Bring Your Own Device (BYOD) - Supporting Personal Devices on the LEA Network

Many LEAs are moving forward with supporting staff- and student-owned personal devices on their network as a way to make end-user devices more widely available to students and ultimately sustain 1:1 computing initiatives, but they have also expressed concerns regarding their readiness to implement bring your own device (BYOD) initiatives. LEA concerns usually fall into one of three categories; a) information technology infrastructure - wireless connectivity and security, b) policy, and c) operations and support. Appropriate wireless infrastructure is important to meet the security and capacity requirements of BYOD initiatives. Sound security practices and infrastructure can reduce the risk of external and internal threats to end-systems by blocking unauthorized connections, detecting suspicious traffic patterns, and filtering malware. BYOD policies typically address acceptable use, lost, stolen, or damaged devices, device selection, LEA access to a personal device, and other legal issues. Finally, supporting personal devices with existing staffing levels and support polices is typically not tenable. Alternative support strategies may be considered.

To deploy a BYOD program, a security model that provides differentiated levels of access by device, user, application, and location is required. The security model should reflect an understanding of where confidential or sensitive LEA data exists, and control and manage access to this data. LEA instructional strategies around teaching and learning systems and application delivery will significantly impact the BYOD security model. For example, the use of software-as-a-service (SaaS) applications like Google Apps for Education and Microsoft Live@edu, or online learning management systems like Haiku or Edmodo may simplify the BYOD security controls required, thus potentially avoiding expensive infrastructure upgrades.

Although much has been written recently about BYOD considerations and strategies, it usually doesn't adequately reflect the challenges facing LEA technology organizations, most notably:

- resource constraints – lack of sufficient funding and IT staff; IT staff often lacks technical depth due to the breadth of their responsibilities
- disparate and end of life (EoL) infrastructure deployed across the LEA enterprise

In addition, vendor BYOD product recommendations typically assume best practices are followed in network infrastructure design which is often not the case in K-12 networks. BYOD strategies should reflect an understanding of LEA legacy networking capability and leverage existing LEA network infrastructure where possible to provide immediate benefit without significant investment and complexity. These initial strategies should serve as a foundation to support more advanced capabilities as funding and staffing allows.

This white paper does not advocate for or against implementing a BYOD initiative. LEA environments are uniquely different and successful strategies in one LEA may not work in another. In addition, LEA cultures will shape policy and potentially operations and support

strategies. There are however many common information technology considerations and solutions. This white paper will focus on IT considerations and recommended practices, and include a cursory discussion of policy and operations and support.

Information Technology Infrastructure

There are numerous network components that comprise a comprehensive network design to support BYOD. As noted earlier, an objective of this white paper is to leverage existing LEA network infrastructure where possible to provide immediate benefit without significant investment and complexity. This can be accomplished by following the recommended design practices for the fundamental components of the LEA network which are identified below. In addition, advanced capabilities are available in network software and hardware that is not typically deployed today in LEA networks. These advanced capabilities can be added as warranted and when funding and staffing allows.

Fundamental

- LAN Layer 2/3 Managed Switches
- Wireless LAN Access Points and Controllers
- Firewall/Security Appliance
- Web Filter
- RADIUS Server
- Directory Services
- Certificate Authority
- Intrusion Prevention System (IPS)
- Monitoring tools, e.g. syslog server

Advanced

- Network Access Control (NAC)
- Mobile Device Management (MDM)
- Desktop Virtualization

These network components will be referenced throughout the Information Technology Infrastructure section.

Wireless Network Capacity

Most LEA wireless networks were designed with wireless coverage as the primary goal and were not designed to support the high user densities typically associated with 1:1 computing and BYOD initiatives. Before proceeding with a BYOD initiative, LEAs should verify that their WLAN capacity is sufficient to meet the expected demand.

A single access point typically should support no more than 15-20 devices. In some cases, this may be less. Understanding the applications that will be delivered over the wireless network and the throughput requirements for those applications will determine the nominal throughput requirements on a per-user basis. For example, the per-user throughput requirement for web browsing is typically 500 Kbps to 1 Mbps and for instructional streaming video or online testing it is typically 2 Mbps to 4 Mbps. Once the per-user throughput requirement is known, it can be compared to the aggregate throughput available per access point for the 802.11 protocol(s) utilized to determine the recommended number of users per access point.

It is important to keep in mind when planning a WLAN deployment, the impact layer 3/4 protocols have on effective throughput. Table 1 compares maximum data rates with effective throughput for the various 802.11 protocols.

802.11 Protocol	Maximum Data Rate	Average TCP Throughput
802.11b	11 Mbps	7 Mbps
802.11b/g	54 Mbps	13 Mbps
802.11g	54 Mbps	25 Mbps
802.11a	54 Mbps	25 Mbps
802.11n (HT20, 1ss)	72 Mbps	35 Mbps
802.11n (HT20, 2ss)	144 Mbps	70 Mbps
802.11n (HT40, 2ss)	300 Mbps	150 Mbps

Table 1: Maximum Data Rate and Average TCP Throughput by 802.11 Protocols

The average TCP throughput rates provided in Table 1 assume good RF conditions, i.e. good signal-to-noise ratios with little or no co-channel and adjacent-channel interference.

As an example, an 802.11n (HT20, 1ss) environment that was going to be used for online testing should be limited to 10-15 devices per AP (35 Mbps divided by 2-4 Mbps per device). Although this is a fairly simplistic approach and assumes good RF conditions, it does provide a reasonable approximation of what wireless infrastructure is required. LEAs should consult with their WLAN equipment provider or reseller to review their wireless infrastructure and application requirements or may contact the MCNC CNE team to conduct a wireless assessment.

Tech Note: Legacy 802.11 b/g equipment operates in the 2.4 GHz ISM band and provides three (3) non-overlapping 20 MHz frequency channels; 1, 6, and 11. 802.11a equipment operates in the 5 GHz UNII band and uses one of twelve (12) 20 MHz non-overlapping channels. 802.11n operates in both the ISM and UNII bands and can utilize 20 MHz or 40 MHz channels. The use of 802.11n operating in the 5 GHz band greatly facilitates dense access point deployments. With only three non-overlapping channels, it's difficult to avoid significant interference issues using 802.11 b/g in a dense access point deployment.

Wireless interference generated by other access point radios on the WLAN is either co-channel interference (CCI), resulting from two access points on the same channel, or adjacent-channel interference (ACI), resulting from two access points operating on

overlapping channels. Since WLANs employ a contention protocol based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), co-channel interference between access points tends to work out somewhat cooperatively, with the interfering access points often sharing channel capacity. In a co-channel interference scenario, effective capacity per access point may be reduced by 50% or more. Adjacent-channel interference may result in similar channel sharing or in transmission errors and retransmissions. The impact of co-channel and adjacent-channel interference may only be noticeable in environments with high client densities, e.g. 1:1 computing initiatives.

802.11ac is an emerging standard for Gigabit Wi-Fi with expected data rates up to 1.7 Gbps. Devices supporting 802.11ac are expected to be available at the end of 2013. LEAs can consult with their WLAN vendors to better understand what to expect from them with regard to their 802.11ac plans.

General WLAN recommended practices can be found at:

https://edspace.mcnc.org/confluence/download/attachments/10027773/Designing+and+Building+a+Campus+Wireless+Network+v1.pdf?version=1

Although this is an older document, it does review WLAN considerations that are still very relevant to current WLAN design and deployment.

Security – Fundamental Considerations

Current WLAN technology provides much of the underlying functionality required to support a BYOD initiative. All the major WLAN equipment vendors have developed recommended practices or design standards for BYOD deployments. LEAs should become familiar with their WLAN vendor feature/functionality options. Many LEAs simply deploy network infrastructure using default values and rarely spend the time to optimize the environment.

LEAs should restrict personal devices from accessing the wired network by implementing 802.1x network access controls on their LAN switches or through LEA policy and oversight.

Network Security Zones

LEA network assessments conducted by MCNC often uncover inadequate security practices. Adherence to general recommended security practices by the LEA typically doesn't require significant infrastructure investments and can mitigate the risks associated with BYOD initiatives. Security design should reflect an understanding of where confidential or sensitive LEA data exists, and control and manage access to this data. The classification and segmentation of the network can be effectively implemented using network security zones. A network security zone is one or more logical network segments with a defined level of network security or trust. A network security zone framework should:

- Identify the systems within a zone - systems are trusted at the same level

- Define discreet entry points
- Implement access control at the discrete entry points
- Authenticate network entities attempting to connect to a security zone
- Monitor network traffic and the entry points

Recommended network security zones with increasing level of trust include:

- Public Zone – the public Internet
- DMZ (Demilitarized Zone) - publicly accessible servers
    - email, web server, LMS
- Operations Zone - end-user devices and workgroup servers
    - end-users, DHCP, file/print
- Restricted Zone – business-critical IT services
    - business operations – finance and human resource systems
    - Infrastructure – directory services, management systems

A network security zone is typically created using virtual local area networks (VLANs). Layer 2 VLANs divide the network into logical segments even when devices from different network segments are in the same physical location. Conversely, hosts not within the same physical location can share the same logical VLAN which allows them to be treated as a singular physical domain and to be collectively segmented from any other domain having a different level of trust.

Managing Inter-VLAN traffic is accomplished using Access Control Lists (ACLs) which are applied on a Layer 3 device. ACLs may be configured on the Layer 3 device nearest the VLAN's hosts such as the edge device of a school campus or on a more centralized Layer 3 capable network device such as the school system's core switch or firewall.

The number of operations zones will depend on who needs access to what LEA resources, i.e. the level of trust assigned to personal devices and LEA issued student and staff end-user devices, and the levels of access to data and services required by those users and devices. Often, user populations are classified into three operations zones: guests, students, and staff, and proper segmentation is maintained through VLANs configurations. Additional operations zones may be created to further segment the network, e.g. central office staff.

Note: The increasing number of devices connected to the network in a BYOD environment may exhaust the available IP addresses in some legacy IP addressing plans. Allocate IP address space by evaluating the user requirements in the operations zones. In addition, content filtering licenses which are based on the number of connected devices may need to be evaluated. Some districts have used a premise-based appliance for student and staff filtering and low cost solutions like OpenDNS for their guest network. The state cloud-based filtering service is also an alternative.

<u>Network Authentication and Authorization, and Data Encryption</u>
Device access to the network should be restricted using proper network authentication and authorization, and network traffic for students and staff should be encrypted. Encryption is

peripherally related to authentication. The major WLAN equipment vendors support a network security zone framework by allowing different groups of users and device types to be mapped to specific VLANs.

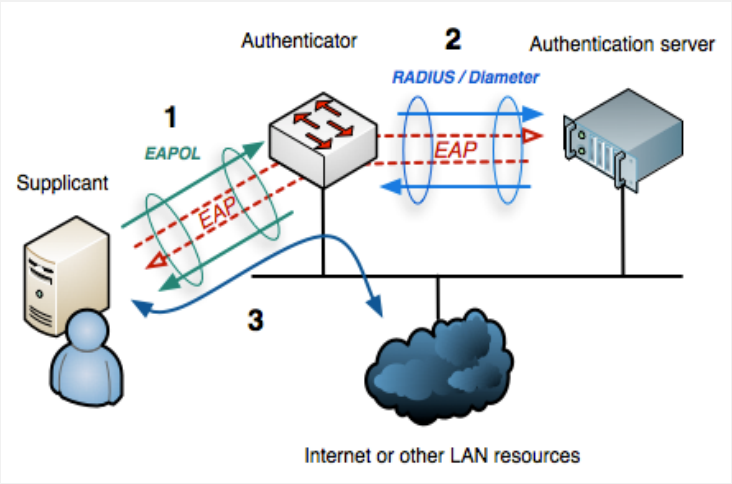
The methods for wireless authentication include:

- MAC-based authentication – authentication based on the MAC address of the wireless device
- shared key encryption – wireless client uses a shared key to encrypt data to/from the access point
- captive portal page login – captive portal page prompts for username/password credentials
- WPA2-Enterprise with 802.1x authentication – user credentials are validated with an authentication server at association time. (See the Tech Note below.)

MAC-based authentication doesn't scale well and is unmanageable for guest wireless networks. In K-12, the shared key is often compromised and subsequently the network is compromised when using shared key encryption. Consequently, the preferred authentication methods are a captive portal page or WPA2-Enterprise with 802.1x.

Tech Note: IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. It uses Extensible Authentication Protocol (EAP) to both the wired and wireless LAN and supports multiple authentication methods, such as token cards, one-time passwords, and certificate authentication.

In the 802.1x architecture, there are three key components: a) Supplicant: the user or client that wants to be authenticated; b) the Authentication Server, typically a RADIUS server; and c) the Authenticator: the device in between, such as a wireless access point. The Authenticator deals with controlled and uncontrolled ports (both are logical). Only the uncontrolled port is open prior to authentication and only EAPOL (EAP over LAN – an encapsulation of EAP authentication) traffic is allowed to pass through. After the Supplant has been authenticated, the controlled port is opened and the access to the network is granted. (Source: http://tldp.org/HOWTO/html_single/8021X-HOWTO/)



(Source: http://en.wikipedia.org/wiki/IEEE_802.1X)

When using 802.1x, the Protected Extensible Authentication Protocol (PEAP) is recommended. Unlike EAP-TLS, PEAP only requires a server-side x.509 digital certificate. The version of PEAP used, e.g. Microsoft PEAP, must be supported by the Supplicant and the Authentication Server.

A Certificate Authority (CA) is required to issue the requisite digital certificates. Microsoft CA Services is most commonly used.

The preferred type of authentication and encryption will depend on who the wireless users are and what LEA issued and personal devices are supported.

Device Identification

WPA2-Enterprise with 802.1x and captive portal authentication can provide the appropriate user authentication controls, but do not address the issue of device identification. These authentication types will not prevent users from using their credentials to log into the network on different devices, i.e. LEA issued versus personal mobile devices. User authentication should be complimented with device profiling and classification. WLAN vendors typically support device profiling which uses the externally observable characteristics of the device, e.g. DHCP or MAC OUI, to identify the device and apply polices based on that identify.

Recommended Authentication and Encryption Practices

Recommended authentication and encryption practices for the three operations zones indentified earlier, i.e. guest, student, and staff are as follows:

Guest Wireless Access

- Guest SSID
  A Guest SSID which does not use authentication or encryption and is mapped to a guest VLAN.
- Captive Portal

The purpose of the captive portal page is to greet users to the network and communicate acceptable use polices. The captive portal optionally may record the device's MAC address, time of visit, and require a user to provide personal information (e.g. name and affiliation) together with his/her mobile phone number. Guest credential delivery may occur via SMS. This practice ties the guest access with his/her mobile phone number rather than a potential fake email address. In addition to keeping of who is on the network, this process provides a way for IT personnel to contact a guest user if necessary.

- Peer-to-Peer Blocking
  Prevents communications between clients on the same WLAN
- Access Control Lists
  ACLs limit access to Internet only and deny access to LEA systems and applications infrastructure.
- Quality of Service (QoS)
  QoS parameters may be applied to guest wireless users to limit the bandwidth to each guest user or to the guest network in aggregate.

Student and Staff Access

- Student and Staff SSIDs
  Student and staff SSIDs use 802.1x and PEAP to authenticate to a RADIUS authentication server. The preferred encryption is WPA2-AES.
- VLAN Mapping
  The WLAN is configured such that user groups are mapped to specific VLANs. Students and staff provide proper IDs and passwords to connect to their respective VLANs.
- Access Control Lists
  ACLs create role-based access domains which limit user access to the Internet, and only the academic and business operations systems they are authorized to use.

<u>Wireless Intrusion Detection</u>
Most tablets and smartphones now have the capability to enable an ad hoc WLAN. This creates a potential vulnerability when an authenticated device is configured with an ad hoc WLAN which is then used by non-authenticated devices and users to gain access to the LEA network.

WLAN equipment typically provides an integrated wireless intrusion detection system (WIDS) that can monitor for rogue APs and unauthorized devices. WIDS functionality should be enabled on the WLAN equipment to monitor for rogue APs in both the 2.4 GHz and 5 GHz bands.

<u>Monitoring and Event Logging</u>
MCNC includes the need for comprehensive security log management in its operations, administration, and management (OA&M) recommended practices which are part of the MCNC network assessment. Log management utilizes the syslog protocol which is defined by the Internet Engineering Task Force in RFC 3164: "the syslog protocol provides a

transport to allow a machine to send event notification messages across IP networks to event message collectors - also known as syslog servers."

Detailed information on log management can be found in the National Institute of Standards and Technology's (NIST) publication "Guide to Computer Security Log Management" at:

http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

NIST summarizes the need for log management as follows:
"Log management can benefit an organization in many ways. It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems."

Open source and low cost syslog infrastructure, e.g. SolarWinds Kiwi Syslog Server are available. In addition, analytical tools like Splunk can be used to facilitate the analysis of real-time and historical security log data.

Summary of BYOD Recommended Design Practices

A summary of BYOD recommended design practices can be found in Table 2.

Recommended Design Practice	Adherence	Comments
WLAN capacity is sufficient to meet the expected demand of the BYOD deployment. Access points are configured for 802.11n operating in the 5 GHz band.		
A network security zone framework is developed which reflects an understanding of where confidential or sensitive LEA data exists, and what users and devices should have access to this data		
Access controls are properly implemented at the discrete entry points defined within the network security zone framework		
The LEA IP addressing scheme will support the number of devices expected to access the network		
CIPA compliant content filter has sufficient capacity and licenses to support the BYOD deployment		
Guest SSID, which does not use authentication or encryption, is mapped to a guest VLAN. Appropriate ACLs are configured to restrict guest access		
Student and staff SSIDs use 802.1x and PEAP to authenticate to a RADIUS authentication server. The preferred encryption is WPA2-AES. ACLs create role-based access domains which limit user access to the Internet, and only the academic and business operations systems they are authorized to use		
User authentication is complimented with device profiling and classification if supported by the WLAN vendor		
WIDS functionality should be enabled on the WLAN equipment to monitor for rogue APs in both the 2.4 GHz and 5 GHz bands		
Deploy a syslog server to capture firewall and IDS log messages		

Table 2: Summary of BYOD Recommended Design Practices

General Recommended Security Practices for K-12

For additional information on recommended security practices, a MCNC white paper on recommended security practices for K-12 can be found at:

https://edspace.mcnc.org/confluence/download/attachments/10027773/NCET+Security+Considerations+for+K12+rev1.pdf?version=1&modificationDate=1319914759000

Security – Advanced Capabilities

The information technology infrastructure discussed in the previous sections looked to leverage existing LEA network infrastructure where possible to support a BYOD initiate and provide immediate benefit without significant investment and complexity. Those fundamental practices serve as a foundation to support more advanced capabilities. Implementing the advanced capabilities discussed in this section should be contingent on a careful analysis of their costs and benefits. As noted earlier, LEA environments are uniquely different and what makes sense in one LEA may not be appropriate in another.

Network Access Control (NAC)

Fundamentally, network access control authenticates users trying to access the enterprise network and enforces security controls based on the user and device identity. As noted earlier, WLAN equipment may provide basic NAC functionality which can be leveraged to help mitigate the risks of a BYOD deployment.

Network access control has evolved significantly in recent years to incorporate context aware access control. Context aware access control uses supplemental information, e.g. device type, OS levels, and security posture, i.e. the device is appropriately protected with the requisite anti-virus and personal firewall software, to enforce granular network access polices. Devices not appropriated protected may be directed to a captive portal to update their security posture. Supplemental NAC tools available from traditional network switch vendors (e.g. Cisco, Enterasys, and HP) or from dedicated NAC vendors like Bradford Networks provide these advanced context aware capabilities.

LEAs should compare the basic NAC functionality available from their WLAN equipment vendor to that available from supplemental NAC tools to determine their relative costs and benefits. Supplemental NAC tools are feature-rich but historically complex and expensive to deploy and operate, and typically require good vendor support to ensure an effective deployment. NAC solutions are typically priced on a per-device basis. Most NAC products will require tight integration with LEA wired and wireless network infrastructure to change VLANs or apply access control lists to individual ports on switches. This can be challenging given the age and disparity of network devices in the typical LEA network. A comprehensive evaluation and pilot is recommended before purchasing. If supplemental NAC tools are deployed, it is recommended that LEAs take a progressive approach by implementing and provisioning NAC in phases. For instance, start with basic policies such as device authentication and role-based access, and add more advanced policies such as device configuration and profile-based access control.

Potential NAC vendors include, but are not limited to, the following:

- Bradford Networks
- Cisco Systems
- Enterasys Networks
- HP
- ForeScout
- Juniper Networks

Mobile Device Management

Where supplemental NAC solutions focus on the network and require tight integration with LEA wired and wireless network infrastructure to control device access to the LEA network, mobile device management (MDM) solutions typically use a lightweight client installed on the mobile devices to configure, secure, and manage the devices directly. MDM solutions can provide complimentary features and functionality which can facilitate a BYOD deployment. These features and functionality include:

- Define device and user eligibility policies and enforce enrollment based on those policies which includes limiting the number of devices allowed per user
- Over-the-air (OTA) distribution, patching, and removal of applications
- Enforce data encryption and password policies on the mobile devices and remotely wipe a device if it is lost or stolen
- Configure Wi-Fi and VPN settings
- Support user self-registration through a web-based Self-Service Portal

Traditional PC management solutions and emerging mobile device management solutions remain mostly independent although there is some consolidation among these solutions providers starting to happen. LEAs should consult their PC management solution provider to understand what, if any value, they can provide related to BYOD. A comprehensive evaluation and pilot is recommended before purchasing a MDM solution.

Potential MDM vendors include, but are not limited to, the following:

- AirWatch
- Good Technology
- Fiberlink
- JAMF Software (Casper)
- Juniper
- McAfee
- MobileIron
- Symantec
- Zenprise

Desktop Virtualization

"Desktop virtualization comes in a number of flavors. The most popular varieties at the moment are application virtualization and virtual desktop infrastructure (VDI). Application virtualization centrally manages apps and distributes them to desktops, where they run via the locally installed operating system. A VDI hosts a user's desktop as a virtual machine running on a central server. Applications, operating system and data all reside in the data center." - Government Computer News, http://gcn.com/Articles/2012/03/15/FEAT-BizTech-desktop-virtualization.aspx?Page=2

As noted earlier, LEA instructional strategies around teaching and learning systems and application delivery will significantly impact the BYOD security model. This is particularly true when it comes to the use of desktop virtualization in BYOD environments. The two primary benefits of a virtual approach to BYOD are consistent secure access to LEA applications and content and increased data security since virtualization allows access to sensitive or confidential data without storing the data on the mobile device. These benefits may have limited relevance when SaaS teaching and learning applications are used extensively in LEAs since consistent secure access is available through a standard web browser and confidential or sensitive data is stored within the application itself.

Desktop virtualization may be appropriate in BYOD environments when the teaching and learning systems are not web-accessible and/or they have disparate requirements for end-user device hardware and software, e.g. browser capabilities and standards or the need for plug-ins.

Additional References:

Intel - Best Practices for Enabling Employee-owned Smart Phones in the Enterprise
http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/enabling-employee-owned-smart-phones-in-the-enterprise.pdf

Aruba Networks - Conquering today's bring-your-own-device challenges
A framework for successful BYOD initiatives
http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf

Bradford Networks – Bring Your Own Device
http://www.bradfordnetworks.com/byod

Cisco – Bring Your Own Device
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.html#wp427155

Enterasys Networks - OneFabric
http://www.onefabric.net/byod/

HP – BYOD in Education
http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-9251ENW.pdf

Policy

In-progress

Operations and Support

In-progress