Visibility and Control Solutions
Dealing with the challenge of BYO

Network Management Drivers

- **LAN/WLAN Visibility**
  - Who, What, Where, When, How

- **Network Access Paradigm Change**
  - Manageable Closed Network
  - De-perimeterization/BYO

- **Secured Guest Access**
  - Students, Contractors, Visitors

- **Registration**
  - Students, devices

- **Compliance**
  - Enforcement of policies
  - Reporting
The Game has Changed

Traditional Networking <2000


Cost
Capacity
Connectivity

Access Layer Concerns

Limited Visibility at the Access Layer
- The devices connected to the network
  - Users
  - Headless IP devices
- Location of each device – switch, port, AP, SSID
  - Trusted area
  - Restricted area
- The access controls applied to each device/user
  - IP Phone role
  - Enterprise user – IT, Faculty, HR, etc
  - Guest
  - Restricted Contractor
  - Quarantine
  - Security state
Application Layer Concerns

Limited Visibility at the Application Layer
- The devices connected to the network
  - What is using the bandwidth?
  - Which device is running prohibited applications?
- Mapping of Device IP address to User
  - Source IP address is of limited value
  - Switch Port to MAC to IP to Username mapping

De-perimeterization and BYO in Education

- Security and compliance mandates require “Least Privilege”
  - Fundamental dichotomy given nature of Universities
  - Give access to a wider range of users
  - Give them more access to more services
  - Allow wider range of devices access - BYO
  - Threats are more likely inside the firewall

- Collaboration orientated architecture in Higher Education
  - Secured, controlled granting of access to quasi-affiliated entities demands;
    - Authentication
    - Risk Assessment
    - Systemic enforcement to be network vendor agnostic
  - EDUROAM
    - Just Internet
    - How about greater collaboration?
Effects of BYO devices

- 3 people are using P2P software
  - BitTorrent & eDonkey2000 used
  - 350 different peers connected to

- People using Social Networking
  - 6 people using LinkedIn
  - 7 browsing Facebook
  - 9 people tweeting

- Bandwidth used by Skype
  - 122 sources have consumed 445Mbps of data

- Where is this network?

BYO – Strengthen the edge

Access Edge
Routing Core
DMZ
Critical servers
Critical servers

Wireless Edge
Comprehensive Visibility

- Ensure health and compliance both prior to and after allowing access
  - Agent and agent-less assessment
  - Integration with other security technologies

- Provide appropriate access (to assets and QoS) based on organizational role, authenticated identity and security posture
  - MAC, IP, Hostname, Kerberos, Web, 802.1x -based authentication
  - Policy, VLAN or ACL enforcement

- Support guest access, sponsored access and end-system / user tracking
  - IP to ID mapping: track username, IP, MAC, location, etc.

- Automatically contain detected threats
  - Quarantine role
  - Assisted remediation
  - Automatic remediation

Device Profiling

- Automated profiling and device type detection
  - Can detects new devices on the infrastructure automatically and profiles them to determine the type of device
  - Automated policy assignment is possible
  - Various sources such as
    - network and agent based assessment
    - DHCP OS fingerprinting
    - captive portal (used for remediation and registration, guest services)
    - and external profilers (via Netflow, IDS Signatures) can be used.
    - The Device type can be an Operating System Family, Operating System or Hardware Type, for example, Windows, Windows 7, Debian 3.0, HP Printer, iPhone, iPad etc.
Assessment – In-depth Visibility and Control

- **Agent-less Assessment**
  - Network based scanning
  - CSV scoring
  - Out-of-box scanning configurations as well as customized configurations
  - Supports multiple OSs
  - Examples:
    - Anti-virus
    - Patches/OS versions
    - Applications

- **Agent-based Assessment**
  - Permanent or dissolvable
  - Examples:
    - Anti-virus (installed, active, up to date, etc.)
    - Firewalls (installed, active, etc.)
    - Services Running
    - Patches/OS versions (automatic patching enabled, up to date, hot fixes enabled, etc.)
    - Applications (installed, active)
    - Registry Keys

Staged Deployment – Big Changes, Zero Risk

- The biggest roadblock to changing network access posture is fear that it will impede connectivity

- **Staged Deployment**
  - Allows full control over infrastructure changes during deployment
  - Minimizes impact to business processes
  - Deploy each function without enforcement
  - Verify results before enabling enforcement
Interoperability

Implementation for any network without network upgrades

Standards-based - integrates with network equipment supporting RFC3580, VLANs and authentication

Network-based appliance allows integration with any network edge regardless of standards support

Enterasys Advantage – Education

Driving Efficiency and Improving the Learning Experience

- Enable open anytime, anywhere access enhancing academic collaboration
- Provide easy network access for a multitude of networked devices

- Leverage technology in the classroom to achieve learning objectives and minimize distraction
- Enable consistent anytime, anywhere access to resources

- Support open access with detailed visibility, user accountability & control
- Automate & simplify student device registration, centralize compliance reporting & enable virtualization initiatives

- Deliver industry-best TCO while supporting cutting edge learning tools
- Lower operational costs while delivering campus wide mobility, resiliency and security
“There is nothing more important than our customers”