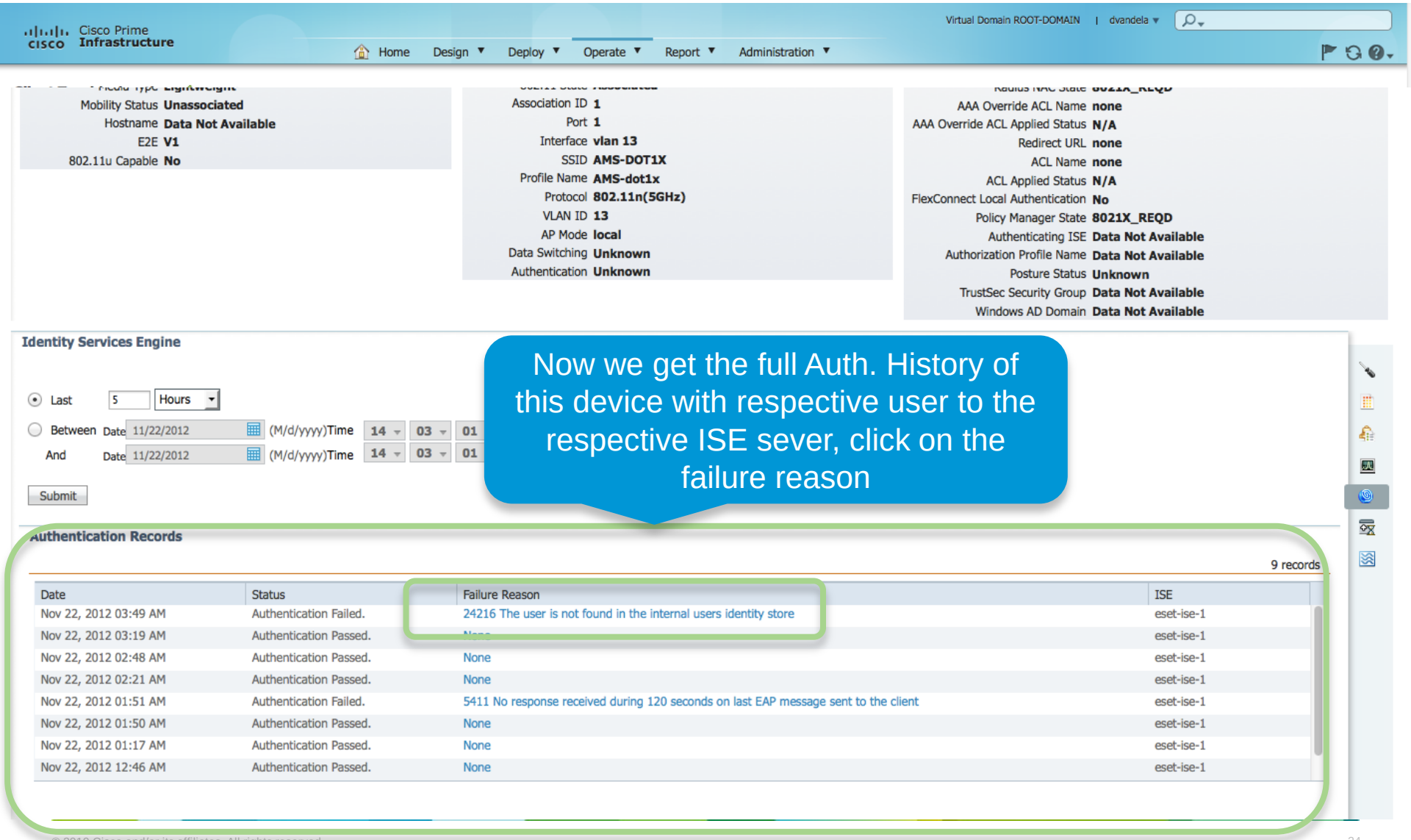
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



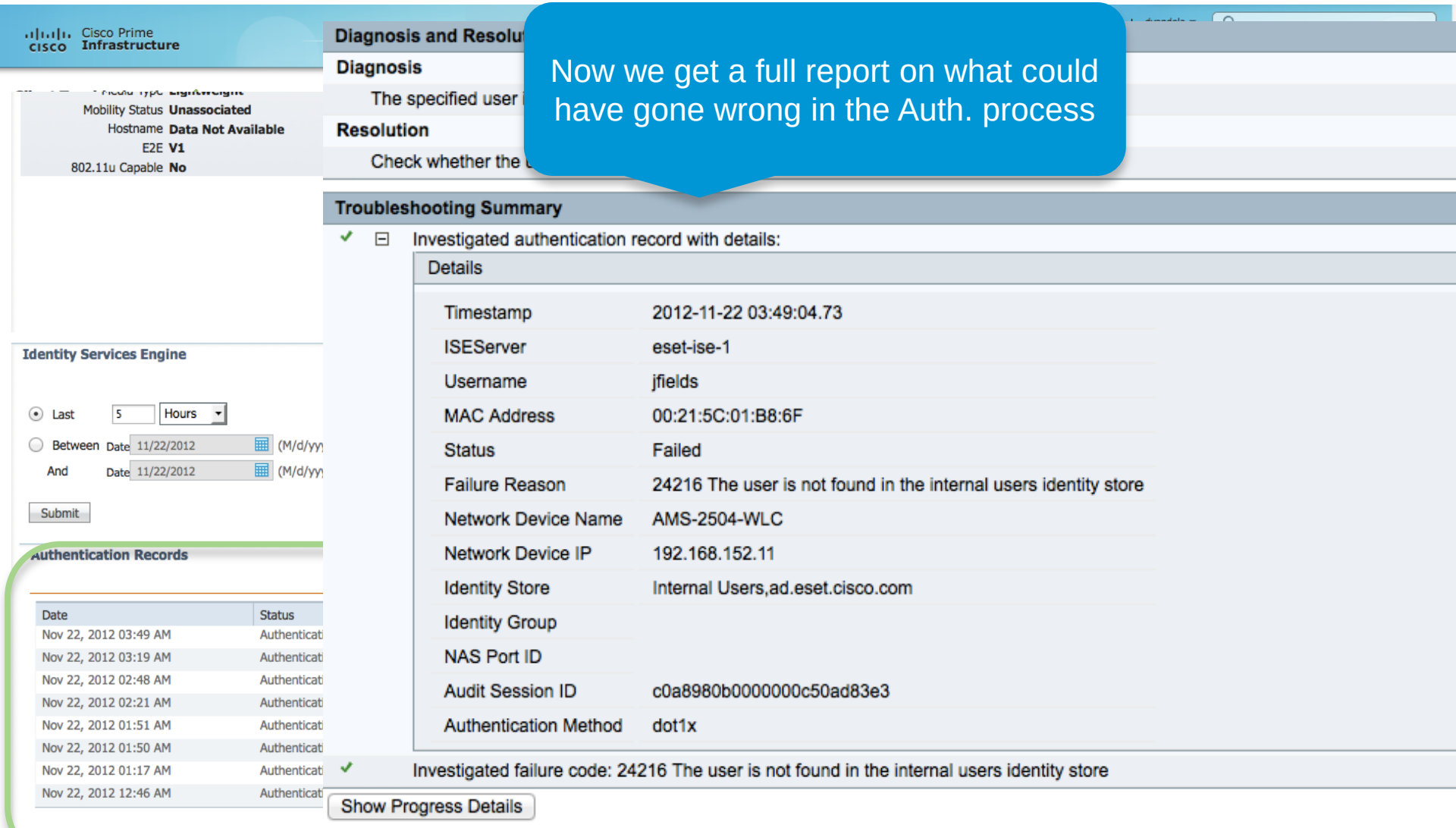
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



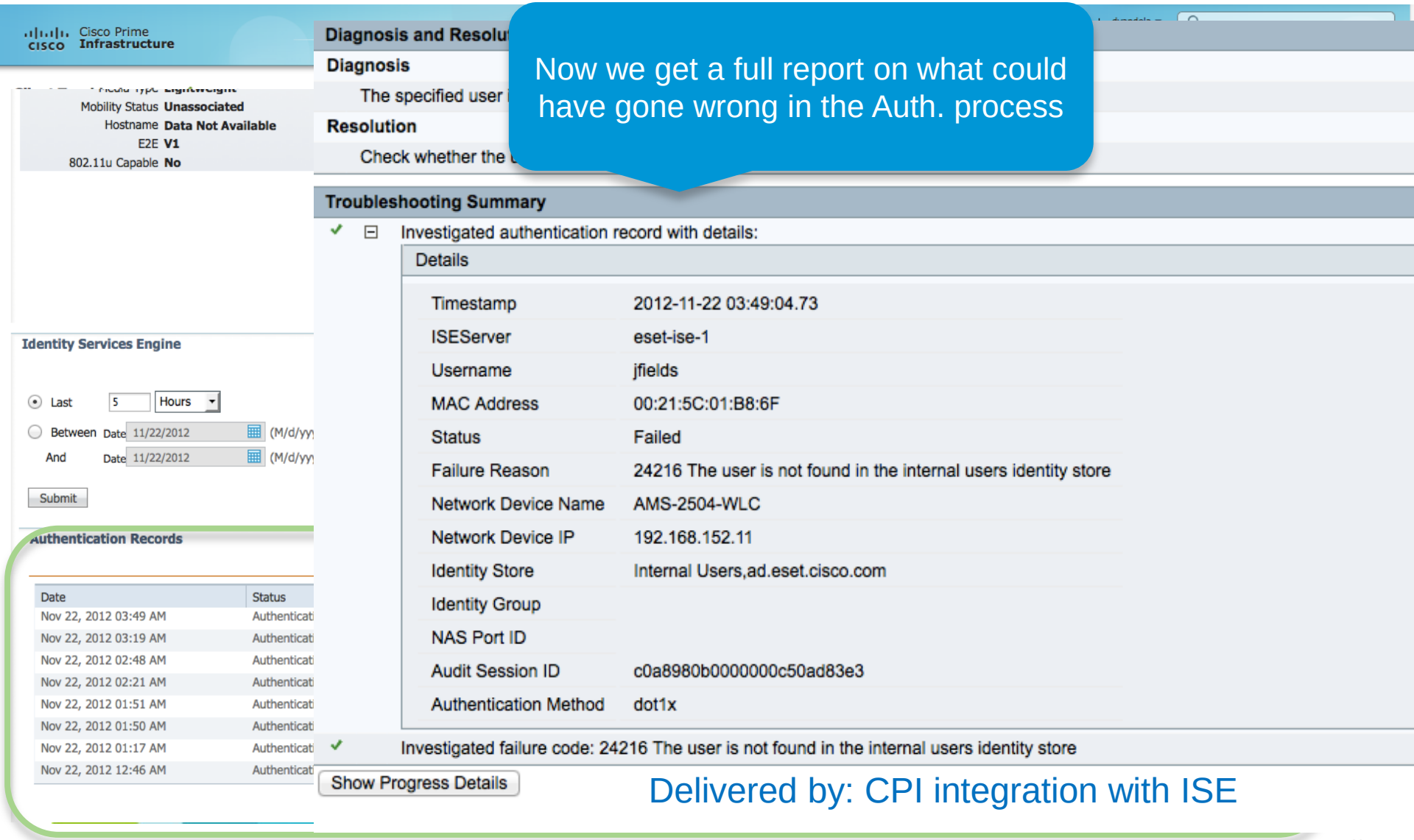
Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity

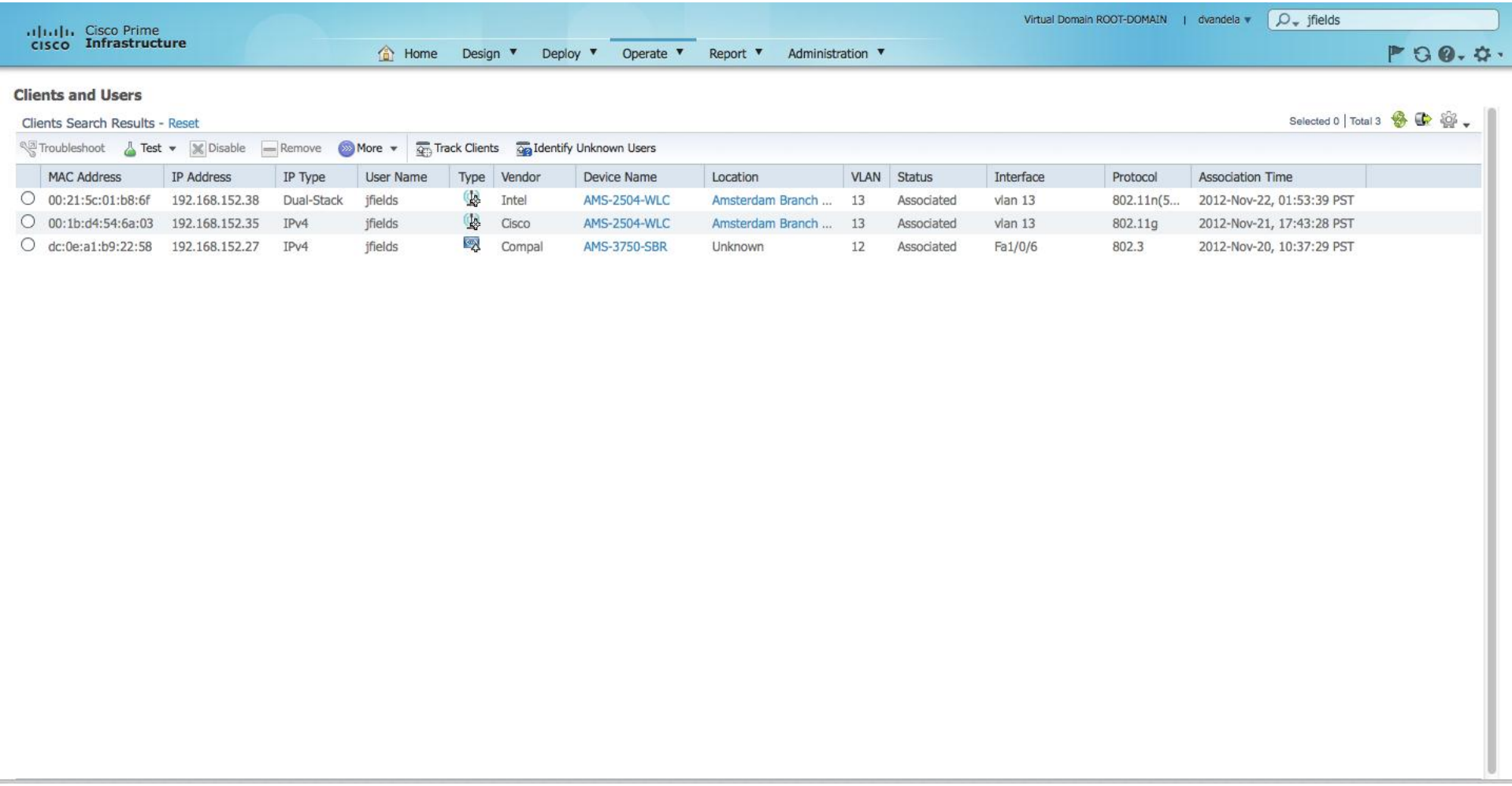


Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 1. Check for Client Connectivity



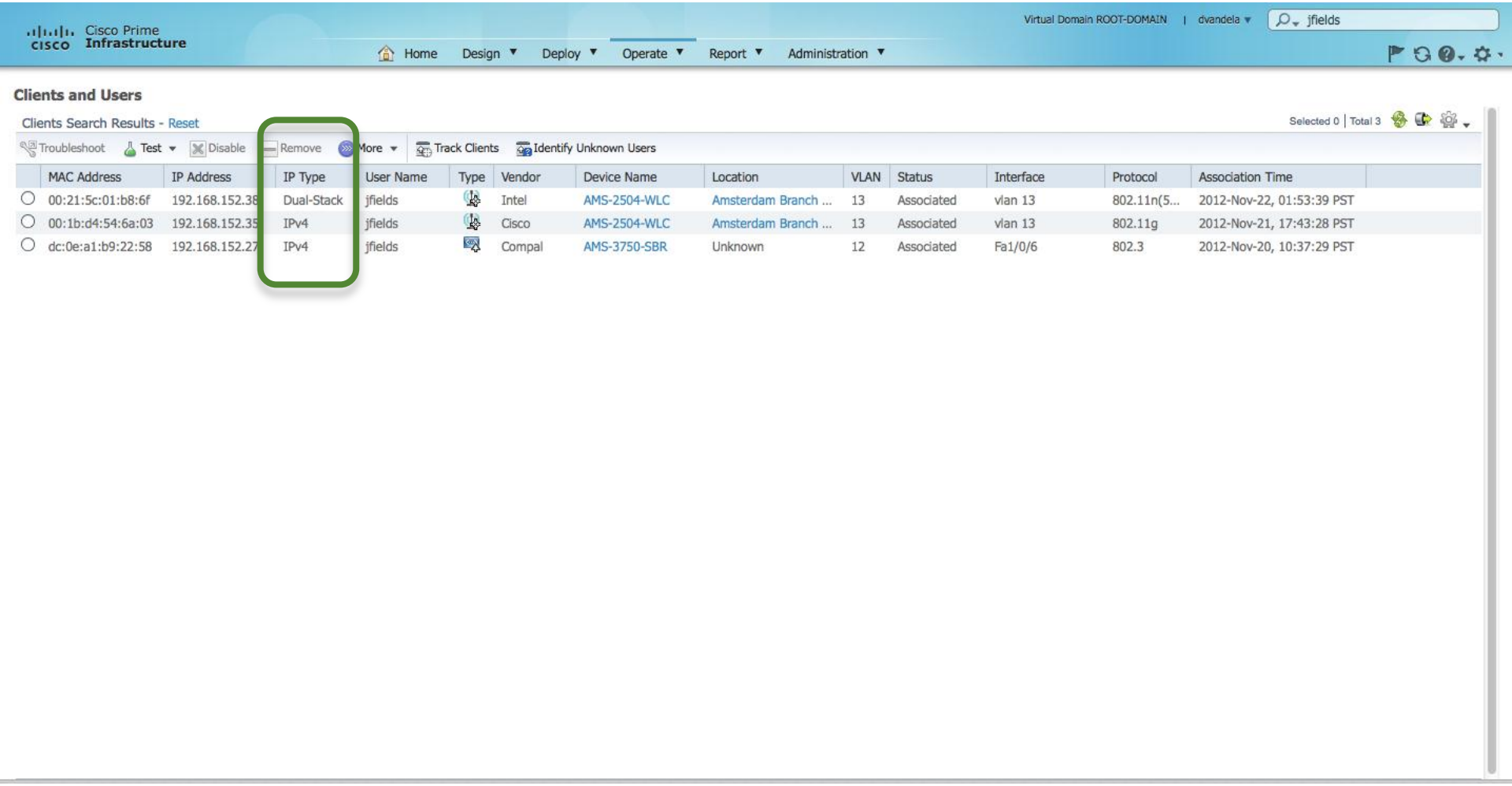
Delivered by: CPI integration with ISE

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



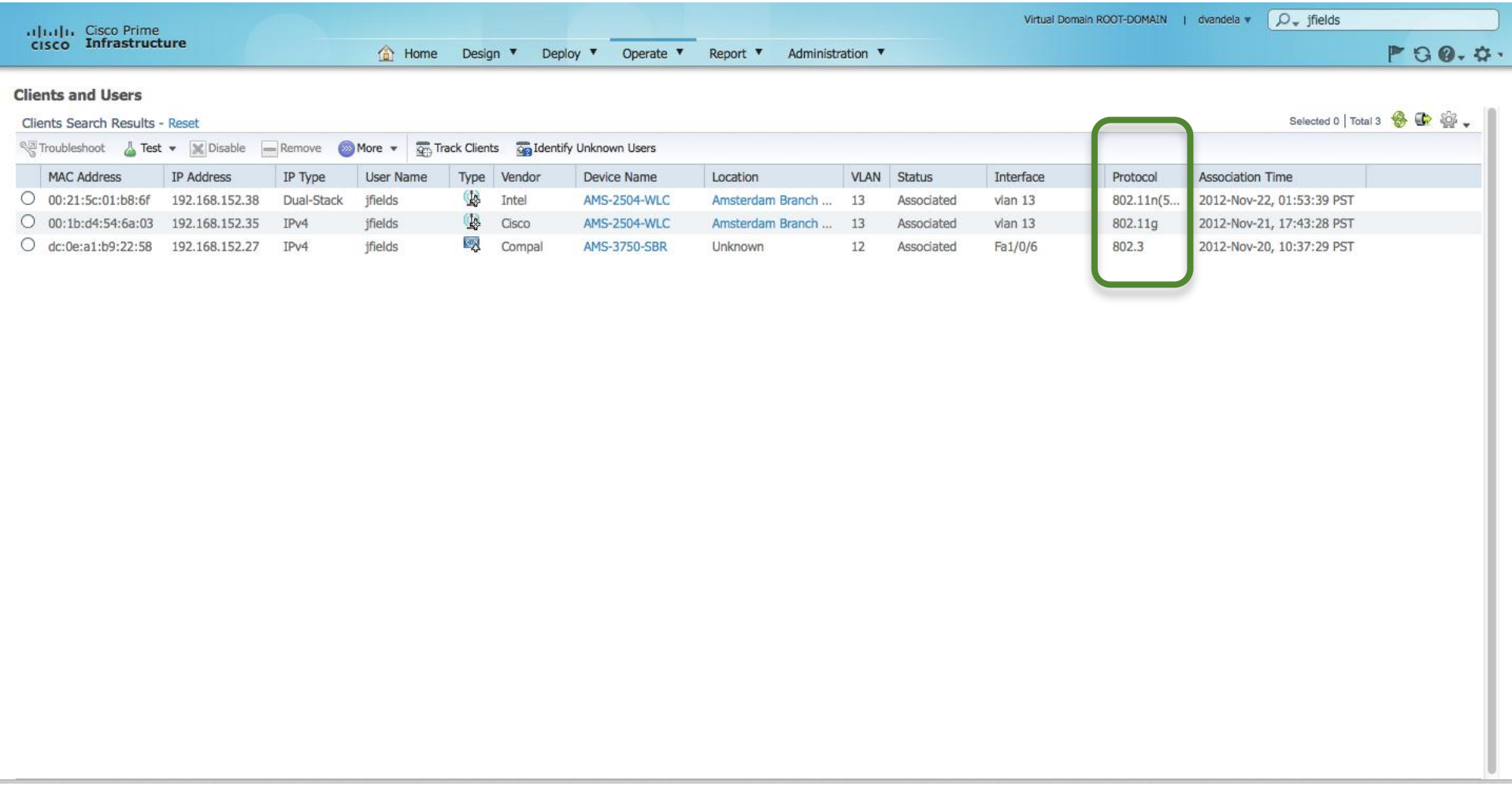
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



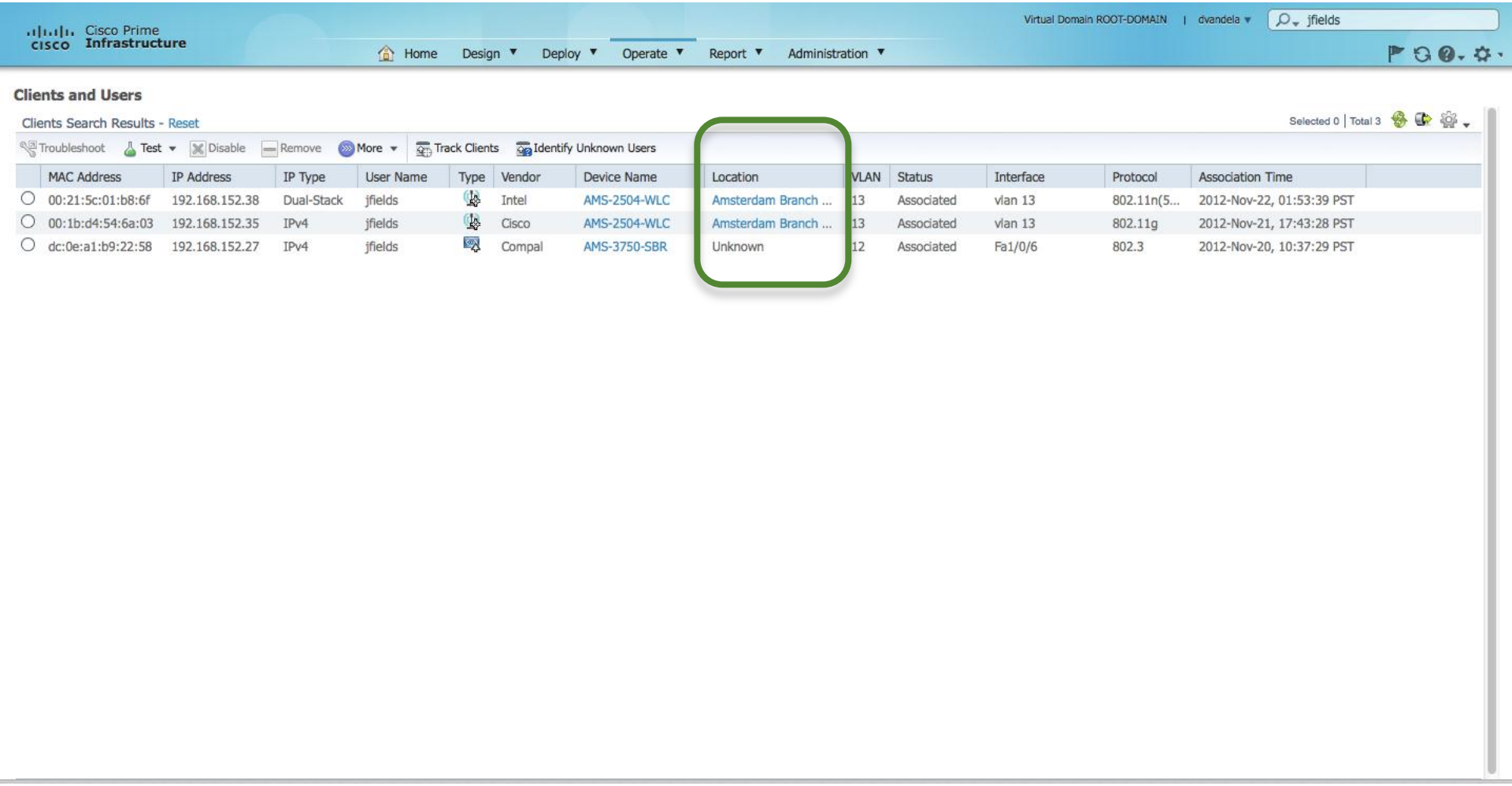
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



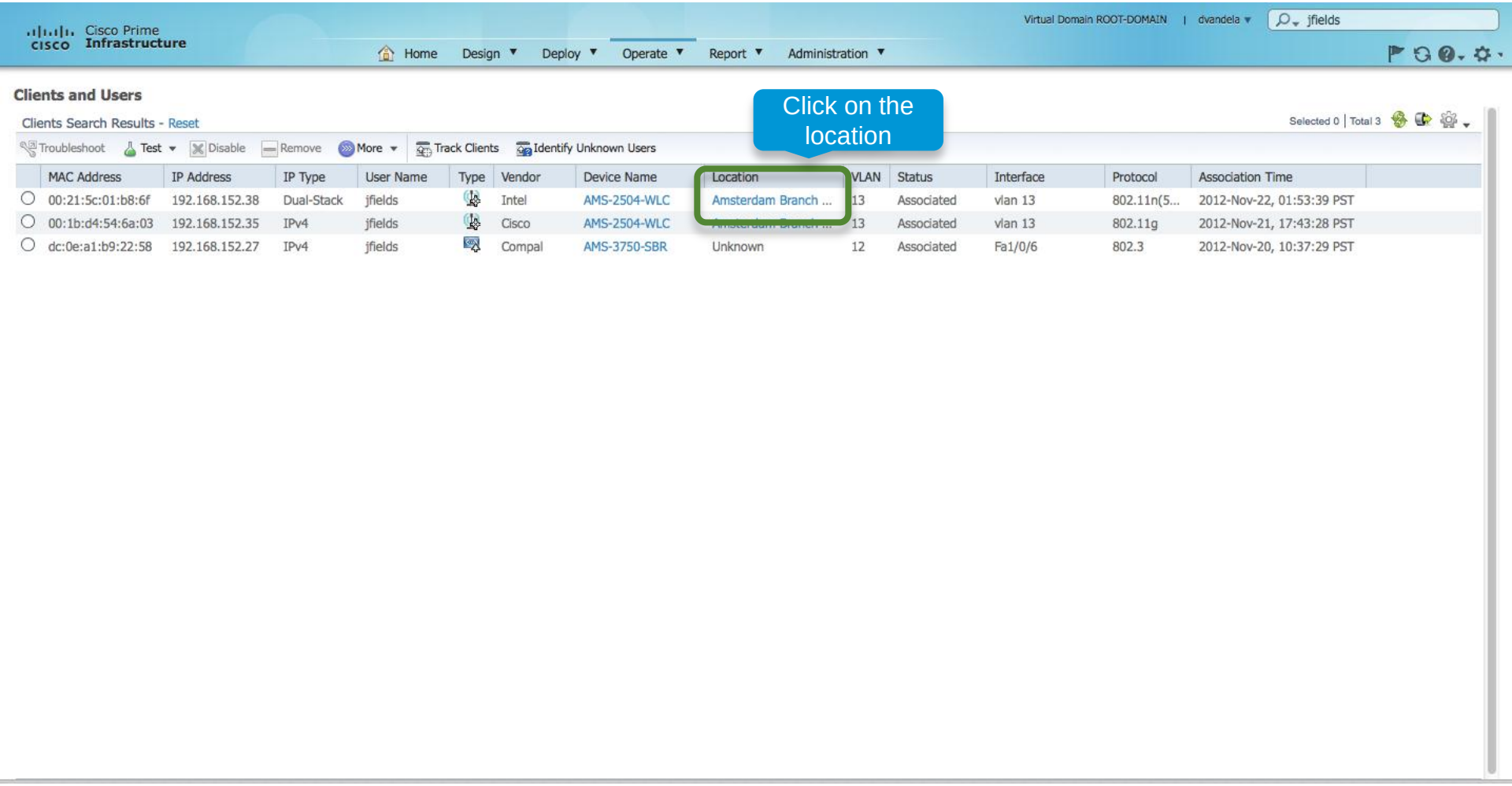
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



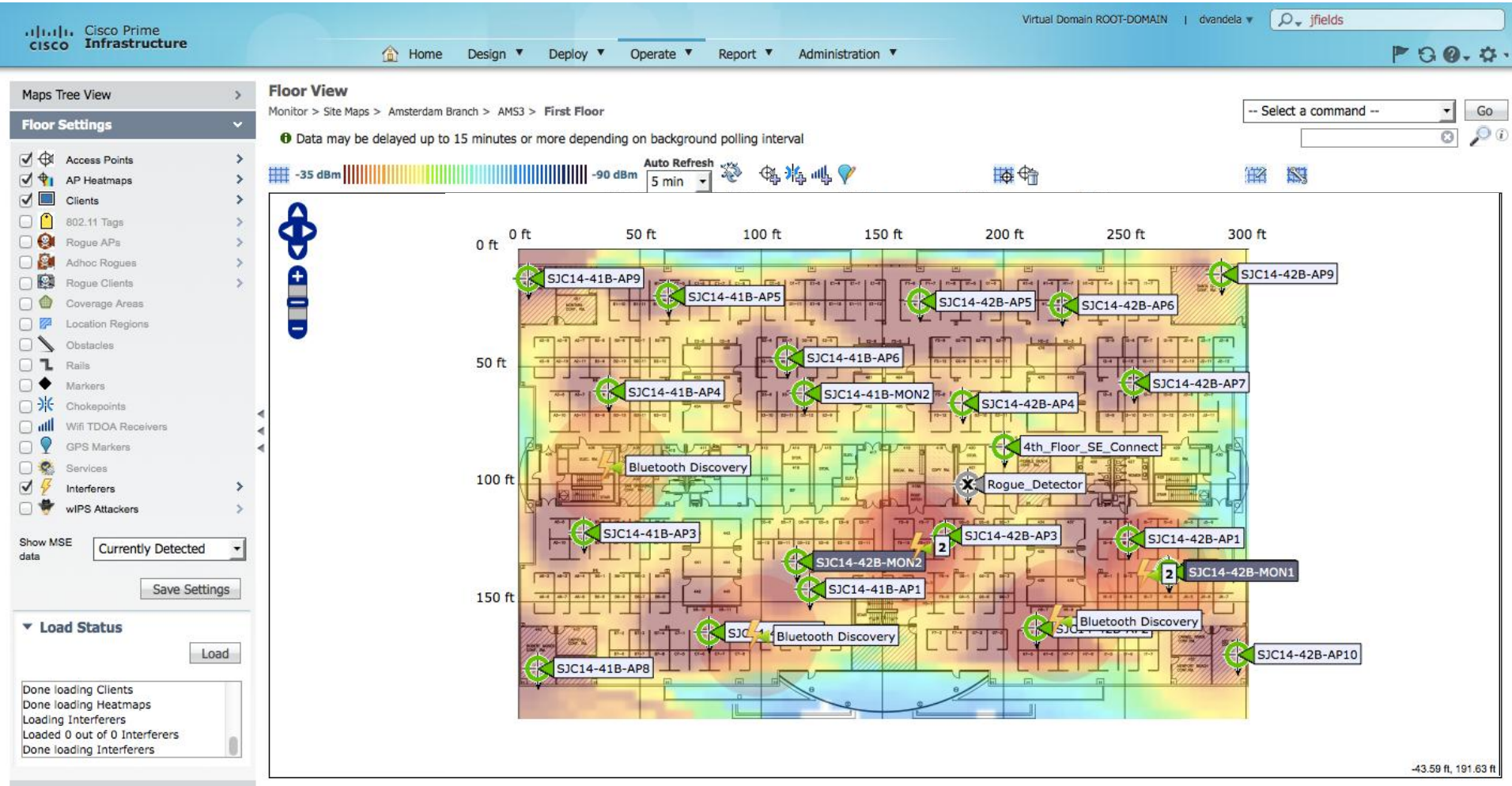
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



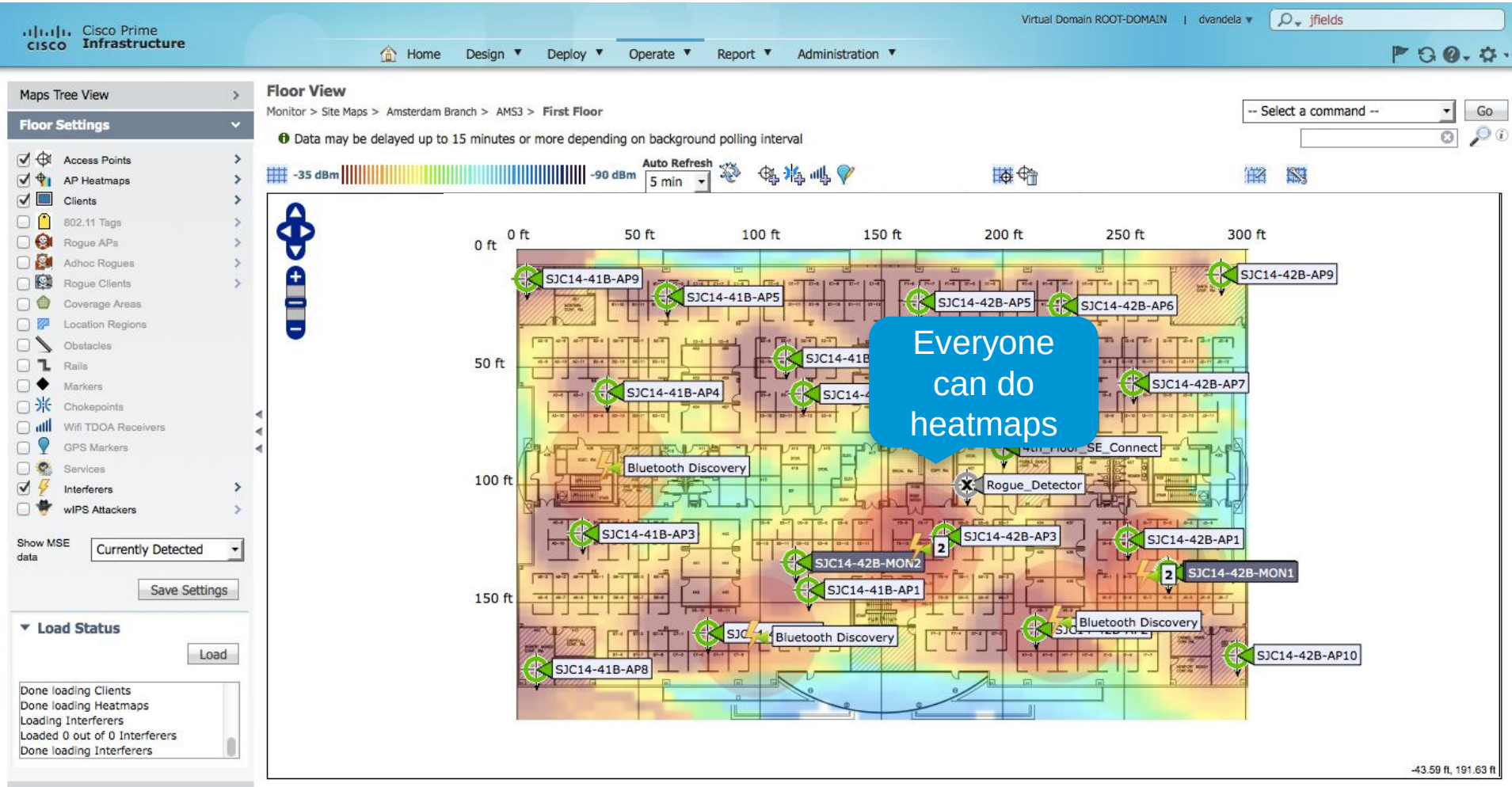
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



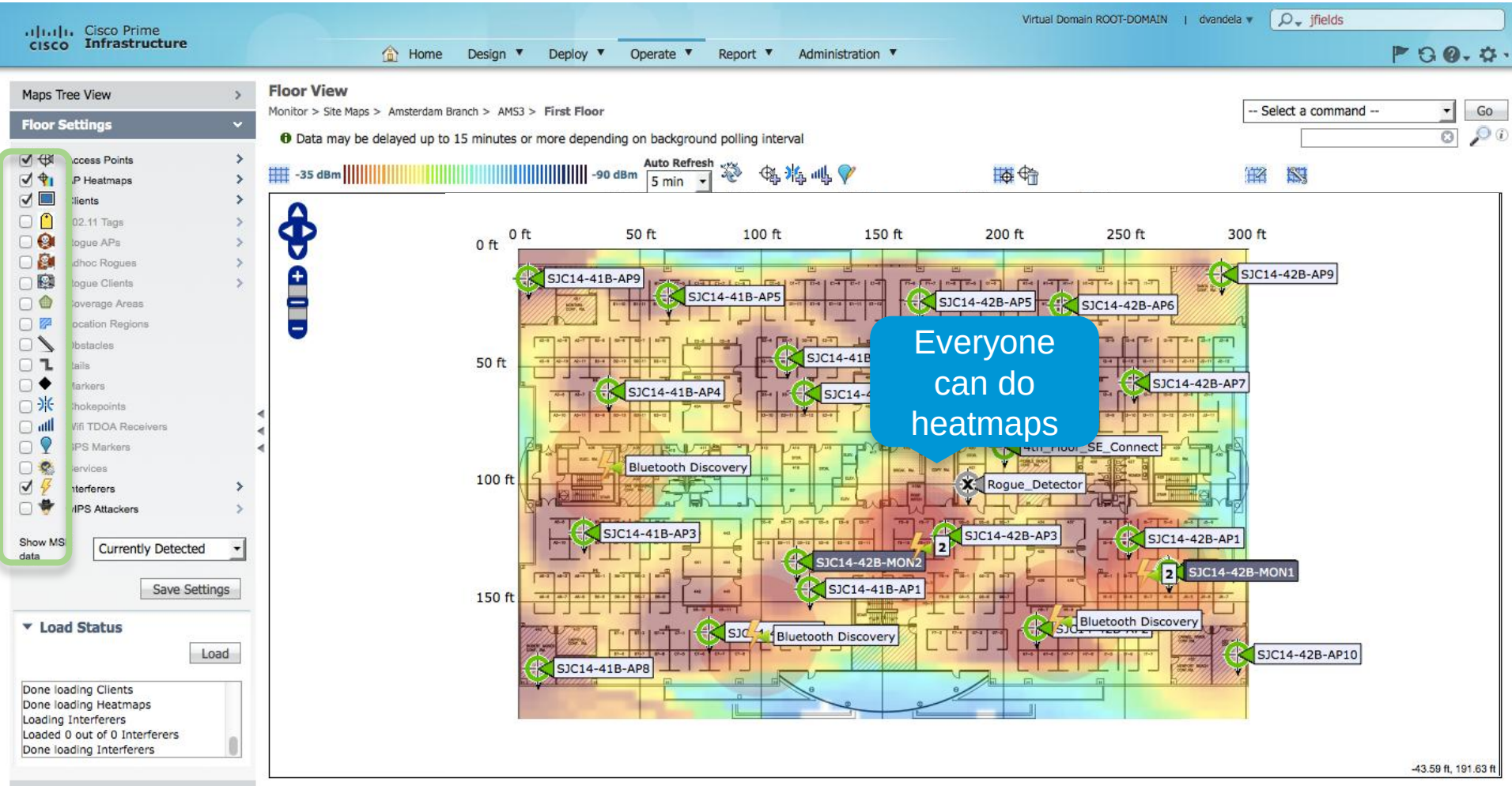
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



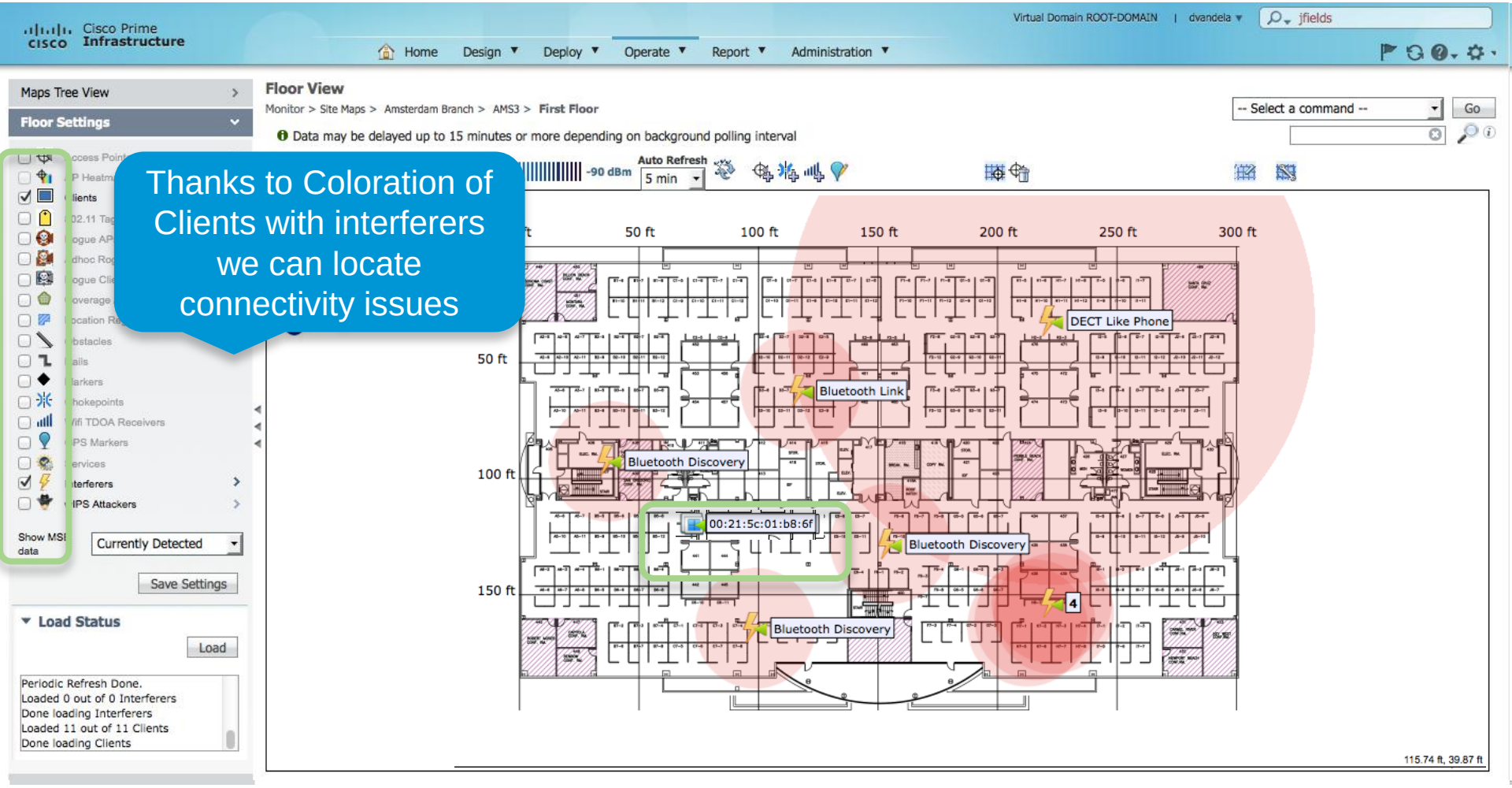
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference



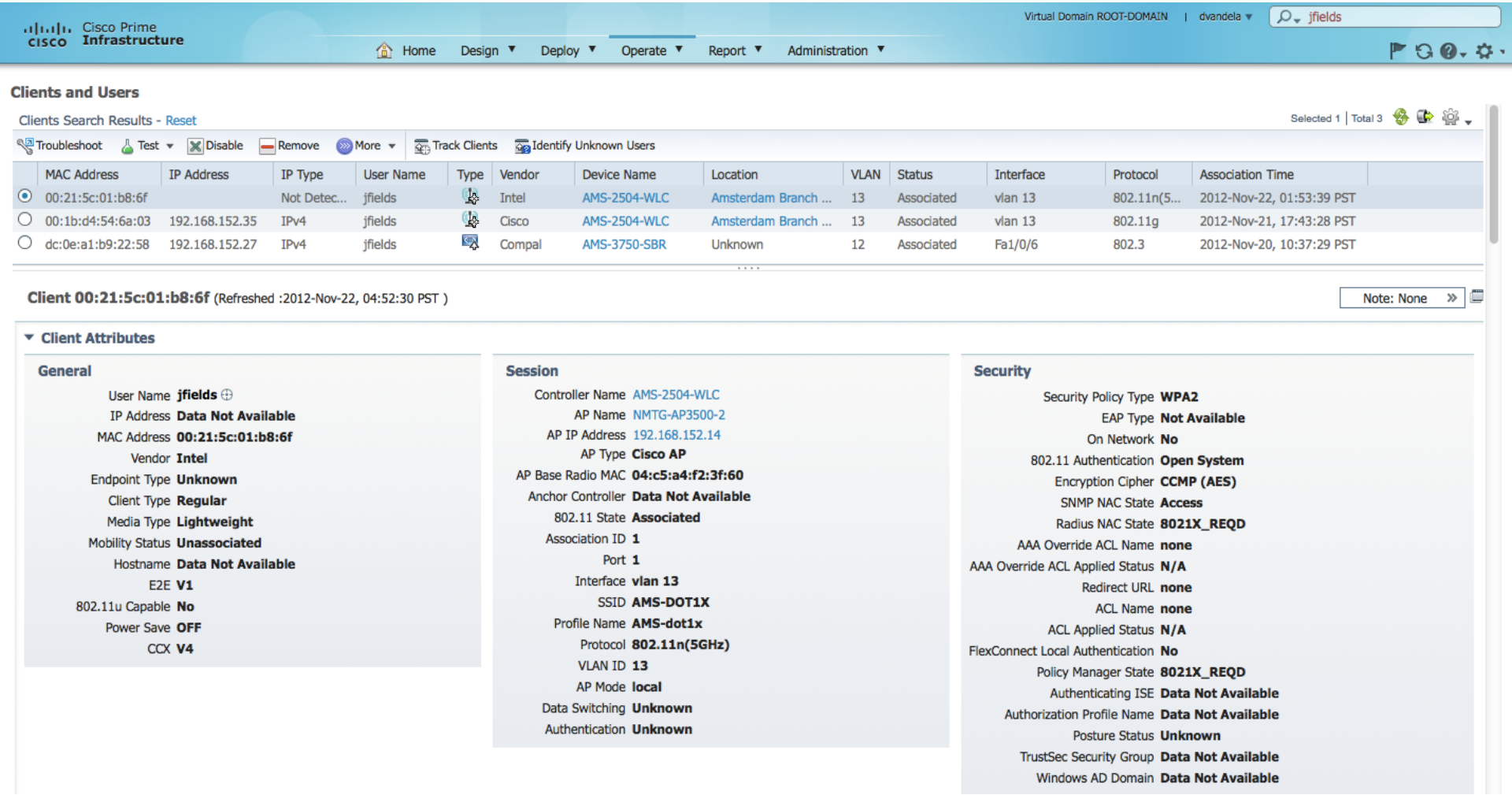
Delivered by: CPI integrated with MSE and CleanAir

Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting
Step 2. Check for RF Interference

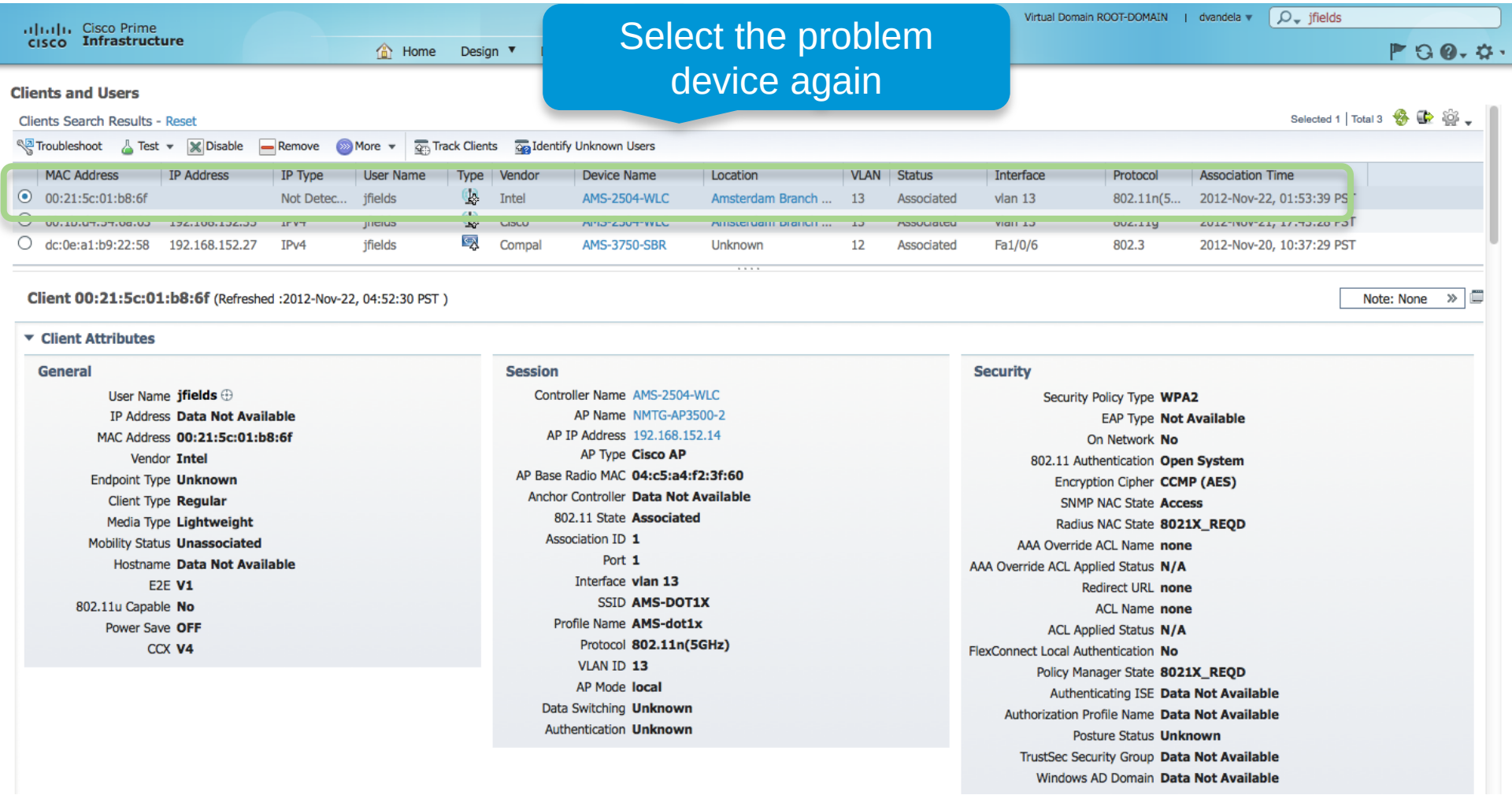


Delivered by: CPI integrated with MSE and CleanAir

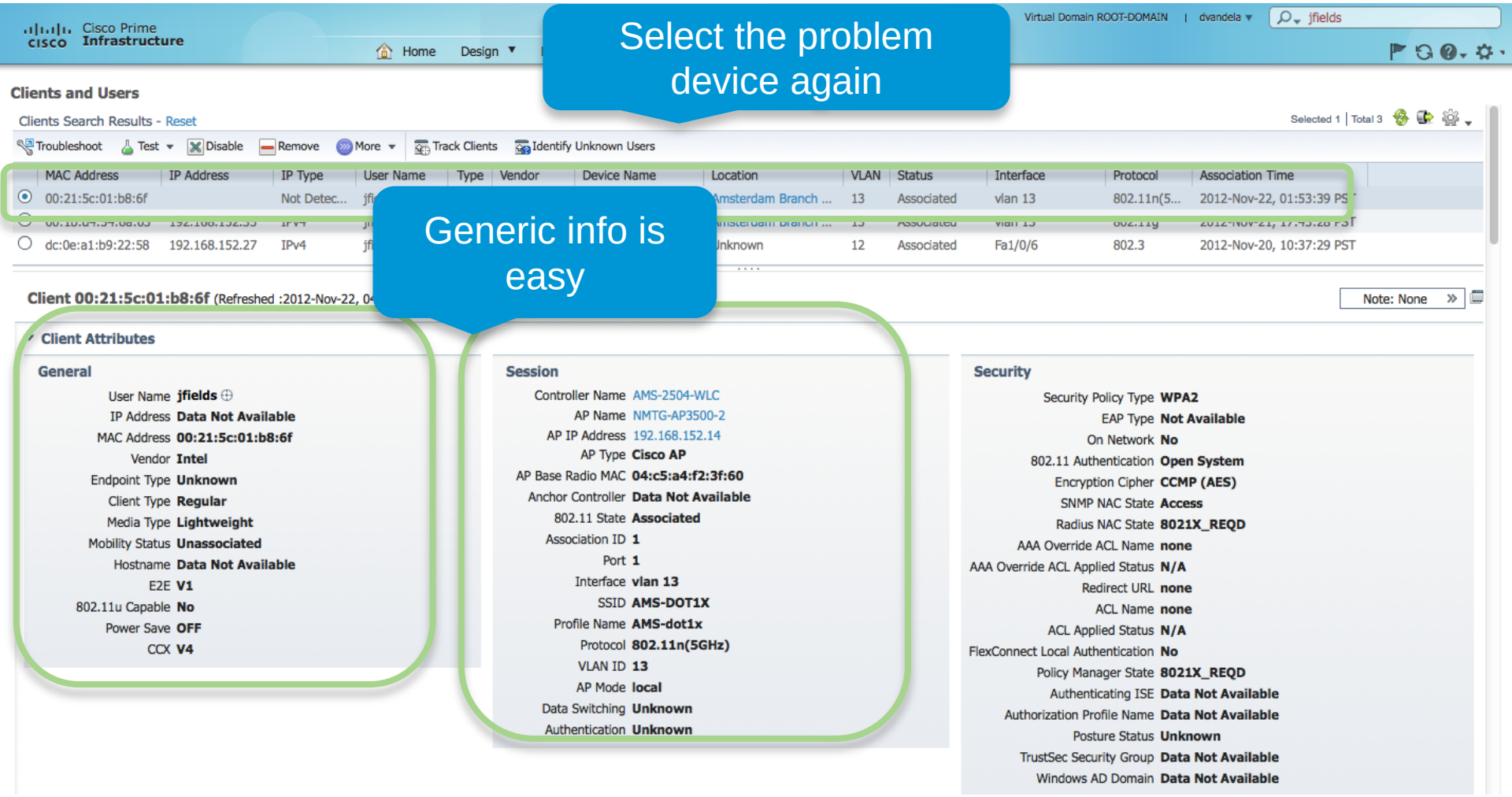
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



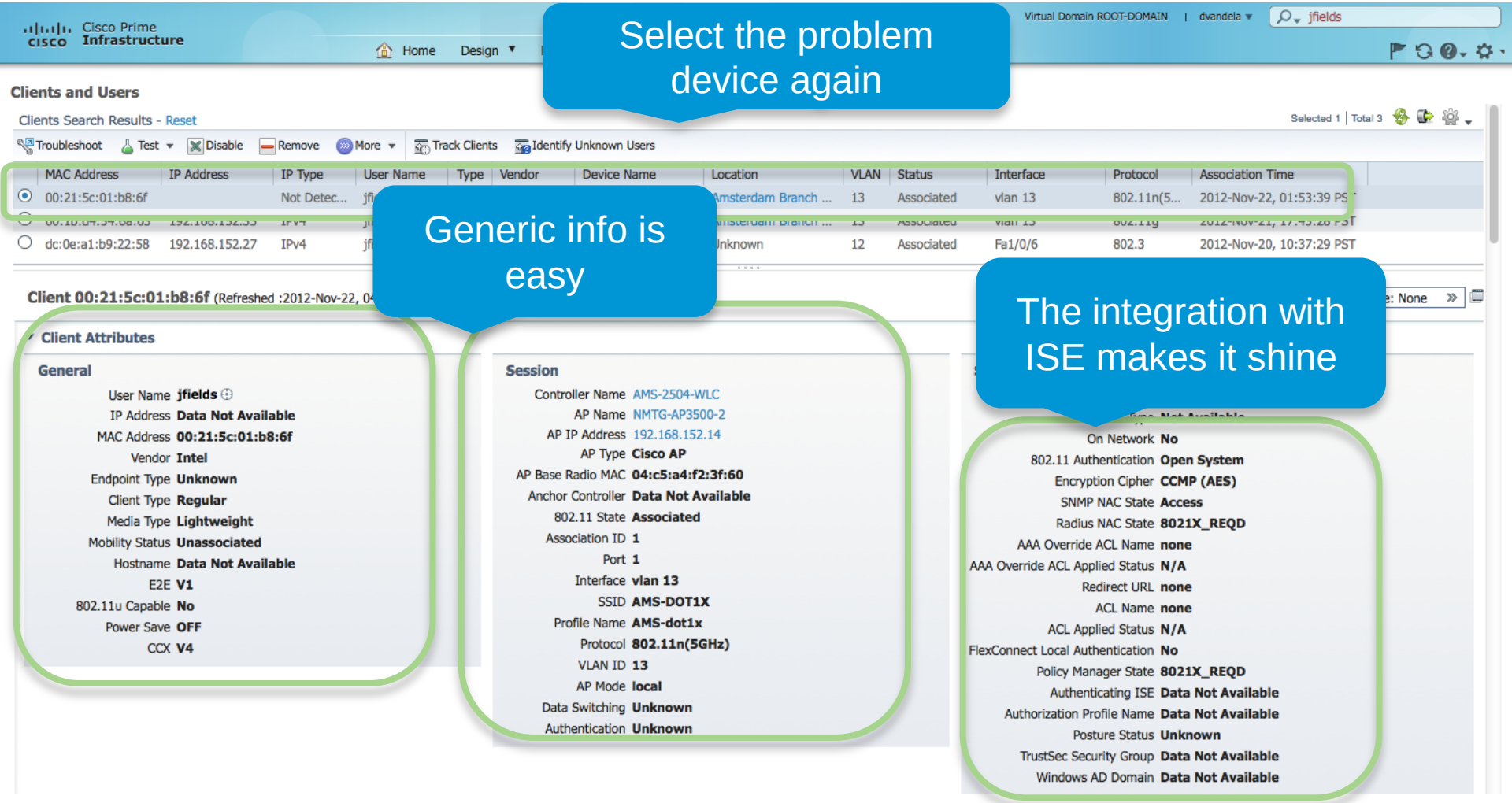
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



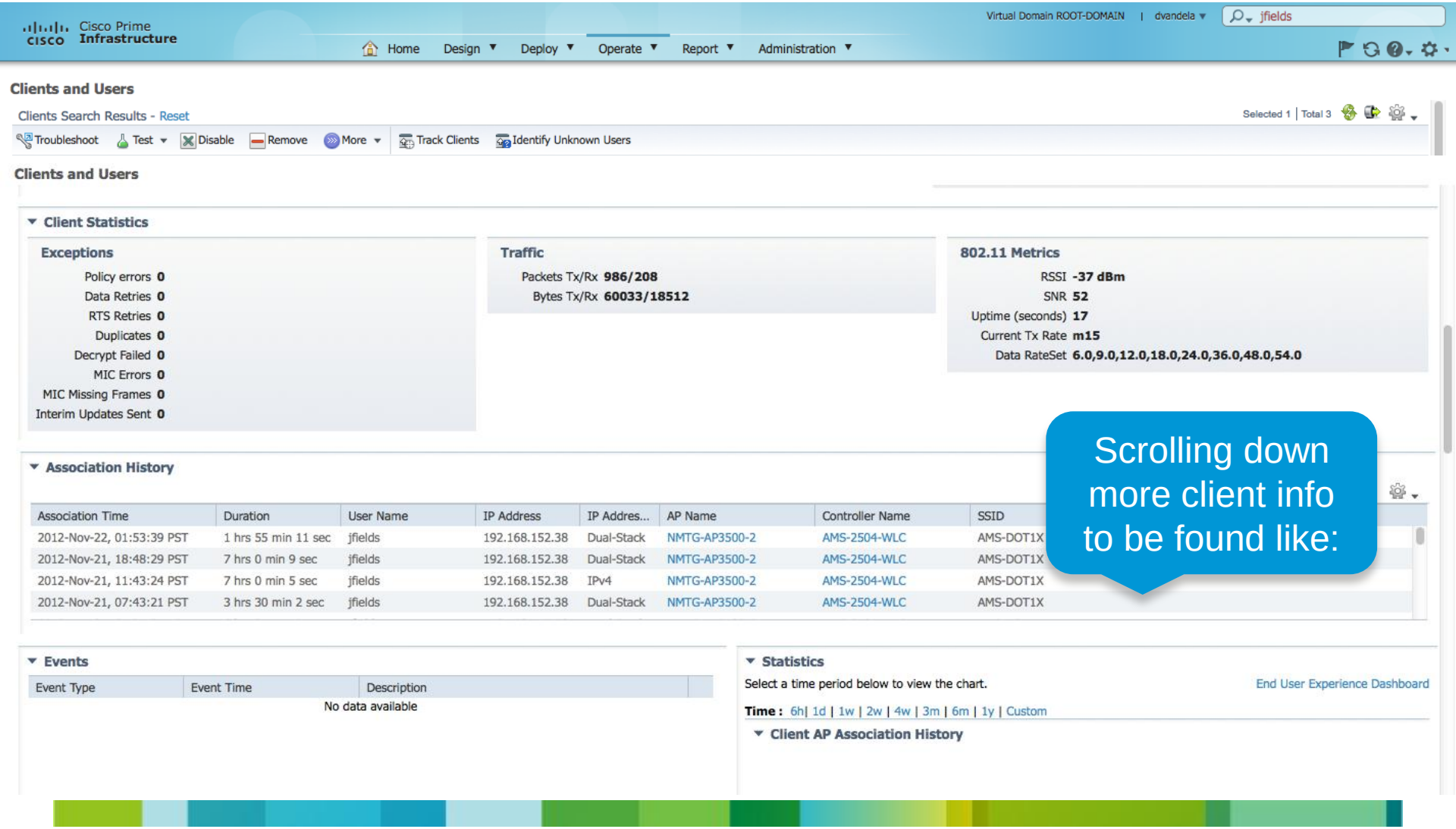
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



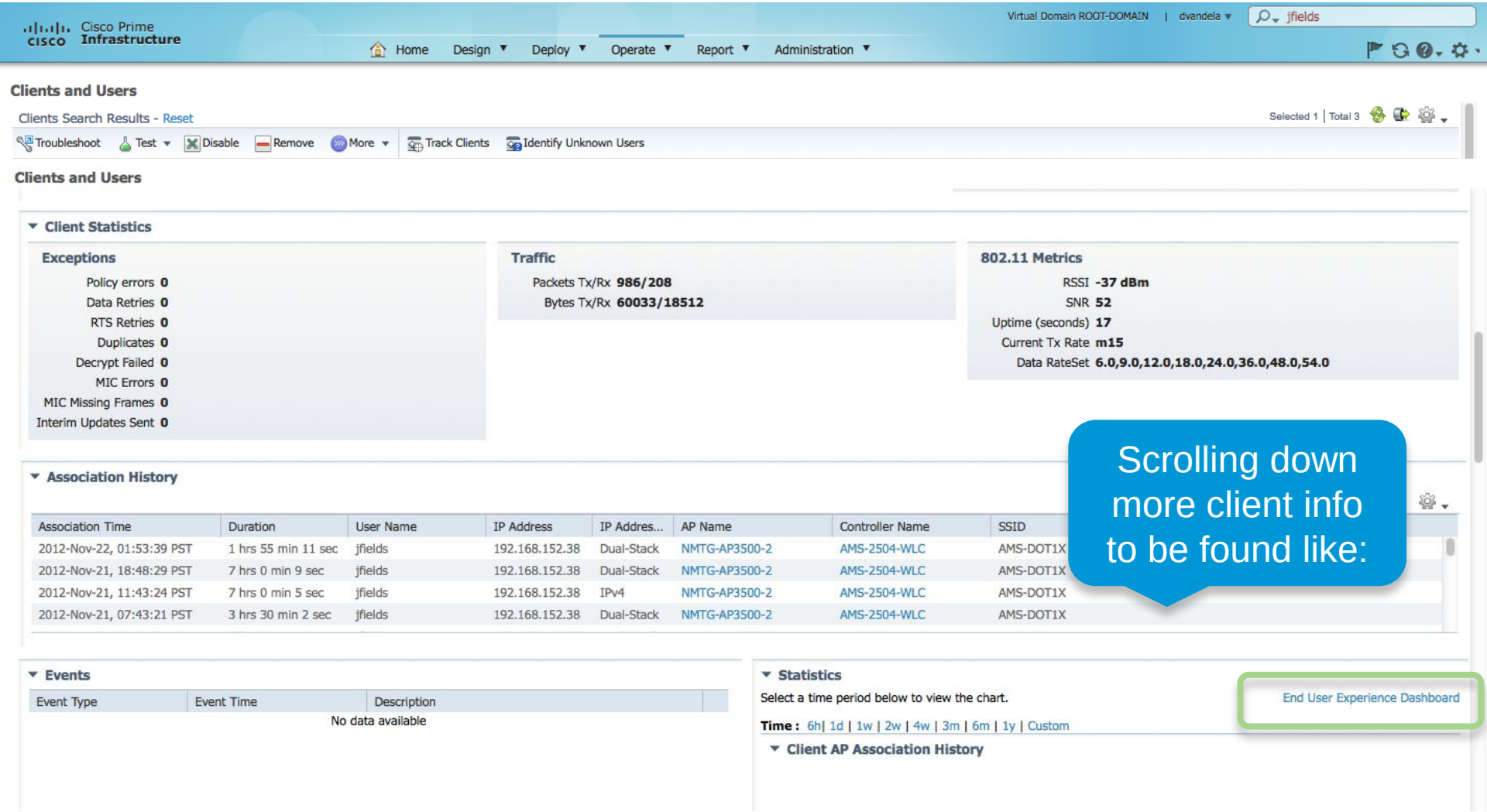
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



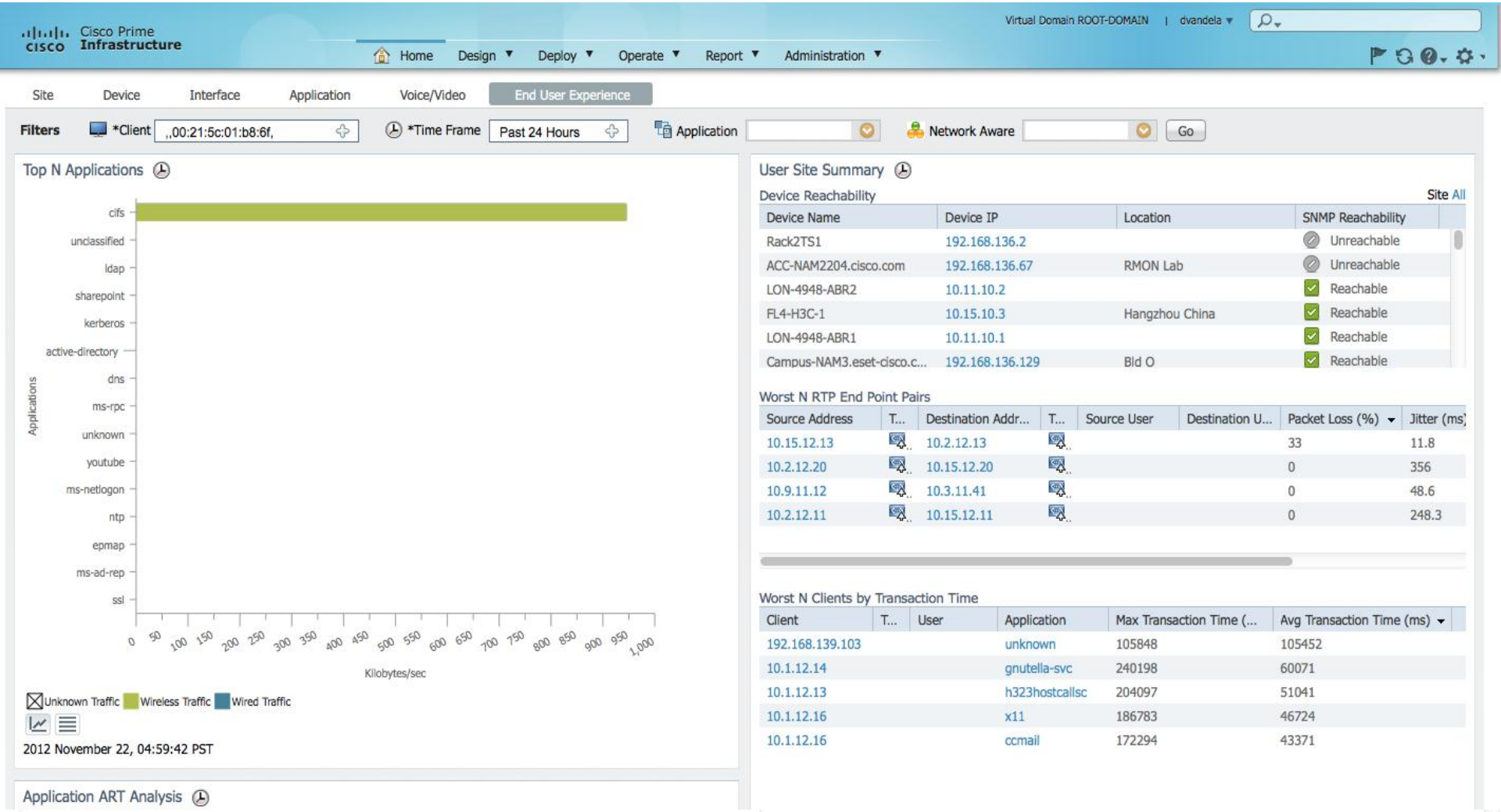
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

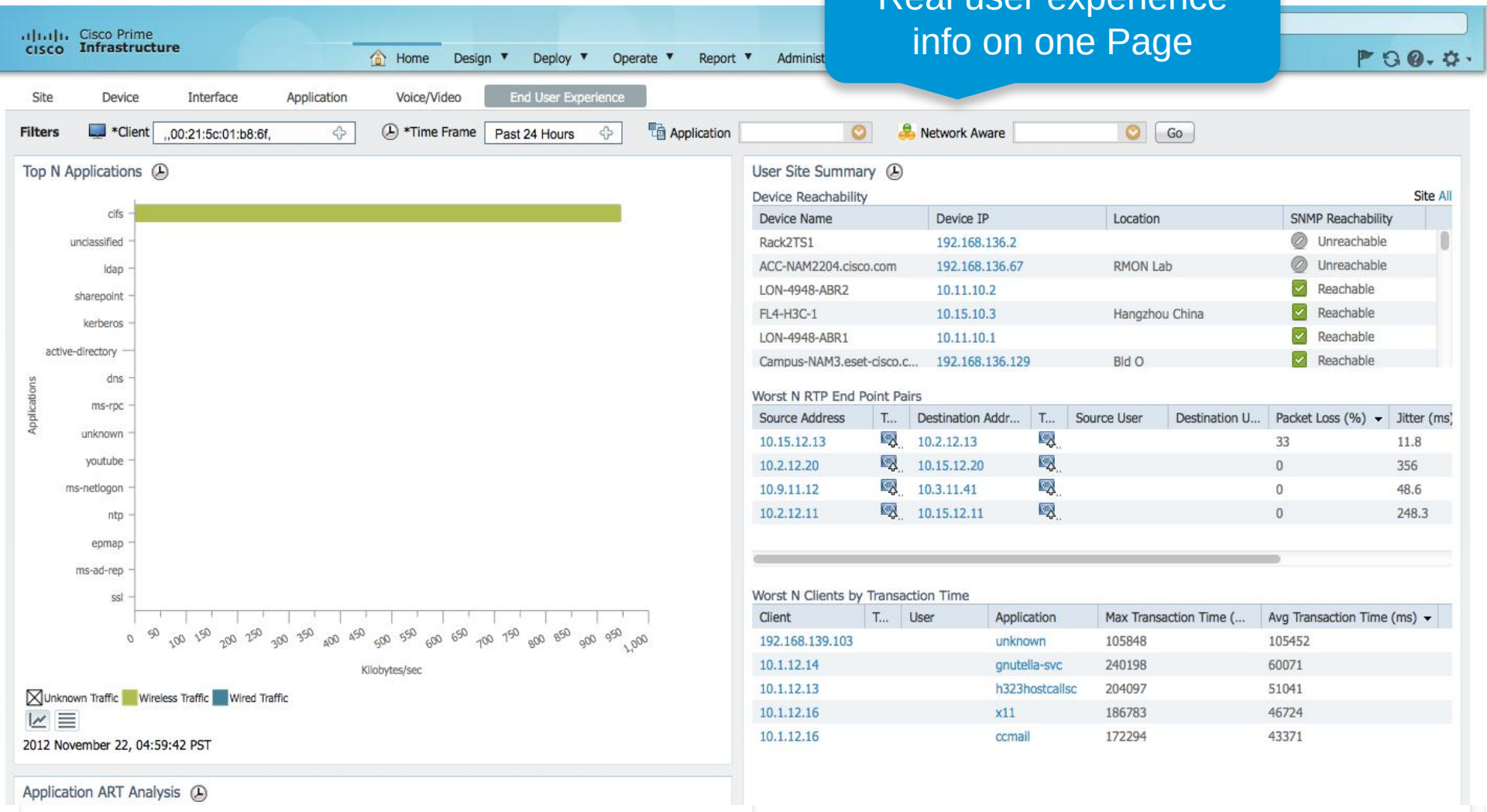


Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time



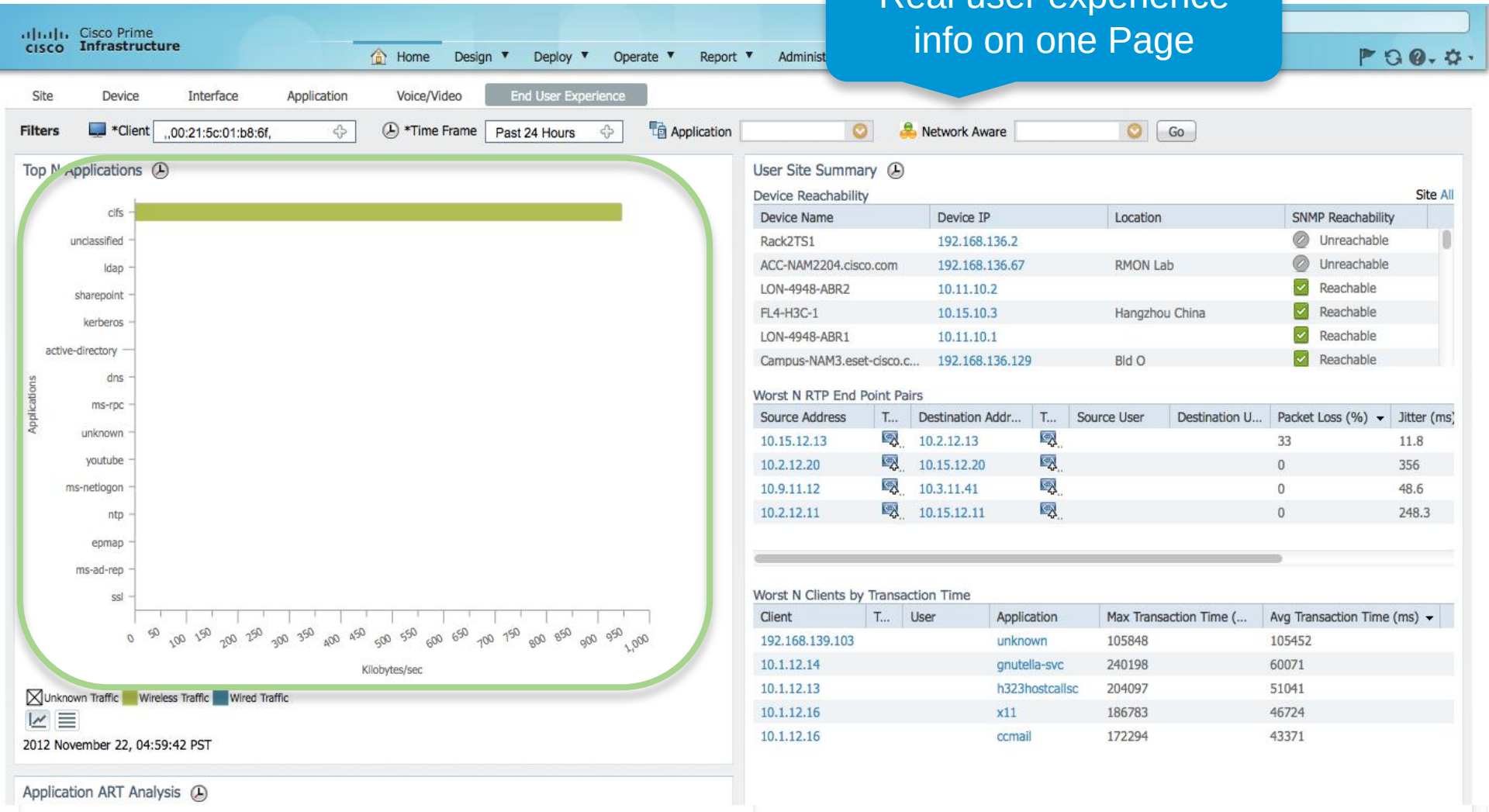
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page



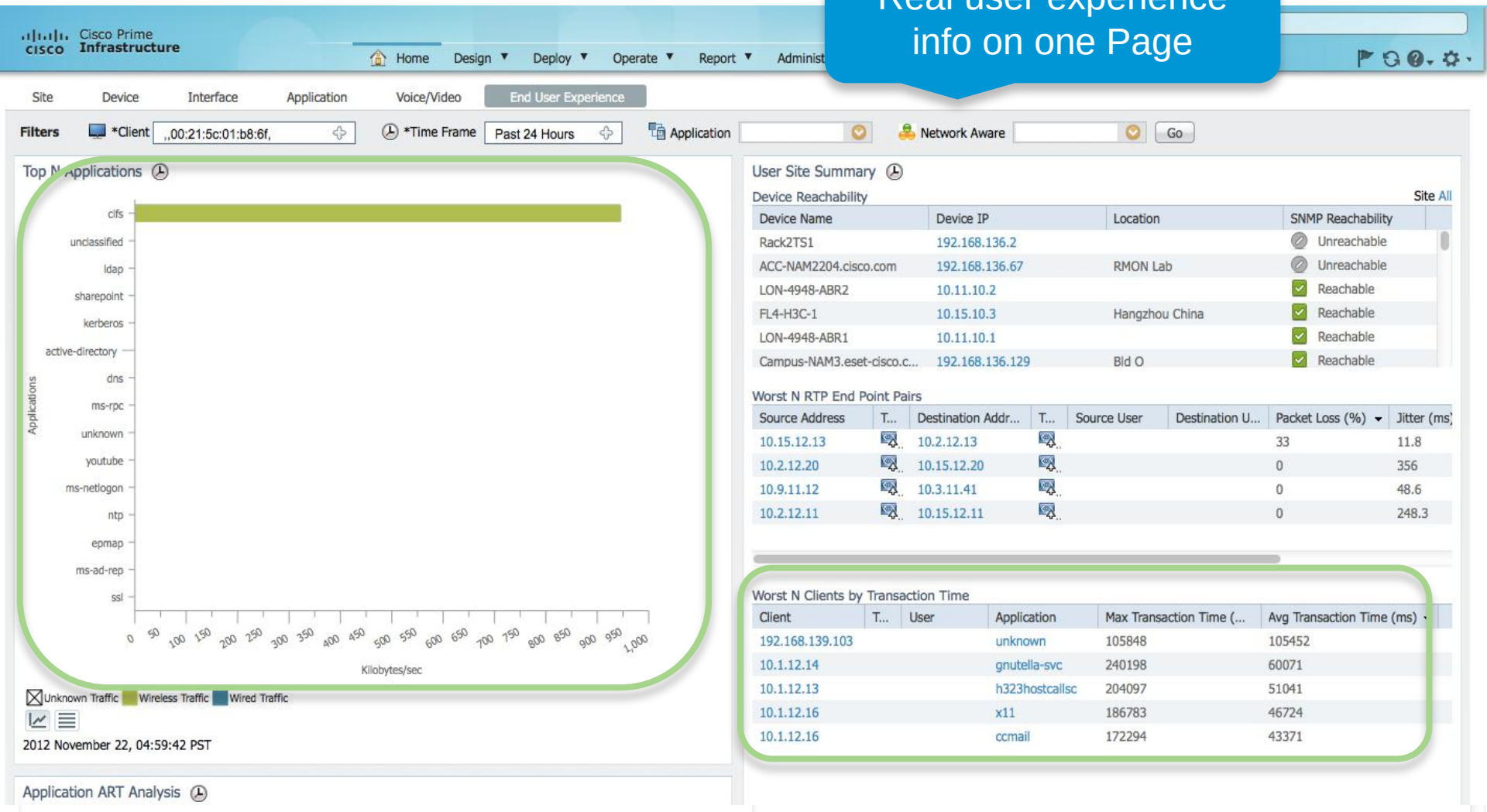
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page



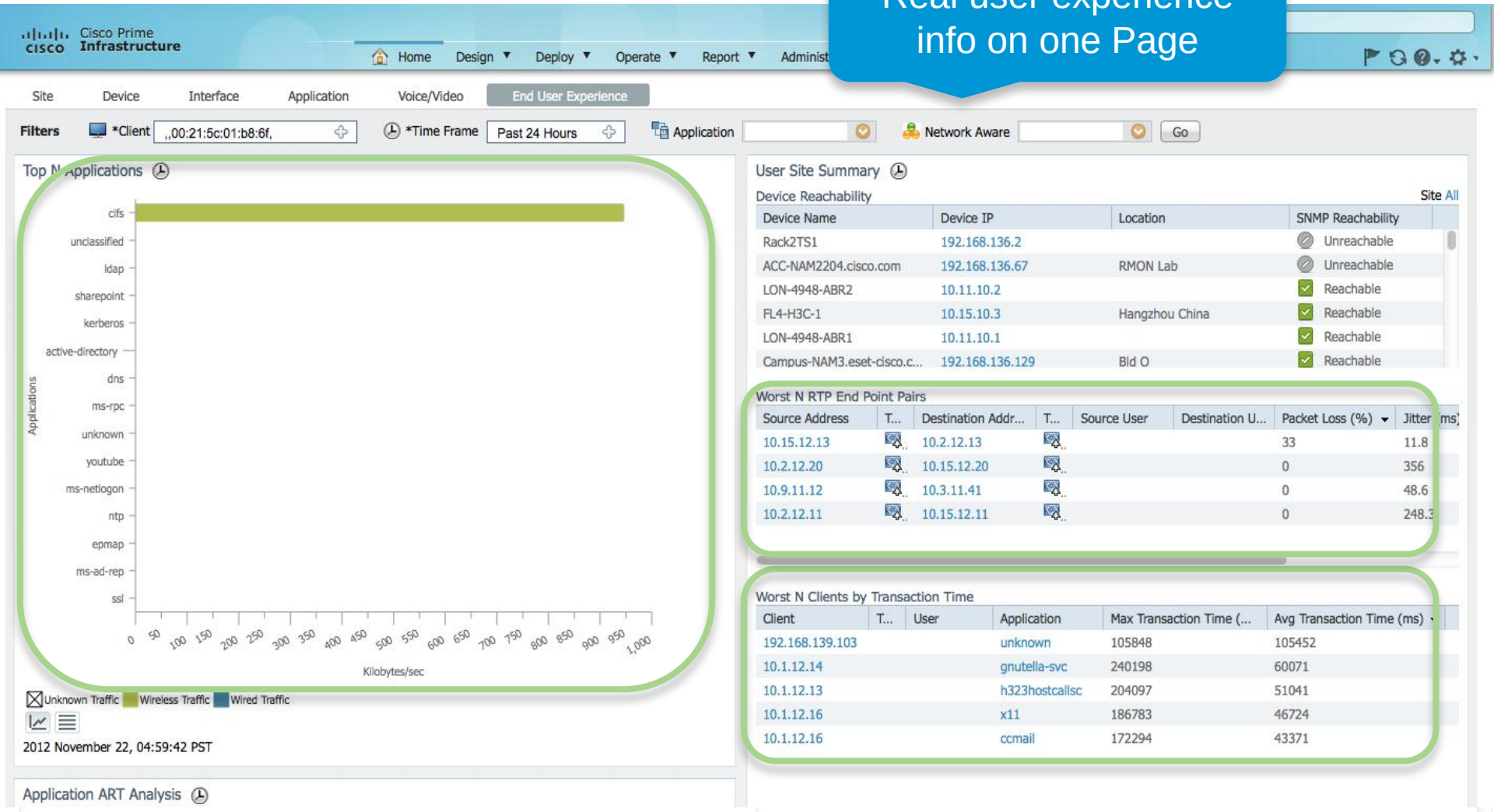
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page



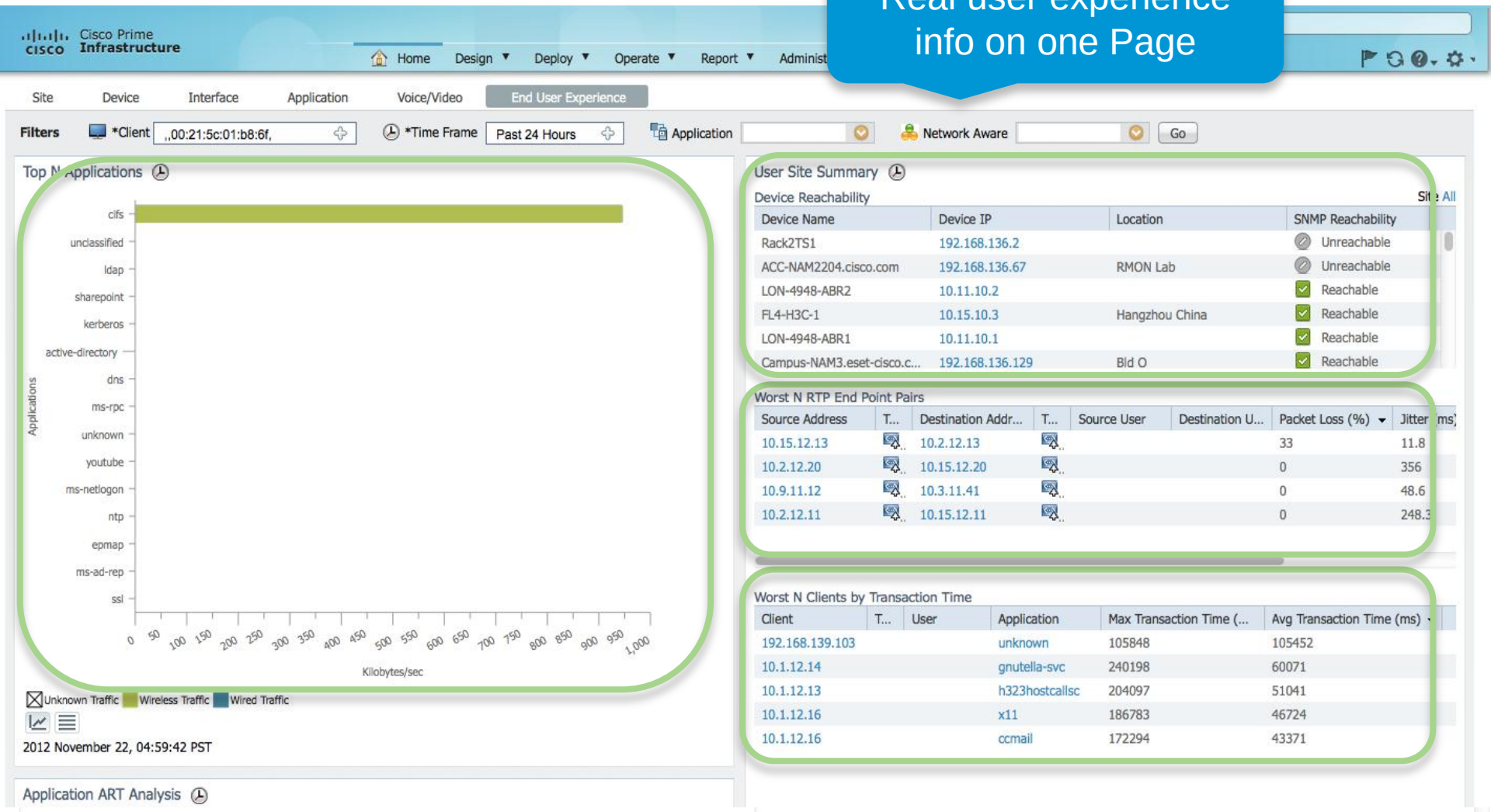
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page



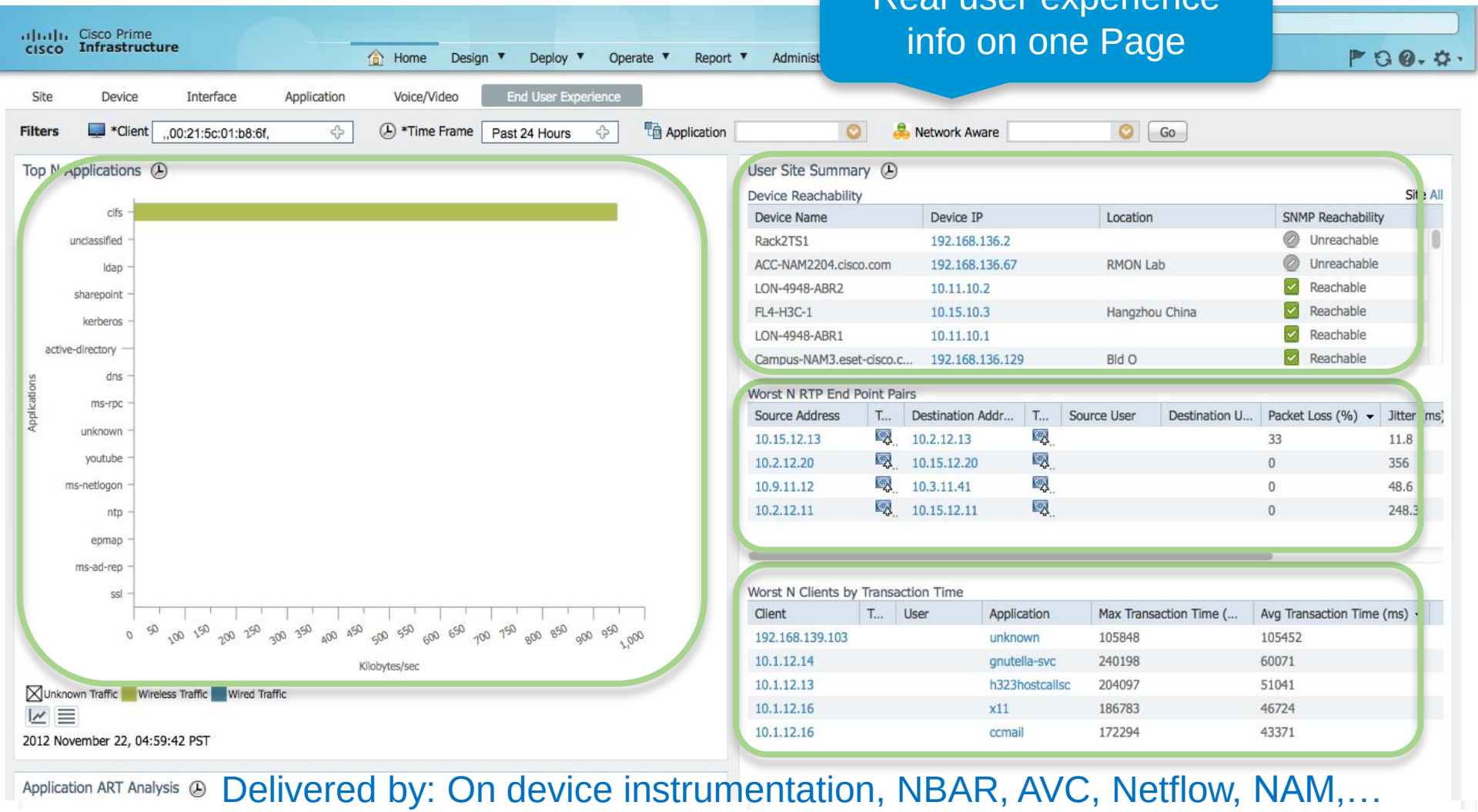
Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page



Prime Infrastructure: Client Connectivity Troubleshooting
Step 3. Check for Application Response time

Real user experience info on one Page

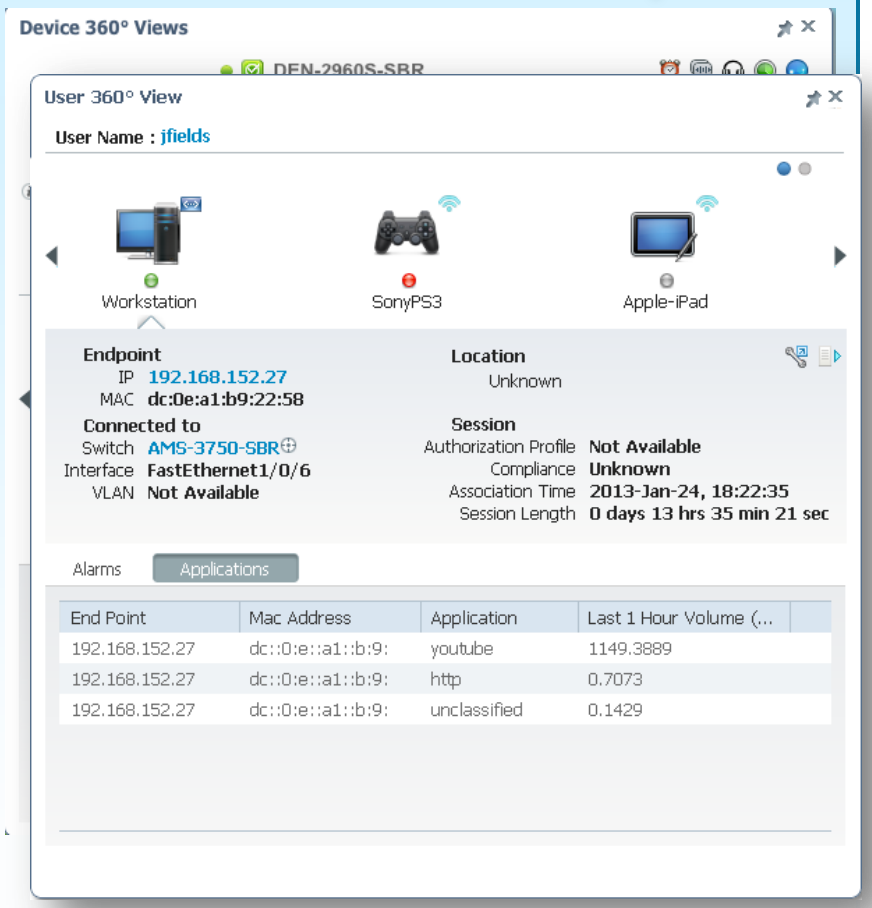


Delivered by: On device instrumentation, NBAR, AVC, Netflow, NAM,…

Achieve Operational Excellence
The 360 Experience

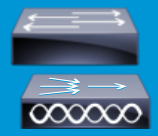
Coming in PI 2.X

- Simplified troubleshooting and remediation improves application, services and end user experience
  - Brings together multiple sources of information for effective problem isolation
- User 360 – quickly isolate and fix end-user or end-point issues (response time, network access, configuration etc.)
- Device 360 – identify and fix device related problems (performance, faults, interface, modules)
- Application 360 – identify and fix network issues related to app delivery (app discovery, utilization, user/device/site association)



One Policy

One Policy Platform - ISE: Use Cases



One Network

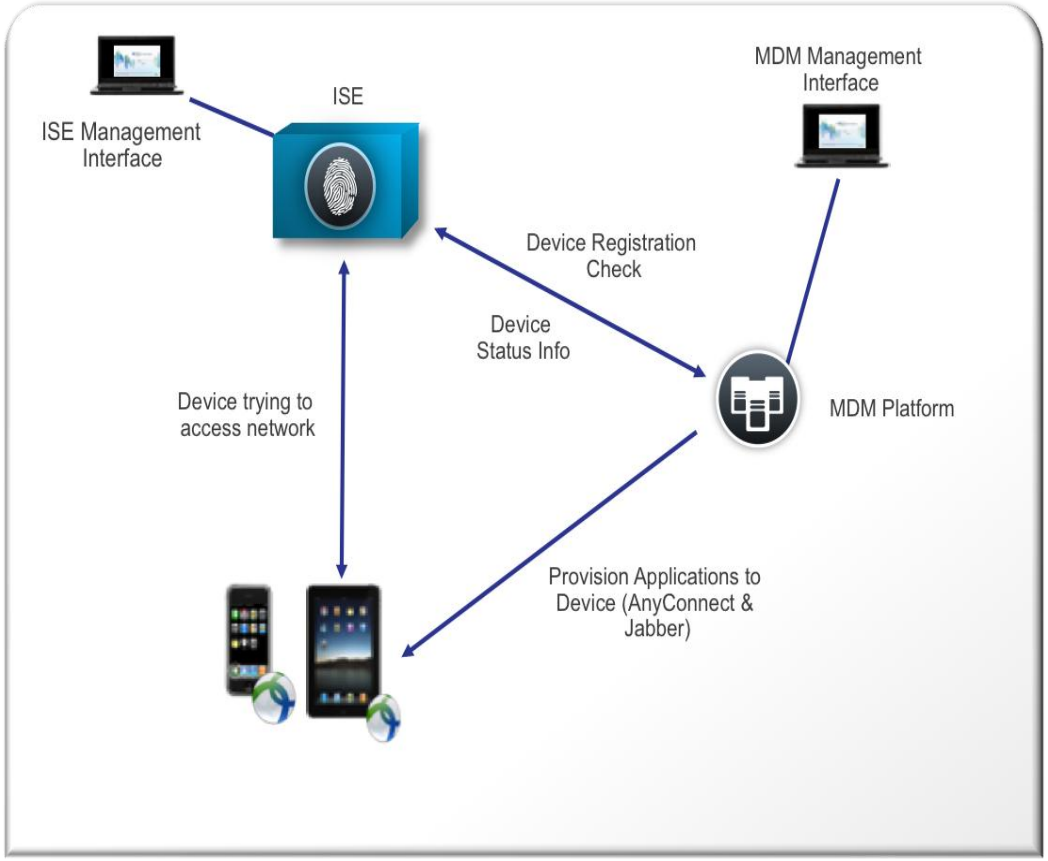
One Policy

One Management

I Only Want to Allow the "Right" Users and Devices on My Network	Authentication Services
I Want User and Devices to Receive Appropriate Network Services	Authorization Services
I Want to Allow Guests into the Network and Control Their Behavior	Guest Lifecycle Management
I Need to Allow/Deny iPads in My Network (BYOD)	Profiling and BYOD Services
I Want to Ensure That Devices on My Network Are Clean	Posture Services
I Need a Scalable Way (Topology Independent) of Enforcing Access Policy Across the Network	TrustSec SGA

ISE 1.2 and MDM Integration

- MDM device registration via ISE
  - Non registered clients redirected to MDM registration page
- Restricted access
  - Non compliant clients will be given restricted access based on policy
- Endpoint MDM agent
  - Compliance
  - Device applications c
- Device Action from ISE
  - Device stolen -> wipe data on client

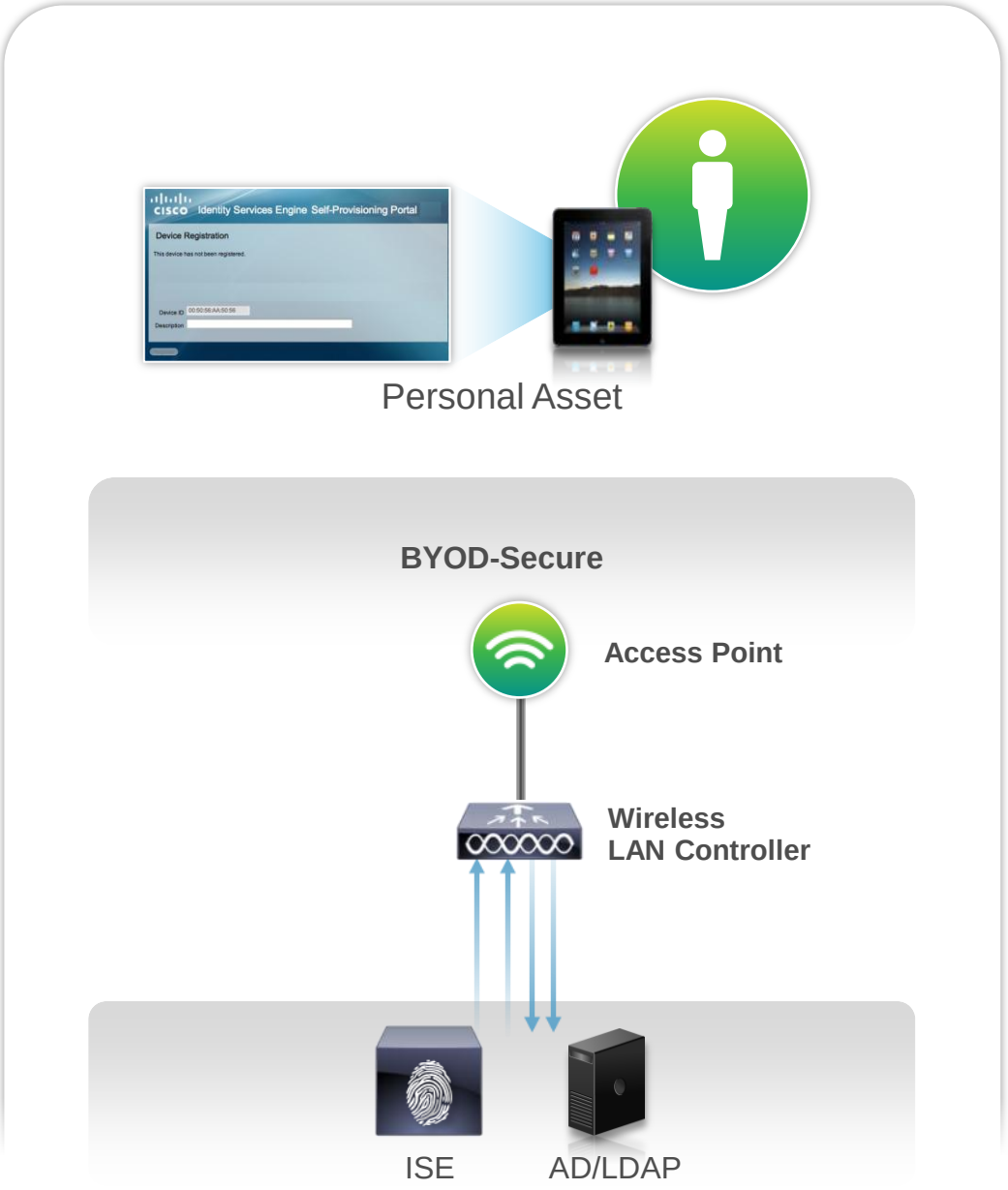


airwatch™ MobileIron® Good ZENPRISE

BYOD Flow

Single SSID, powered by ISE

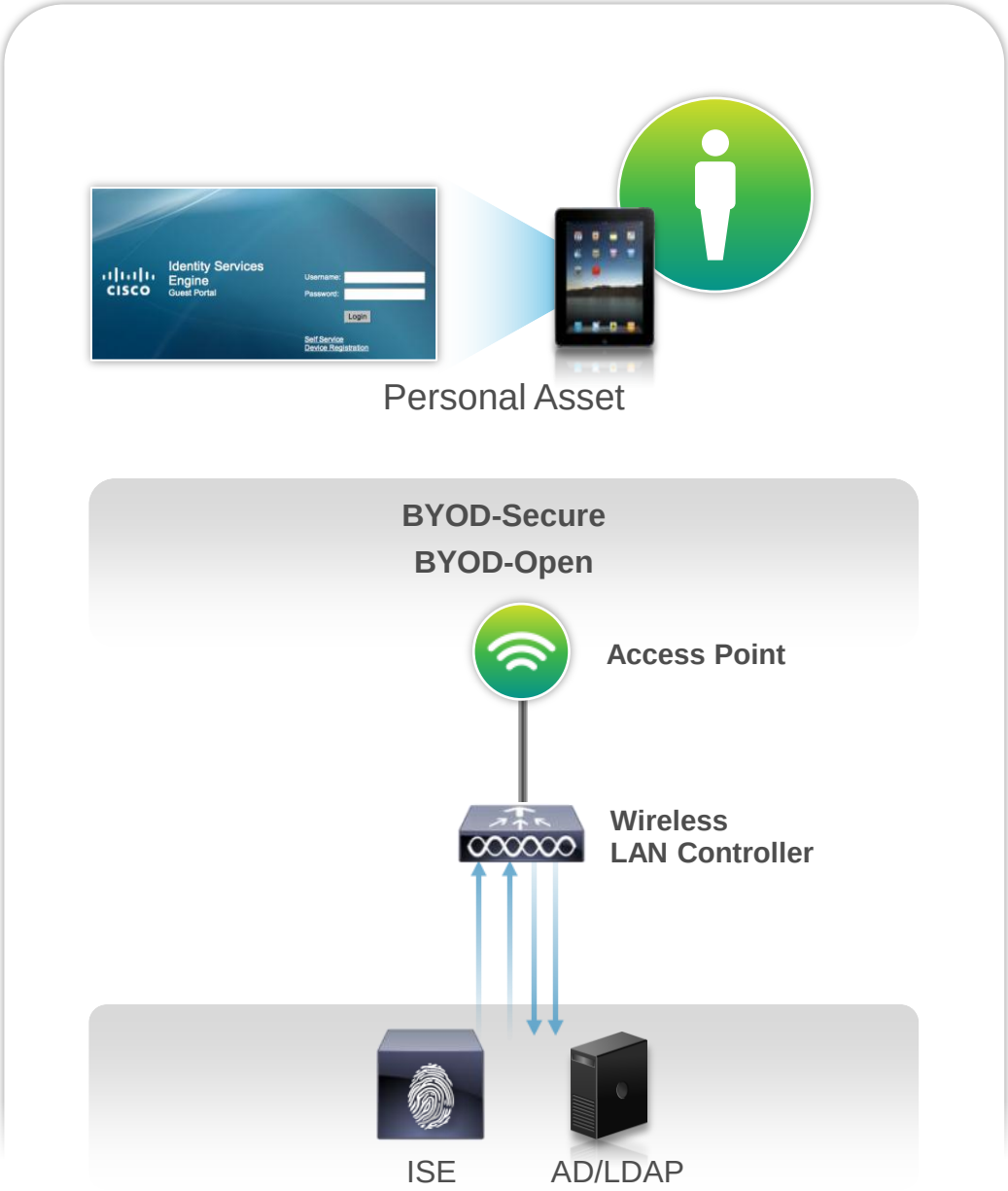
- User connects to Secure SSID
- PEAP: Username/Password
- Redirected to Provisioning Portal
- User registers device
  - Downloads Certificate
  - Downloads Supplicant Config
- User reconnects using EAP-TLS



BYOD Flow

Dual SSID, powered by ISE

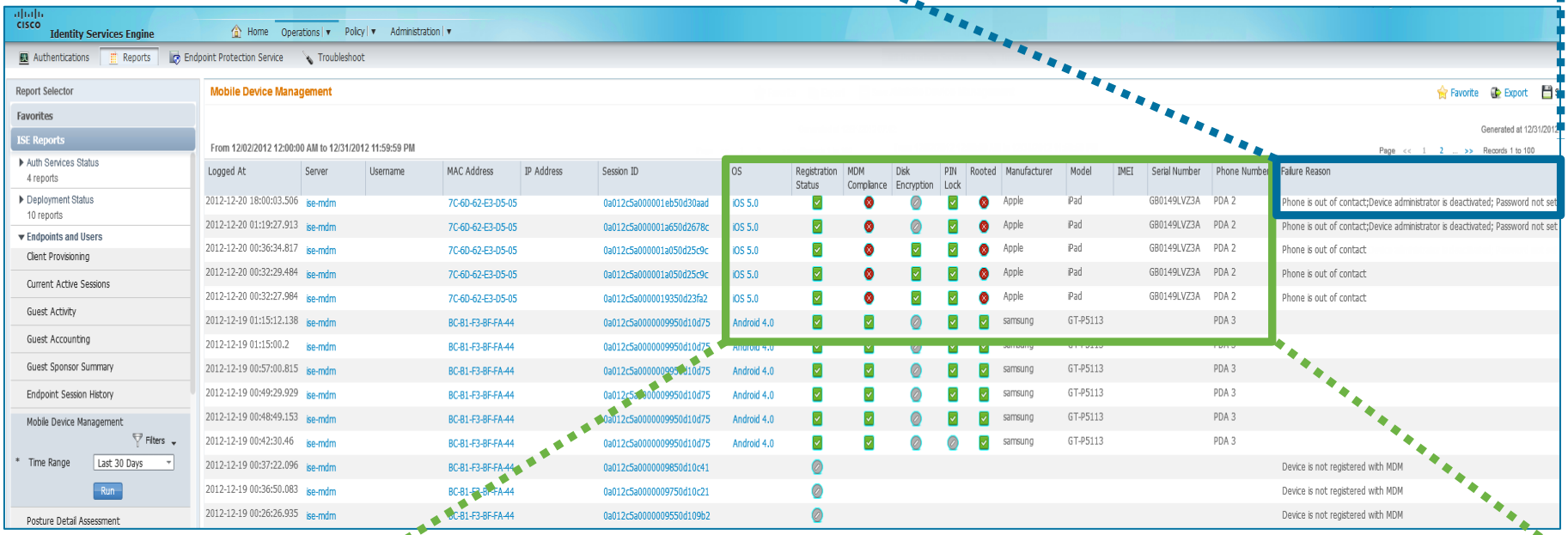
- User connects to Open SSID
- Redirected to WebAuth portal
- User enters employee or guest credentials
- Guest signs AUP and gets Guest access
- Employee registers device
  - Downloads Certificate
  - Downloads Supplicant Config
- Employee reconnects using EAP-TLS



ISE Reporting with MDM

Failure Reason

Phone is out of contact;Device administrator is deactivated; Password not set



OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number
iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3

Industry Leading Identity Features
of Cisco Infrastructure

Cisco Innovation

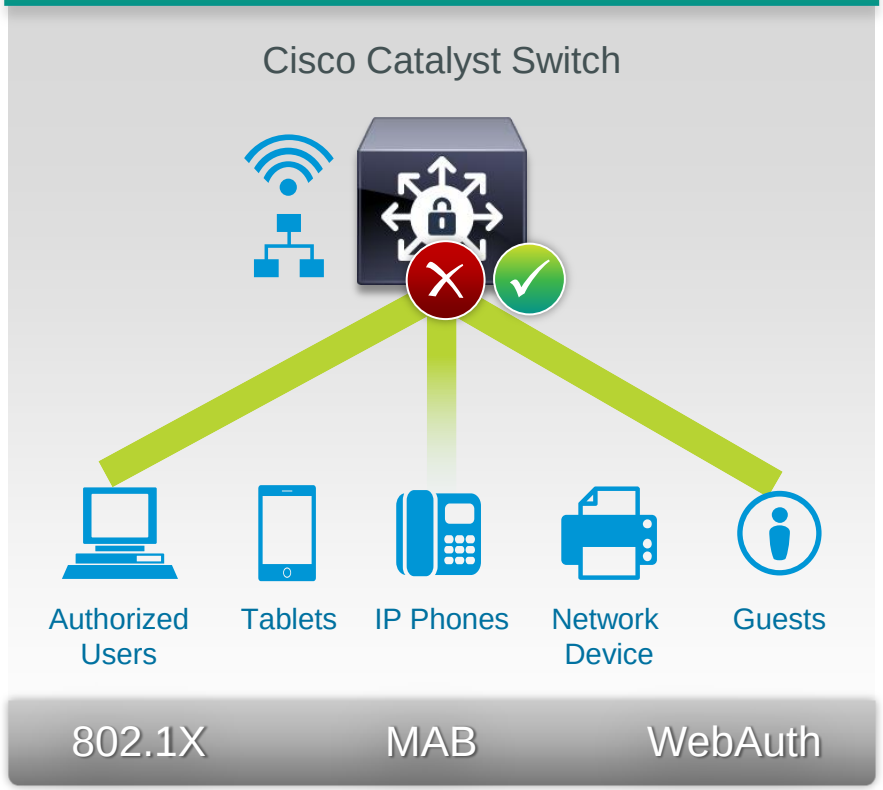
Identity Differentiators

- Monitor Mode
  - Unobstructed access
  - No impact on productivity
  - Gain visibility
- Flexible Authentication Sequence
  - Enables single configuration for most use cases
  - Flexible fallback mechanism and policies

Rich and Robust 802.1X

- IP Telephony Support for Virtual Desktop Environments
  - Single host mode
  - Multihost mode
  - Multiauth mode
  - Multidomain authentication
- Critical Data/Voice Authentication
  - Business continuity in case of failure

Authentication Features



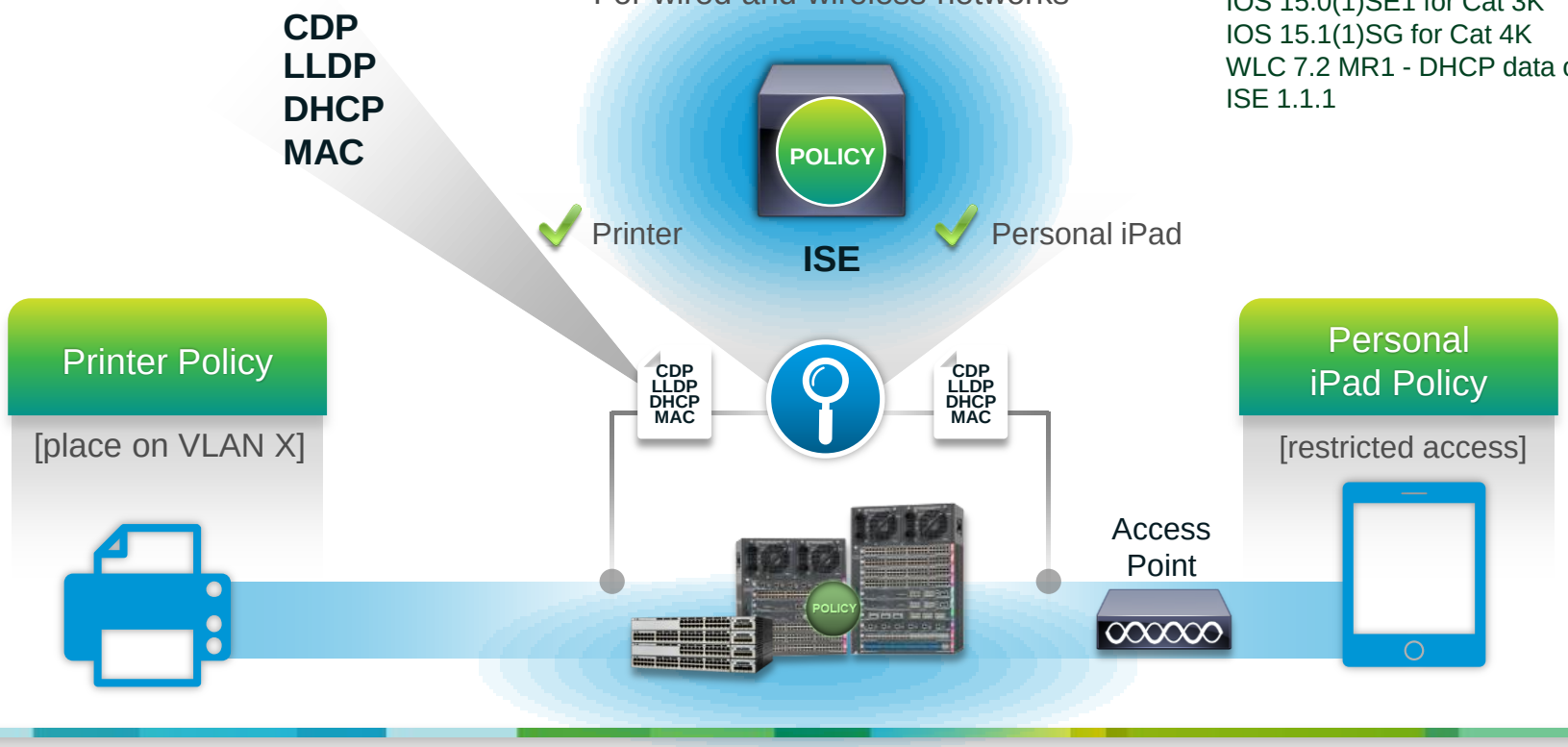
Device Sensor

Automated Device Classification Using Cisco Infrastructure

Cisco Innovation

DEVICE PROFILING

For wired and wireless networks



Supported Platforms:
IOS 15.0(1)SE1 for Cat 3K
IOS 15.1(1)SG for Cat 4K
WLC 7.2 MR1 - DHCP data only
ISE 1.1.1

The Solution

Efficient Device Classification Leveraging Infrastructure

Deployment Scenario With Cisco Device Sensors

COLLECTION
Switch Collects Device Related Data and Sends Report to ISE

CLASSIFICATION
ISE Classifies Device, Collects Flow Information and Provides Device Usage Report

AUTHORIZATION
ISE Executes Policy Based on User and Device

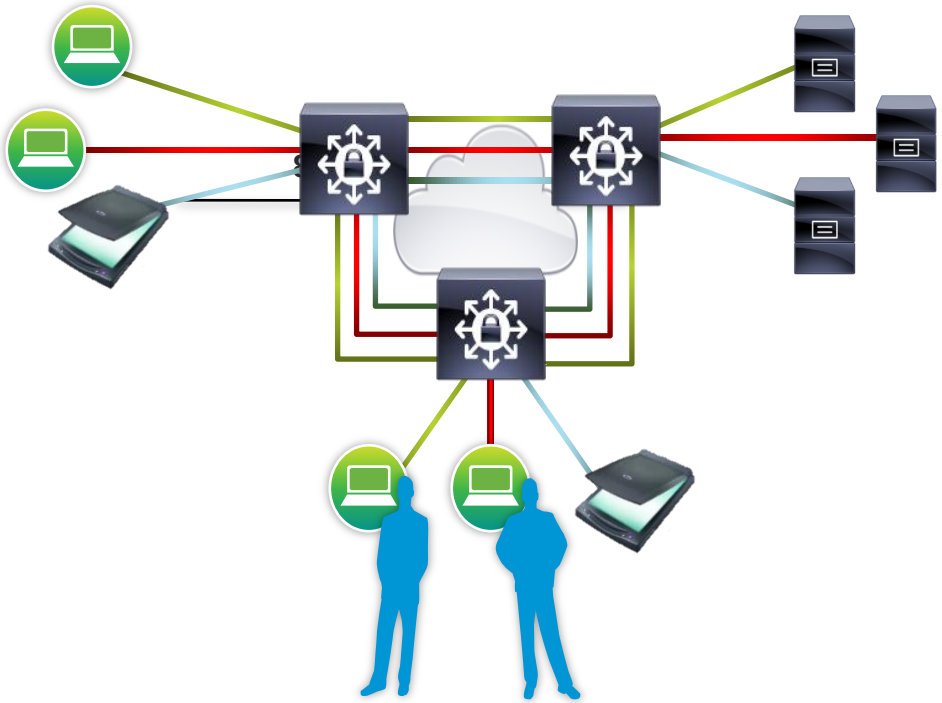
Policy Enforcement: VLANs or ACLs?

VLAN Architecture

Scaling Concerns

Highly topology dependent

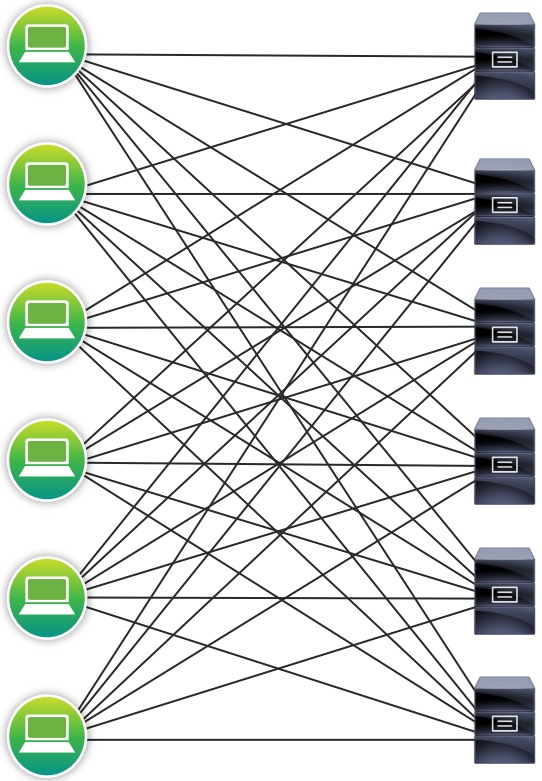
Endpoint IP address release/renew challenging



ACL Architecture

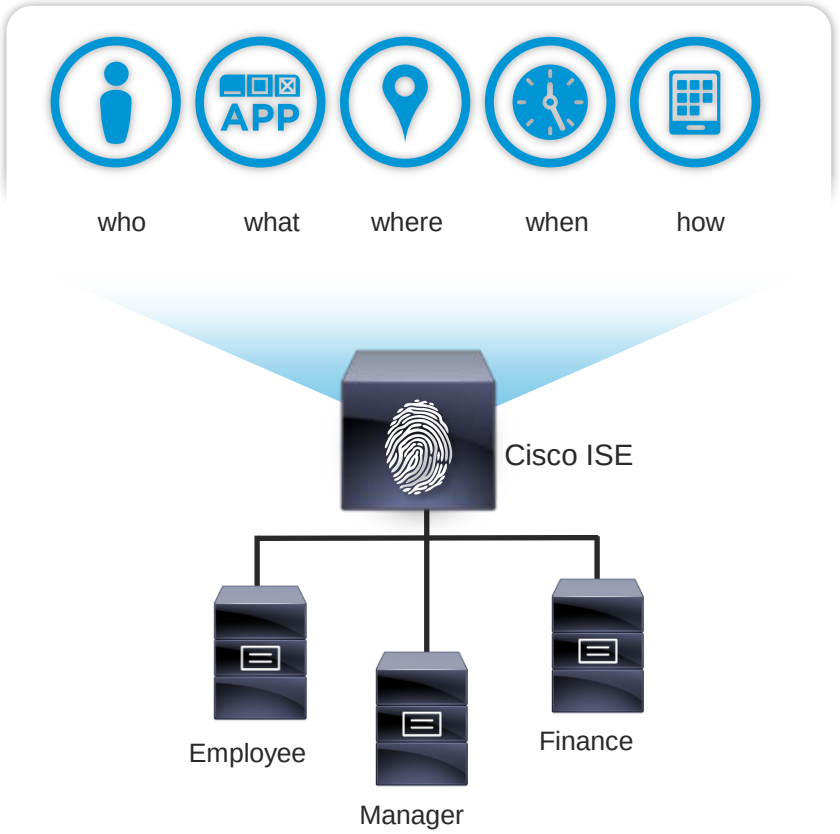
Hard to Maintain

100s–1000s of ACEs

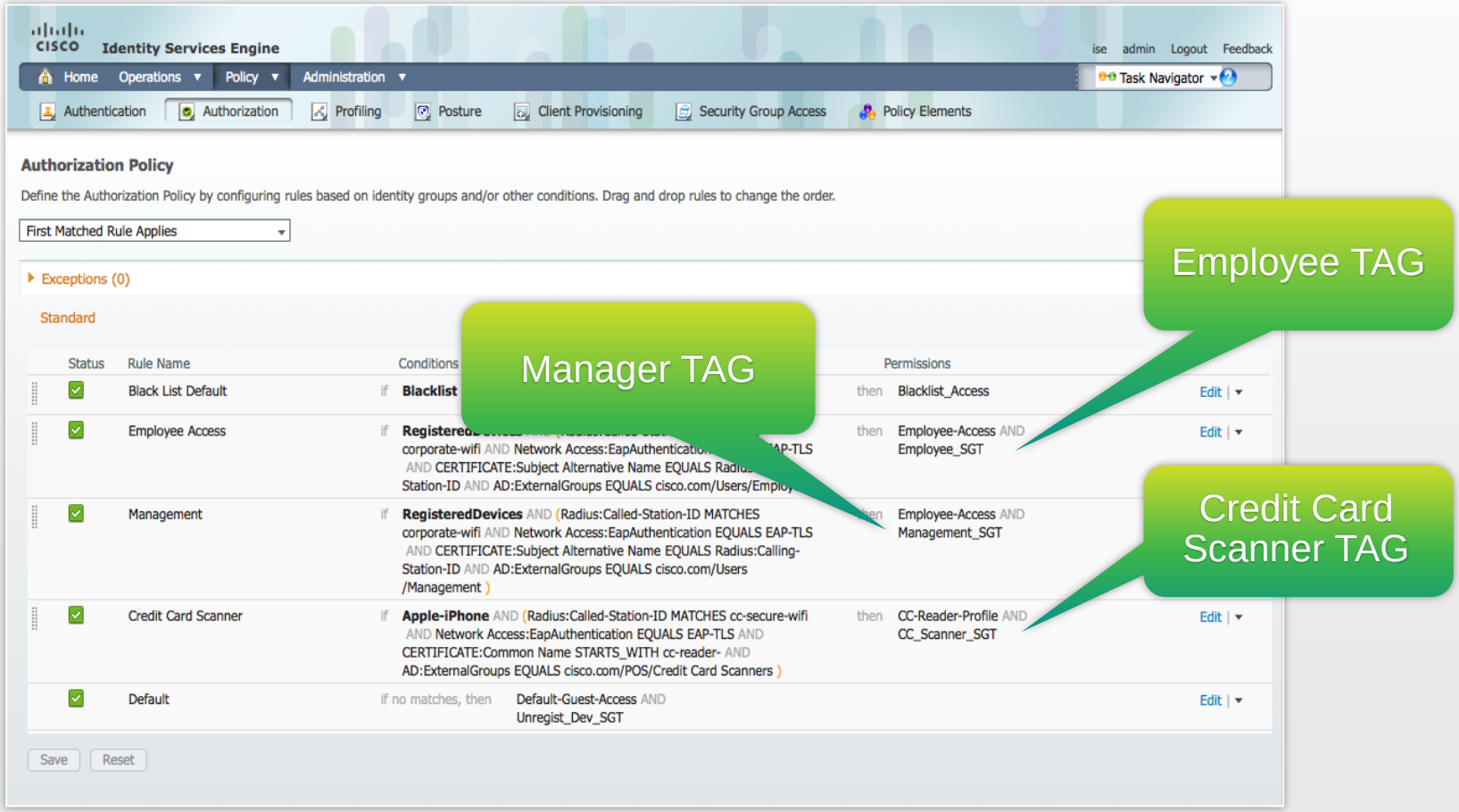


Policy Enforcement: Security Group Access!
SGA – Topology Independent

User and Device Role	SGA TAG - Policy
Public SSID	Unregistered Device (Unregist_Dev_SGT)
Corporate SSID Member of group “Employee” Certificate matches endpoint	Employee (Employee_SGT)
Corporate SSID Member of group Employee and Manager Certificate matches endpoint	Management (Management_SGT)
Credit_Card SSID Member of group “Credit_Scanners” Profiled as “iphone”	Credit Card Scanners (CC_Scanner_SGT)

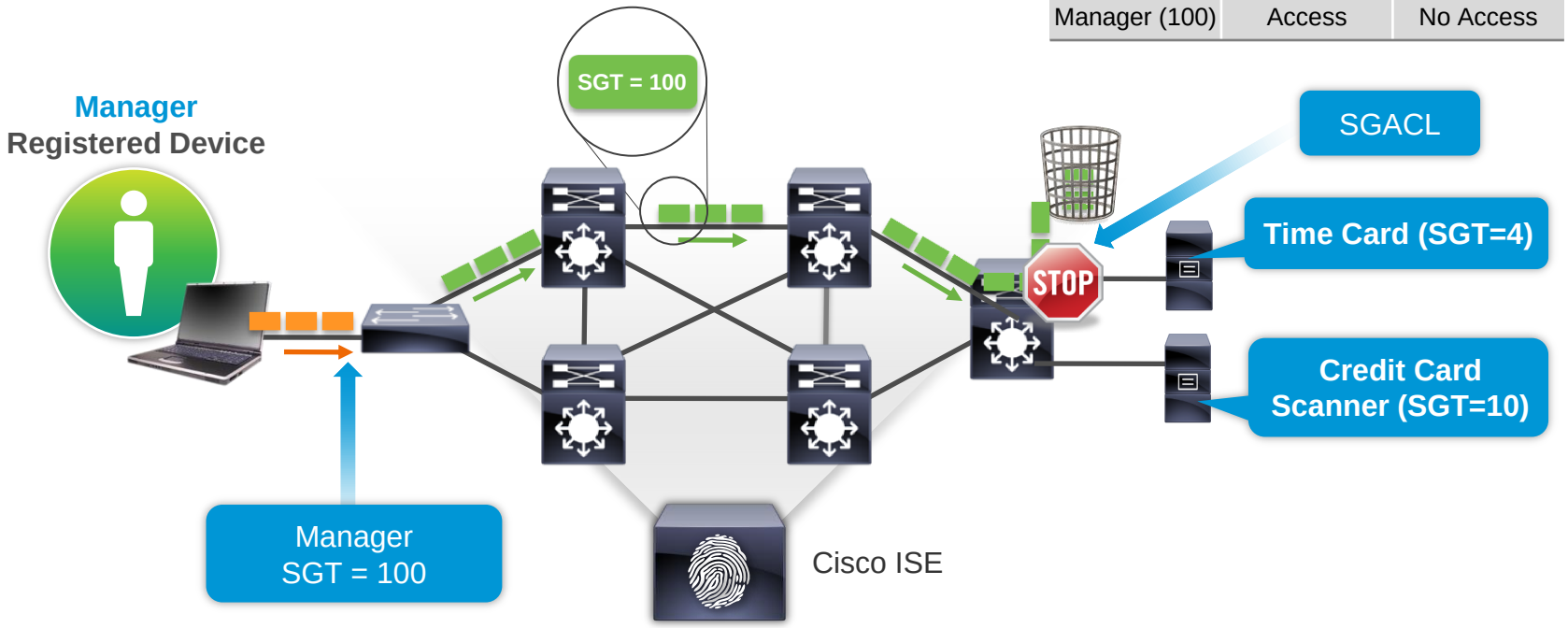


SGA Inside ISE



SGA Policy Enforcement Flow

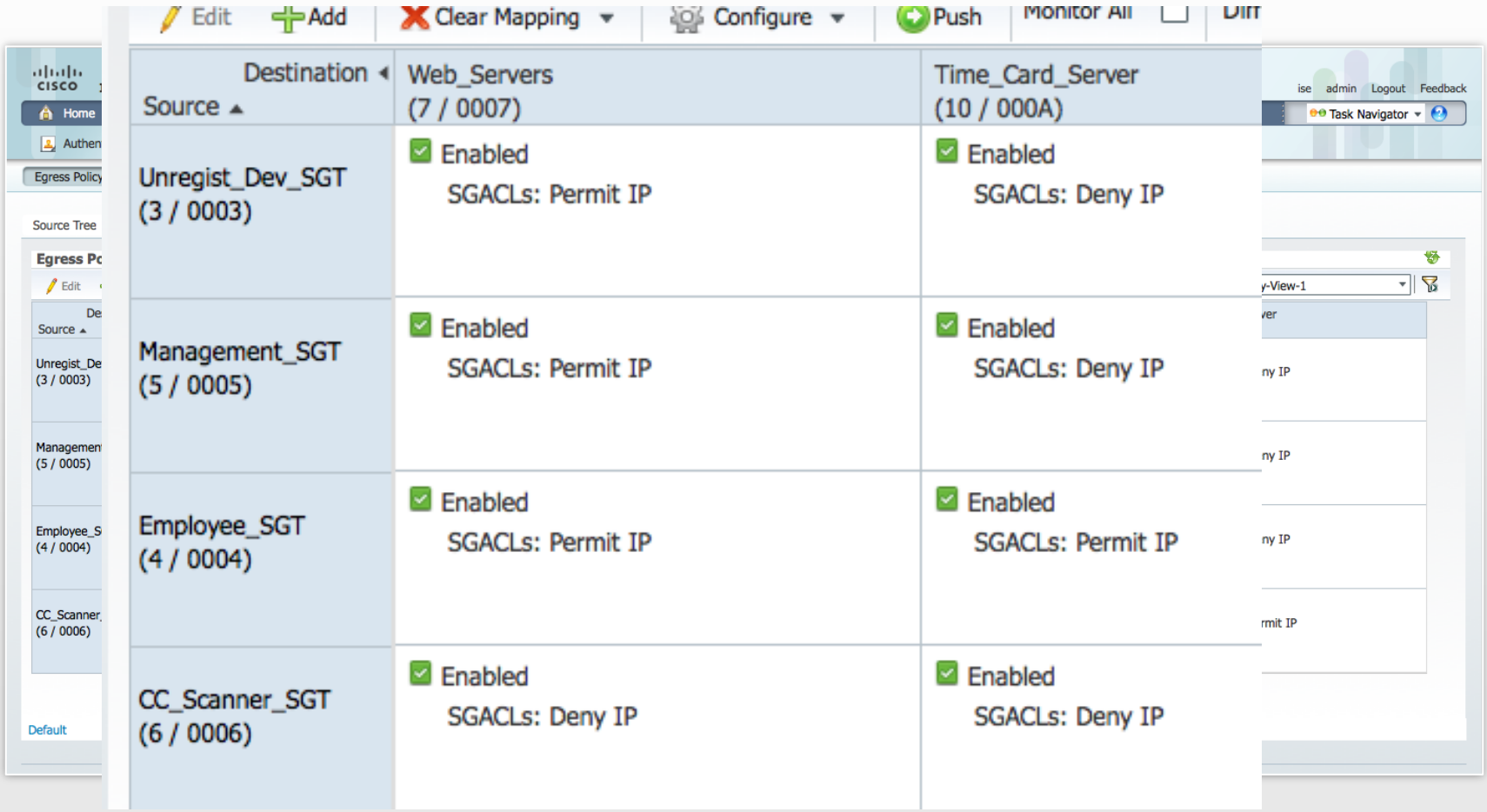
SRC\DST	Time Card	Credit Card
Manager (100)	Access	No Access



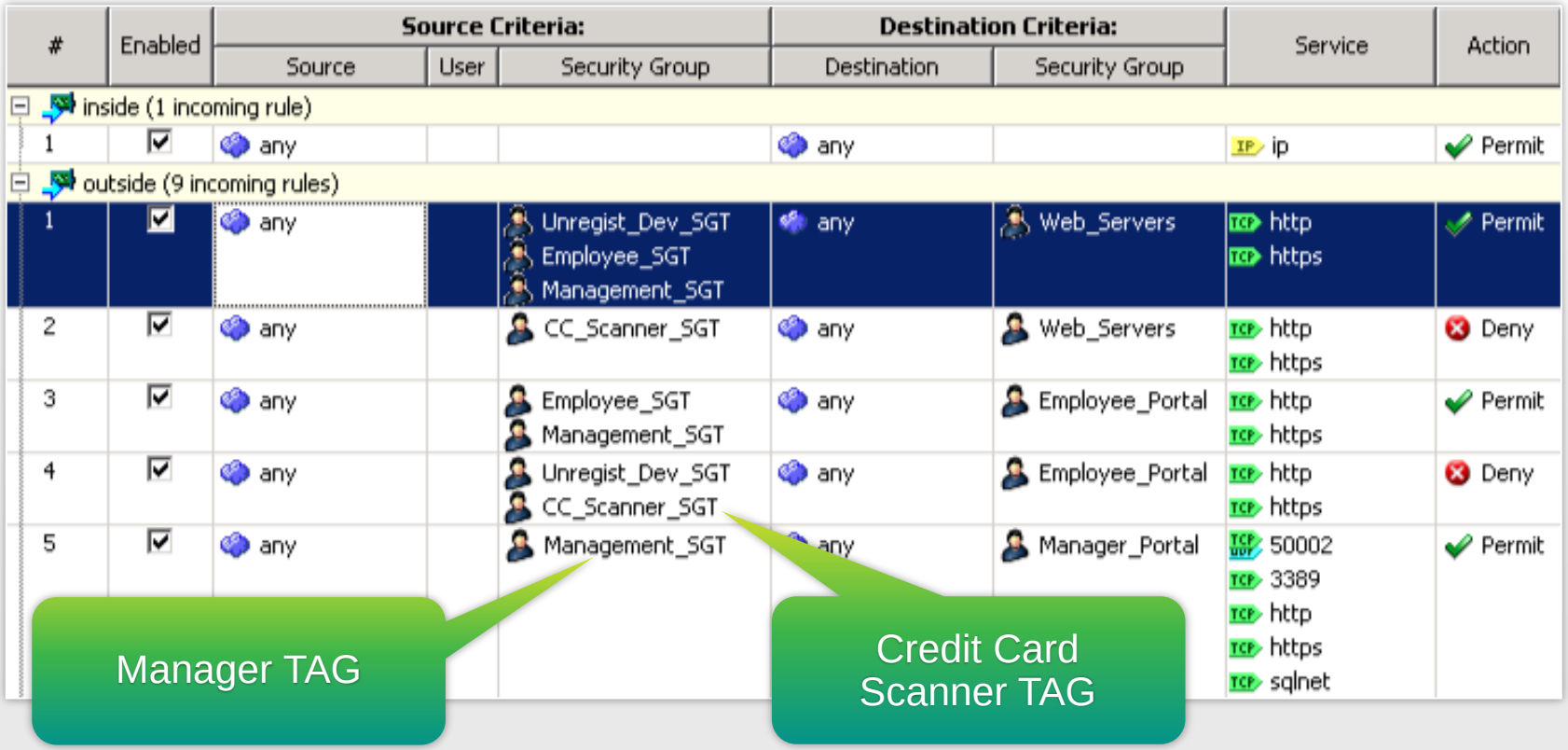
Security Group Based Access Control

- ISE maps tags (SGT) with user identity
- ISE Authorization policy pushes SGT to ingress NAD (switch/WLC)
- ISE Authorization policy pushes ACL (SGACL) to egress NAD (ASA or Nexus or Catalyst)

SGA Enforced on Switches



SGA Enforced at ASA Firewall

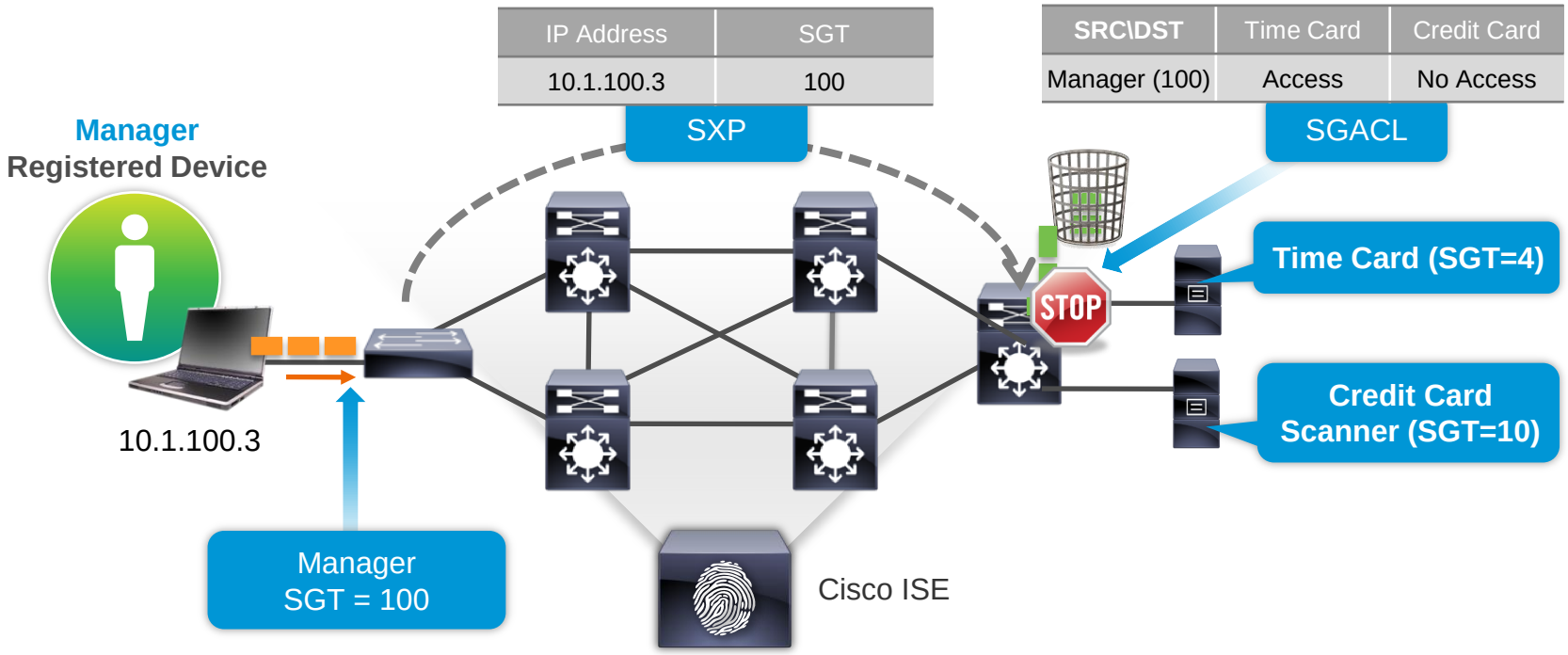


#	Enabled	Source Criteria: Source	Source Criteria: User	Source Criteria: Security Group	Destination Criteria: Destination	Destination Criteria: Security Group	Service	Action
inside (1 incoming rule)								
1	☑	any			any		ip	Permit
outside (9 incoming rules)								
1	☑	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit
2	☑	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny
3	☑	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit
4	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny
5	☑	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit

Migrating to Security Group Access

SGT eXchange Protocol (SXP)

Cisco Innovation

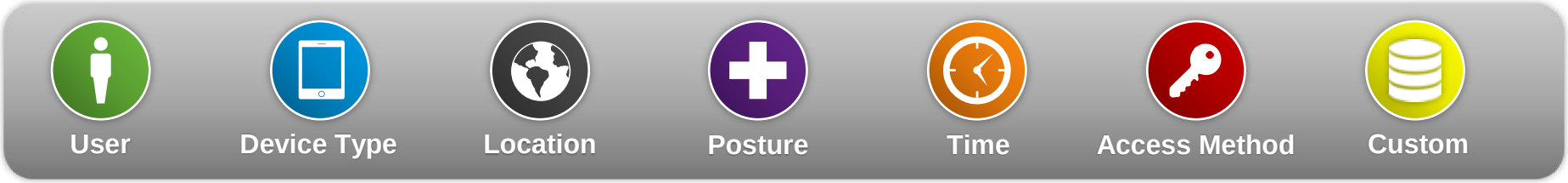


Security Group Access Protocol

- For transport through a non SGT core

Tying it All Together

ISE Authorization Policy Definition



Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
Enabled	Game_Console	Game_Console-Registered		Game_Console
Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San_Jose AND CERTIFICATE:Subject Alternative Nam MATCHES .*(demo.local)$ AND Radius:User-Name MATCHES ^(host/).*	AD_Login
Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND LDAP1:badPwdCour MATCHES [0-5]	Employee_Wireless
Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry	Contrator_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
Disabled	Default-Posture	Any		CWA_Posture_Remediation
Enabled	Default	Any		Central_Web_Auth

One Policy - ISE

BYOD

- User Self Onboarding
- MDM Vendor Partnerships

Access Control

- Context: Who/What/How/Where
- Visibility: Profiling

Holistic Solution

- SGA: Topology independent, Business language
- Enforcement: Router/Switch/Controller feature
- Endpoint: Posture, VPN
- Info stores: AD, LDAP, DHCP, MDM
- MACSec: L2 encryption

One Network

Cisco Aironet 802.11n + 802.11ac AP Portfolio

TELEWORKER READY

600

- Basic Connectivity
- Deployment Flexibility
- Teleworker

ENTERPRISE READY

1600

- Enterprise-class Performance
- Voice/Video/Multimedia

MISSION CRITICAL

2600

- Any Device / BYOD Optimized
- Client Scalability
- RF Interference Mitigation

BEST IN CLASS

3600

- High Client Density
- HD Video/VDI
- Investment Protection
- 11ac Migration
- Comprehensive Security

H1 2013

New

802.11ac Module
WSSI Module

Home | Sm/Med | Sm/Med/Large | Med/Large Enterprise

WLAN Controller Portfolio

Large Campus

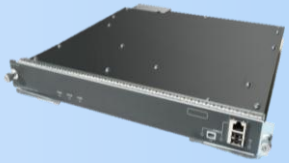
Catalyst 3850

- 1 to 50 APs per switch/stack (Directly connected APs)
- 2000 clients per stack
- 40 Gbps per switch

5508

- 12 to 500 APs
- 7000 clients
- 8 Gbps

WISM2



- 100 to 1000 APs
- 15,000 clients
- 20 Gbps

5760

- 25 to 1000 APs
- 12,000 clients
- 60 Gbps

Service Provider

8500

- 300 to 6000 APs
- 64,000 clients
- 10 Gbps

Small Campus / Branch (Controller On-Premise)

SRE ISR G2

- 5 to 50 APs
- 500 clients
- 500 Mbps

2500

- 5 to 75 APs
- 1000 clients
- 1 Gbps

Virtual Controller

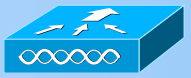
- 5 to 200 APs
- 3000 clients
- 500 Mbps

Catalyst 3850

- 1 to 50 APs per switch/stack (Directly connected)
- 2000 clients per stack
- 40 Gbps per switch

Branch (Controller in DC)

Virtual Controller



- 5 to 200 APs
- 3000 clients
- 500 Mbps

Flex 7500

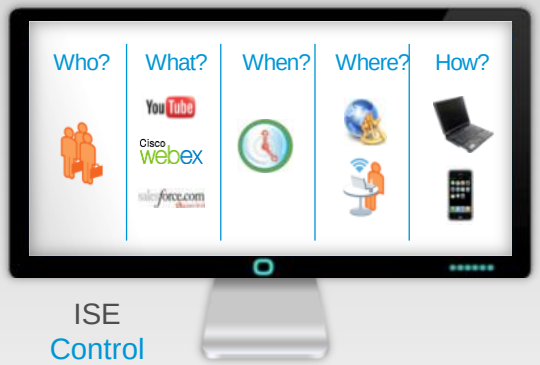
- 300 to 6000 APs
- 64,000 clients
- 1 Gbps

Cisco Mobility Highlights

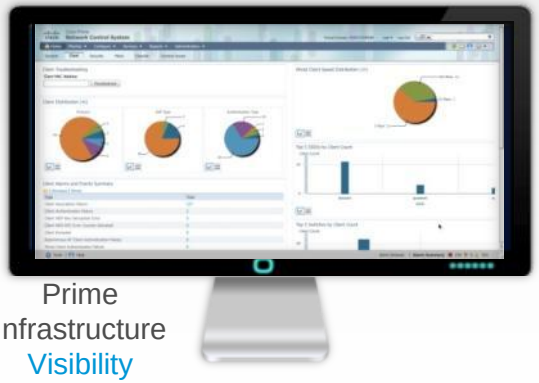
Mobility/RF Innovation
Predictability and Reliability

Award Wining Design	Purpose-Built Wi-Fi Chipset with 4x4 MIMO, with robust platform - No Open Vents
ClientLink	Best-in-class performance to a/g/n clients
CleanAir	Chip level proactive and automatic interference mitigation
Committed to Standards	First to introduce 802.11r, 802.11u, 802.11w and 802.11ac to Enterprises
VideoStream	Optimized multicast to unicast
Stateful fail-over	Sub second failover to hot standby controller
AVC	Classification and policies on 1000+ Apps
MSE and Thinksmart	Analytics that aid business decisions Meaningful Interaction with your customers

Policy and Network Management

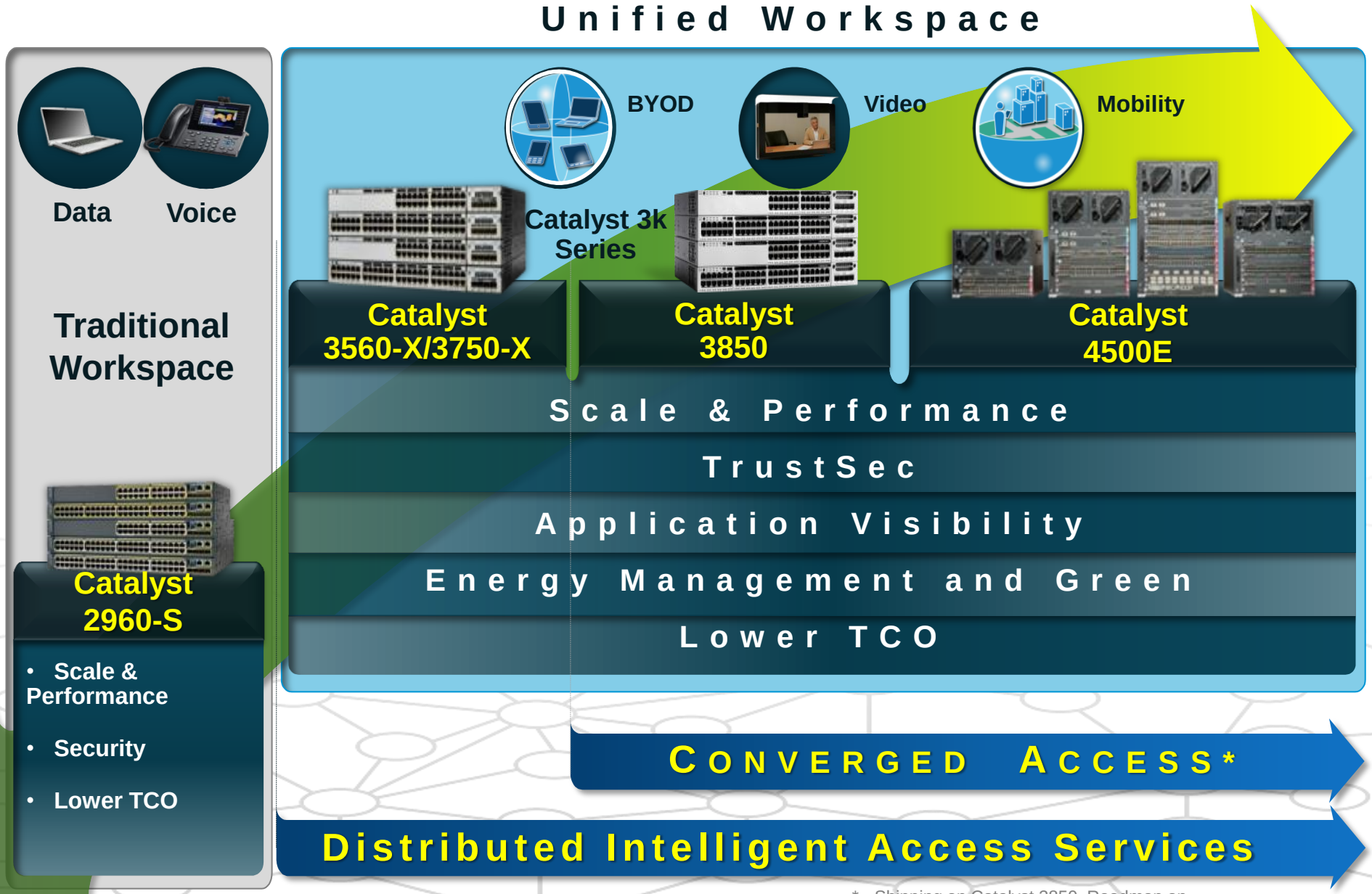


ISE
Control



Prime
Infrastructure
Visibility

Catalyst Access Switching Portfolio



* - Shipping on Catalyst 3850, Roadmap on Catalyst 4500E

Single Platform for Wired and Wireless

20+ Years of IOS Richness – Now on Wireless

WIRELESS

Features:

- 802.11n
- CleanAir
- VideoStream
- Radio Resource Management (RRM)
- Wireless Intrusion Prevention System (WiPS)
- 802.11ac Ready

WIRED

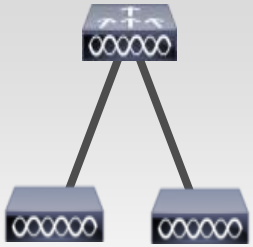
Features:

- Stacking
- Stackpower
- Flexible Netflow
- Granular QoS
- Trustsec*/Identity
- AVC/Medianet*
- Smart Operations*
- EnergyWise*

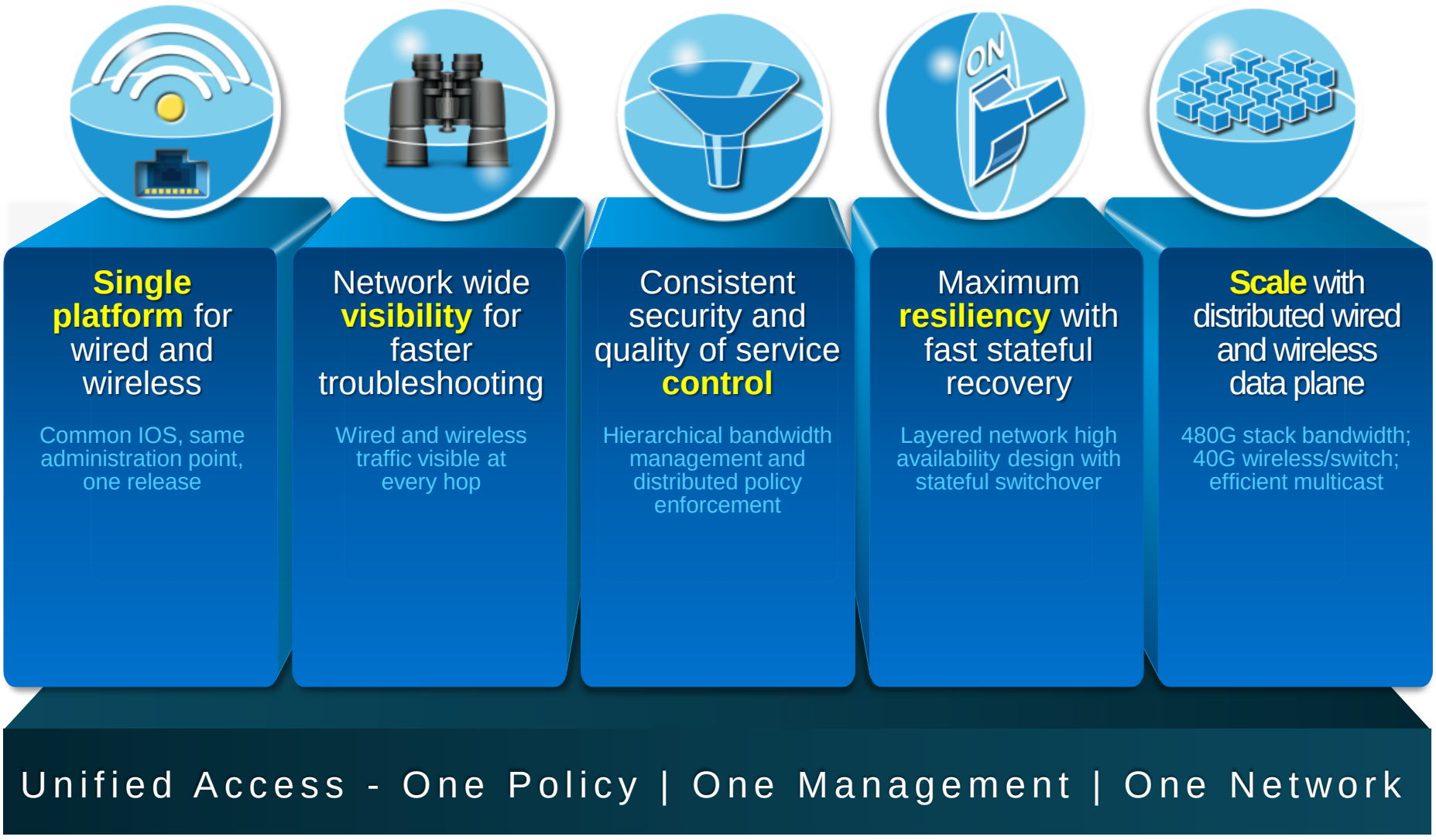
Benefits

- Built on **UADP ASIC** – Cisco's Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

One Network – Wireless Deployment Mode Options

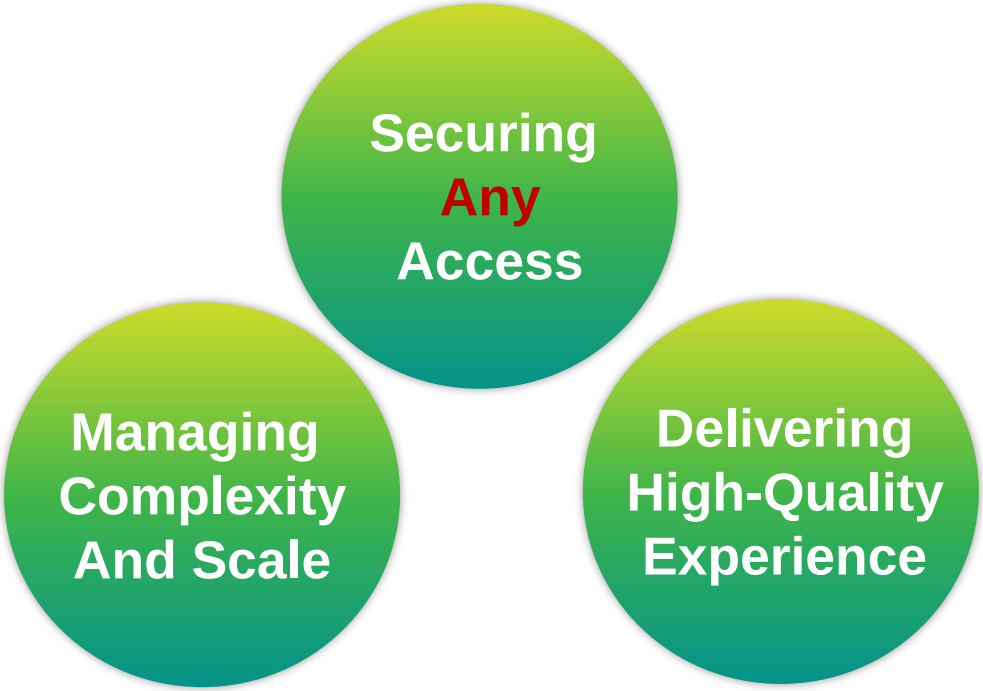
	Autonomous	FlexConnect	Centralized	Converged Access
	 Standalone APs	 Traffic Distributed at AP	 Traffic Centralized at Controller	 Traffic Distributed at Switch
Where it fits	**Small Wireless Network**	**Branch**	**Campus**	**Branch and Campus**
	Wireless access is your primary focus	Wireless services in the Branch	Wireless coverage	Wired and Wireless infrastructure reflexion
Benefits	• Simple and cost-effective for small networks	• Highly scalable for large number of remote branches • Simple wireless operations with DC hosted controller	• Simplified operations with centralized control for Wireless • Wireless Traffic visibility at the controller	• Wired and Wireless common operations • One Enforcement Point • One OS (IOS) • Traffic visibility at every network layer • Performance optimized for 11ac
Key Consi-derations	• Limited RRM, no Rogue detection	• L2 roaming only • WAN BW & latency requirements	• System throughput	• Catalyst 3850 in the access layer

Converged Wired/Wireless Access – Additional Benefits



Summary

Unified Access – The Challenges & Solution



One Policy

- Single Business Policy
  - **Wired, Wireless, and VPN**
  - Managed & BYOD assets

One Management

- Comprehensive Visibility
  - **Single Pane of Glass**
  - **User/device centric**
  - Users, devices, location, posture

One Network

- Uncompromised Experience
  - **Best in class RF: ClientLink, CleanAir VideoStream**
  - **Always-on VPN**
  - **Wired/Wireless convergence**

Unified Access – The Challenges & Solution

bez námahy

ale kontrolovaně

SE PŘIPOJIT!

Dimension Data Network Barometer Report, TLMA

Ing. Adam Horník - (adam.hornik@dimensiondata.com)
Presales konzultant

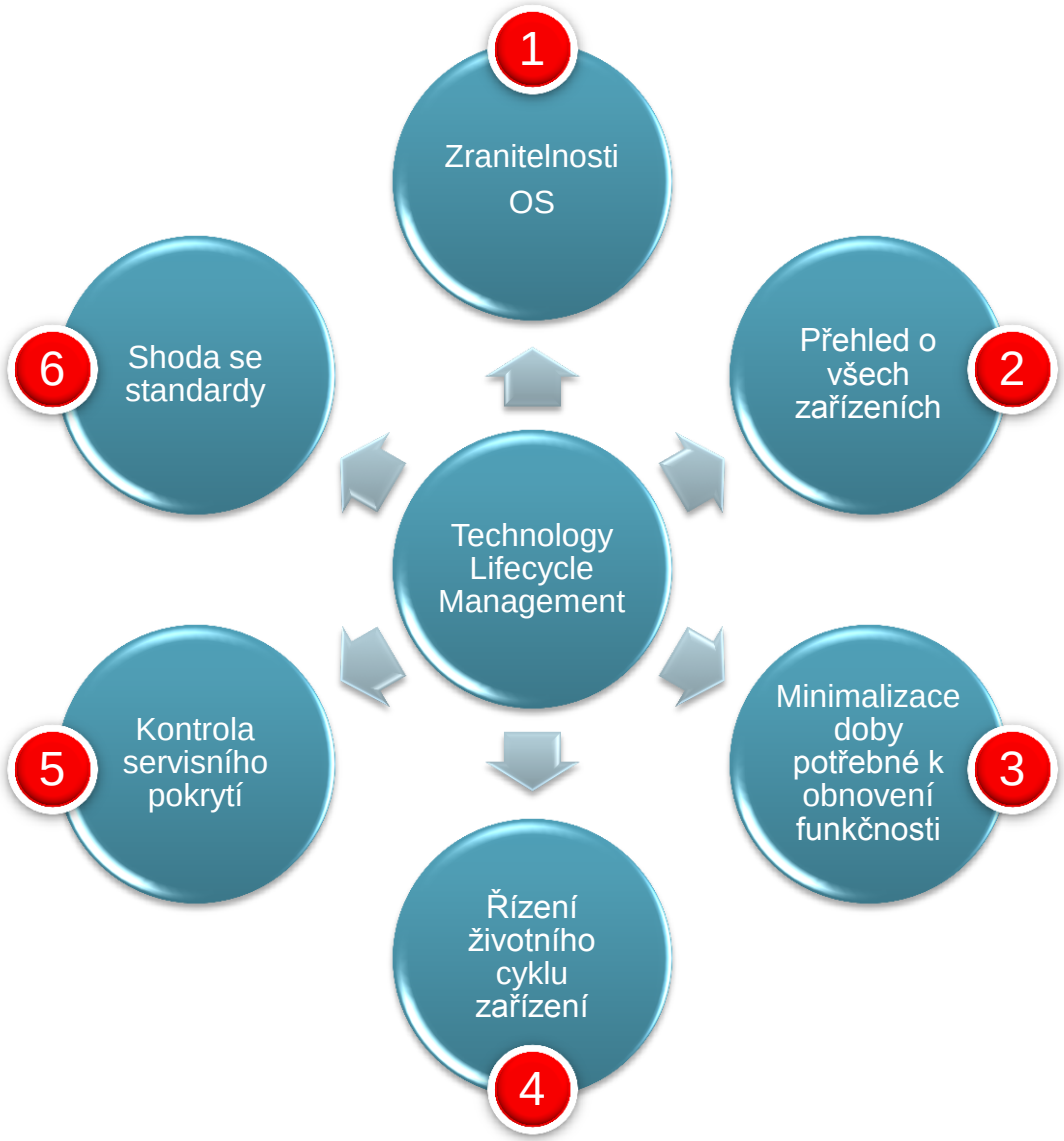
dimension data

Network Integration

Wednesday, 24 April, 2013

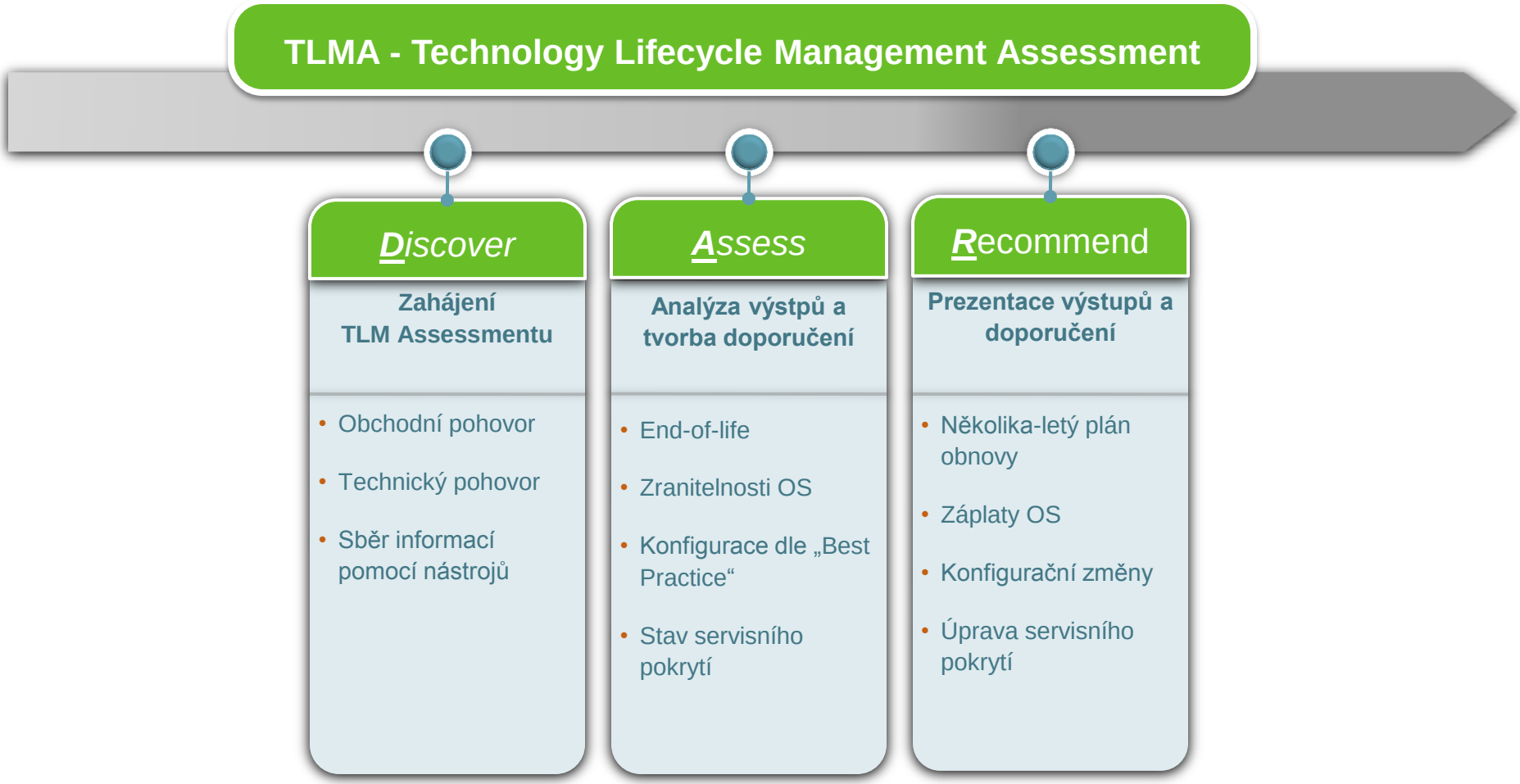
Agenda

Při správě síťových zařízení se potýkáme s určitými výzvami



1. Odhalování zranitelností OS
2. Organizace nemají povědomí až o 25% jejich síťových zařízeních
3. Neznámé zařízení a neoptimální konfigurace prodlužují střední dobu do obnovy (MTTR)
4. Odůvodnění upgradu zařízení
5. Zajištění servisního pokrytí všech zařízení při minimalizaci nákladů
6. Příprava sítě pro audit

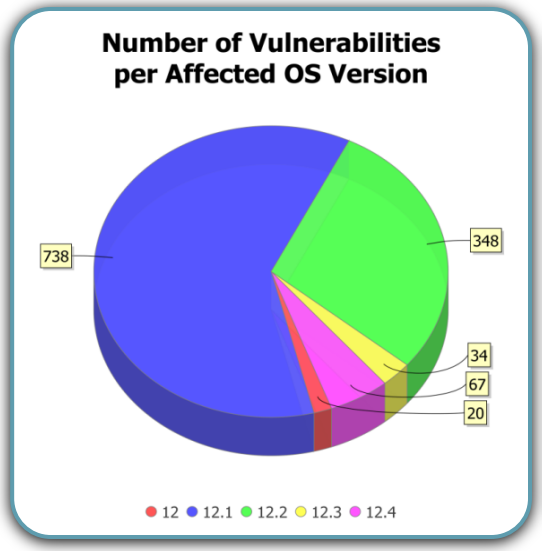
TLM Assessment je základem pro náš přístup k TLM metodice

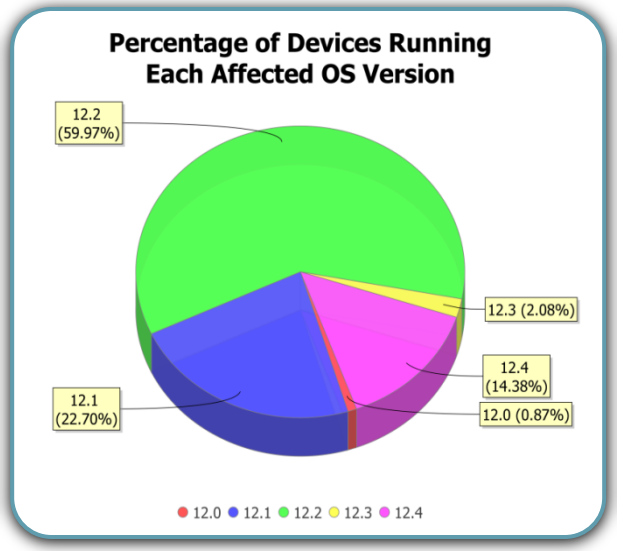


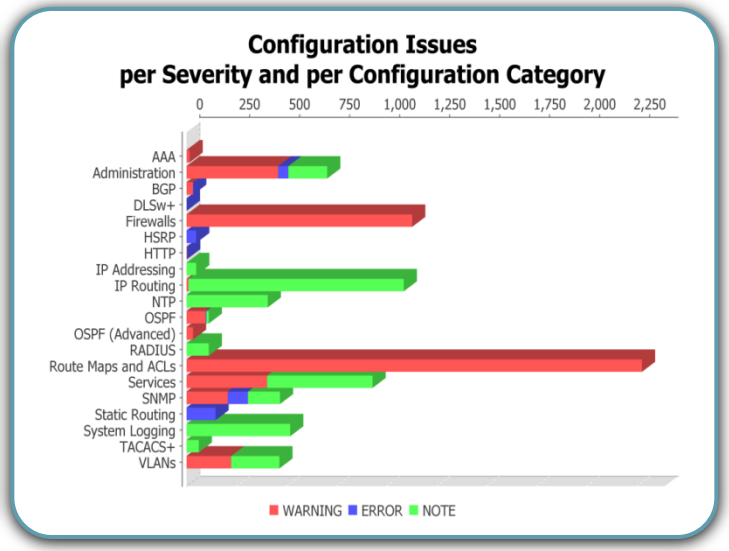
TLMA - Technology Lifecycle Management Assessment

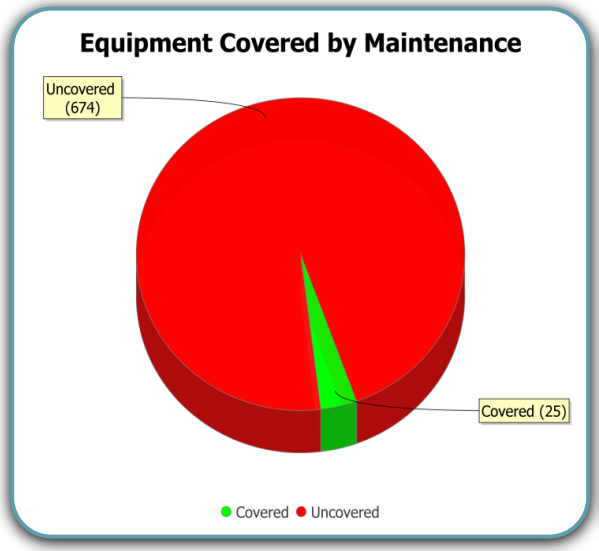
- ✓ Komplexní shrnutí
- ✓ Provozní shrnutí
- ✓ Detailní výsledky analýzy
  - ✓ Seznam všech nalezených zařízení
  - ✓ Stav životního cyklu
  - ✓ Stav servisního pokrytí
  - ✓ Stav zranitelností OS
  - ✓ Porušení konfigurační politiky
- ✓ Doporučení dle priorit

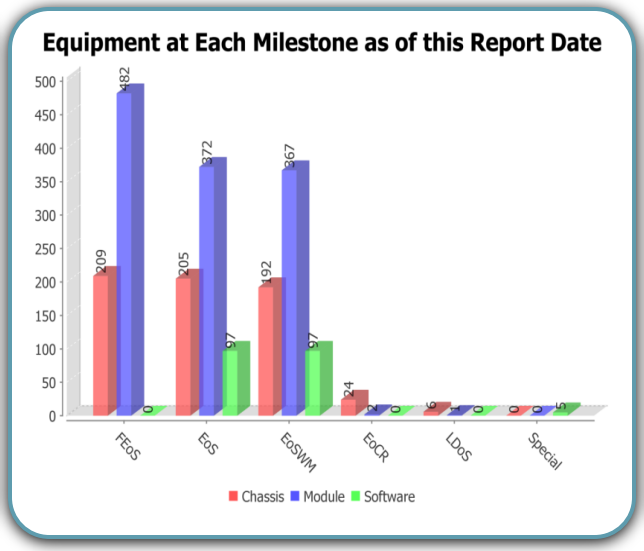
TLMA uvádí jednotlivé nedostatky, které by měly být napraveny.

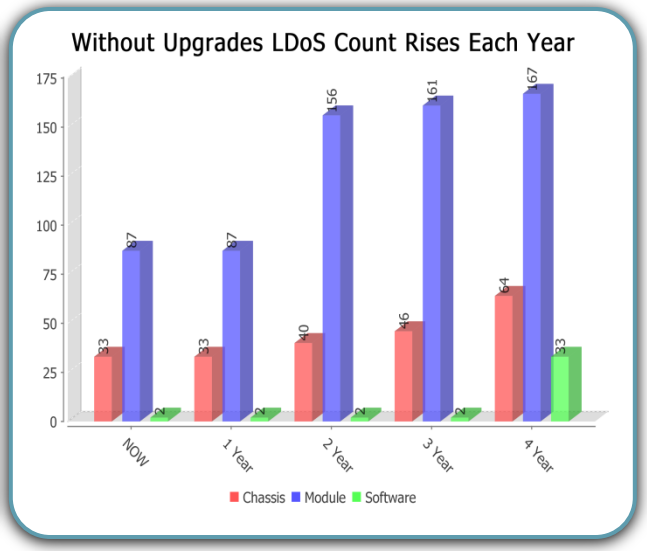












Výhody přístupu podle TLMA

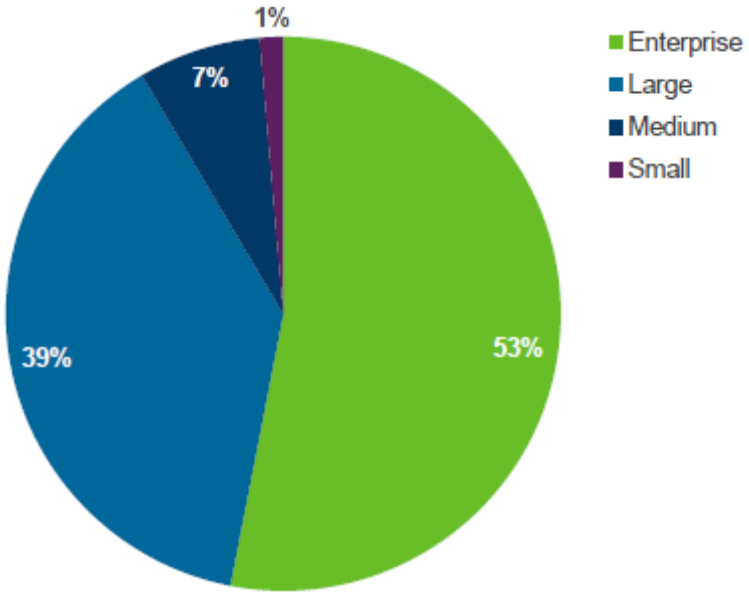
1. Zvýšení pružnosti podnikání
2. Proaktivní několika-letý investiční plán
3. Plánovaný postup k požadovanému stavu
4. Snížení provozních nákladů
5. Konsolidace potřebných znalostí
6. Snížení rizik spojených s nedostupností sítě
7. Snížení různorodosti (zvýšení standardizace)
8. Připravenost sítě na audit (SoX, PCI, etc.)
9. Snížení technologického stárnutí
10. Snížení uhlíkového „otisku“

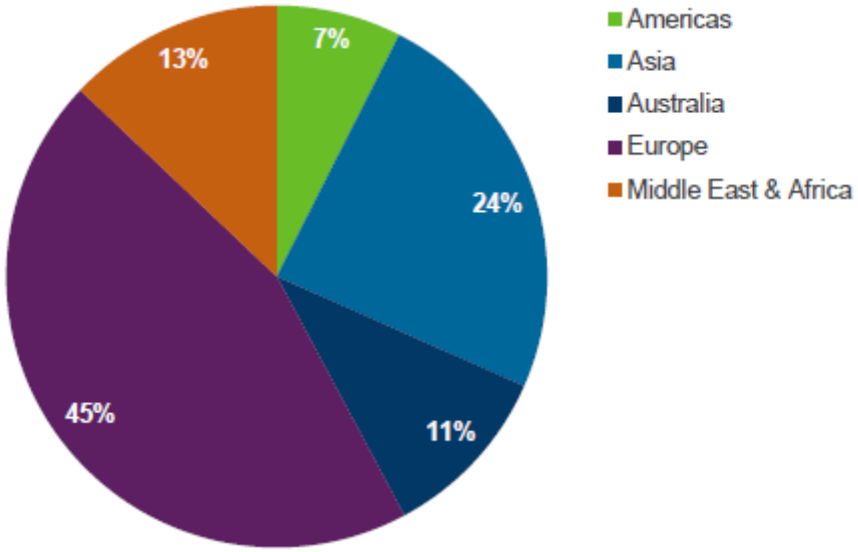
Dimension Data Network Barometer Report

Shrnuje data ze 294 TLMA reportů probíhajících od roku 2009 zahrnující přes 60,000 zařízení

- **Bezpečnostní hrozby**
- **End-of-Life přehledy použitých zařízení**
- **Analýza konfigurační politiky s doporučením**
- **Použité verze Cisco IOS**

Kdo poskytl data pro Network Barometer Report 2012





Small - méně než 100 uživatelů

Medium – mezi 100 až 500 uživatelů

Large – 500 až 2500 uživatelů

Enterprise – 2500 až 5000 uživatelů

Europe - Belgium, Czech Republic, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Switzerland and the United Kingdom

Americas - Canada, USA, Brazil and Mexico

Middle East and Africa - South Africa

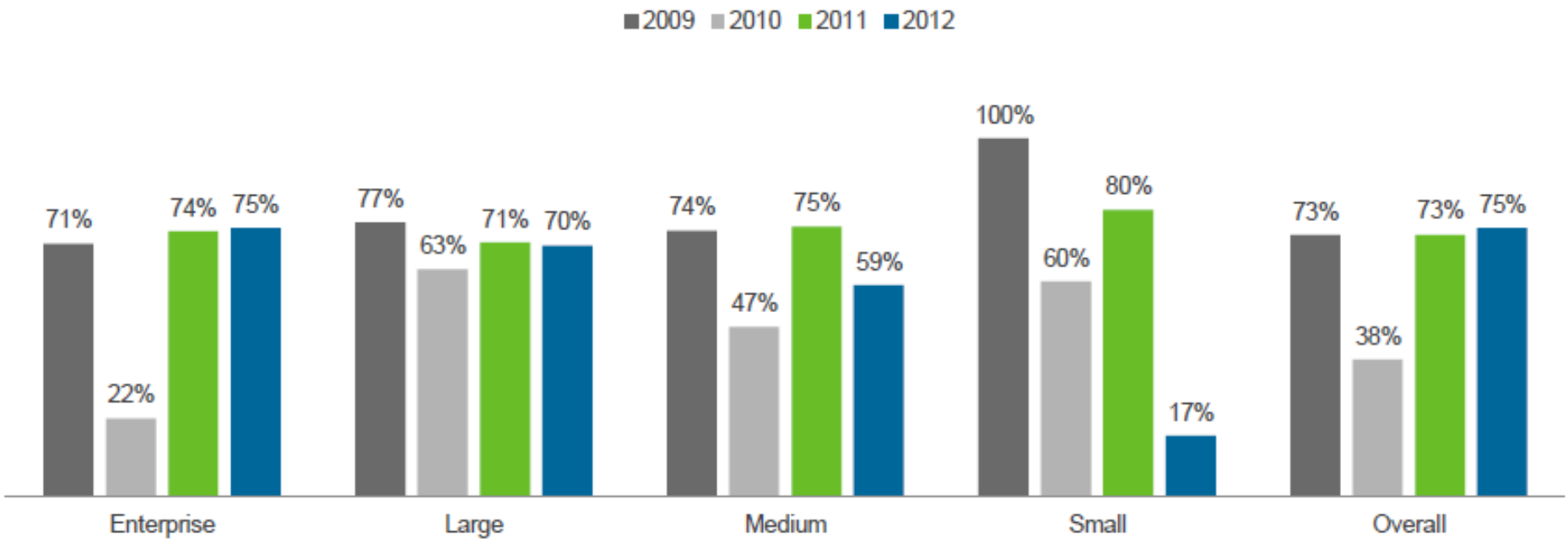
Asia - China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore and Vietnam

Každoroční počet nových zranitelností identifikovaných Cisco

PSIRT - Product Security Incident Response Team

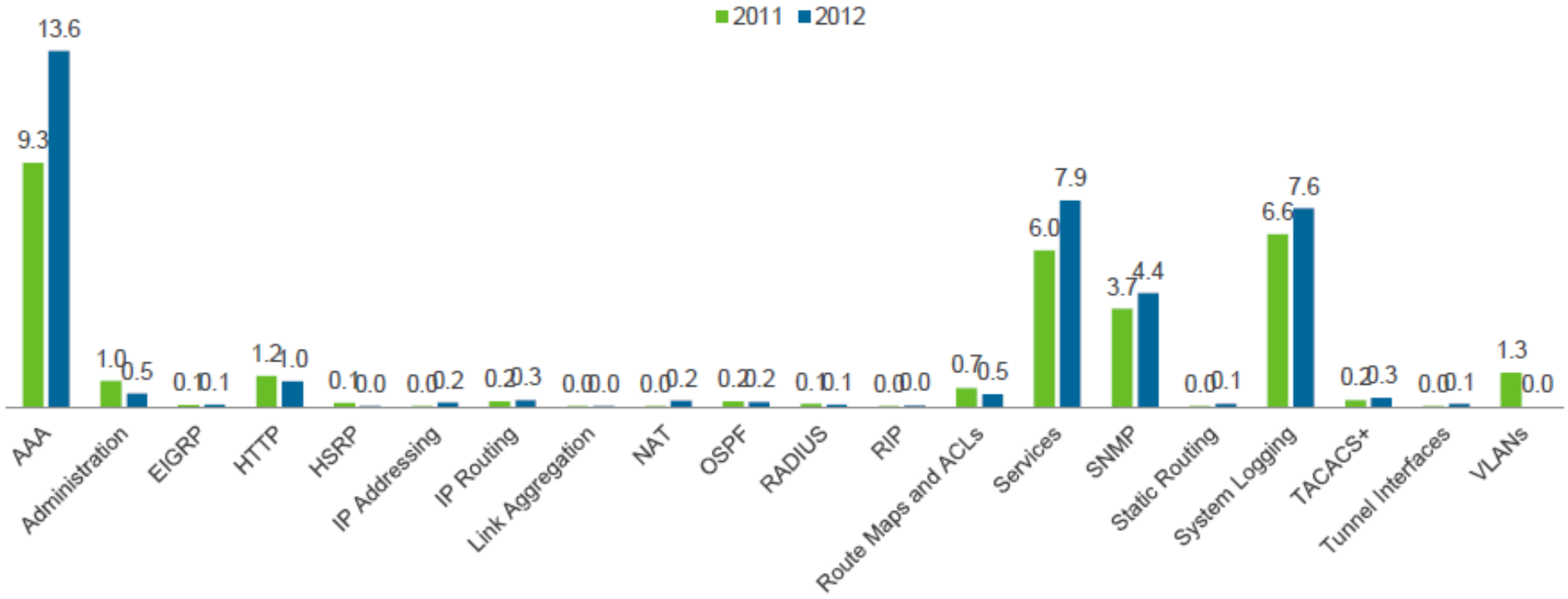
Společnost Cisco Systems disponuje globálním týmem PSIRT, který eviduje, zkoumá a zveřejňuje podklady a informace týkající se možné zneužitelnosti chyb v software Cisco zařízení.

Ze všech zařízení, které byly analyzovány obsahují alespoň jednu bezpečnostní chybu



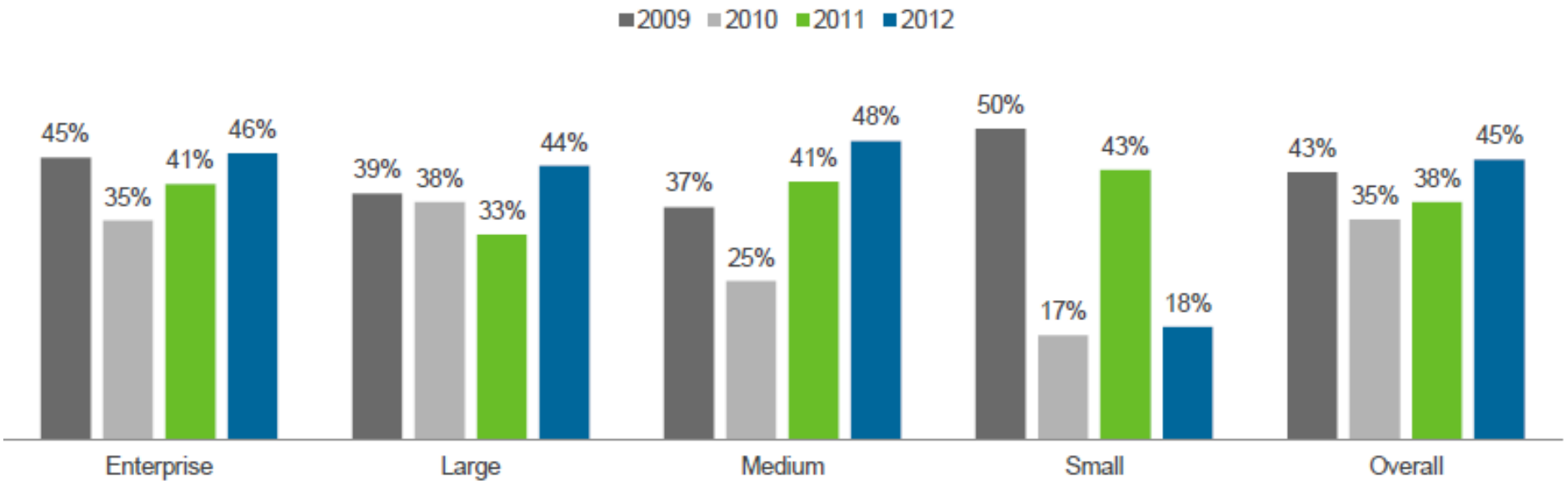
Počet zařízení s bezpečnostní zranitelnosti PSIRT podle velikosti organizace

Celkový počet chyb v konfiguraci se od roku 2011 zvýšil



AAA Authentication – nejběžnější konfigurační chyba

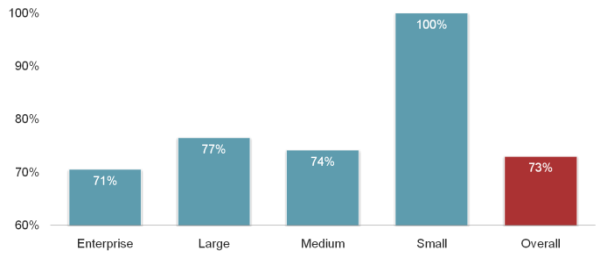
Průměrný počet End od Sale (EoS) zařízení síti



Zvyšující se trend EoS zařízení může mít nepříznivý vliv na fungování sítě

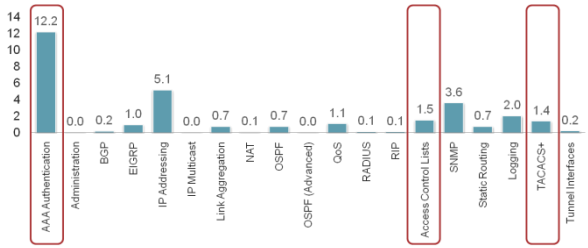
Report „Network Barometer 2012“ ukazuje, jak jsou sítě organizací vystaveny obchodním a provozním rizikům.

Průmerný počet zařízení obsahující PSIRT dle velikosti organizace



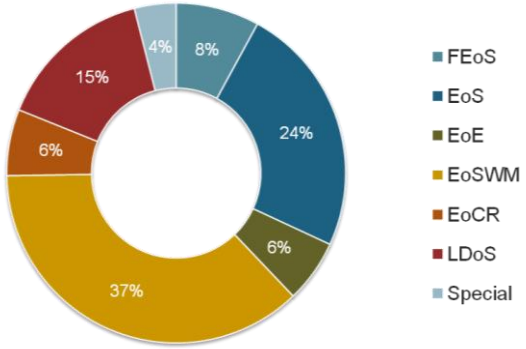
75% zařízení má alespoň jednu bezpečnostní zranitelnost ...

Průměrný počet porušení politiky v dané kategorii



. . . každé zařízení má 30 konfig. nedostatků – 15 jich je spojených s bezpečností . . .

Rozdělení zařízení do jednotlivých životních cyklů



. . . 45% dosáhlo stávu EoS, a 56% z tohoto počtu dosáhlo stavu EoSWM or LDoS

Dimension Data’s Network Barometer Report

Založen na 294 TLMA reportech z celého světa

www.dimensiondata.com/networkbarometer

Závěry Dimension Data Network Barometer Reportu

1. **50% nárůst WiFi AccessPointů pracujících na 802.11n v roce 2012**
2. **32% všech přístupových přepínačů v roce 2012 podporuje Gigabit Ethernet**
3. **48% všech přístupových přepínačů v roce 2012 podporuje PoE**
4. **18% všech přístupových přepínačů v roce 2012 podporuje PoE+**

Q&A

Dotazy…

Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v sále LEO v 17:45 – 18:30

e-mail: connect-cz@cisco.com

Prosíme, ohodnoťte tuto přednášku.

Děkujeme za pozornost.