Cyber Security in a Connected World
The Evolution of the Network and Security Considerations

Nathan Look
Chief Technology Officer
Los Angeles World Airports

September 8-9, 2012
Calgary, AB
Network Evolution (logical)

The Network is evolving by CONVERGING logically

- One Network

  The Borderless Network Becomes a Reality:
  - A bit is a bit-- does not matter where it came from (wired or wireless)
  - Security – can apply security to any bit (wired or wireless)
  - Quality of Service (wired or wireless)

- Unified Communications
  - Data
  - Phone
  - Public Safety Radio
Network Evolution (logical) Convergence Over Time

Enterprise Communications Infrastructure circa 2000

Data Services
- Data

Voice Services
- Voice

Video Services
- Video

Converged Network Services

Unified Network Services

Unified Wired and Wireless Network

Mobile E-Mail
- Video Surveillance
- Guest and Identity
- Voice and UC
- RFID and Location
- Outdoor

Enterprise Communications Infrastructure 2008+

Wireless Services

Wireless

Courtesy - Cisco
Network Evolution (Physical)
The silos begin to CONVERGE... and are becoming irrelevant

Network Convergence (Physical)

The TYPE of physical media becomes irrelevant.
The CHOICE of physical media becomes driven by usage.
Network Convergence (Physical)
The type of physical media is becoming irrelevant:
It’s ALL Ethernet and IP

HEARD ON THE STREET – Wall Street Journal
Updated August 17, 2012, 10:44 a.m. ET
Apple May Put Cable in a Box

Apple wants to make its streaming set-top box double as a cable box and is in talks with operators, according to a Wall Street Journal report.
Design Parameters for an Evolving Network

Wireless Only

- Mobility required for devices, and all devices wireless-capable
- Wired factors not applicable
- Cost considerations limit wired ports

Wired & Wireless

- Mobility and wired factors both important
- Different applications require different media

Examples
- Laptops, Tablets, Smart Phones, Other Mobile Devices

Wired Only

- Deterministic Behavior
  - High Availability
  - Scalability
  - Security
  - Power
  - Bandwidth / Video
  - Legacy Devices
- Mobility not required for devices / users
- Cost considerations limit wireless APs

Examples
Network Evolution

IF
the network is evolving by CONVERGING logically and physically
THEN
what are the implications for:
• Mobility
• Security

Do we need a new VISION?
**Vision:** Employees and other authorized personnel can access the applications and data to do their work from anywhere, anytime, SECURELY.

**Mission:** To enable secure fixed and mobile usage of applications and data via authorized platforms in a secure manner and to reduce costs by supporting a Bring Your Own Device strategy (BYOD).
Mobility Implications

- Fixed / Mobile Market Transition
- Evolving Enterprise Workspace
- Wireless Access
- Wireless Trends
- IT Challenges to Mobile Freedom
- BYOD
IT Infrastructure
Mobile Market Transition

Mobility

7 Billion New Wireless Devices by 2015

- Mobile data traffic will increase 39 times between 2009 and 2014. (Cisco VNI)
- IPv6 lends itself to network applications that require massive scale. (Gartner)

Workplace Experience

Blurring the Borders:
Workforce ↔ Customer
Employee ↔ Partner
Physical ↔ Virtual

- New technologies and user behaviors drive significant changes to networks. (Burton Group)
- Business user devices use almost twice the energy as data centers. (The Climate Group)

Video

Changing Way We Work
Video projected to quadruple IP traffic by 2014 to 767 exabytes*

- Simply throwing bandwidth at this problem is insufficient as application demands rise. (IDC)
- Video will replace voice and text as the preferred method of business communication. (Forrester)
IT Infrastructure
Evolving Enterprise Workspace – Requirements for Networks

BYOD
- Secure access
- Customized experience
- Guest access

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

Video
- Multicast Streaming
- Video conferencing
- Reliable Performance

IT Requirements
- Performance / Scale
- Security
- Seamless Experience
- Availability
- Lower TCO
Wireless Access – Evolution of Requirements

Evolution of wireless performance

- **802.11b** – 11Mbps
- **802.11a/g** – 54Mbps
- **802.11n** – 450Mbps
- **802.11ac** – 1Gbps+ ...
Wireless Trends

- 41% of employee-owned devices used to access business applications —Forrester
- 40% of college students/young employees prefer a lower-paying job that has more flexibility —CCWTR
- 56% of US information workers spend time working outside the office —Forrester
- 100% of IT staff is struggling to keep up with mobility trends —Gartner
IT Challenges to Mobile Freedom

- Securing Any Access
- Managing Complexity And Scale
- Delivering High-Quality Experience
# BYOD Spectrum

<table>
<thead>
<tr>
<th>Limited</th>
<th>Basic</th>
<th>Enhanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment requires tight controls</td>
<td>Focus on basic services, easy access, almost anybody</td>
<td>Enable differentiated services, on-boarding with security – onsite/offsite</td>
<td>Corp native apps, new services, full control</td>
</tr>
</tbody>
</table>
Beyond BYOD
Uncompromised Experience for Any Workspace

Device Onboarding and Guest Access
Unified Policy
Uncompromised Experience
Simplified Operations

BYOD  Beyond BYOD
Security Implications

If there is no network border… you must:

• Create a secure network using public assets

• Be able to apply enterprise class security on mobile (BYOD) assets and monitor the security posture of these assets.

• Choose a secure platform
Security Implications

• Create a secure network using public assets

How?

• VPNs
• Hard/Soft Tokens
• Frame Tagging (a la MPLS)
Security Implications

• Be able to apply enterprise class security on mobile (BYOD) assets and monitor the security posture of these assets.

  How?
  
  Mobile Device Management (MDM)
  • Create sand-boxes/firewalls between Corporate and Personal Apps/Data
  • Enforce OS and patching via policies

  Mobile Application Management
  • Control what applications are loaded, where they can go and what they can do.

  Identity Management
  • Know who is accessing what data using what device
  • Use this to dynamically control data/app access via network
Security Implications

• Choose a secure platform

Look at the possibilities:

Courtesy: gizmodo.com
Security Implications

• Can your secure platform do what you need?

Copyright:
http://www.pcworld.com/article/208491/mobile_os_smackdown_windows_phone_7_vs_ios_vs_android.html
Security Implications

• Choose a secure platform...that can do what you need

and the WINNER is...drum roll please...

Courtesy: gizmodo.com
Security Implications

• Choose a secure platform... that can do what you need

The WINNER is....

Courtesy: ZDNet
Dialogue – Let’s Talk!

THANK YOU!