The Context Aware Network
A Holistic Approach to BYOD
Bring Your Own Device

Trends
BYOD at Cisco
Cisco® BYOD Solution
Use Cases
Summary
Demand for Mobility

- 15 billion new networked mobile devices by 2015
- 56% of information workers spend time working OUTSIDE THE OFFICE
- 3/4 of employees uses MULTIPLE DEVICES for work
- 100% of IT staff STRUGGLE to keep up with mobile needs
BYOD: An Enterprise Wide Project
A New Approach Is Required

An Integrated and Holistic, Network-Based Approach
Cisco Unique BYOD Value Proposition
One Network, One Policy, One Management

Device ownership is irrelevant: corporate, personal, guest, etc…

BYO devices need wired, wireless, remote and mobile access

BYO devices can be any device: Windows PCs, Mac OS devices, any tablet, any smartphone, gaming consoles, printers…etc
BYOD at Cisco
Cisco-On-Cisco Client Mix

- 20,581 iPhones (3.9% Growth)
- 87,000+ Windows PCs
- 6,700+ Linux Desktops
- 12,000+ Apple Macs
- 2,104 Cius
- 5,234 Android Devices (9.5% Growth)
- 2,185 Other Devices (-3.8% Growth)
- 2,104 Cius
- 8,144 iPad
- 9,500+ BlackBerry Devices (-1.6% Growth)
- 8,144 iPad
- 2,104 Cius
- 8,144 iPad
- 2,104 Cius
Cisco-On-Cisco Realized Gain

59% more devices

32% more users

20% fewer cases
Cisco BYOD Solution
BYOD Spectrum
Where are you on this BYOD spectrum?

Limit
Environment requires tight controls
- Company’s only device
- Manufacturing environments
- Trading floors
- Classified government networks
- Traditional enterprises

Basic
Focus on basic services and easy access for almost anybody
- Broader device types but Internet only
- Education environments
- Public institutions
- Simple guests

Enhanced
Enable differentiated services and on-boarding with security both onsite and offsite
- Multiple device types plus access methods
- Healthcare
- Early BYOD adopters
- Contractor enablement

Advanced
Company’s native applications, new services, and full control
- Multiple device types, company issued
- Innovative enterprises
- Retail on demand
- Mobile sales services (video, collaboration, etc.)
400 IT professionals interviewed about BYOD, more than 65 percent said they don't have the necessary tools in place to manage personal devices on the corporate network, and 27 percent said they aren’t certain of all the personal devices that are accessing the network.
Cisco BYOD Smart Solution Elements

- Collaboration Application
- Policy Management
- Central Management
- Core Infrastructure
- Secure Mobility
Cisco Switching Differentiators for BYOD
Cisco Switches Scale to Meet Diverse Deployment Scenarios

Next Generation Workspace

- Any Device
- HD Video
- VDI

Catalyst 3K-X
- Security
- Video

Catalyst 4K
- PoE Leadership
- High Availability

Cisco Switching Differentiators
- Unique Support of Next Generation Workspace populated by smartphones, tablets and virtual desktops
- Support Widest Range of Devices
- Prevent eavesdropping and facilitate compliance with MACSec Encryption
- Device profilers and device Sensors, Deliver Consistent Policy
- Monitor mode greatly simplifies 802.1x deployments

Smart Operations
- Lower TCO

Enabling the BYOD Experience
Cisco Wireless Technology for BYOD

Best-of-Breed Mobility Technology

**AP3600**
Access Point Innovation
The Tablet AP, Enhanced throughput and coverage targeting advanced applications for tablets and smart devices

**Clean Air**
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
Prime NCS – Central Network Management
Universal Management for BYOD Deployments
Cisco Prime NCS for Unified Network Management

Converged Access Management for Wired and Wireless Networks
- Wireless  |  Wired  |  Security Policy  |  Network Services

Converged Security and Policy Monitoring
Contextual status and monitoring across wired & wireless networks

Centrally Organizes Day 1-to-n Management tasks
Instructional configuration workflows

Reduces the Time to Troubleshoot
Integration with Cisco NCS Prime

Improved Network Visibility - Faster Troubleshooting - Eliminate Configuration Errors
TrustSec Architecture

Identity and Context Centric Security

Security Policy Attributes

Centralized Policy Engine
Dynamic Policy & Enforcement

Business-Relevant Policies

Identity

WHO

WHAT

WHERE

WHEN

HOW

User and Devices

User and Devices

Security Policy Enforcement

Monitoring and Reporting

Application Controls

Identity Services Engine (ISE) for Advanced Policy Management

**IDENTITY**
- 802.1x EAP User Authentication
- Company asset
- Personal asset
- Posture of the device
- Unified Access Management

**PROFILING**
- HTTP
- NETFLOW
- SNMP
- DNS
- RADIUS
- DHCP

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

**HQ**
- 2:38pm
Putting the End User in Control

- **Reduced Burden on IT staff**
  - Device On-Boarding
  - Self Registration
  - Supplicant Provisioning

- **Reduced Burden on Help Desk Staff**
  - Seamless, Intuitive User Experience

- **Self Service Model**
  - My Device Registration Portal
  - Guest Sponsorship Portal
Device Authentication
Leveraging Your Infrastructure Network

Cisco Catalyst® Switch

Identity Differentiators
- Monitor Mode
- Flexible Authentication Sequence
- IP Telephony Support
- Support for Virtual Desktop Environments

Authentication Features
- IEEE 802.1x
- MAC Auth Bypass
- Web Authentication

Consistent identity features supported on all Catalyst switch models
Device Profiling
Automated Device Classification Using Cisco Infrastructure

DEPLOYMENT SCENARIO WITH CISCO IOS SENSOR

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

The Solution
Efficient Device Classification Leveraging Infrastructure
Device Posture Assessment
ISE Posture Ensures Endpoint Health before Network Access

Sample Employee Policy:
- Microsoft patches updated
- McAfee AV installed, running, and current
- Corp asset checks
- Enterprise application running

Challenge:
- Understanding health of device
- Varying level of control over devices
- Cost of Remediation

Value:
- Temporal (web-based) or Persistent Agent
- Automatic Remediation
- Differentiated policy enforcement-based on role
Guest Management
ISE Guest Service for Managing Guests

**Guest Policy**
- Wireless or Wired Access
- Internet-Only Access

**Guest Management**

**Web Authentication**

**Provision:**
- Guest Accounts via Sponsor Portal

**Manage:**
- Sponsor Privileges, Guest Accounts and Policies, Guest Portal

**Notify:**
- Guests of Account Details by Print, Email, or SMS

**Report:**
- On All Aspects of Guest Accounts

**Internet**
Extended Security on and off-premise
AnyConnect, ASA, IPS, WSA & ScanSafe
Remote Access: Cisco AnyConnect
Optimized User Mobility

• User friendly design
• Industry-leading connectivity features
• Integrated connection manager for enhanced security
• Key Features:
  • Always On or On-Demand VPN
  • Auto Re-Connect (Persistence)
  • IPSec, SSL & DTLS VPN
  • Clientless WebVPN
  • Optimal Gateway Selection
  • Endpoint Posture Assessment
Device Management
MDM & Cisco Solutions

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
- IPS

Cisco
- AnyConnect
- ASA
Simple BYOD Deployment Diagram
Tying all the pieces together
Advanced Collaboration with Cisco Jabber

Win, Mac

iPad, Cius

Smartphone

Web
### WebEx: Industry-Leading Meeting Solutions

#### Industry-leading Web Conferencing
- Audio, web, and high-quality video
- Meeting, Training, Event, and Support versions

#### Document, Application, Desktop Sharing

#### Integrated with TelePresence and Jabber for Enhanced Collaboration

#### Delivered Securely Over Cisco Collaboration Cloud

#### Consistent, Cross-Platform Experience
- Windows, Mac, Linux, Unix, Solaris
- Supported on leading mobile devices
- Available in 13 languages
Use Cases
Unified Policy-Based Management
- Provide identity-aware networking and data integrity
- Universally and effectively control user and device access

Uncompromised Security
- Provide secure, scalable guest access solutions
- Authenticate users and endpoints through wired wireless access with consistent policy across the enterprise network

Simplified On-Boarding
- Provide zero-touch device registration and provisioning of employee and guest devices

Business Policy: Enable Wired and Wireless Access for Company and Personal Devices

Devices Layer
- Smartphones
- Tablets
- Games and Printers
- Thin and Virtual Clients
- Desktop/Notebooks

Wireless Technologies
- Cisco® ISE
- Cisco Prime™ NCS
BYOD Use Case: Advanced Implementation

Business Policy: Provide Granular Access to Full Company Workspace, Both On and Off Site

Enable a Full Mobile and Collaboration Experience
Provide integrated policy management with mobile device management, deliver granular endpoint controls, provide layered security, and enforce network security policies for BYOD deployments

Cisco WebEx
Cisco Jabber™
Cisco Quad™
Cisco ISE
Cisco Prime™ NCS
Enterprise Applications

Cisco AnyConnect™
Cisco ScanSafe
Cisco WSA
Cisco ASA

Cisco ASA

Router
Wireless
Wired

Devices Layer
Smartphones
Tablets
Games and Printers
Thin and Virtual Clients
Desktop and Notebook Computers
Summary
Embrace Mobility While Ensuring Security

- Do I have the WLAN capacity and reliability to support an increased number of mobile devices and future applications?
- How do I enforce security policies on noncompliant devices?
- How do I grant different levels of access to protect my network?
- How do I help ensure data loss prevention on devices for which I do not have visibility?
- How do I mitigate emerging threats targeted at mobile devices?
- How do I monitor and troubleshoot user and client connectivity problems on my access (wired and wireless) network?
- Is my network capable of delivering the scalability and performance required to achieve the benefits of a BYOD strategy?
Looking Ahead

Is the Network Ready for Next Generation Applications?

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

Next Generation Applications require more bandwidth and performance

Before: 1 Employee = 1 PC

Today: 1 Employee = 3 or more Devices

Tomorrow: Multimedia Applications = High Bandwidth Use
Q&A
We value your feedback.
Please be sure to complete the Evaluation Form for this session.

Access today’s presentations at cisco.com/ca/plus

Follow @CiscoCanada and join the #CiscoPlusCA conversation