Bring Your Own Device Challenge
Bring Your Own Device

Trends
Cisco-On-Cisco
Cisco Solution Specifics
Use Cases
Summary
Trends
Market Transitions

5 Billion Mobile Users by 2016

Blurring the Borders

Consumer ↔ Workforce
Employee ↔ Partner
Physical ↔ Virtual

Changing the Way We Work

71% of the World’s Mobile Data Traffic will be Video in 2016

MOBILITY

WORKPLACE EXPERIENCE

VIDEO
BYOD – An Enterprise-Wide Project

- Compliance Operations
- Network Team
- Endpoint Team
- Security Operations
- Application Team
- Human Resources

© 2012 Cisco and/or its affiliates. All rights reserved.
Security Considerations

Visibility & Context are Critical

- Mobility
  - Enabling BYOD Transformation
- Escalating Threats
  - Protecting Network Edges
- Collaboration & Social Media
  - Authorizing Content Usage
- Virtualization & Cloud
  - Securing Cloud Transition
A New Approach is Required

Sources All Data

Handles All Devices

Routes All Requests

Shapes All Streams

Sees All Traffic

Controls All Flows

Touches All Users

An integrated and holistic, network-based approach
SecureX: Enabling Secure BYOD

Secure Unified Access
Enabling BYOD Transformation

Threat Defense
Protecting Network Edges

Collaboration & Social Media
Authorizing Content Usage

Virtualization & Cloud
Securing Cloud Transition

Threat Intelligence
Contextual Policy

Network

CONTEXT

Services
BYOD at Cisco
Cisco-on-Cisco Client Mix

- 73M online meetings/yr.
- 2,104 Cius
- 8,144 iPad
- 12,290 BlackBerry Devices
- 2,185 Other Devices
- 6,700+ Linux Desktops
- 87,000+ Windows PCs
- 12,000+ Apple Macs
- 8,144 iPad
- 20,581 iPhones

Growth rates:
- 3.9% Growth
- 1.6% Growth
- 9.5% Growth
- 3.8% Growth

© 2012 Cisco and/or its affiliates. All rights reserved.
Cisco-On-Cisco Realized Gains

- 59% more devices
- 32% more users
- 20% fewer cases
- 30 minutes per day more productivity
- 25% per year savings using VXI
- 17 weeks faster acquisition integration
BYOD Spectrum
Where are you on your BYOD journey?

Limit

Basic

Enhanced

Advanced

Environment requires tight controls
Corp Only Device
Mfg Environment
Trading Floor
Classified Gov
Networks
Traditional Enterprise

Focus on basic services, easy access, almost anybody
Broader Device Types
But Internet Only
Edu Environments
Public Institutions
Simple Guest

Enable differentiated services, on-boarding with security – onsite/offsite
Multiple Device Types + Access Methods
Healthcare
Early BYOD Adopters
Contractor Enablement

Corp native apps, new services, full control
Multiple Device Types, Corp Issued
Innovative Enterprises
Retail on Demand
Mobile Sales Services
(Video, Collaboration, etc.)
Cisco BYOD Solution Elements

- Applications
- Virtualization
- Contextual Policy
- Management
- Network
- Security

SecureX Building Blocks
BYOD: Unified Access

Connectivity Layer
- VPN
- External Wi-Fi
- Internal Wi-Fi
- Wired

Devices Layer
- Smartphones
- Tablets
- Thin/Virtual Clients
- Desktop/Notebooks

FW  Router  Wireless  Wired  ISE  NCS Prime

Bought In
Encouraged
Allow
Deny or Restrict
Unified Infrastructure: Wired Access
Cisco Switches scale to meet diverse deployment scenarios

Cisco Switching Differentiators
- Uniquely supports the next generation workspace populated by smart phones, tablets and virtual desktops
- Cisco’s Universal PoE 60W capabilities support the widest range of devices
- Prevents eavesdropping and facilitates regulatory compliance with regulations with MACsec encryption
- Device Profiler and IOS Sensor deliver consistent policy and device mobility
- Monitor mode greatly simplifies 802.1X deployments
- Offers comprehensive and fully functional QoS capabilities

Lead Platforms
- Cisco Catalyst® 6500
- Cisco Nexus® 7000
- Cisco Catalyst 6500
- Cisco Catalyst 4500
- Cisco Catalyst 3750 and 3560
Unified Infrastructure: Wireless Access
Cisco Mobility Technology for High Performance Wireless Network

Best-of-Breed Mobility Technology

AP 3600
Access Point Innovation
The Tablet AP, Enhanced throughput and coverage targeting advanced applications for tablets and smart devices

CleanAir
Improved Performance
Proactive and automatic interference mitigation

ClientLink 2.0
Improved Performance
Proactive and automatic beamforming
For 802.11n and legacy clients

VideoStream
Improved Performance
Wired multicast over a Wireless network

Identity Services Engine (ISE) - Unified Policy Management
NCS Prime – Central Network Management
Identity Services Engine (ISE) for Advanced Policy Management

1. 802.1x EAP User Authentication
2. Profiling to identify device
3. Posture of the device
4. Policy Decision
5. Enforce policy in the network
6. Full or partial access granted

IEEE 10 VLAN 20

- Corporate Resources
- Internet Only

- HTTP
- NETFLOW
- SNMP
- DNS
- RADIUS
- DHCP

ISE
Wireless LAN Controller
Unified Access Management
Comprehensive Policy Solution for Any Device

Purpose-Built, Complete, and Reliable Profiling

- Cisco ISE uses SNMP, NetFlow, DNS, RADIUS, HTTP, and DHCP to increase accuracy, reduce spoofability
- Works across wired and wireless
- Completely integrated with RADIUS/AAA
- Includes additional services (posture, guest/portal, etc.)

Scalable Policy Enforcement

- Switch, WLAN controller, and VPN as an enforcement point
- Flexible control (VLAN, dACL/ACL, QoS, SGA, etc.) based on any contextual attributes (user, device, group, location, time, etc.)

Unified Management

- ISE detailed reports and troubleshooting tools (user, device, session, etc.) can be accessed from within NCS 1.0 providing a single pane of glass into user, device, and network across wired and wireless infrastructure
Dynamic Policy With ISE

- Corporate device with AD credential and certificate (EAP-TLS), is corporate access to the network
- Bring Your Own Devices (BYOD) with AD username and password, will be give only limited access (PEAP MSCHAPv2)
- Guest or Sponsored Guest, Open SSID with WebAuth for internet access only.
Cisco NCS Provides a Single View Point into Troubleshooting, Posture and Profiling

- Posture and Authorization Profile Insight
- Comprehensive 802.1x Troubleshooting
- Device Endpoint Type Extracted from ISE
Apple Device Provisioning – ISE 1.1 MR

1. Initial Connection Using PEAP
2. Device Provisioning Wizard
3. Future Connections Using EAP-TLS

Change of Authorization
Android Device Provisioning – ISE 1.1 MR

1. Initial Connection Using PEAP
2. Redirection to Android Marketplace to Install Provisioning Utility
3. Provisioning using Cisco Wi-Fi Setup Assistant
4. Change of Authorization

Future Connections Using EAP-TLS
“My Devices” Portal – ISE 1.1 MR

Devices Can be Self-Registered, Up to an Administrator Defined Limit

Register a New Device

To register a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

Current Registered Devices

<table>
<thead>
<tr>
<th>State</th>
<th>Device ID</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40:FC:89:7D:6F:3C</td>
<td>Motorola Xoom</td>
<td>Edit</td>
</tr>
<tr>
<td></td>
<td>60:FA:CD:8E:0D:79</td>
<td>Apple iPhone</td>
<td>Edit</td>
</tr>
<tr>
<td></td>
<td>F0:B4:79:DF:0F:3B</td>
<td>Macbook Pro</td>
<td>Edit</td>
</tr>
<tr>
<td></td>
<td>FB:1E:DF:E5:0A:25</td>
<td>Apple iPod</td>
<td>Edit</td>
</tr>
</tbody>
</table>

Devices can be Revoked By the User.
Monitoring and Troubleshooting
Quickly Access the Information You Need – When You Need IT

Centralized Monitoring of the entire WLAN and LAN

- Identify and diagnose RF Interference events, air quality and interference security threats with Cisco CleanAir
- Robust fault event and alarm management
- Guided step-by-step client troubleshooting tools
- Ever-present search for cross network historical information
- Cisco ISE and ACS views for additional endpoint data

- Efficiently assess, prioritize and manage RF interference issues
- Analyze problems and misconfigurations for all client devices across all connection media
- Troubleshoot large-scale LAN and WLAN environments with minimal IT staffing
- Quickly discover events occurring outside baseline parameters
Easily Monitor Each Location

- Simplified Customization of Display
- Ever-Present Search
- Mapping Hierarchy and Icons (Expandable)
- Heat Map of Each Location
- Quick Access To Tools
- Ever-Present Alarm Summary (Expandable)
Services Management and Integration

**CleanAir**
- Detect RF Interference
- Locate the source
- Automatically adjust to optimize the environment

**Adaptive WIPS**
- Assess wireless vulnerabilities
- Auto-classify threats
- Protect the wireless network

**Context-Aware**
- Contextual Info about Wi-Fi clients and tagged mobile devices
- Optimize application delivery

**Identity Services Integration**
- Shows where security & policy problems exist
- Drill deeper into issue details
BYOD: Security

Connectivity Layer
- Wired
- Internal Wi-Fi
- External Wi-Fi
- VPN

Devices Layer
- Smartphones
- Tablets
- Thin/VirtualClients
- Desktop/Notebooks

FW
Router
Wireless
Wired

AnyConnect
ScanSafe
ESA/WSA
ISE
NCS Prime

Bought In
Encouraged
Allow
Deny or Restrict
Secure Mobility with Always-On Security
Security: Remote Access & Threat Defense
AnyConnect, ASA, WSA, ScanSafe

Information Sharing Between ASA and WSA

Users Outside Network

ASA

Cisco Cloud and Web Security

ScanSafe

Corporate AD

Cisco Web Security Appliance

Social Networking

Enterprise SaaS

Email

News
Device Management
MDM is a key element but there is more

MDM Partners
- Device inventory
- Device provisioning/de-provisioning
- Device data security
- Device application security
- Cost management
- Full or selective device remote wipe

Cisco
- User/device authentication
- Posture assessment
- Policy enforcement
- Context aware access control
- Threat defense
- Web usage policy
- Web application DLP
- Secure remote access

MDM Partners
- ISE
- ScanSafe
- WSA
- AnyConnect
- ASA

© 2012 Cisco and/or its affiliates. All rights reserved.
BYOD: Next Generation Workspace

Connectivity Layer
- VPN
- External Wi-Fi
- Internal Wi-Fi
- Wired

Devices Layer
- Smartphones
- Tablets
- Thin/Virtual Clients
- Desktop/Notebooks

- FW
- Router
- Wireless
- Wired

- AnyConnect
- ScanSafe
- ESA/WSA
- VXI

- ISE
- ISE
- ISE
- NCS Prime
- NCS Prime
- NCS Prime

Bought In
Encouraged
Allow
Deny or Restrict
Native vs. Virtual Approach to BYOD

Native, Browser and Virtual Modes

Native
- Local data on device
- Maximum performance
- Native device experience

Browser
- Local data on device
- Portable to many devices
- Browser experience

Virtual
- No local data on device
- Maximum security
- Translated experience
Some Components of Cisco BYOD Solution
Backed by Cisco SecureX
Use Cases
## BYOD Use Cases & Solutions

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Limit</th>
<th>Basic</th>
<th>Enhanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Policy</td>
<td>Block Access</td>
<td>Role Based Access; (Guest Access)</td>
<td>Secure granular On-site and Off-Site Mobility</td>
<td>Full Workspace Experience</td>
</tr>
<tr>
<td>IT Requirements</td>
<td>• Visibility to who/what is on network</td>
<td>• Restrict personal devices to public internet.</td>
<td>• Allow granular on-site and off-site access to network/applications</td>
<td>• Enable a full mobile and collaboration experience</td>
</tr>
<tr>
<td>User Scenario (Example)</td>
<td>Hospital extends wired access to medical staff only</td>
<td>Hospital provides guest access to patients</td>
<td>Doctor uses personal device in hospital and in an offsite coffee-shop</td>
<td>Hospital administrator is granted full network access and uses native applications (i.e. HR applicant tracking system)</td>
</tr>
</tbody>
</table>

### Solution Technology

<table>
<thead>
<tr>
<th>Technology</th>
<th>Network</th>
<th>Management</th>
<th>Contextual Policy</th>
<th>Security</th>
<th>Virtualization</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco Switches</td>
<td>Cisco Prime NCS</td>
<td>Cisco Identity Services Engine (ISE)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Wireless LAN Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2012 Cisco and/or its affiliates. All rights reserved.
BYOD Use Case: Basic Implementation

Business policy is enable wired and wireless access for corporate and personal devices

**Unified Policy-based Management**
- Identity-aware networking, and data integrity
- Universally and effectively control user and device access

**Uncompromised Security**
- Secure, scalable guest access solutions
- Authenticate users and endpoints via wired, wireless with consistent policy across the enterprise network

**Simplified On-Boarding**
- Zero touch device registration and provisioning of employee/guest devices

Devices Layer
- Smartphones
- Tablets
- Game, Printer
- Thin/VirtualClients
- Desktop/Notebooks

Components
- Wireless
- Wired
- ISE
- NCS Prime
BYOD Use Case: Advanced Implementation

Business policy is to provide granular access to a full corporate workspace, both on and off site.

Enable a Full Mobile and Collaboration Experience
Integrated policy management with mobile device management, deliver granular endpoint controls, provide layered security, and enforce network security policies for BYOD deployments.
Summary
Embrace Mobility While Ensuring Security
Some Questions to Answer

- Do I have the WLAN capacity and reliability to support increase in mobile devices and future applications?
- How do I enforce security policies on non-compliant devices?
- How do I grant different levels of access to protect my network?
- How do I ensure data loss prevention on devices where I don’t have visibility?
- How do I minimize emerging threats targeted at mobile devices?
- How do I monitor and troubleshoot user and client connectivity issues on my access (wired/wireless) network?
- Is my network capable of delivering the scalability and performance required to realize the benefits of a BYOD strategy?
Network Scalability
Is the Network Ready for Next Generation Applications?

Mobile BYOD clients drive advanced applications for Voice, Video, and VXI

- 802.11n at the edge for performance requires 1G connectivity in the core

Next Generation Applications require more bandwidth and performance

- QoS throughout the network to support Voice and Video
- VDI Applications are sensitive to network delays
- “Good Enough” networks won’t be able to handle time sensitive, high performance, high density applications.
- WAN acceleration to assist performance sensitive “cloud” applications

Before: 1 Employee = 1 PC
Today: 1 Employee = 3 or more Devices
Tomorrow: Multimedia Applications = High Bandwidth Use
Enabling Transformations with SecureX

Secure Unified Access
- AnyConnect
- Web Security Appliance
- Cloud Web Security
- WLAN Controller

Threat Defense
- Adaptive Security
- Email | Web Security
- Intrusion Prevention
- Router Security

Application Visibility & Control
- Adaptive Security (CX)
- Web Security
- Router Security

Virtualization & Cloud
- Adaptive Security
- Virtual Security Gateway
- Nexus 1000v
- VPN

Threat Intelligence:

Contextual Policy:
- Identity Services Engine
- Security | SMX
- Network | NCS Prime

Network:
- Router
- Switch
- Appliance
- Cloud
- Virtual

Services:
- Cisco Advanced Services
- Partner Shared Services

Secure BYOD Solution
Thank you.