

# 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

## IT Requirement

Deliver an  
Uncompromised  
User Experience  
on Any  
Workspace



### BYOD

- Secure access
- Customized experience
- Guest access



### Mobility

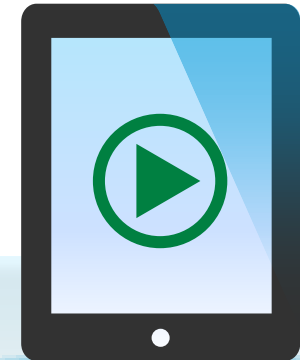
- Seamless roaming
- Optimal client performance
- Cloud access/VXI



### Video

- Multicast streaming
- Video conferencing
- Reliable performance

# Uncompromised User Experience - Challenges

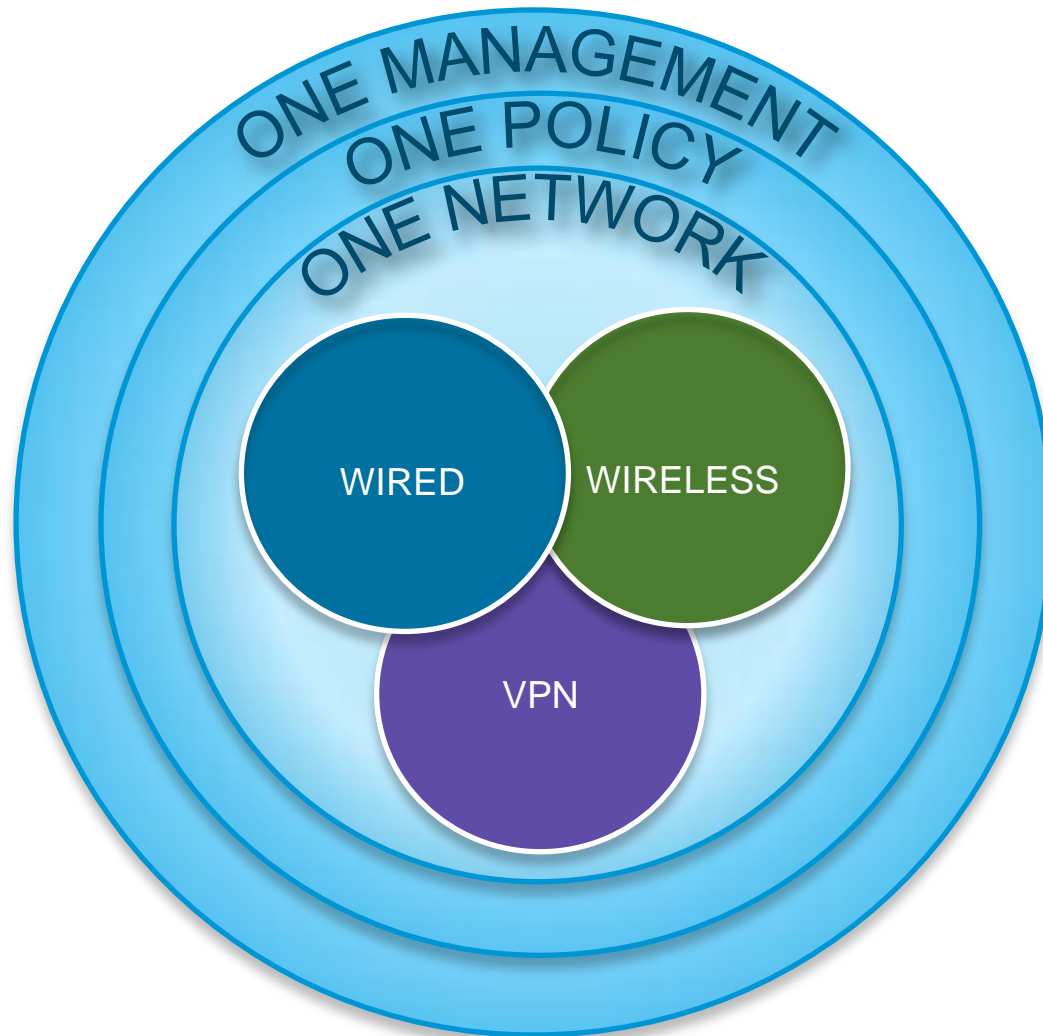


Securing  
Any  
Access

Managing  
Complexity  
And Scale

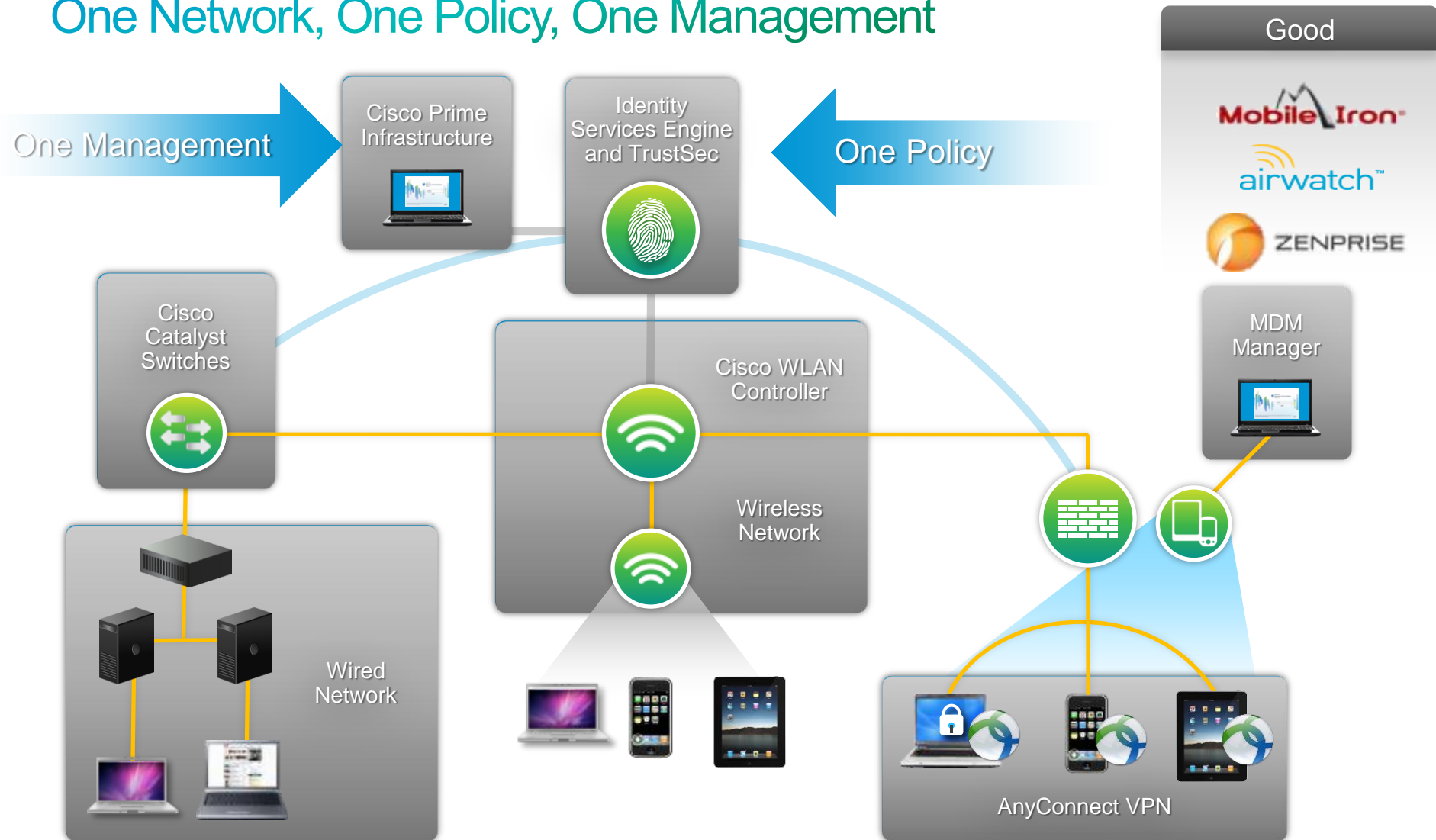
Delivering  
High-Quality  
Experience

# 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

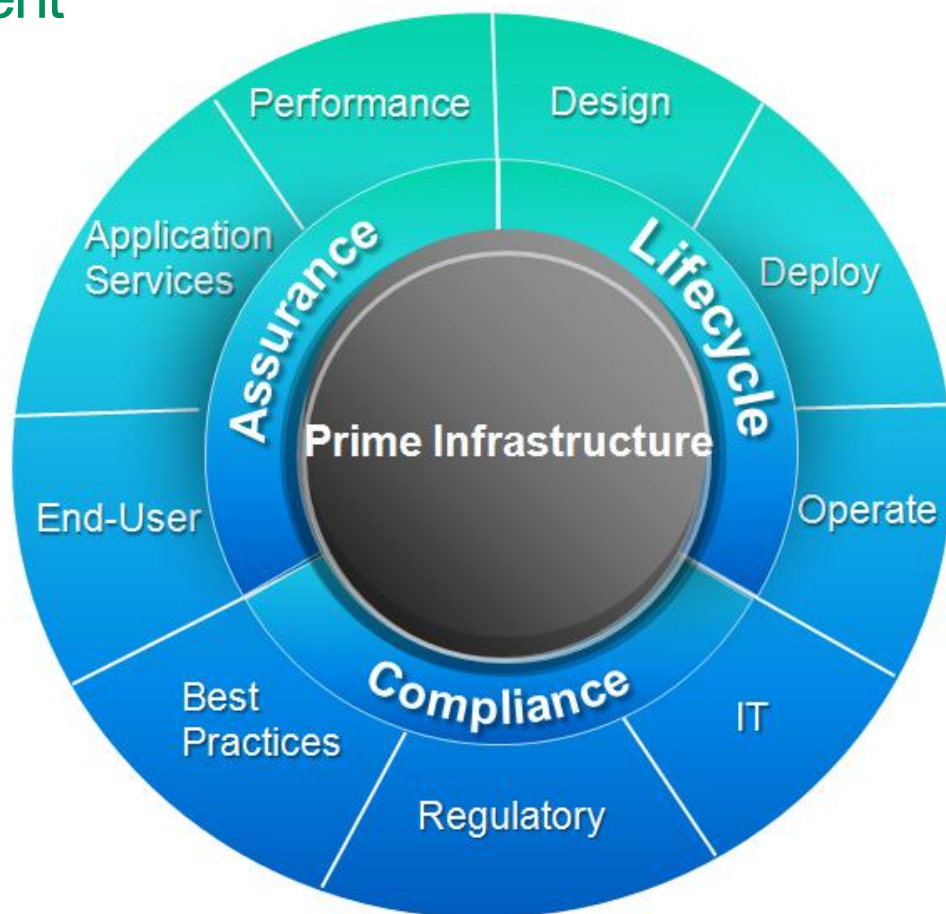


# Cisco Prime Infrastructure

## 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)

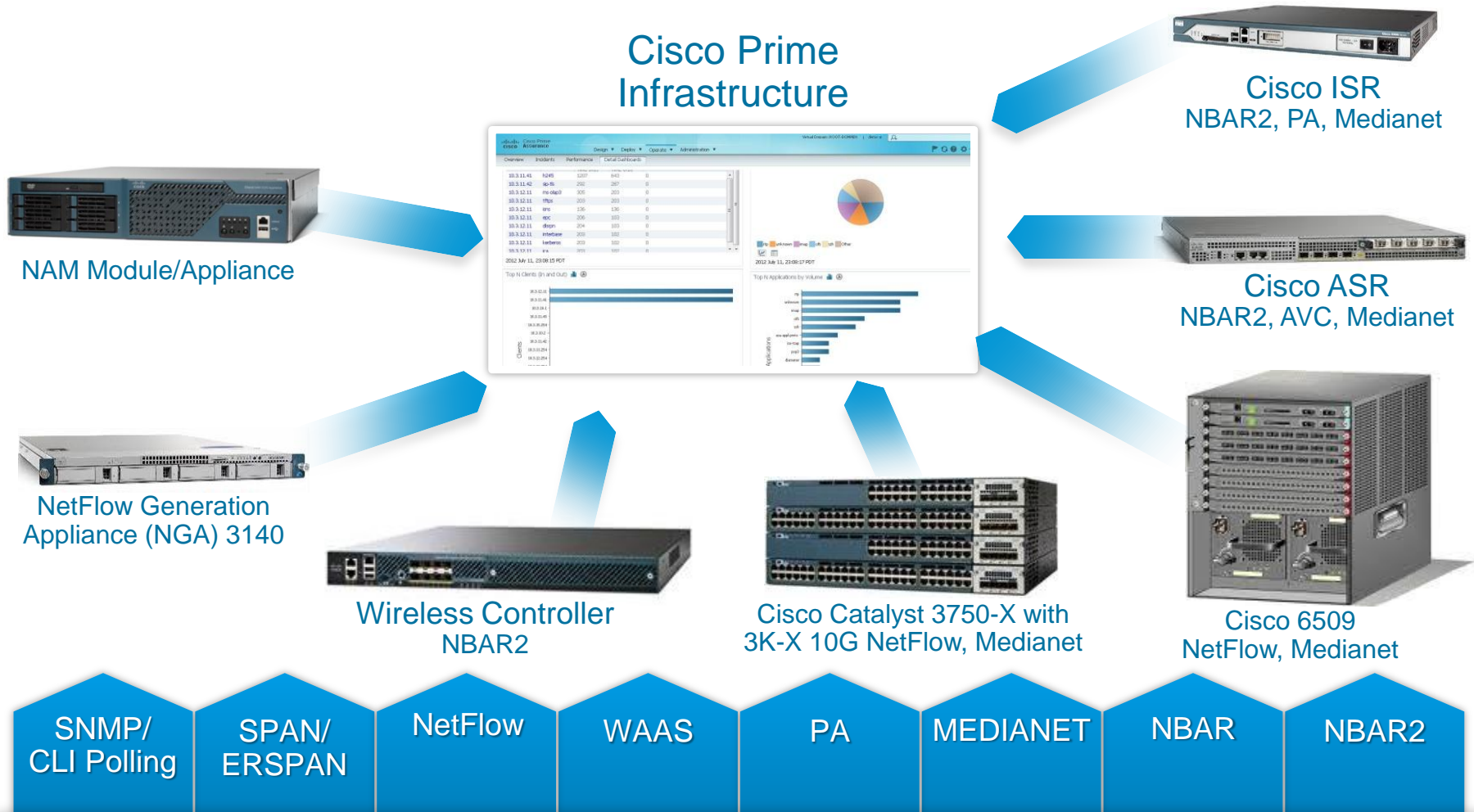
### Visibility

- ✓ 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?



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

The screenshot displays the Cisco Prime Network Control System interface. At the top, a 'Troubleshoot' section shows a workflow with steps: '802.11 Association' (checked), '802.1X Authentication' (checked), 'IPAddress Assignment' (warning icon), and 'Successful Association' (checked). Below this, a 'Problem' section states 'Client could not complete the dhcp interaction.' and a 'Recommendation' section suggests 'Check whether the DHCP server is reachable.'

The main section is titled 'Clients and Users' and shows search results for 'EndUser1'. A table lists the following data:

IP Address	MAC Address	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface
192.168.217.88	7e:16:7a:8c:1f:00	EndUser1		Cisco	sjc14-wl-wlc3	Cisco San Jose - Site 5	251	Associated	voice
192.168.42.13	d0:d1:d0:d0:66:67:a4	EndUser1		Unknown	sjc14-wl-wlc3	Cisco San Jose - Site 5	260	As associated	corp1
192.168.241.214	2b:1c:02:48:59:5e	EndUser1		Apple	sjc14-wl-wlc3	Cisco San Jose - Site 5	260	Associated	corp1

Below the table, a 'System Detail' section shows: 'Client PSM State: DHCP\_REQD', 'Client is using dot1x security', and 'Checked at : 2011-Apr-25, 12:50:56 PDT' with a 'Check Again!' button.



- ✓ 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

### Clients and Users

Clients Search Results - Reset Selected 1 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f		Not Detec...	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

### Client 00:21:5c:01:b8:6f (Refreshed :2012-Nov-22, 05:01:31 PST )

Note: None

#### Client Attributes

<p><b>General</b></p> <p>User Name <b>jfields</b></p> <p>IP Address <b>Data Not Available</b></p> <p>MAC Address <b>00:21:5c:01:b8:6f</b></p> <p>Vendor <b>Intel</b></p> <p>Endpoint Type <b>Unknown</b></p> <p>Client Type <b>Regular</b></p> <p>Media Type <b>Lightweight</b></p> <p>Mobility Status <b>Unassociated</b></p> <p>Hostname <b>Data Not Available</b></p> <p>E2E <b>V1</b></p> <p>802.11u Capable <b>No</b></p> <p>Power Save <b>OFF</b></p> <p>CCX <b>V4</b></p>	<p><b>Session</b></p> <p>Controller Name <b>AMS-2504-WLC</b></p> <p>AP Name <b>NMTG-AP3500-2</b></p> <p>AP IP Address <b>192.168.152.14</b></p> <p>AP Type <b>Cisco AP</b></p> <p>AP Base Radio MAC <b>04:c5:a4:f2:3f:60</b></p> <p>Anchor Controller <b>Data Not Available</b></p> <p>802.11 State <b>Associated</b></p> <p>Association ID <b>1</b></p> <p>Port <b>1</b></p> <p>Interface <b>vlan 13</b></p> <p>SSID <b>AMS-DOT1X</b></p> <p>Profile Name <b>AMS-dot1x</b></p> <p>Protocol <b>802.11n(5GHz)</b></p> <p>VLAN ID <b>13</b></p>	<p><b>Security</b></p> <p>Security Policy Type <b>WPA2</b></p> <p>EAP Type <b>Not Available</b></p> <p>On Network <b>No</b></p> <p>802.11 Authentication <b>Open System</b></p> <p>Encryption Cipher <b>CCMP (AES)</b></p> <p>SNMP NAC State <b>Access</b></p> <p>Radius NAC State <b>8021X_REQD</b></p> <p>AAA Override ACL Name <b>none</b></p> <p>AAA Override ACL Applied Status <b>N/A</b></p> <p>Redirect URL <b>none</b></p> <p>ACL Name <b>none</b></p> <p>ACL Applied Status <b>N/A</b></p> <p>FlexConnect Local Authentication <b>No</b></p> <p>Policy Manager State <b>8021X_REQD</b></p>
--	---	--

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

The screenshot shows the Cisco Prime Infrastructure interface. At the top, there's a navigation bar with 'Home', 'Design', 'Deploy', and 'Operate' tabs. A search bar on the right shows 'Virtual Domain ROOT-DOMAIN | dvandela'. A blue callout box points to the first row in the table with the text 'Select the device with the connectivity problem'.

**Clients and Users**

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f		Not Detec...	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:14:15:1c:18	192.168.152.25	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:18:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Client 00:21:5c:01:b8:6f (Refreshed :2012-Nov-22, 05:01:31 PST)

Note: None

**Client Attributes**

**General**

- User Name: **jfields**
- IP Address: **Data Not Available**
- MAC Address: **00:21:5c:01:b8:6f**
- Vendor: **Intel**
- Endpoint Type: **Unknown**
- Client Type: **Regular**
- Media Type: **Lightweight**
- Mobility Status: **Unassociated**
- Hostname: **Data Not Available**
- E2E: **V1**
- 802.11u Capable: **No**
- Power Save: **OFF**
- CCK: **V4**

**Session**

- Controller Name: **AMS-2504-WLC**
- AP Name: **NMTG-AP3500-2**
- AP IP Address: **192.168.152.14**
- AP Type: **Cisco AP**
- AP Base Radio MAC: **04:c5:a4:f2:3f:60**
- Anchor Controller: **Data Not Available**
- 802.11 State: **Associated**
- Association ID: **1**
- Port: **1**
- Interface: **vlan 13**
- SSID: **AMS-DOT1X**
- Profile Name: **AMS-dot1x**
- Protocol: **802.11n(5GHz)**
- VLAN ID: **13**

**Security**

- Security Policy Type: **WPA2**
- EAP Type: **Not Available**
- On Network: **No**
- 802.11 Authentication: **Open System**
- Encryption Cipher: **CCMP (AES)**
- SNMP NAC State: **Access**
- Radius NAC State: **8021X\_REQD**
- AAA Override ACL Name: **none**
- AAA Override ACL Applied Status: **N/A**
- Redirect URL: **none**
- ACL Name: **none**
- ACL Applied Status: **N/A**
- FlexConnect Local Authentication: **No**
- Policy Manager State: **8021X\_REQD**

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

Select troubleshooting

Select the device with the connectivity problem

Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate

Client Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f		Not Detec...	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:10:00:00:00:00	192.168.152.25	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Client 00:21:5c:01:b8:6f (Refreshed :2012-Nov-22, 05:01:31 PST) Note: None

Client Attributes

**General**

User Name **jfields**

IP Address **Data Not Available**

MAC Address **00:21:5c:01:b8:6f**

Vendor **Intel**

Endpoint Type **Unknown**

Client Type **Regular**

Media Type **Lightweight**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

Power Save **OFF**

CCK **V4**

**Session**

Controller Name **AMS-2504-WLC**

AP Name **NMTG-AP3500-2**

AP IP Address **192.168.152.14**

AP Type **Cisco AP**

AP Base Radio MAC **04:c5:a4:f2:3f:60**

Anchor Controller **Data Not Available**

802.11 State **Associated**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

**Security**

Security Policy Type **WPA2**

EAP Type **Not Available**

On Network **No**

802.11 Authentication **Open System**

Encryption Cipher **CCMP (AES)**

SNMP NAC State **Access**

Radius NAC State **8021X\_REQD**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate Report Administration

### Client Troubleshooting

Go back

#### Properties

##### General

User Name **jfields**

IP Address **Data Not Available**

MAC Address **00:21:5c:01:b8:6f**

Vendor **Intel**

Endpoint Type **Unknown**

Client Type **Regular**

Media Type **Lightweight**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

#### Session

Controller Name **AMS-2504-WLC**

AP Name **NMTG-AP3500-2**

AP IP Address **192.168.152.14**

AP Type **Cisco AP**

AP Base Radio MAC **04:c5:a4:f2:3f:60**

Anchor Controller **Data Not Available**

802.11 State **Associated**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

#### Security

Security Policy Type **WPA2**

EAP Type **Not Available**

On Network **No**

802.11 Authentication **Open System**

Encryption Cipher **CCMP (AES)**

SNMP NAC State **Access**

Radius NAC State **8021X\_REQD**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

#### Troubleshoot

✔ 802.11 Association
 ⚠ 802.1X Authentication
 ? IP Address Assignment
 ? Successful Association

##### Problem

802.1X Authentication Failure

##### Recommendation

- Check whether Radius server(s) is reachable
- Check whether client's choice of EAP method is supported by radius server
- Check Clients username/password/cert is valid
- Check to see if the certificates used by the Authentication server are accepted by the client.

- [Search Cisco Support Community](#)
- [Open or Update](#) a service request

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

The screenshot shows the Cisco Prime Infrastructure Client Troubleshooting interface. The top navigation bar includes Home, Design, Deploy, Operate, Report, and Administration. The main content area is divided into three sections: General, Session, and Security. A blue callout box highlights the 802.1X Authentication failure. Below the properties, a Troubleshoot section shows a list of diagnostic steps, with 802.1X Authentication marked as failed. A Recommendations section provides troubleshooting steps for the failure.

**Client Troubleshooting** [Go back](#)

**Properties**

- General**
  - User Name: **jfields**
  - IP Address: **Data Not Available**
  - MAC Address: **00:21:5c:01:b8:6f**
  - Vendor: **Intel**
  - Endpoint Type: **Unknown**
  - Client Type: **Regular**
  - Media Type: **Lightweight**
  - Mobility Status: **Unassociated**
  - Hostname: **Data Not Available**
  - E2E: **V1**
  - 802.11u Capable: **No**
- Session**
  - Controller Name: **AMS-2504-WLC**
  - AP Name: **NMTG-AP3500-2**
  - AP IP Address: **192.168.152.14**
  - AP Type: **Cisco AP**
  - AP Base Radio MAC: **04:c5:a4:f2:3f:60**
  - Anchor Controller: **Data Not Available**
  - 802.11 State: **Associated**
  - Association ID: **1**
  - Port: **1**
- Security**
  - Security Policy Type: **WPA2**
  - EAP Type: **Not Available**
  - On Network: **No**
  - 802.11 Authentication: **Open System**
  - Encryption Cipher: **CCMP (AES)**
  - SNMP NAC State: **Access**
  - Radius NAC State: **8021X\_REQD**
  - AAA Override ACL Name: **none**
  - AAA Override ACL Applied Status: **N/A**
  - Redirect URL: **none**
  - ACL Name: **none**
  - ACL Applied Status: **N/A**
  - FlexConnect Local Authentication: **No**
  - Policy Manager State: **8021X\_REQD**
  - Authenticating ISE: **Data Not Available**
  - Authorization Profile Name: **Data Not Available**
  - Posture Status: **Unknown**
  - TrustSec Security Group: **Data Not Available**
  - Windows AD Domain: **Data Not Available**

**Troubleshoot**

802.11 Association **✓** 802.1X Authentication **⚠** IP Address Assignment **?** Successful Association **?**

**Problem**  
802.1X Authentication Failure

**Recommendation**

- Check whether Radius server(s) is reachable
- Check whether client's choice of EAP method is supported by radius server
- Check Clients username/password/cert is valid
- Check to see if the certificates used by the Authentication server are accepted by the client.
- [Search Cisco Support Community](#)
- [Open or Update](#) a service request

policy manager State **8021X\_REQD**

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

The screenshot displays the Cisco Prime Infrastructure Client Troubleshooting interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The main content area is divided into three columns: 'General', 'Session', and 'Security'. The 'General' column shows client details like 'User Name: jfields', 'IP Address: Data Not Available', and 'MAC Address: 00:21:5c:01:b8:6f'. The 'Session' column shows 'Controller Name: AMS-2504-WLC', 'AP Name: NMTG-AP3500-2', and '802.11 State: Associated'. The 'Security' column shows 'Security Policy Type: WPA2', 'EAP Type: Not Available', and '802.11 Authentication: Open System'. Below these columns is a 'Troubleshoot' section with a 'Problem' of '802.1X Authentication Failure'. A 'Recommendation' section lists several steps to check, such as 'Check whether Radius server(s) is reachable'. A blue callout bubble points to the '802.1X Authentication' step, stating 'This results in a real-time connectivity test, in this case Auth. fails'. Another blue callout bubble points to the 'ISE' button in the bottom right corner, stating 'Integration with ISE becomes very useful in this stage, select the ISE button'. The bottom right corner also features a small toolbar with icons for home, search, and other functions.

**General**

- User Name: **jfields**
- IP Address: **Data Not Available**
- MAC Address: **00:21:5c:01:b8:6f**
- Vendor: **Intel**
- Endpoint Type: **Unknown**
- Client Type: **Regular**
- Media Type: **Lightweight**
- Mobility Status: **Unassociated**
- Hostname: **Data Not Available**
- E2E: **V1**
- 802.11u Capable: **No**

**Session**

- Controller Name: **AMS-2504-WLC**
- AP Name: **NMTG-AP3500-2**
- AP IP Address: **192.168.152.14**
- AP Type: **Cisco AP**
- AP Base Radio MAC: **04:c5:a4:f2:3f:60**
- Anchor Controller: **Data Not Available**
- 802.11 State: **Associated**
- Association ID: **1**
- Port: **1**

**Security**

- Security Policy Type: **WPA2**
- EAP Type: **Not Available**
- On Network: **No**
- 802.11 Authentication: **Open System**
- Encryption Cipher: **CCMP (AES)**
- SNMP NAC State: **Access**
- Radius NAC State: **8021X\_REQD**
- AAA Override ACL Name: **none**
- AAA Override ACL Applied Status: **N/A**
- Redirect URL: **none**
- ACL Name: **none**
- ACL Applied Status: **N/A**
- FlexConnect Local Authentication: **No**
- Policy Manager State: **8021X\_REQD**
- Authenticating ISE: **Data Not Available**

**Troubleshoot**

**Problem**

802.1X Authentication Failure

**Recommendation**

- Check whether Radius server(s) is reachable
- Check whether client's choice of EAP method is supported by radius server
- Check Clients username/password/cert is valid
- Check to see if the certificates used by the Authentication server are accepted by the client.

- Search Cisco Support Community
- Open or Update a service request

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate Report Administration

**Mobility Status** **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

### Identity Services Engine

Last

Between Date  (M/d/yyyy) Time

And Date  (M/d/yyyy) Time

### Authentication Records

9 records

Date	Status	Failure Reason	ISE
Nov 22, 2012 03:49 AM	Authentication Failed.	24216 The user is not found in the internal users identity store	eset-ise-1
Nov 22, 2012 03:19 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:48 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:21 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:51 AM	Authentication Failed.	5411 No response received during 120 seconds on last EAP message sent to the client	eset-ise-1
Nov 22, 2012 01:50 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:17 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 12:46 AM	Authentication Passed.	None	eset-ise-1

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate Report Administration

**Client Profile**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

**Client State**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

**Client Profile**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

**Identity Services Engine**

Last:  Hours

Between Date:  (M/d/yyyy) Time:

And Date:  (M/d/yyyy) Time:

Now we get the full Auth. History of this device with respective user to the respective ISE sever, click on the failure reason

**Authentication Records** 9 records

Date	Status	Failure Reason	ISE
Nov 22, 2012 03:49 AM	Authentication Failed.	24216 The user is not found in the internal users identity store	eset-ise-1
Nov 22, 2012 03:19 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:48 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:21 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:51 AM	Authentication Failed.	5411 No response received during 120 seconds on last EAP message sent to the client	eset-ise-1
Nov 22, 2012 01:50 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:17 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 12:46 AM	Authentication Passed.	None	eset-ise-1

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate Report Administration

**Client Type: Smartphone**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

**Client State Information**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

**Client Policy Information**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

**Identity Services Engine**

Last:  Hours

Between Date:  (M/d/yyyy) Time:

And Date:  (M/d/yyyy) Time:

Now we get the full Auth. History of this device with respective user to the respective ISE sever, click on the failure reason

**Authentication Records** 9 records

Date	Status	Failure Reason	ISE
Nov 22, 2012 03:49 AM	Authentication Failed.	24216 The user is not found in the internal users identity store	eset-ise-1
Nov 22, 2012 03:19 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:48 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 02:21 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:51 AM	Authentication Failed.	5411 No response received during 120 seconds on last EAP message sent to the client	eset-ise-1
Nov 22, 2012 01:50 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 01:17 AM	Authentication Passed.	None	eset-ise-1
Nov 22, 2012 12:46 AM	Authentication Passed.	None	eset-ise-1

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

**Diagnosis and Resolution**

**Diagnosis**  
The specified user

**Resolution**  
Check whether the

**Troubleshooting Summary**

Investigated authentication record with details:

Details	
Timestamp	2012-11-22 03:49:04.73
ISEServer	eset-ise-1
Username	jfields
MAC Address	00:21:5C:01:B8:6F
Status	Failed
Failure Reason	24216 The user is not found in the internal users identity store
Network Device Name	AMS-2504-WLC
Network Device IP	192.168.152.11
Identity Store	Internal Users,ad.eset.cisco.com
Identity Group	
NAS Port ID	
Audit Session ID	c0a8980b0000000c50ad83e3
Authentication Method	dot1x

Investigated failure code: 24216 The user is not found in the internal users identity store

Show Progress Details

Now we get a full report on what could have gone wrong in the Auth. process

Cisco Prime Infrastructure

Mobility Status **Unassociated**  
Hostname **Data Not Available**  
E2E **V1**  
802.11u Capable **No**

**Identity Services Engine**

Last 5 Hours  
Between Date 11/22/2012 (M/d/yy)  
And Date 11/22/2012 (M/d/yy)  
Submit

**Authentication Records**

Date	Status
Nov 22, 2012 03:49 AM	Authenticati
Nov 22, 2012 03:19 AM	Authenticati
Nov 22, 2012 02:48 AM	Authenticati
Nov 22, 2012 02:21 AM	Authenticati
Nov 22, 2012 01:51 AM	Authenticati
Nov 22, 2012 01:50 AM	Authenticati
Nov 22, 2012 01:17 AM	Authenticati
Nov 22, 2012 12:46 AM	Authenticati

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 1. Check for Client Connectivity

**Diagnosis and Resolution**

**Diagnosis**  
The specified user

**Resolution**  
Check whether the

**Troubleshooting Summary**

✓ Investigated authentication record with details:

Details	
Timestamp	2012-11-22 03:49:04.73
ISEServer	eset-ise-1
Username	jfields
MAC Address	00:21:5C:01:B8:6F
Status	Failed
Failure Reason	24216 The user is not found in the internal users identity store
Network Device Name	AMS-2504-WLC
Network Device IP	192.168.152.11
Identity Store	Internal Users,ad.eset.cisco.com
Identity Group	
NAS Port ID	
Audit Session ID	c0a8980b0000000c50ad83e3
Authentication Method	dot1x

✓ Investigated failure code: 24216 The user is not found in the internal users identity store

Show Progress Details

Now we get a full report on what could have gone wrong in the Auth. process

Cisco Prime Infrastructure

Mobility Status **Unassociated**  
 Hostname **Data Not Available**  
 E2E **V1**  
 802.11u Capable **No**

**Identity Services Engine**

Last 5 Hours  
 Between Date 11/22/2012 (M/d/yy)  
 And Date 11/22/2012 (M/d/yy)  
 Submit

**Authentication Records**

Date	Status
Nov 22, 2012 03:49 AM	Authenticati
Nov 22, 2012 03:19 AM	Authenticati
Nov 22, 2012 02:48 AM	Authenticati
Nov 22, 2012 02:21 AM	Authenticati
Nov 22, 2012 01:51 AM	Authenticati
Nov 22, 2012 01:50 AM	Authenticati
Nov 22, 2012 01:17 AM	Authenticati
Nov 22, 2012 12:46 AM	Authenticati

Delivered by: CPI integration with ISE

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset

Selected 0 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

The screenshot displays the Cisco Prime Infrastructure web interface. At the top, the navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The 'Operate' tab is active. The user is logged in as 'jfields' in the 'Virtual Domain ROOT-DOMAIN'. The main content area is titled 'Clients and Users' and shows 'Clients Search Results - Reset'. There are three rows of client data in a table. The 'IP Type' column for the first two rows is highlighted with a green box. The table columns are: MAC Address, IP Address, IP Type, User Name, Type, Vendor, Device Name, Location, VLAN, Status, Interface, Protocol, and Association Time.

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields	Intel	Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields	Cisco	Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields	Compal	Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

Selected 0 | Total 3

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

The screenshot displays the Cisco Prime Infrastructure interface for monitoring RF interference. The main view is a heatmap of the first floor of the Amsterdam Branch, showing signal strength levels from -35 dBm (blue) to -90 dBm (red). The heatmap is overlaid on a floor plan with various rooms and corridors. Several access points (APs) and monitors are labeled with their IDs, such as SJC14-41B-AP9, SJC14-41B-AP5, SJC14-41B-AP6, SJC14-41B-AP4, SJC14-41B-MON2, SJC14-41B-AP3, SJC14-41B-AP1, SJC14-41B-AP8, SJC14-42B-AP9, SJC14-42B-AP5, SJC14-42B-AP6, SJC14-42B-AP7, SJC14-42B-AP4, SJC14-42B-AP3, SJC14-42B-AP1, SJC14-42B-MON2, SJC14-42B-MON1, SJC14-42B-AP10, and SJC14-42B-AP11. Other features include Bluetooth Discovery, 4th Floor SE Connect, and Rogue Detector. The interface includes a left sidebar with 'Floor Settings' and 'Load Status', a top navigation bar, and a bottom status bar showing coordinates -43.59 ft, 191.63 ft.

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

The screenshot displays the Cisco Prime Infrastructure interface for monitoring RF interference. The main view is a heatmap of the first floor, with a color scale ranging from -35 dBm (blue) to -90 dBm (red). The heatmap shows signal strength variations across the floor plan, with several access points (APs) labeled. A blue callout bubble in the center of the heatmap reads "Everyone can do heatmaps". The interface includes a left sidebar with "Floor Settings" and "Load Status", a top navigation bar, and a bottom status bar showing coordinates (-43.59 ft, 191.63 ft).

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

The screenshot displays the Cisco Prime Infrastructure interface. At the top, the navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The main content area is titled 'Floor View' and shows a heatmap of the first floor of the Amsterdam Branch (AMS3). The heatmap uses a color scale from -35 dBm (red) to -90 dBm (blue) to indicate signal strength. Various access points (APs) are labeled, including SJC14-41B-AP9, SJC14-41B-AP5, SJC14-41B-AP4, SJC14-41B-AP3, SJC14-41B-AP1, SJC14-41B-AP8, SJC14-42B-AP9, SJC14-42B-AP5, SJC14-42B-AP6, SJC14-42B-AP7, SJC14-42B-AP3, SJC14-42B-AP1, SJC14-42B-MON2, SJC14-42B-MON1, and SJC14-42B-AP10. A 'Rogue\_Detector' is also visible. A blue callout box with the text 'Everyone can do heatmaps' is overlaid on the heatmap. The interface includes a left sidebar for 'Floor Settings' and 'Load Status', and a top right search bar.

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: 3 Steps to Client Connectivity Troubleshooting

## Step 2. Check for RF Interference

The screenshot displays the Cisco Prime Infrastructure interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The main content area is titled 'Floor View' and shows a site map for 'Amsterdam Branch > AMS3 > First Floor'. A signal strength indicator shows -90 dBm. A blue callout bubble on the left contains the text: 'Thanks to Coloration of Clients with interferers we can locate connectivity issues'. The floor plan is overlaid with a color gradient from light pink to dark red, indicating signal strength. Several yellow lightning bolt icons mark interference points, with labels: 'DECT Like Phone', 'Bluetooth Link', 'Bluetooth Discovery', and 'Bluetooth Discovery'. A specific client MAC address '00:21:5c:01:b8:6f' is highlighted with a green box. The left sidebar shows a 'Maps Tree View' and 'Floor Settings' menu. The bottom left corner shows 'Load Status' with a 'Load' button and a progress indicator: 'Periodic Refresh Done. Loaded 0 out of 0 Interferers Done loading Interferers Loaded 11 out of 11 Clients Done loading Clients'. The bottom right corner shows the dimensions '115.74 ft, 39.87 ft'.

Delivered by: CPI integrated with MSE and CleanAir

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

### Clients and Users

Clients Search Results - Reset Selected 1 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
<input checked="" type="radio"/> 00:21:5c:01:b8:6f		Not Detec...	jfields		Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PST
<input type="radio"/> 00:1b:d4:54:6a:03	192.168.152.35	IPv4	jfields		Cisco	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
<input type="radio"/> dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Client 00:21:5c:01:b8:6f (Refreshed :2012-Nov-22, 04:52:30 PST)

Note: None

#### Client Attributes

##### General

User Name **jfields**

IP Address **Data Not Available**

MAC Address **00:21:5c:01:b8:6f**

Vendor **Intel**

Endpoint Type **Unknown**

Client Type **Regular**

Media Type **Lightweight**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

Power Save **OFF**

CCX **V4**

##### Session

Controller Name **AMS-2504-WLC**

AP Name **NMTG-AP3500-2**

AP IP Address **192.168.152.14**

AP Type **Cisco AP**

AP Base Radio MAC **04:c5:a4:f2:3f:60**

Anchor Controller **Data Not Available**

802.11 State **Associated**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

##### Security

Security Policy Type **WPA2**

EAP Type **Not Available**

On Network **No**

802.11 Authentication **Open System**

Encryption Cipher **CCMP (AES)**

SNMP NAC State **Access**

Radius NAC State **8021X\_REQD**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Select the problem device again

Cisco Prime Infrastructure Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design

### Clients and Users

Clients Search Results - Reset Selected 1 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	Not Detec...	Not Detec...	jfields	Client	Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PS
00:10:07:07:08:05	192.168.152.25	IPv4	jfields	Client	Cisco	AMS-2504-WLC	Amsterdam branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:49:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields	Client	Compal	AMS-3750-SBR	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

**Client 00:21:5c:01:b8:6f** (Refreshed :2012-Nov-22, 04:52:30 PST) Note: None

#### Client Attributes

##### General

User Name **jfields**

IP Address **Data Not Available**

MAC Address **00:21:5c:01:b8:6f**

Vendor **Intel**

Endpoint Type **Unknown**

Client Type **Regular**

Media Type **Lightweight**

Mobility Status **Unassociated**

Hostname **Data Not Available**

E2E **V1**

802.11u Capable **No**

Power Save **OFF**

CCX **V4**

##### Session

Controller Name **AMS-2504-WLC**

AP Name **NMTG-AP3500-2**

AP IP Address **192.168.152.14**

AP Type **Cisco AP**

AP Base Radio MAC **04:c5:a4:f2:3f:60**

Anchor Controller **Data Not Available**

802.11 State **Associated**

Association ID **1**

Port **1**

Interface **vlan 13**

SSID **AMS-DOT1X**

Profile Name **AMS-dot1x**

Protocol **802.11n(5GHz)**

VLAN ID **13**

AP Mode **local**

Data Switching **Unknown**

Authentication **Unknown**

##### Security

Security Policy Type **WPA2**

EAP Type **Not Available**

On Network **No**

802.11 Authentication **Open System**

Encryption Cipher **CCMP (AES)**

SNMP NAC State **Access**

Radius NAC State **8021X\_REQD**

AAA Override ACL Name **none**

AAA Override ACL Applied Status **N/A**

Redirect URL **none**

ACL Name **none**

ACL Applied Status **N/A**

FlexConnect Local Authentication **No**

Policy Manager State **8021X\_REQD**

Authenticating ISE **Data Not Available**

Authorization Profile Name **Data Not Available**

Posture Status **Unknown**

TrustSec Security Group **Data Not Available**

Windows AD Domain **Data Not Available**

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

The screenshot shows the Cisco Prime Infrastructure web interface. At the top, there's a navigation bar with 'Home' and 'Design' menus. A search bar contains 'jfields'. A blue callout bubble points to the search bar with the text 'Select the problem device again'. Below the navigation bar, the 'Clients and Users' section is active, showing 'Clients Search Results - Reset'. A table lists search results with columns for MAC Address, IP Address, IP Type, User Name, Type, Vendor, Device Name, Location, VLAN, Status, Interface, Protocol, and Association Time. The first row is selected and highlighted in green. A second blue callout bubble points to the first row with the text 'Generic info is easy'. Below the table, the 'Client 00:21:5c:01:b8:6f' details are shown, divided into three sections: 'General', 'Session', and 'Security'. The 'General' section is circled in green. The 'Session' section is also circled in green. The 'Security' section is not circled.

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	Not Detec...	Not Detec...	jfields	Regular	Intel	AMS-2504-WLC	Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5G...	2012-Nov-22, 01:53:39 PST
00:10:07:37:08:03	192.168.152.33	IPv4	jfields	Regular	Intel	AMS-2504-WLC	Amsterdam branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:43:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields	Regular	Intel	Unknown	Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Generic info is easy

Select the problem device again

**Client Attributes**

**General**

- User Name: **jfields**
- IP Address: **Data Not Available**
- MAC Address: **00:21:5c:01:b8:6f**
- Vendor: **Intel**
- Endpoint Type: **Unknown**
- Client Type: **Regular**
- Media Type: **Lightweight**
- Mobility Status: **Unassociated**
- Hostname: **Data Not Available**
- E2E: **V1**
- 802.11u Capable: **No**
- Power Save: **OFF**
- CCX: **V4**

**Session**

- Controller Name: **AMS-2504-WLC**
- AP Name: **NMTG-AP3500-2**
- AP IP Address: **192.168.152.14**
- AP Type: **Cisco AP**
- AP Base Radio MAC: **04:c5:a4:f2:3f:60**
- Anchor Controller: **Data Not Available**
- 802.11 State: **Associated**
- Association ID: **1**
- Port: **1**
- Interface: **vlan 13**
- SSID: **AMS-DOT1X**
- Profile Name: **AMS-dot1x**
- Protocol: **802.11n(5GHz)**
- VLAN ID: **13**
- AP Mode: **local**
- Data Switching: **Unknown**
- Authentication: **Unknown**

**Security**

- Security Policy Type: **WPA2**
- EAP Type: **Not Available**
- On Network: **No**
- 802.11 Authentication: **Open System**
- Encryption Cipher: **CCMP (AES)**
- SNMP NAC State: **Access**
- Radius NAC State: **8021X\_REQD**
- AAA Override ACL Name: **none**
- AAA Override ACL Applied Status: **N/A**
- Redirect URL: **none**
- ACL Name: **none**
- ACL Applied Status: **N/A**
- FlexConnect Local Authentication: **No**
- Policy Manager State: **8021X\_REQD**
- Authenticating ISE: **Data Not Available**
- Authorization Profile Name: **Data Not Available**
- Posture Status: **Unknown**
- TrustSec Security Group: **Data Not Available**
- Windows AD Domain: **Data Not Available**

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Select the problem device again

Clients and Users

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	Not Detec...	Not Detec...	jfields	Regular	Intel		Amsterdam Branch ...	13	Associated	vlan 13	802.11n(5...	2012-Nov-22, 01:53:39 PS
00:10:07:37:08:03	192.168.152.55	IPv4	jfields	Regular	Intel		Amsterdam branch ...	13	Associated	vlan 13	802.11g	2012-Nov-21, 17:49:28 PST
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields	Regular	Intel		Unknown	12	Associated	Fa1/0/6	802.3	2012-Nov-20, 10:37:29 PST

Generic info is easy

Client 00:21:5c:01:b8:6f (Refreshed :2012-Nov-22, 04:00:00)

**Client Attributes**

**General**

- User Name **jfields**
- IP Address **Data Not Available**
- MAC Address **00:21:5c:01:b8:6f**
- Vendor **Intel**
- Endpoint Type **Unknown**
- Client Type **Regular**
- Media Type **Lightweight**
- Mobility Status **Unassociated**
- Hostname **Data Not Available**
- E2E **V1**
- 802.11u Capable **No**
- Power Save **OFF**
- CCX **V4**

**Session**

- Controller Name **AMS-2504-WLC**
- AP Name **NMTG-AP3500-2**
- AP IP Address **192.168.152.14**
- AP Type **Cisco AP**
- AP Base Radio MAC **04:c5:a4:f2:3f:60**
- Anchor Controller **Data Not Available**
- 802.11 State **Associated**
- Association ID **1**
- Port **1**
- Interface **vlan 13**
- SSID **AMS-DOT1X**
- Profile Name **AMS-dot1x**
- Protocol **802.11n(5GHz)**
- VLAN ID **13**
- AP Mode **local**
- Data Switching **Unknown**
- Authentication **Unknown**

The integration with ISE makes it shine

- On Network **No**
- 802.11 Authentication **Open System**
- Encryption Cipher **CCMP (AES)**
- SNMP NAC State **Access**
- Radius NAC State **8021X\_REQD**
- AAA Override ACL Name **none**
- AAA Override ACL Applied Status **N/A**
- Redirect URL **none**
- ACL Name **none**
- ACL Applied Status **N/A**
- FlexConnect Local Authentication **No**
- Policy Manager State **8021X\_REQD**
- Authenticating ISE **Data Not Available**
- Authorization Profile Name **Data Not Available**
- Posture Status **Unknown**
- TrustSec Security Group **Data Not Available**
- Windows AD Domain **Data Not Available**

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset | Selected 1 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

#### Client Statistics

##### Exceptions

- Policy errors **0**
- Data Retries **0**
- RTS Retries **0**
- Duplicates **0**
- Decrypt Failed **0**
- MIC Errors **0**
- MIC Missing Frames **0**
- Interim Updates Sent **0**

##### Traffic

Packets Tx/Rx **986/208**

Bytes Tx/Rx **60033/18512**

##### 802.11 Metrics

RSSI **-37 dBm**

SNR **52**

Uptime (seconds) **17**

Current Tx Rate **m15**

Data RateSet **6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0**

#### Association History

Association Time	Duration	User Name	IP Address	IP Address...	AP Name	Controller Name	SSID
2012-Nov-22, 01:53:39 PST	1 hrs 55 min 11 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 18:48:29 PST	7 hrs 0 min 9 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 11:43:24 PST	7 hrs 0 min 5 sec	jfields	192.168.152.38	IPv4	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 07:43:21 PST	3 hrs 30 min 2 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X

#### Events

Event Type	Event Time	Description
No data available		

#### Statistics

Select a time period below to view the chart. [End User Experience Dashboard](#)

Time: 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom

##### Client AP Association History

Scrolling down more client info to be found like:

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela | jfields

Home Design Deploy Operate Report Administration

### Clients and Users

Clients Search Results - Reset | Selected 1 | Total 3

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

#### Client Statistics

##### Exceptions

- Policy errors 0
- Data Retries 0
- RTS Retries 0
- Duplicates 0
- Decrypt Failed 0
- MIC Errors 0
- MIC Missing Frames 0
- Interim Updates Sent 0

##### Traffic

Packets Tx/Rx **986/208**  
Bytes Tx/Rx **60033/18512**

##### 802.11 Metrics

RSSI **-37 dBm**  
SNR **52**  
Uptime (seconds) **17**  
Current Tx Rate **m15**  
Data RateSet **6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0**

#### Association History

Association Time	Duration	User Name	IP Address	IP Address...	AP Name	Controller Name	SSID
2012-Nov-22, 01:53:39 PST	1 hrs 55 min 11 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 18:48:29 PST	7 hrs 0 min 9 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 11:43:24 PST	7 hrs 0 min 5 sec	jfields	192.168.152.38	IPv4	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Nov-21, 07:43:21 PST	3 hrs 30 min 2 sec	jfields	192.168.152.38	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X

Scrolling down more client info to be found like:

#### Events

Event Type	Event Time	Description
No data available		

#### Statistics

Select a time period below to view the chart.

Time: 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom

##### Client AP Association History

[End User Experience Dashboard](#)

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | dvandela

Home Design Deploy Operate Report Administration

Site Device Interface Application Voice/Video **End User Experience**

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

2012 November 22, 04:59:42 PST

### User Site Summary

Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Administ

Site Device Interface Application Voice/Video End User Experience

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

2012 November 22, 04:59:42 PST

### User Site Summary

#### Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

#### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

#### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Administ

Site Device Interface Application Voice/Video End User Experience

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

### User Site Summary

#### Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

2012 November 22, 04:59:42 PST

Application ART Analysis

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Administ

Site Device Interface Application Voice/Video End User Experience

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

### User Site Summary

#### Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

#### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

#### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

2012 November 22, 04:59:42 PST

Application ART Analysis

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Admin

Site Device Interface Application Voice/Video **End User Experience**

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

### User Site Summary

#### Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

2012 November 22, 04:59:42 PST

Application ART Analysis

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Administ

Site Device Interface Application Voice/Video End User Experience

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

### User Site Summary

Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

2012 November 22, 04:59:42 PST

Application ART Analysis

# Prime Infrastructure: Client Connectivity Troubleshooting

## Step 3. Check for Application Response time

Real user experience info on one Page

Cisco Prime Infrastructure

Home Design Deploy Operate Report Administ

Site Device Interface Application Voice/Video End User Experience

Filters \*Client 00:21:5c:01:b8:6f, \*Time Frame Past 24 Hours Application Network Aware Go

### Top N Applications

Applications

Kilobytes/sec

Unknown Traffic Wireless Traffic Wired Traffic

2012 November 22, 04:59:42 PST

### User Site Summary

Device Reachability

Device Name	Device IP	Location	SNMP Reachability
Rack2TS1	192.168.136.2		Unreachable
ACC-NAM2204.cisco.com	192.168.136.67	RMON Lab	Unreachable
LON-4948-ABR2	10.11.10.2		Reachable
FL4-H3C-1	10.15.10.3	Hangzhou China	Reachable
LON-4948-ABR1	10.11.10.1		Reachable
Campus-NAM3.eset-cisco.c...	192.168.136.129	Bld O	Reachable

### Worst N RTP End Point Pairs

Source Address	T...	Destination Addr...	T...	Source User	Destination U...	Packet Loss (%)	Jitter (ms)
10.15.12.13		10.2.12.13				33	11.8
10.2.12.20		10.15.12.20				0	356
10.9.11.12		10.3.11.41				0	48.6
10.2.12.11		10.15.12.11				0	248.3

### Worst N Clients by Transaction Time

Client	T...	User	Application	Max Transaction Time (...)	Avg Transaction Time (ms)
192.168.139.103			unknown	105848	105452
10.1.12.14			gnutella-svc	240198	60071
10.1.12.13			h323hostcallsc	204097	51041
10.1.12.16			x11	186783	46724
10.1.12.16			ccmail	172294	43371

Application ART Analysis 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)

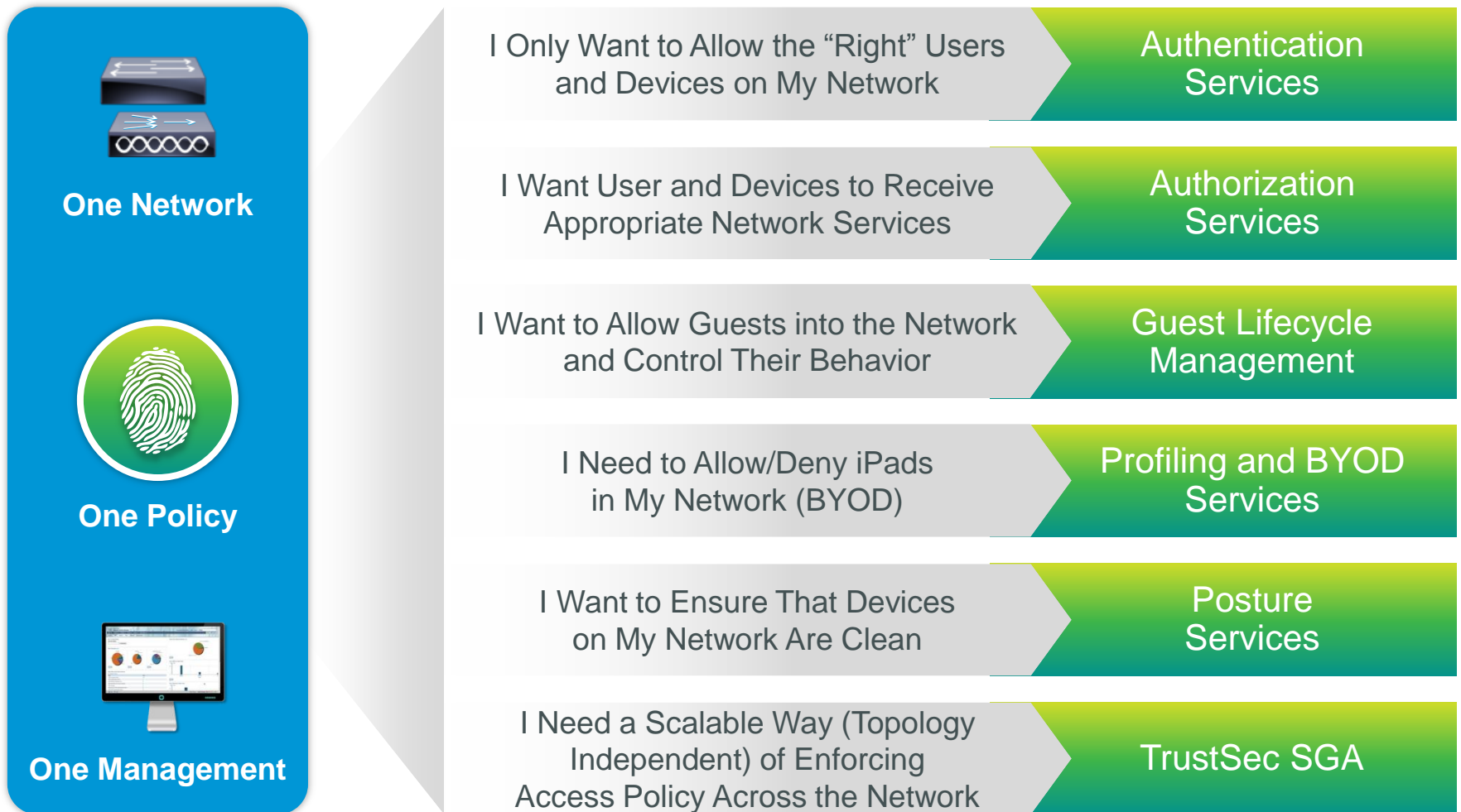
The screenshot displays the 'Device 360 Views' interface. At the top, it shows the device identifier 'DEN-2960S-SBR'. Below this, the 'User 360 View' is shown for 'User Name : jfields'. The interface features three device icons: 'Workstation', 'SonyPS3', and 'Apple-iPad'. A detailed view of the 'Workstation' endpoint is shown, including its IP address (192.168.152.27), MAC address (dc:0e:a1:b9:22:58), and connection details to switch 'AMS-3750-SBR' via 'FastEthernet1/0/6'. Session information indicates the user is associated with the device since 2013-Jan-24, 18:22:35, with a session length of 0 days 13 hrs 35 min 21 sec. A table at the bottom lists applications running on the endpoint.

End Point	Mac Address	Application	Last 1 Hour Volume (...)
192.168.152.27	dc::0:e::a1::b:9:	youtube	1149.3889
192.168.152.27	dc::0:e::a1::b:9:	http	0.7073
192.168.152.27	dc::0:e::a1::b:9:	unclassified	0.1429

# One Policy

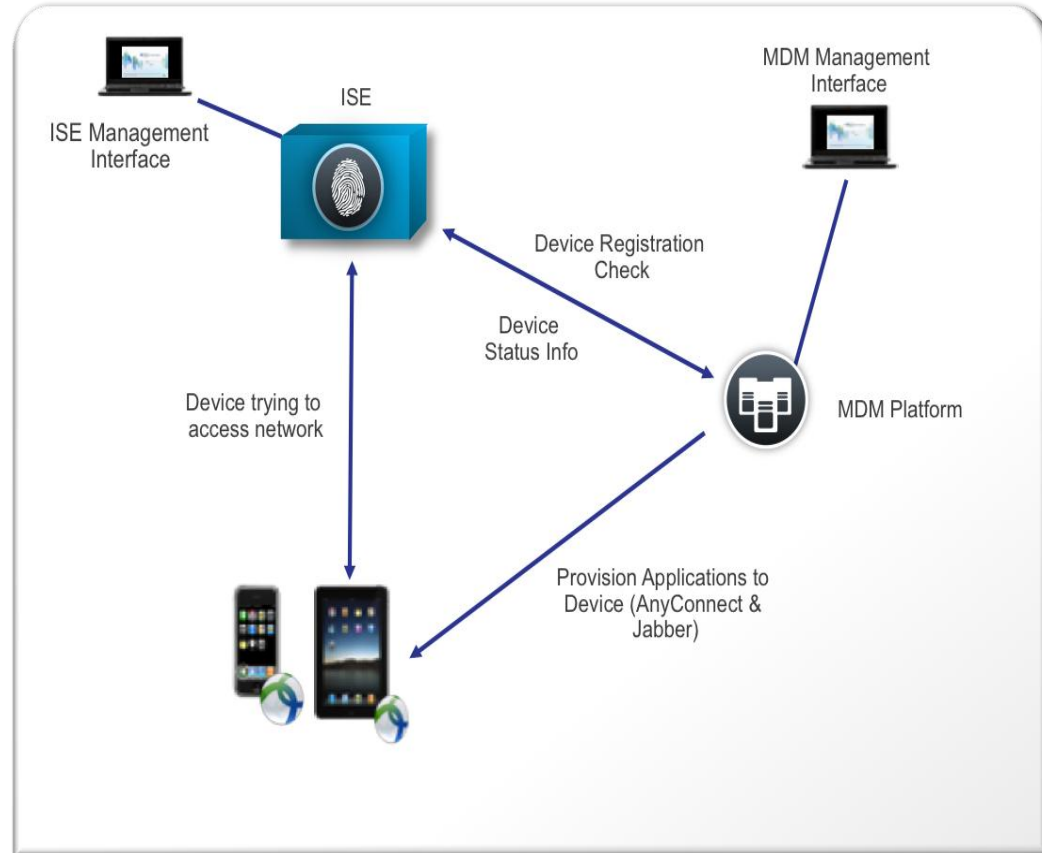


# One Policy Platform - ISE: Use Cases



# ISE 1.2 and MDM Integration

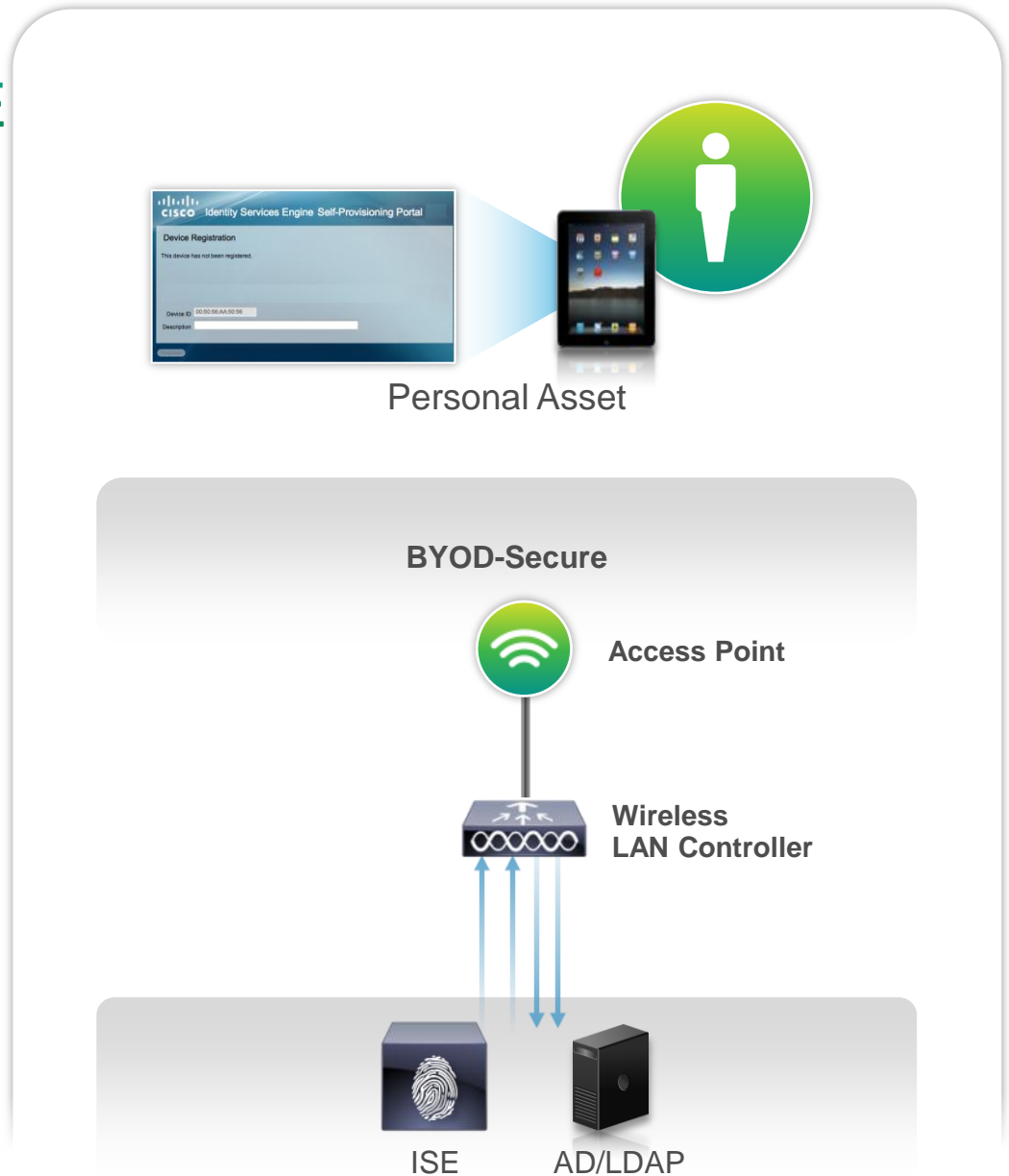
- MDM device registration via ISE
  - Non registered clients redirected to MDM registration page
- Restricted access
  - Non compliant clients will be given restricted access based on policy
- Endpoint MDM agent
  - Compliance
  - Device applications c
- Device Action from ISE
  - Device stolen -> wipe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



# BYOD Flow

## Single SSID, powered by ISE

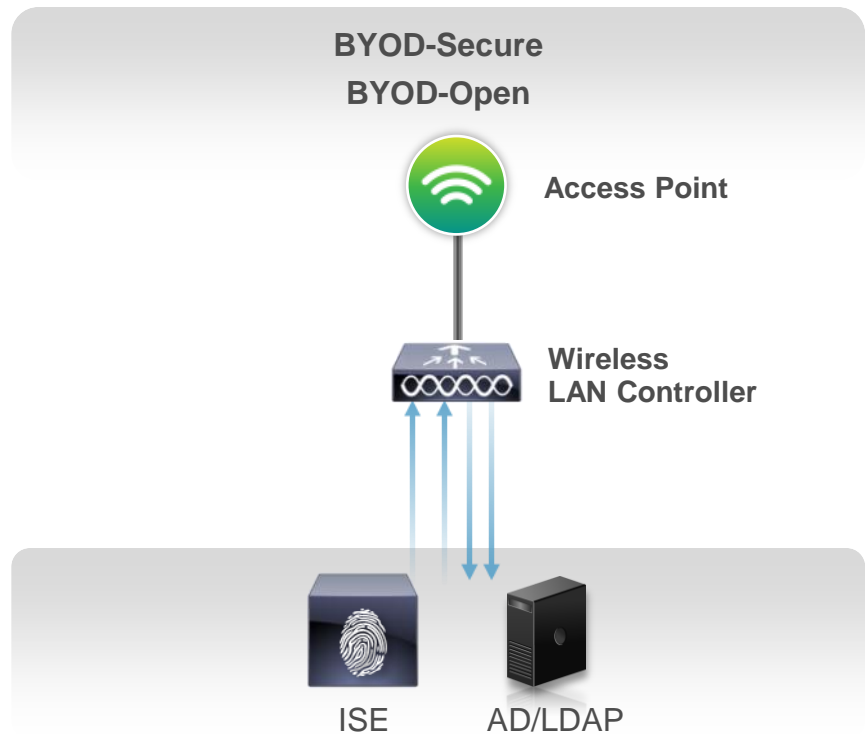
- User connects to Secure SSID
- PEAP:  
Username/Password
- Redirected to Provisioning Portal
- User registers device
  - Downloads Certificate
  - Downloads Supplicant Config
- User reconnects using EAP-TLS



# 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

Identity Services Engine

Authentications | Reports | Endpoint Protection Service | Troubleshoot

Report Selector

Mobile Device Management

From 12/02/2012 12:00:00 AM to 12/31/2012 11:59:59 PM

Logged At	Server	Username	MAC Address	IP Address	Session ID	OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number	Failure Reason
2012-12-20 18:00:03.506	ise-mdm		7C-60-62-E3-05-05		0a012c5a000001eb50430aad	iOS 5.0	✓	✗	🔒	✓	✗	Apple	Pad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2012-12-20 01:19:27.913	ise-mdm		7C-60-62-E3-05-05		0a012c5a000001a650d2678c	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2012-12-20 00:36:34.817	ise-mdm		7C-60-62-E3-05-05		0a012c5a000001a050d25c9c	iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:29.484	ise-mdm		7C-60-62-E3-05-05		0a012c5a000001a050d25c9c	iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:27.984	ise-mdm		7C-60-62-E3-05-05		0a012c5a0000019350d23f62	iOS 5.0	✓	✗	✓	✓	✗	Apple	Pad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-19 01:15:12.138	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 01:15:00.2	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 00:57:00.815	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 00:49:29.929	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 00:48:49.153	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 00:42:30.46	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009950d10475	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113				
2012-12-19 00:37:22.096	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009850d10c41		🔒										Device is not registered with MDM
2012-12-19 00:36:50.083	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009750d10c21		🔒										Device is not registered with MDM
2012-12-19 00:26:26.935	ise-mdm		BC-81-F3-8F-FA-44		0a012c5a0000009550d109b2		🔒										Device is not registered with MDM

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



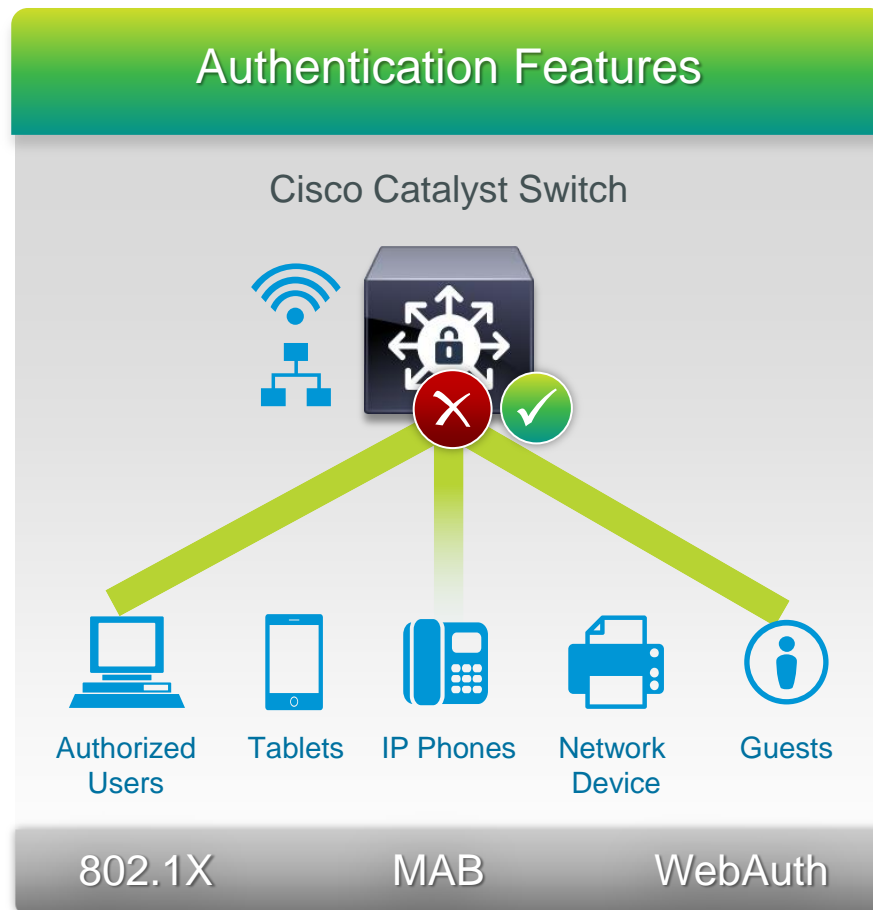
## Identity Differentiators

- ✓ 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

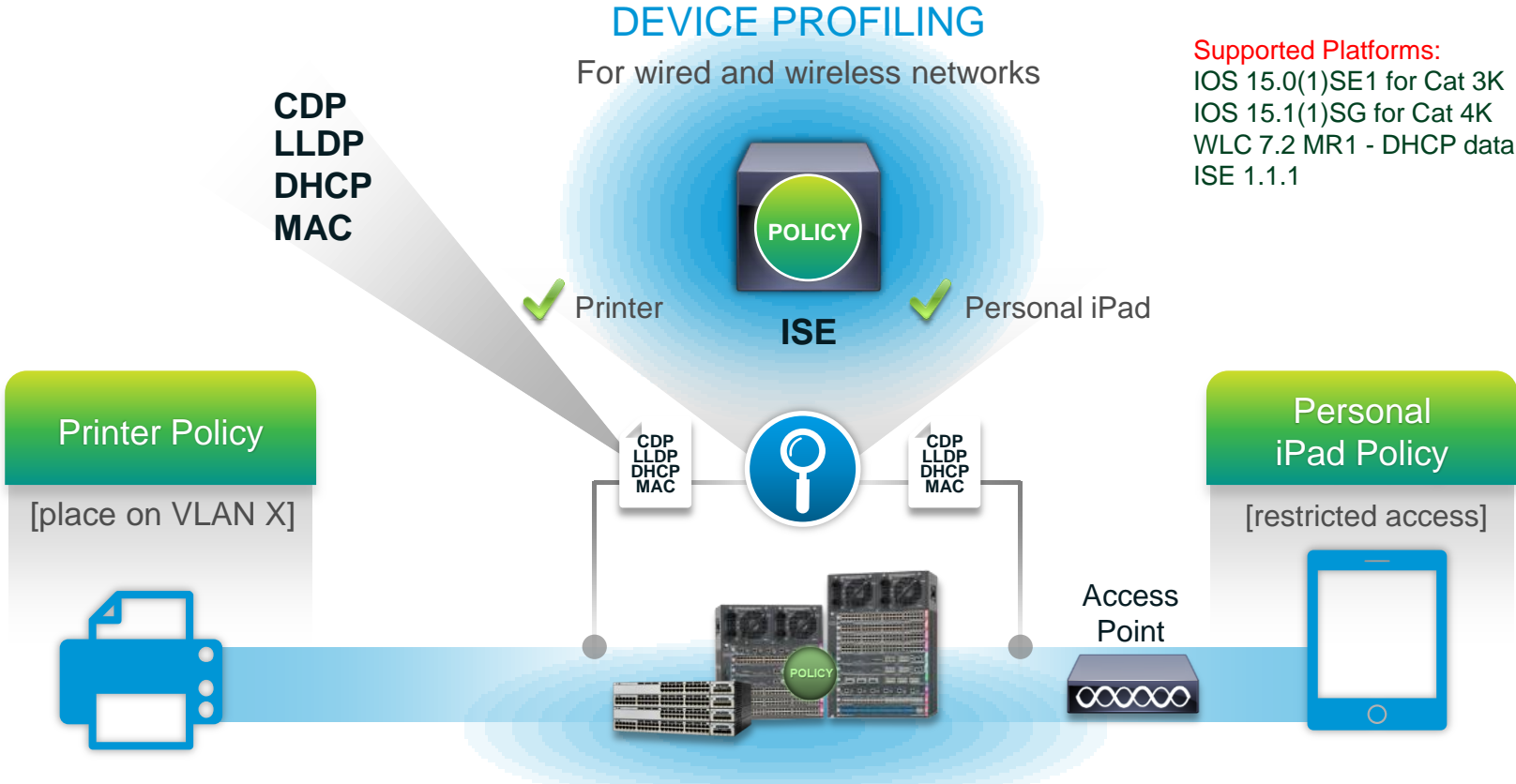
- ✓ IP Telephony Support for Virtual Desktop Environments
  - Single host mode
  - Multihost mode
  - Multiauth mode
  - Multidomain authentication
- ✓ Critical Data/Voice Authentication
  - Business continuity in case of failure

## Authentication Features



# Device Sensor

## Automated Device Classification Using Cisco Infrastructure



**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

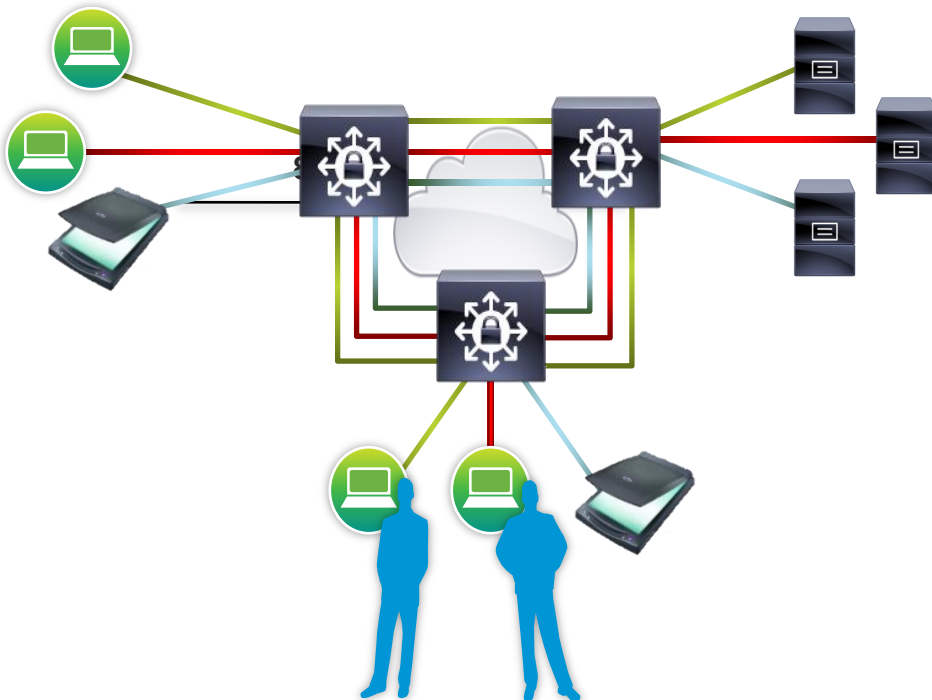
# Policy Enforcement: VLANs or ACLs?

## VLAN Architecture

Scaling Concerns

Highly topology dependent

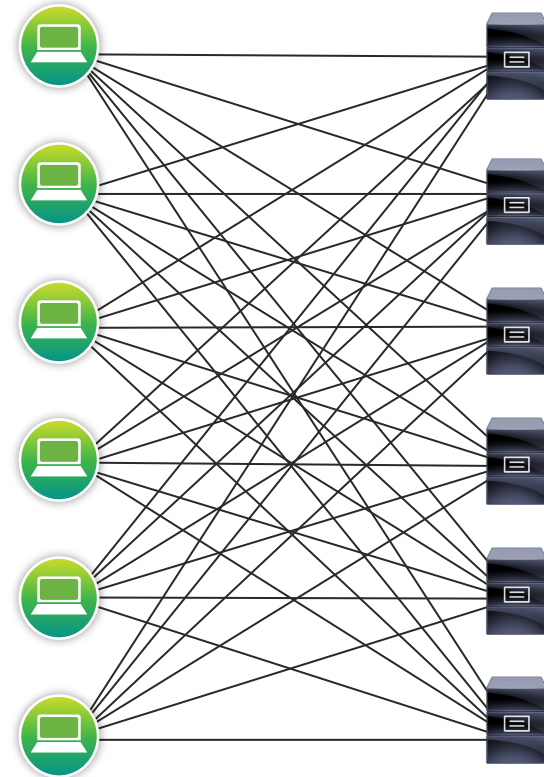
Endpoint IP address release/renew challenging



## ACL Architecture

Hard to Maintain

100s–1000s of ACEs



# Policy Enforcement: Security Group Access!

## SGA – Topology Independent

### User and Device Role

Public SSID

Corporate SSID  
Member of group “Employee”  
Certificate matches endpoint

Corporate SSID  
Member of group Employee and Manager  
Certificate matches endpoint

Credit\_Card SSID  
Member of group  
“Credit\_Scanners”  
Profiled as “iphone”

### SGA TAG - Policy

Unregistered Device  
(Unregist\_Dev\_SGT)

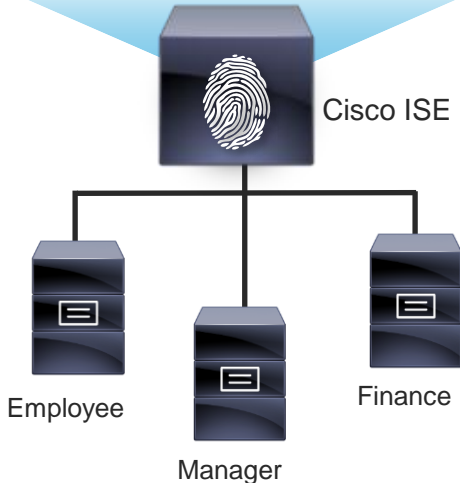
Employee  
(Employee\_SGT)

Management  
(Management\_SGT)

Credit Card Scanners  
(CC\_Scanner\_SGT)



who      what      where      when      how



# SGA Inside ISE

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions	Permissions	
✓	Black List Default	if <b>Blacklist</b>	then Blacklist_Access	<a href="#">Edit</a>   ▾
✓	Employee Access	if <b>RegisteredDevices</b> AND (Radius:Called-Station-ID MATCHES corporate-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD:ExternalGroups EQUALS cisco.com/Users/Employee)	then Employee-Access AND Employee_SGT	<a href="#">Edit</a>   ▾
✓	Management	if <b>RegisteredDevices</b> AND (Radius:Called-Station-ID MATCHES corporate-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD:ExternalGroups EQUALS cisco.com/Users/Management )	then Employee-Access AND Management_SGT	
✓	Credit Card Scanner	if <b>Apple-iPhone</b> AND (Radius:Called-Station-ID MATCHES cc-secure-wifi AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Common Name STARTS_WITH cc-reader- AND AD:ExternalGroups EQUALS cisco.com/POS/Credit Card Scanners )	then CC-Reader-Profile AND CC_Scanner_SGT	<a href="#">Edit</a>   ▾
✓	Default	if no matches, then	Default-Guest-Access AND Unregist_Dev_SGT	<a href="#">Edit</a>   ▾

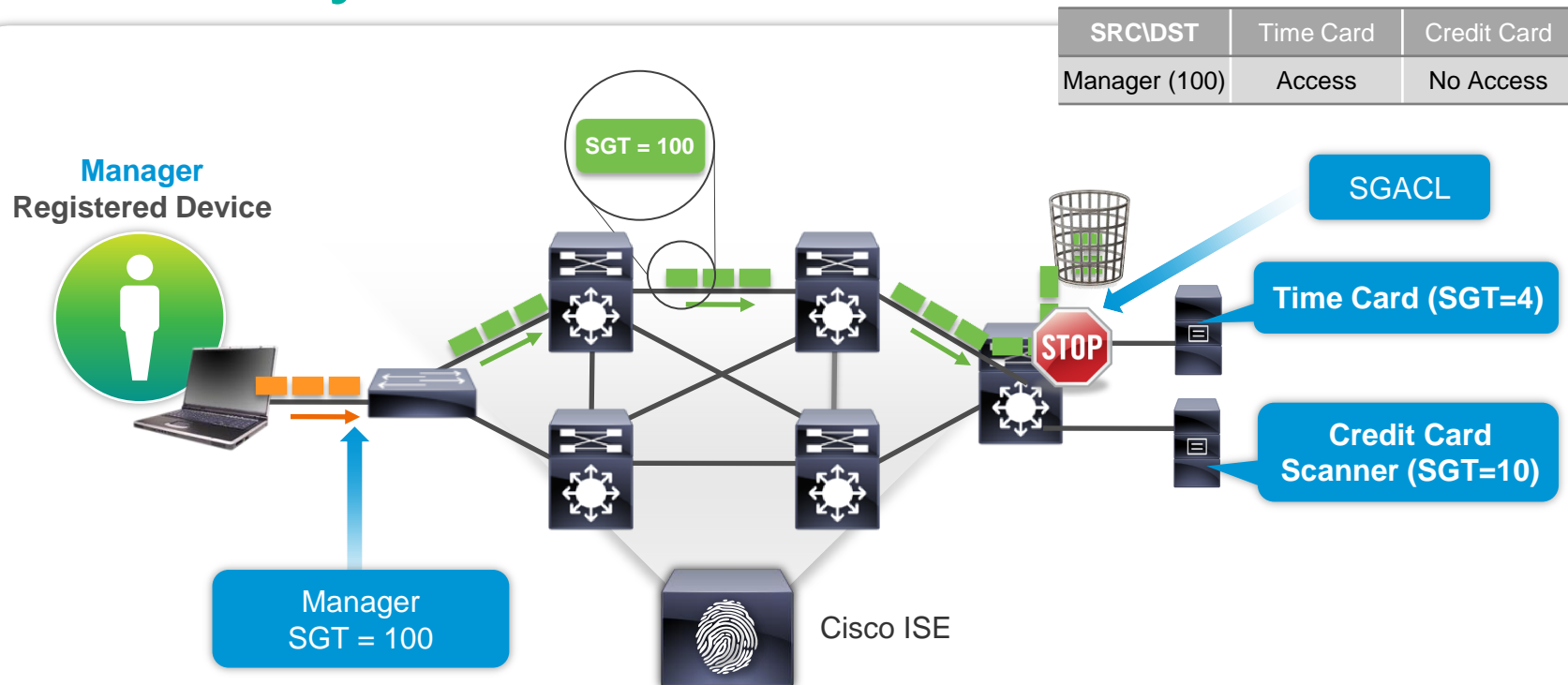
Save Reset

**Manager TAG**

**Employee TAG**

**Credit Card Scanner TAG**

# SGA Policy Enforcement Flow



## 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

The screenshot displays the Cisco ISE configuration interface for SGA enforcement. The main table shows the configuration for various source groups across two destinations: Web\_Servers and Time\_Card\_Server. The interface includes a top navigation bar with options like Edit, Add, Clear Mapping, Configure, Push, and Monitor All. A left sidebar shows the configuration tree, and a right sidebar shows the task navigator.

Destination	Web_Servers (7 / 0007)	Time_Card_Server (10 / 000A)
Source		
Unregist_Dev_SGT (3 / 0003)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP
Management_SGT (5 / 0005)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP
Employee_SGT (4 / 0004)	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP	<input checked="" type="checkbox"/> Enabled SGACLs: Permit IP
CC_Scanner_SGT (6 / 0006)	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP	<input checked="" type="checkbox"/> Enabled SGACLs: Deny IP

# SGA Enforced at ASA Firewall

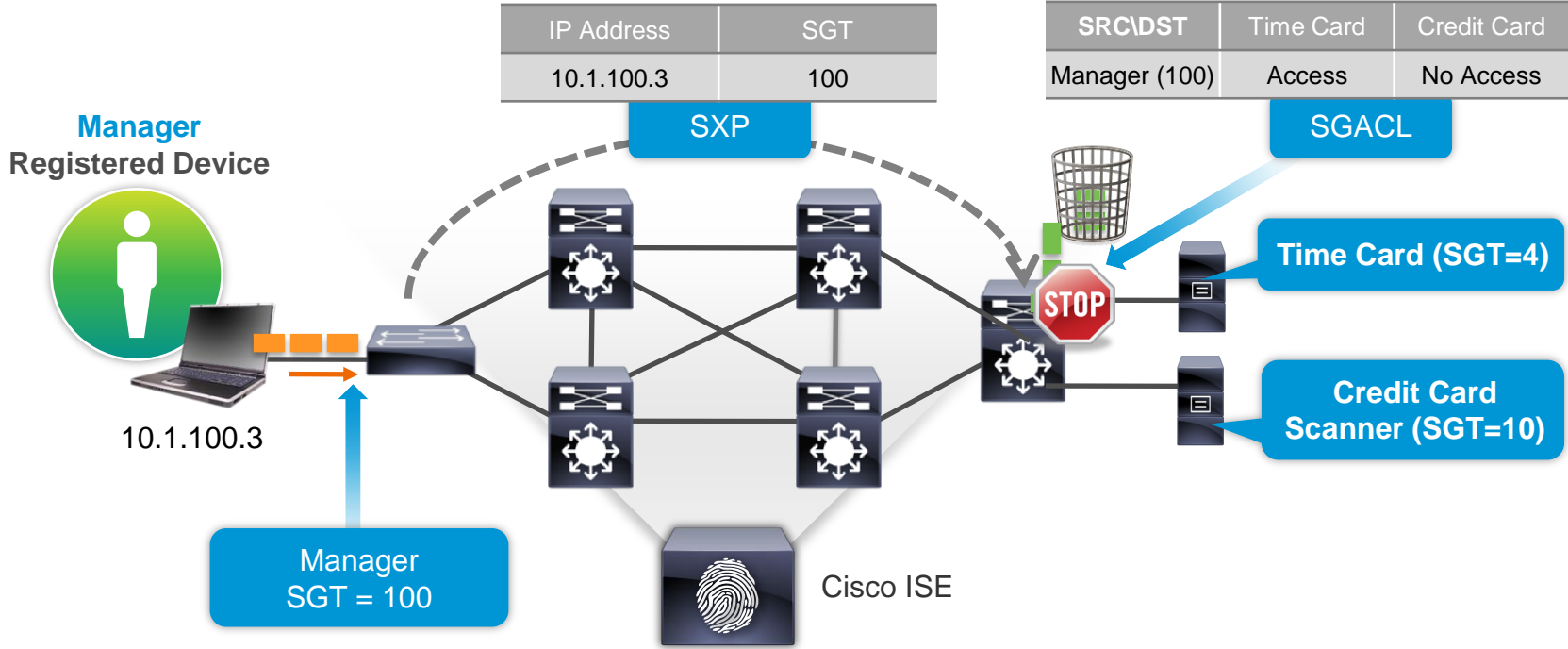
#	Enabled	Source Criteria:			Destination Criteria:		Service	Action
		Source	User	Security Group	Destination	Security Group		
[-]  inside (1 incoming rule)								
1	<input checked="" type="checkbox"/>	any			any		ip	Permit
[-]  outside (9 incoming rules)								
1	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit
2	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny
3	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit
4	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny
5	<input checked="" type="checkbox"/>	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit

Manager TAG

Credit Card Scanner TAG

# Migrating to Security Group Access

## SGT eXchange Protocol (SXP)



### Security Group Access Protocol

- For transport through a non SGT core

# Tying it All Together

## ISE Authorization Policy Definition



User



Device Type



Location



Posture



Time



Access Method



Custom

### Authorization Policy At A Glance

First Matched Rule Applies

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 Name 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	Contractor_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

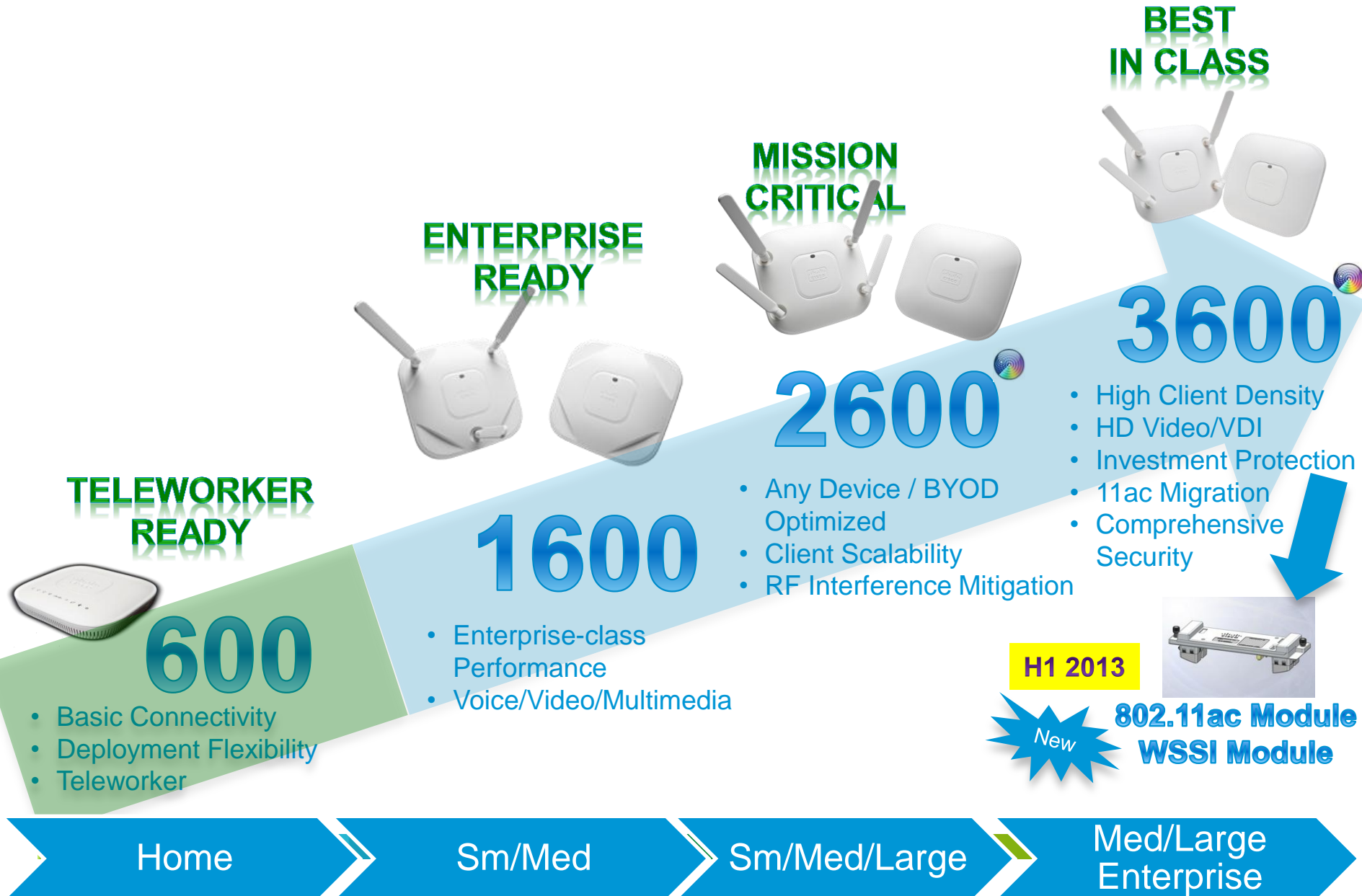
- SGA: Topology independent, Business language
- Enforcement: Router/Switch/Controller feature
- Endpoint: Posture, VPN
- Info stores: AD, LDAP, DHCP, MDM
- MACSec: L2 encryption



# One Network



# Cisco Aironet 802.11n + 802.11ac AP Portfolio



**BEST  
IN CLASS**



**3600**

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

**MISSION  
CRITICAL**



**2600**

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

**ENTERPRISE  
READY**



**1600**

- Enterprise-class Performance
- Voice/Video/Multimedia

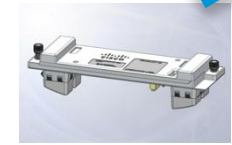
**TELEWORKER  
READY**



**600**

- Basic Connectivity
- Deployment Flexibility
- Teleworker

**H1 2013**



**802.11ac Module  
WSSI Module**

Home

Sm/Med

Sm/Med/Large

Med/Large  
Enterprise

# WLAN Controller Portfolio

## Large Campus

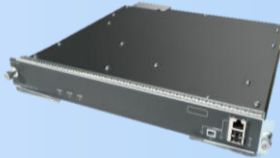
Catalyst  
3850



5508



WISM2



5760



- 1 to 50 APs per switch/stack (Directly connected APs)
- 2000 clients per stack
- 40 Gbps per switch
- 12 to 500 APs
- 7000 clients
- 8 Gbps
- 100 to 1000 APs
- 15,000 clients
- 20 Gbps
- 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



2500



Virtual  
Controller



Catalyst  
3850



- 5 to 50 APs
- 500 clients
- 500 Mbps
- 5 to 75 APs
- 1000 clients
- 1 Gbps
- 5 to 200 APs
- 3000 clients
- 500 Mbps
- 1 to 50 APs per switch/stack (Directly connected)
- 2000 clients per stack
- 40 Gbps per switch

## Branch (Controller in DC)

Virtual  
Controller



Flex 7500



- 5 to 200 APs
- 3000 clients
- 500 Mbps
- 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

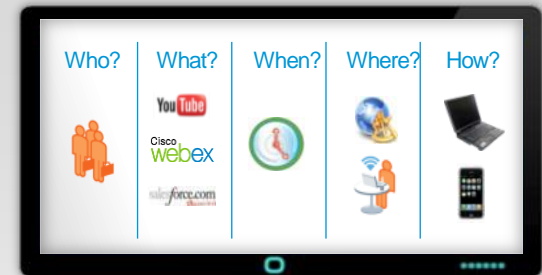
AVC

Classification and policies on 1000+ Apps

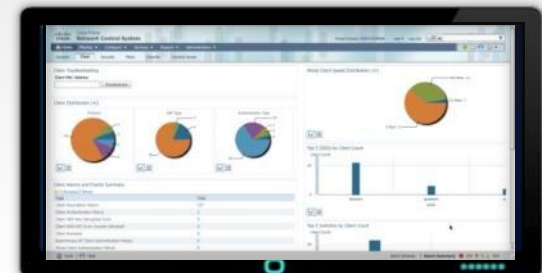
MSE and Thinksmart

Analytics that aid business decisions  
Meaningful Interaction with your customers

## Policy and Network Management



ISE Control



Prime Infrastructure Visibility

# Catalyst Access Switching Portfolio

## Unified Workspace



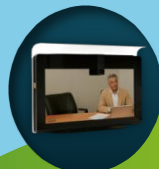
Data



Voice



BYOD



Video



Mobility

Traditional  
Workspace



**Catalyst  
2960-S**

- Scale & Performance
- Security
- Lower TCO



**Catalyst  
3560-X/3750-X**



**Catalyst  
3850**



**Catalyst  
4500E**

Scale & Performance

TrustSec

Application Visibility

Energy Management and Green

Lower TCO

**CONVERGED ACCESS\***

**Distributed Intelligent Access Services**

# 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:

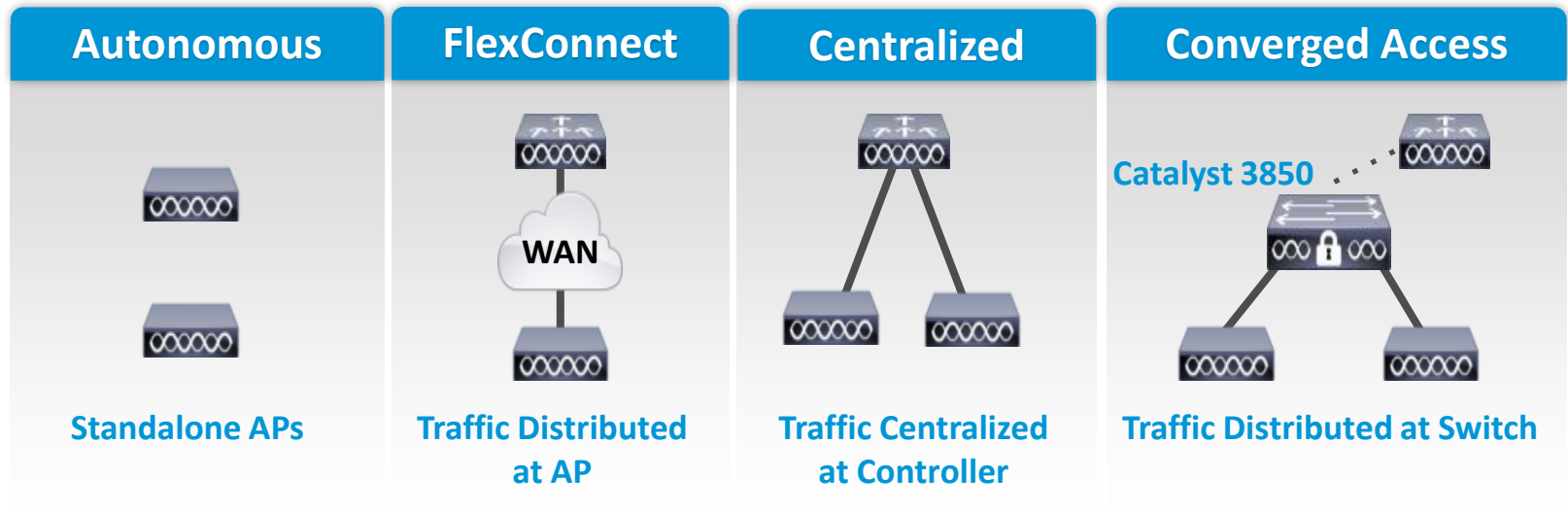
- Stacking
- Stackpower
- Flexible Netflow
- Granular QoS
- Trustsec\*/Identity
- AVC/Medianet\*
- Smart Operations\*
- EnergyWise\*



## 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



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
<b>Benefits</b>	<ul style="list-style-type: none"> <li>Simple and cost-effective for small networks</li> </ul>	<ul style="list-style-type: none"> <li>Highly scalable for large number of remote branches</li> <li>Simple wireless operations with DC hosted controller</li> </ul>	<ul style="list-style-type: none"> <li>Simplified operations with centralized control for Wireless</li> <li>Wireless Traffic visibility at the controller</li> </ul>	<ul style="list-style-type: none"> <li>Wired and Wireless common operations</li> <li>One Enforcement Point</li> <li>One OS (IOS)</li> <li>Traffic visibility at every network layer</li> <li>Performance optimized for 11ac</li> </ul>
<b>Key Considerations</b>	<ul style="list-style-type: none"> <li>Limited RRM, no Rogue detection</li> </ul>	<ul style="list-style-type: none"> <li>L2 roaming only</li> <li>WAN BW &amp; latency requirements</li> </ul>	<ul style="list-style-type: none"> <li>System throughput</li> </ul>	<ul style="list-style-type: none"> <li>Catalyst 3850 in the access layer</li> </ul>

# Converged Wired/Wireless Access – Additional Benefits



**Single platform** for wired and wireless

Common IOS, same administration point, one release



Network wide **visibility** for faster troubleshooting

Wired and wireless traffic visible at every hop



Consistent security and quality of service **control**

Hierarchical bandwidth management and distributed policy enforcement



Maximum **resiliency** with fast stateful recovery

Layered network high availability design with stateful switchover



**Scale** with distributed wired and wireless data plane

480G stack bandwidth; 40G wireless/switch; efficient multicast

Unified Access - One Policy | One Management | One Network

# 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!**

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

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

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

# Dimension Data Network Barometer Report, TLMA

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



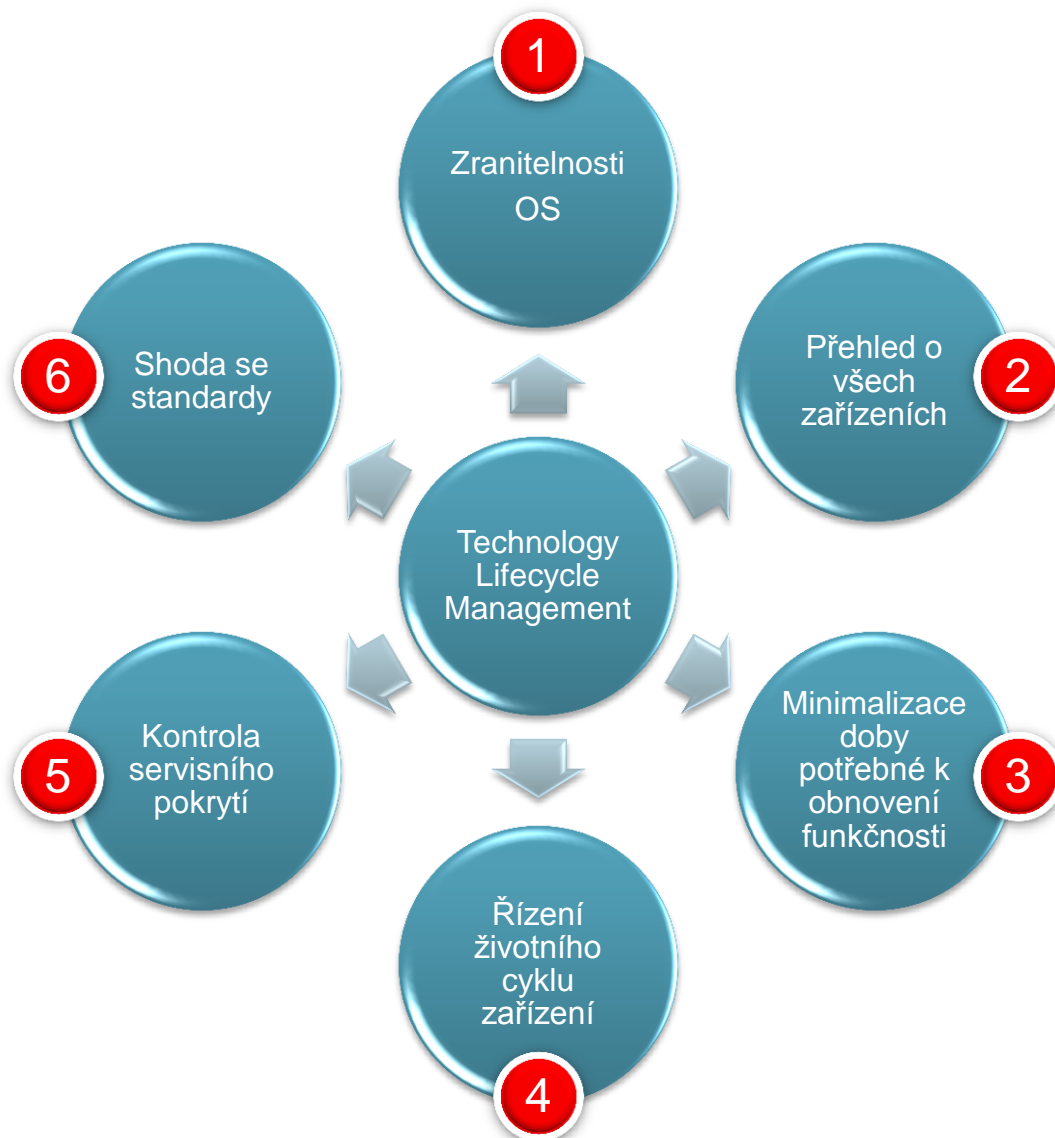
dimension  
data 

Network Integration  
Wednesday, 24 April, 2013

**Správa životního cyklu zařízení - TLMA**

**Výstupy TLMA - Dimension Data Network  
Barometer Report**

# 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

### Discover

#### Zahájení TLM Assessmentu

- Obchodní pohovor
- Technický pohovor
- Sběr informací pomocí nástrojů

### Assess

#### Analýza výstupů a tvorba doporučení

- End-of-life
- Zranitelnosti OS
- Konfigurace dle „Best Practice“
- Stav servisního pokrytí

### Recommend

#### Prezentace výstupů a doporučení

- Několika-letý plán obnovy
- Záplaty OS
- Konfigurační změny
- Úprava servisního pokrytí

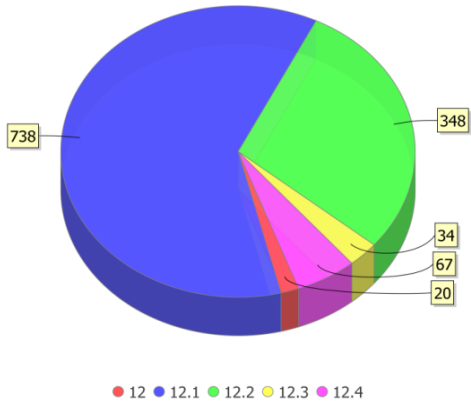
# TLMA - Technology Lifecycle Management Assessment



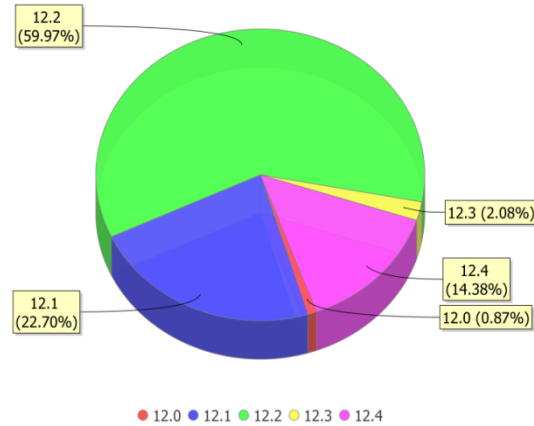
- ✓ Komplexní shrnutí
- ✓ Provozní shrnutí
- ✓ Detailní výsledky analýzy
  - ✓ Seznam všech nalezených zařízení
  - ✓ Stav životního cyklu
  - ✓ Stav servisního pokrytí
  - ✓ Stav zranitelností OS
  - ✓ Porušení konfigurační politiky
- ✓ Doporučení dle priorit

# TLMA uvádí jednotlivé nedostatky, které by měly být napraveny.

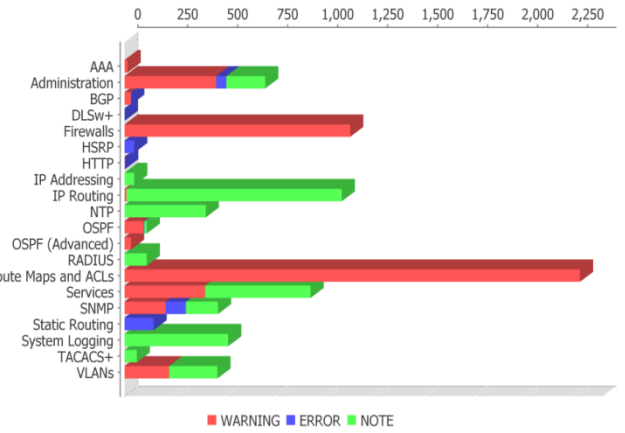
### Number of Vulnerabilities per Affected OS Version



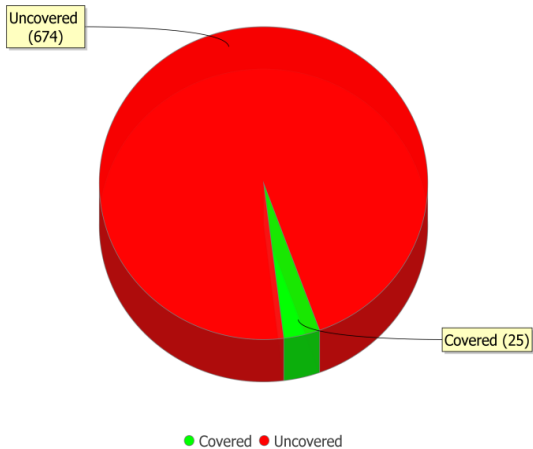
### Percentage of Devices Running Each Affected OS Version



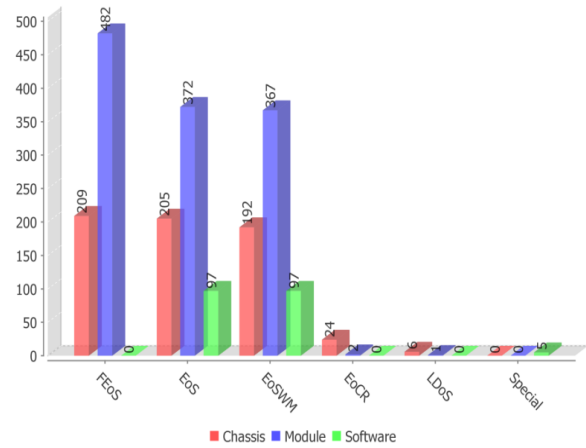
### Configuration Issues per Severity and per Configuration Category



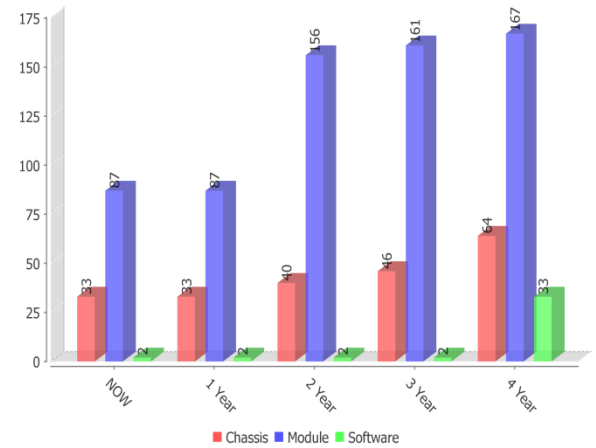
### Equipment Covered by Maintenance



### Equipment at Each Milestone as of this Report Date



### Without Upgrades LDoS Count Rises Each Year



# 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“



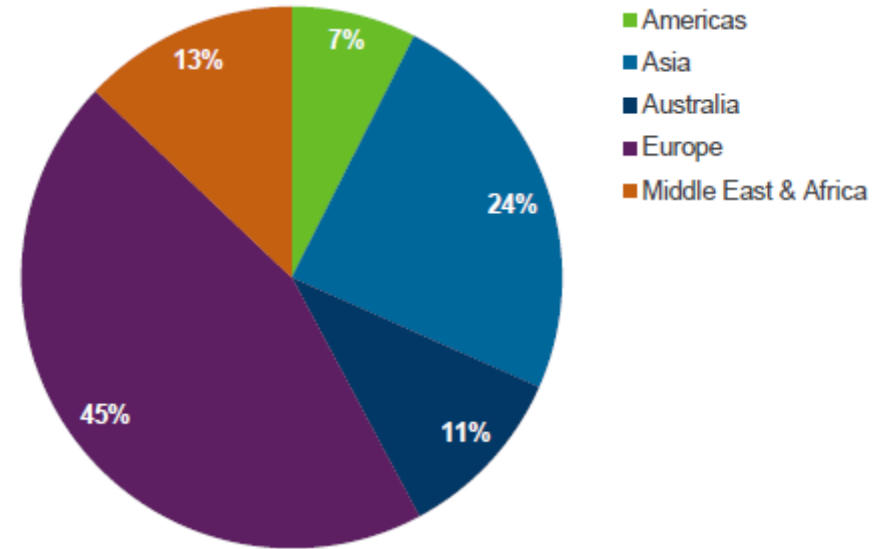
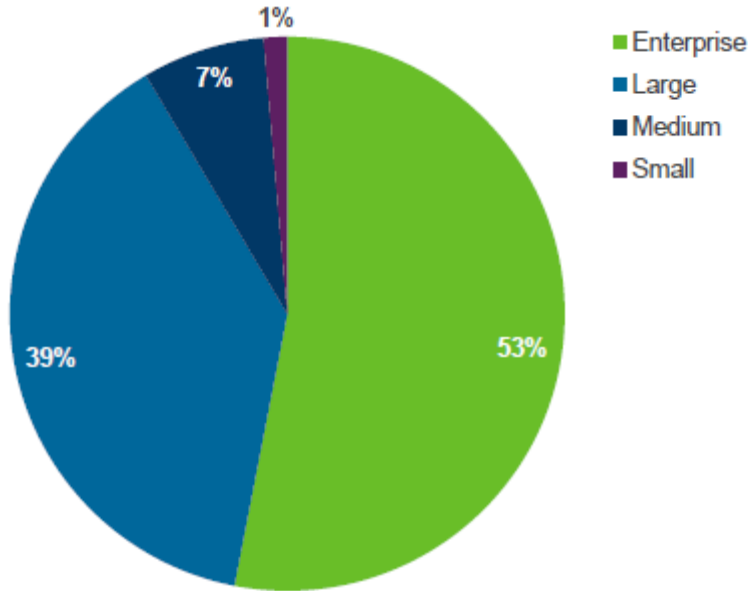
# Dimension Data Network Barometer Report

**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**



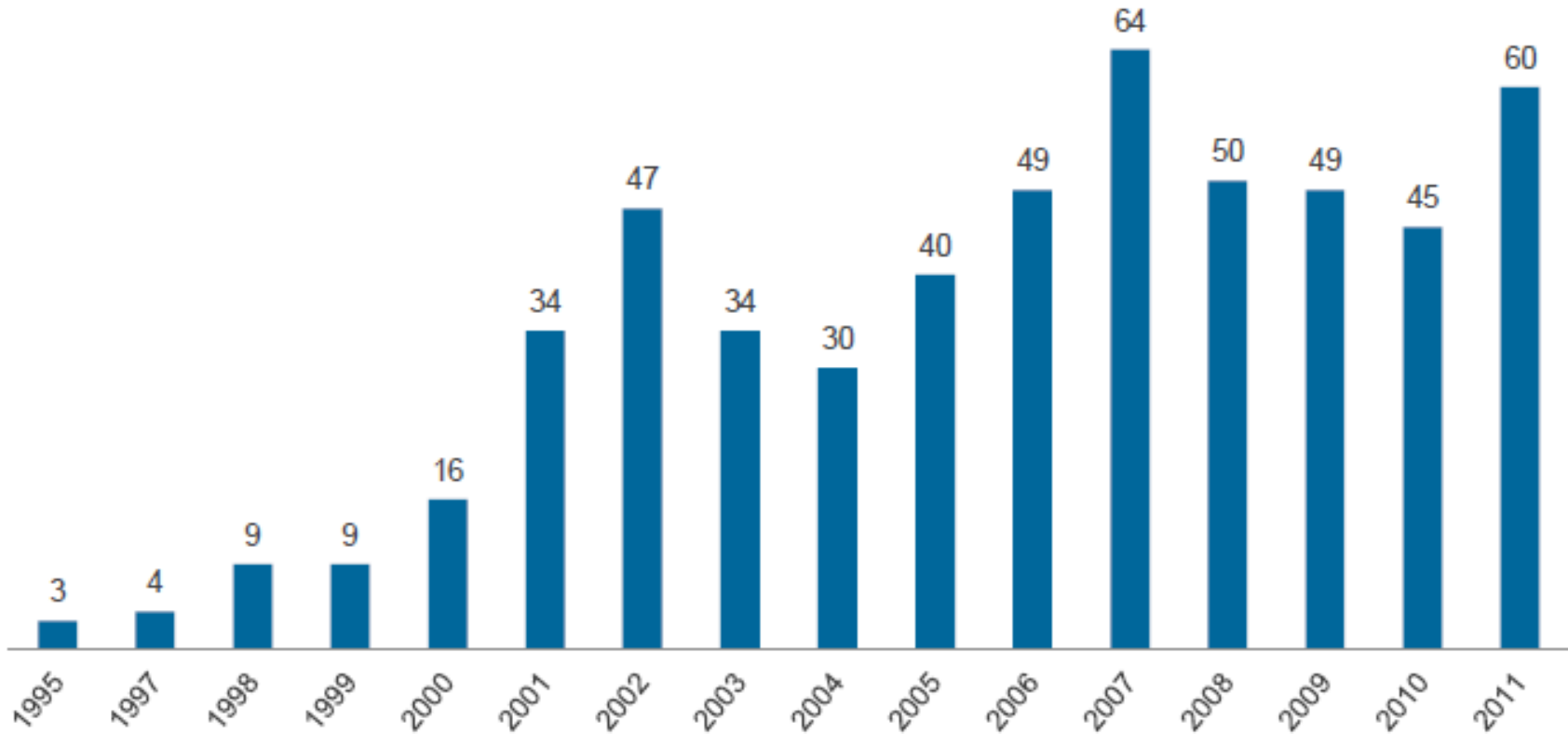
# Kdo poskytl data pro Network Barometer Report 2012



**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

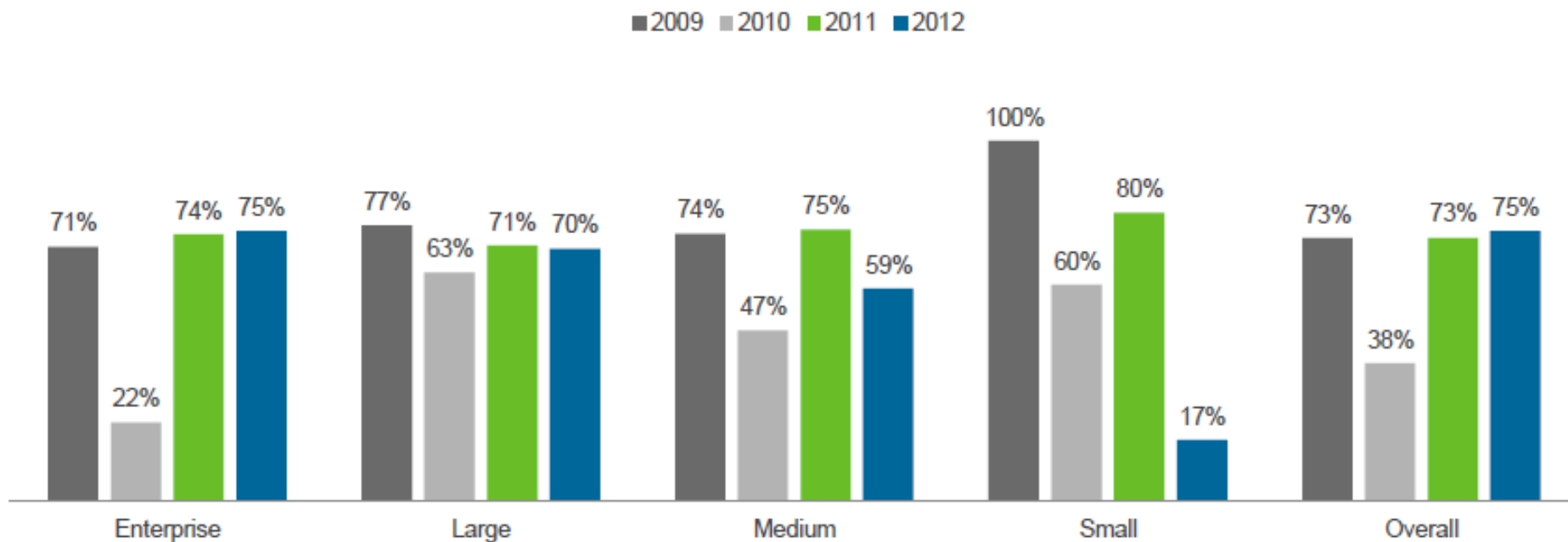
# Každoroční počet nových zranitelností identifikovaných Cisco



## PSIRT - Product Security Incident Response Team

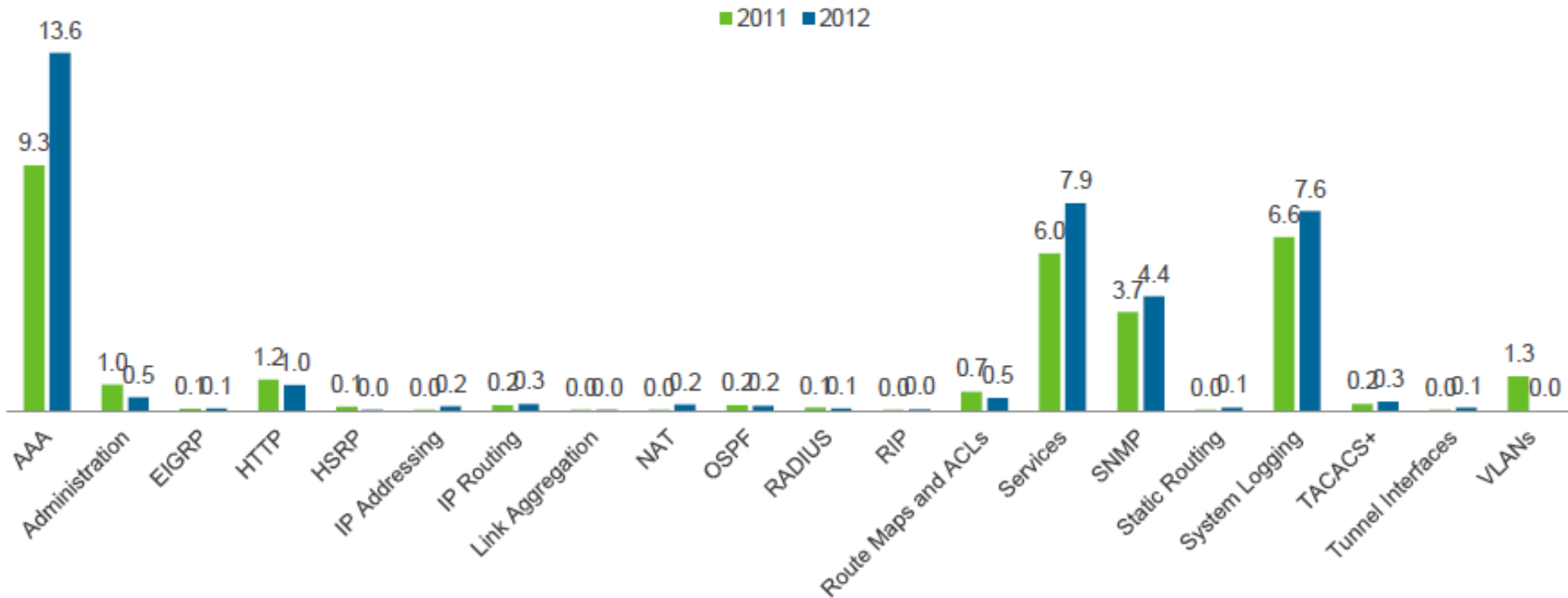
Společnost Cisco Systems disponuje globálním týmem PSIRT, který eviduje, zkoumá a zveřejňuje podklady a informace týkající se možné zneužitelnosti chyb v software Cisco zařízení.

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



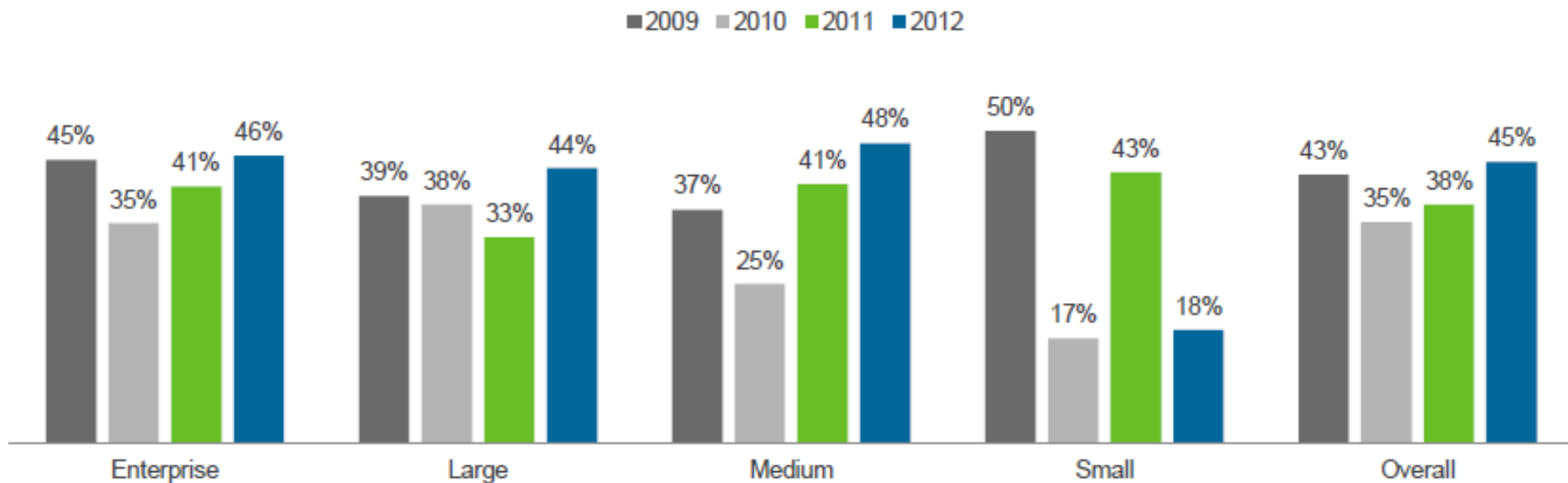
Počet zařízení s bezpečnostní zranitelností PSIRT podle velikosti organizace

# Celkový počet chyb v konfiguraci se od roku 2011 zvýšil



**AAA Authentication – nejběžnější konfigurační chyba**

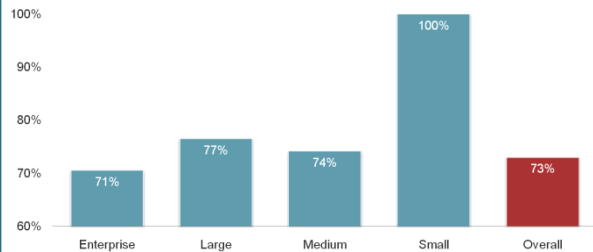
# Průměrný počet End od Sale (EoS) zařízení sítě



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

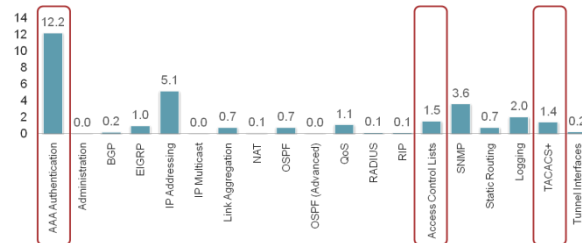
# Report „Network Barometer 2012“ ukazuje, jak jsou sítě organizací vystaveny obchodním a provozním rizikům.

## Průměrný počet zařízení obsahující PSIRT dle velikosti organizace



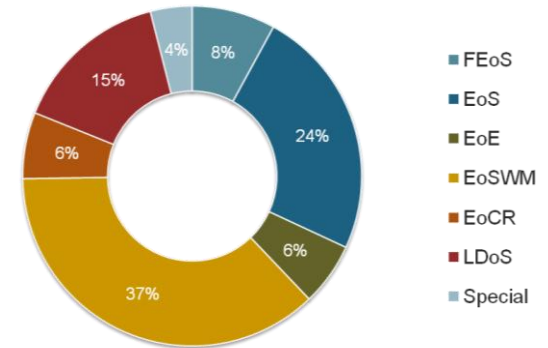
75% zařízení má alespoň jednu bezpečnostní zranitelnost ...

## Průměrný počet porušení politiky v dané kategorii



... každé zařízení má 30 konfigurací s bezpečnostními nedostatky – 15 jich je spojených s bezpečností ...

## Rozdělení zařízení do jednotlivých životních cyklů



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

## Dimension Data's Network Barometer Report

Založen na 294 TLMA reportech z celého světa

[www.dimensiondata.com/networkbarometer](http://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+**



# Dotazy...



# Otázky a odpovědi

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

e-mail: [connect-cz@cisco.com](mailto:connect-cz@cisco.com)

Prosíme, ohodnotte  
tuto přednášku.

Děkujeme za pozornost.

