ATTACHMENT A

EXISTING SYSTEMS

PART 1 - GENERAL

1.01 General Information

A. The information is presented so that the vendors have an understanding of the existing network and systems, and the vendor's responsibility to decommission, removal off-site, and data wiping of existing legacy systems.

PART 2 - EXISTING SYSTEMS

2.01 WIDE AREA NETWORK INFORMATION

A. Palm Beach State College is comprised of 5 primary campuses, each having their own network services supporting voice, video and data. The heaviest use is from 7:00AM-10:00PM M-F over the Internet connections. Inbound traffic is largely web, social networking traffic, and Email. Outbound traffic is streaming video, web, and Outlook Web Access. Palm Beach State College will require flexible network solutions that provide a predictable and scalable platform for existing and future communications requirements.

2.02 NETWORK ARCHITECTURE

A. Applications

1. The greatest numbers of applications are Microsoft maintenance, database, VMware and monitoring tools. The most critical application is Panthernet. This proprietary consortium-supported LINUX-based ERP system powers the College, and has grown to over 10,000 active users. Critical applications include:

- **Panthernet**: Software AG/ADABAS ERP application, Student, Finance, business services.
- **Microsoft Exchange**: Faculty/Staff
- **Microsoft SQL**: Faculty/Staff/Students
- **Checkpoint Firewalls**: heart of all communications – Faculty/Staff/Students
- **Microsoft SharePoint**: Students initially, in the future Faculty/Staff, this will become a major application moving forward

VMs will be increasingly deployed to support curriculum development and classroom activities. IT does not currently have the infrastructure in place to support this effort.

2. The most recent applications survey describes up to 60,000 packages discovered through an automated network-based inventory process on server machines and provides a count of the number of times a particular version of software was found. The data in this report is based solely upon results from systems responding at that time. The following table lists the top 20 software packages by installed copy supported by the data center network. A complete version of the survey will be available separately.

Application	**Version**	**Installed Copies**
Microsoft Operations Manager 2005 Agent	5.0.2911.0	133
Microsoft Forefront Client Security State Assessment Service	1.0.1703.0	123
Active Directory Management Pack Helper Object	1.0.3	119
Microsoft Forefront Client Security Antimalware Service	1.5.1973.0	114
Security Update for CAPICOM (KB931906)	2.1.0.2	60
VMware Tools	3.1.2.10559	55
Microsoft .NET Framework 3.5 SP1	3.5.30729	55
MSXML 6 Service Pack 2 (KB954459)	6.20.1099.0	53
Windows Presentation Foundation	3.0.6920.0	36
MSXML 4.0 SP2 (KB954430)	4.20.9870.0	32
Microsoft .NET Framework 2.0 Service Pack 1	2.1.21022	31
MSXML 4.0 SP2 (KB936181)	4.20.9848.0	27
IBM 32-bit Runtime Environment for Java 2, v1.4.2	1.4.2	24
IBM Tivoli Storage Manager Client	05.05.0100	23
IBM Tivoli Monitoring	61041	22
Microsoft .NET Framework 2.0	2.0.50727	22
Microsoft .NET Framework 3.0 Service Pack 1	3.1.21022	21
Microsoft .NET Framework 2.0 Service Pack 2	2.2.30729	19
IBM Tivoli Storage Manager Client	06.01.0000	19
Microsoft SQL Server Native Client	9.00.3042.00	19

B. End Devices

1. End Users:

a. There are approximately 38,000 student users on all campuses for any given Semester. Simultaneous users peak between 15,000 and 20,000 a day. This includes students equipped with laptops and mobile WiFi devices as well as students that connect remotely over the Internet and to campus-based rich-media objects through on-line courseware hosted externally by Blackboard™.

b. There are approximately 5,000 faculty and staff. Faculty both developing and delivering curriculum as well as staff communications for all supported services and facilities management. Simultaneous faculty and staff usage are ½ this number at peak usage. Facilities control systems rely on the campus network to monitor and maintain building control systems. Campus Security will increasingly rely on the campus network (and PoE) to support camera, alarm, and notification systems.

c. There are approximately 3,800 MS/Windows end-user workstations and peripherals typically connected to the access layer with 100 Mb full duplex links.

2. Rack mounted servers

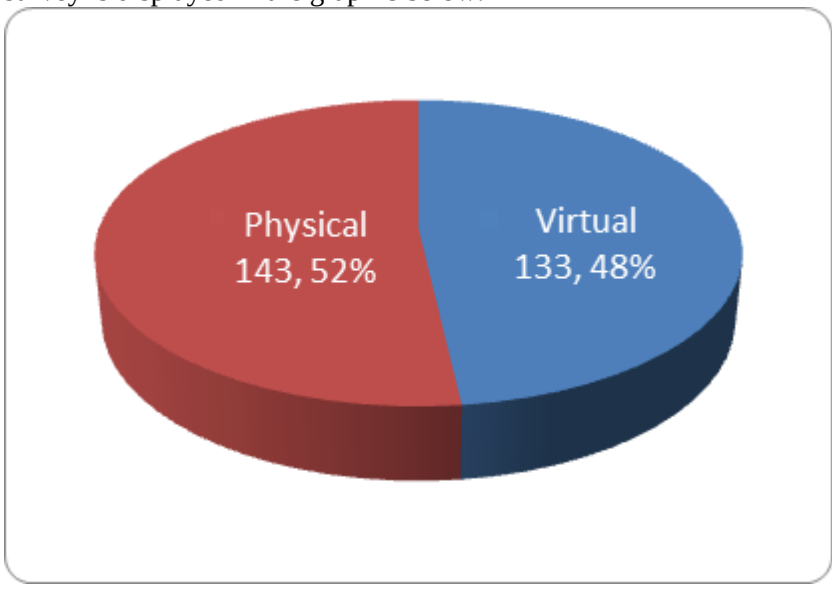
a. There are approximately 146 MS/Windows servers in the Lake Worth data center. The physical rack-mounted servers are predominately Dell 2950, IBM BladeCenter and X-series systems, and 2 Macintosh servers supporting 200 Mac clients. Servers are centralized on the Lake Worth campus.

Platforms at Lake Worth DC	**Count**
VMware Virtual Platform	133
PowerEdge 2950	25
IBM BladeCenter HS20	28
PowerEdge R300	5
PowerEdge R710	4
PowerEdge 1950	7
IBM BladeCenter LS20	5
IBM System x3550	14
PowerEdge 2970	3
PowerEdge 2900	4
PowerEdge R410	3
PowerEdge 2650	4
IBM System x3650	1
HP Proliant DL380G6	1
IBM x3850	2
IBM x3950	3
IBM x346	3
Dell R200	1
PowerEdge 2550	1
PowerEdge 2600	1
PowerEdge 2850	1
PowerEdge 4600	3
PowerEdge 860	2
PowerEdge R200	4
PowerEdge R610	6

b. The rack-mounted servers production link are predominantly connected to the access layer with single 100Mps or 1Gbps NICs

c. The SAN environment is currently based on a DS5100 with 60 TB and a DS3512 with 72TB virtualized by an IBM SAN Volume Controller, a DS3512 with 72 TB for Backup, and a DS4700 with 67 TB for off site replication. There are currently 3 Tiers of Application Server storage between the DS5100 and the DS3512 that is virtualized by the SVC. AppAssure REPLAY 4.6 is the backup solution used for disk to disk backup and off site replicationPalm Beach State College has begun to implement VMWare. All applications will be evaluated to determine suitability, with "virtual first" policy whenever possible.

d. The distribution of physical to virtual hosts from the most recent network survey is displayed in the graphic below.



C. Network Devices

1. Access Layer

a. End Users

(1) Primarily Cisco Catalyst switches, quantity 283, distributed in telecommunications closets throughout multiple campus locations.

(2) Uplinks from IDF closets to the respective campus Core Layers are typically 62.5-micron fiber. Typical backbone fiber connections are SC. Typical intra-building connections are ST.

(3) Most of the current Access Layer hardware supports PoE, but it is not unusual to find PoE injectors in the IDF closets to support wireless access points on older switch hardware. PoE will be an important service at this layer moving forward.

2. Core Layer

   a. The core layer is controlled and accessed through the Lake Worth campus with connectivity to the Palm Beach County backbone (PBC). The Boca Raton campus has a connection to the Florida LambdaRail that provides 150Mb of Internet1. Internet connectivity is balanced between the connections and travels over the WAN before exiting the firewalls in Lake Worth. LambdaRail provides a fiber connection between the Boca Raton campus and Florida Atlantic University (refer to WAN network diagram T101).

   b. The core layer at Lake Worth consists of a single Cisco 3750 Metro device providing connectivity to the PBC. PBC connections are fiber: 2 ports SM uplink and 2 ports SM downlink. The core router is a Cisco Catalyst 4506.

   c. Cisco 4506 slot configuration

      (1) Slot 1: WSX4550

      (2) Slot 2: WSX4306-GB six of six SC MM ports

      (3) Slot 3: WSX4448-GBSFP 37 of 48 LC MM

      (4) Slot 4: WSX4548-GBRJ45 11 of 48

      (5) Slot 5: BLANK

      (6) Slot 6: WSX4548-GBRJ45 29 of 48

   d. Cisco 4506 layer-3 switches are used at three campus locations to connect to the WAN and provide core routing.

3. Enterprise VLANs

   a. The following is a list of VLANs currently implemented between the campus networks:

      (1) Network Switches and Building Controls

      (2) Employees

      (3) Students

      (4) Phones

      (5) Printers

      (6) Emergency Services

4. Wi-Fi Services

   a. Bluesocket WG-2100

   b. Cisco AIR-LOC2710-L-K9

   c. Cisco AIR-WLC4402-50-K9 (x3)

5. SAN Fabric
   a. Existing SAN fabric switches (to remain) are provided with fiber channel ports for storage traffic and Ethernet ports for management.

6. Traffic Shaping: Procera Packet Logic PL7720

7. Firewall
   a. Two Checkpoint NGX firewalls configured in cluster mode.

8. Internet Switches: Cisco 3825 (x2)

9. VPN Concentrator: Nortel VPN 3050

10. Summary Inventory of Existing Network Equipment

Device Model	Quantity	In Storage room	End-Of-Life (Y / N)
Cisco Catalyst 2924	70	7	Y
Cisco Catalyst 2980	1	1	Y
Cisco Catalyst 3524 PWR XL	2		Y
Cisco Catalyst 3524 XL	1		Y
Cisco Catalyst 3500 48p	15		Y
Cisco Catalyst 3550	95	5	Y
Cisco Catalyst 3560-48PS	8		N
Cisco Catalyst 3560G-48TS	6		N
Cisco Catalyst 3560G-48PS	14		N
Cisco Catalyst 3560E-48PD-F	20	5	N
Cisco Catalyst 3560X-48PF-L	26	16	N
Cisco Catalyst 3750G-48TS	7		N
Cisco Catalyst 3712	2		N
Cisco Catalyst 3508G XL	5	2	Y
Cisco Catalyst 2912MF-XL	6	5	Y
Cisco Catalyst 3550-12G	1	2	Y
Cisco 4506	3		N
Cisco Router 3825	1		N
Cisco Router 2821	3		N
Cisco Router 2811	2		N
Cisco Aironet AIR-AP1142N-A-K9	7		Y
Cisco Aironet AIR-AP1231G-A-K9	82		Y
Cisco Aironet AIR-AP1242AG-A-K9	2		Y
Cisco Aironet AIR-AP1242G-A-K9	6		Y
Cisco Aironet AIR-LAP1231G-A-K9	63		Y
Cisco Aironet AIR-LAP1242G-A-K9	2		Y
Cisco WLC 4404	8		N
BayStack 350-24T	5	2	Y
HP Procure 2848 J4904	4		Y
SFP		39	

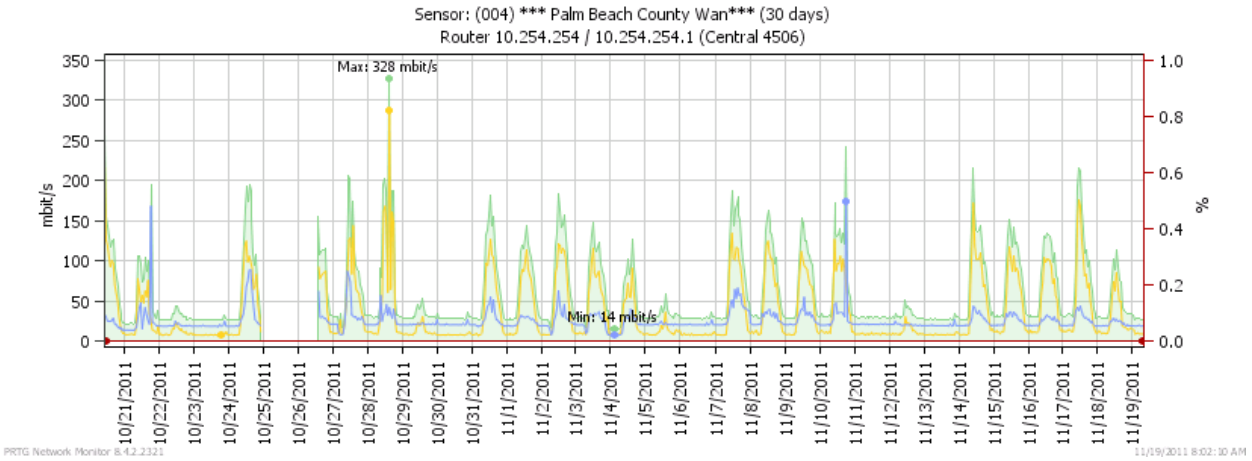
2.03 EXISTING NETWORK

A. Data network services are provided to each campus via a metropolitan area connection provided by PBC with the Belle Glade location on a MetroE circuit provided by AT&T tied to the PBC data center. A network diagram is provided as an attachment that defines bandwidth into each location.

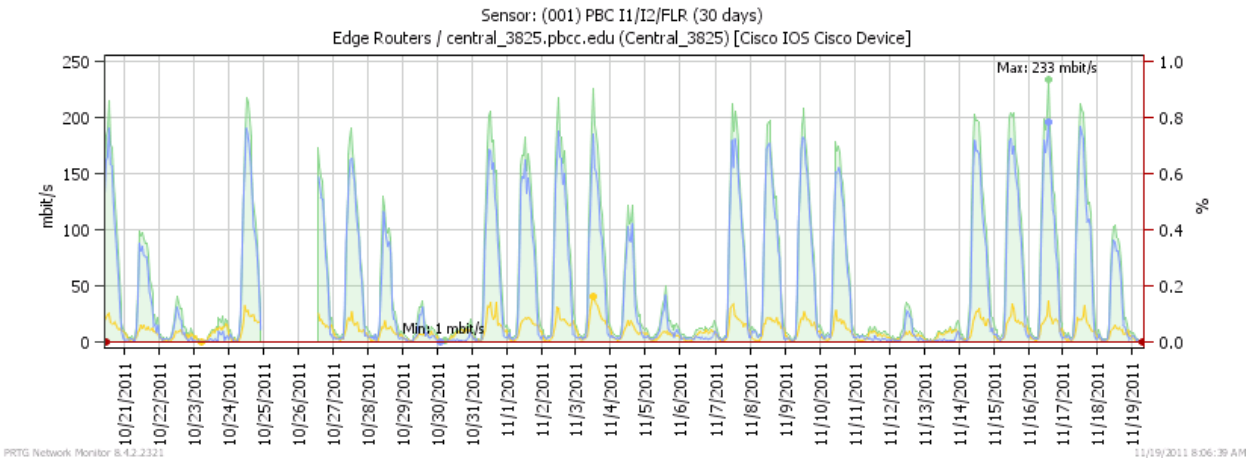
B. There are 2 providers of Internet services to Palm Beach State College, PBC and LambdaRail (2 connections, 1 to the public internet and 1 connection to internet 2, a quasi government internet service). All internet traffic regardless of campus origination or which service provider traffic is directed to is first routed to the Lake Worth campus, then routed through the PBC service to the respective provider.

2.04 NETWORK TRAFFIC TRENDS

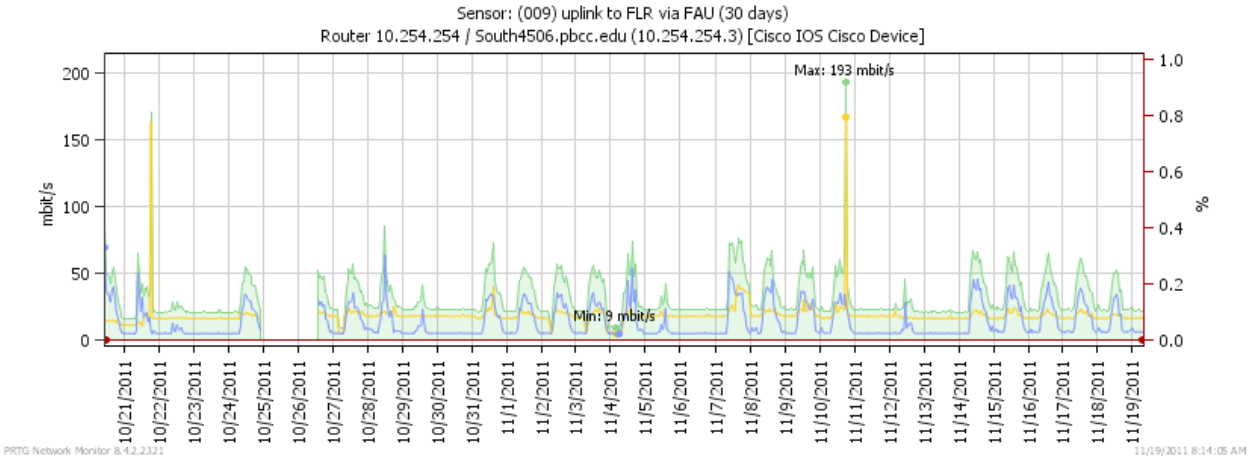
A. Central – PBC WAN circuit



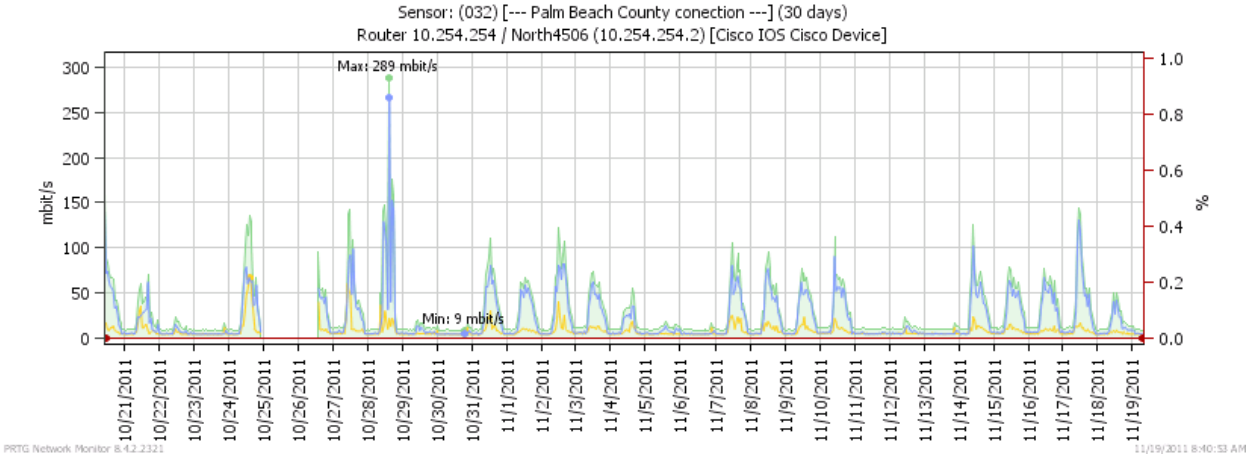
B. Central – PBC Internet



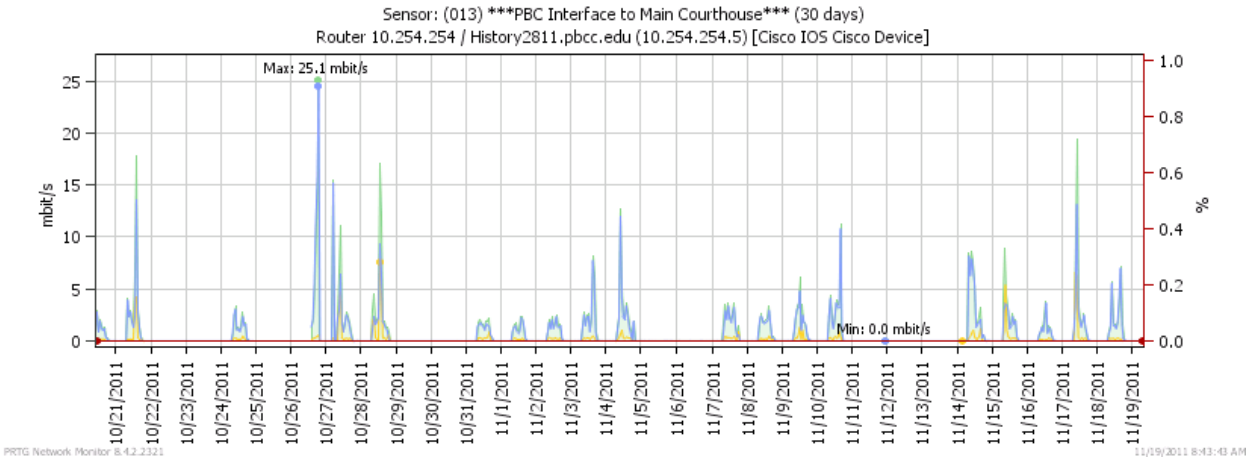
C. South - FLR uplink to PBC



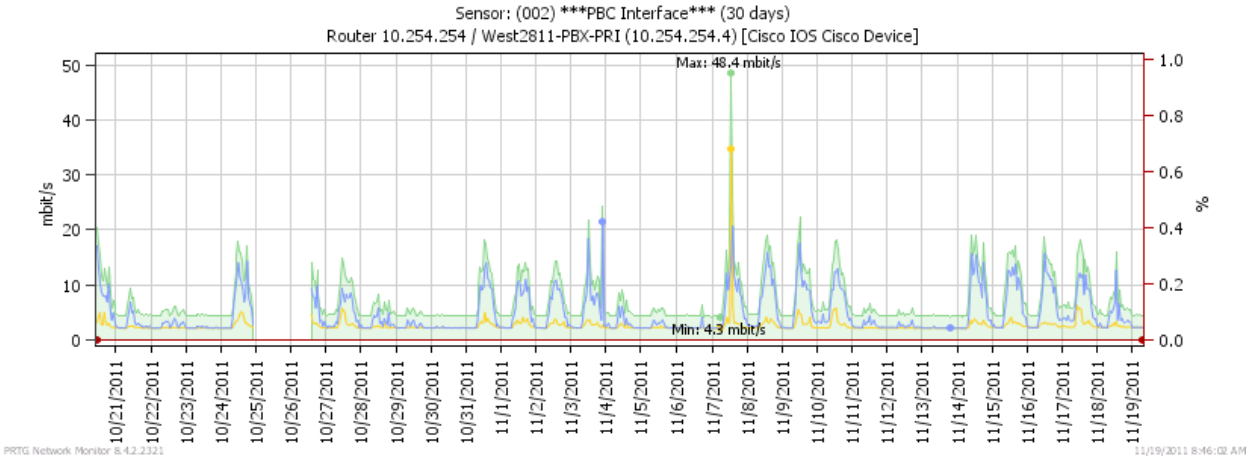
D. North – PBC



E. Historical – PBC



F. West – PBC


Sensor: (002) ***PBC Interface*** (30 days)
Router 10.254.254 / West2811-PBX-PRI (10.254.254.4) [Cisco IOS Cisco Device]
Max: 48.4 mbit/s
Min: 4.3 mbit/s
mbit/s
%
50
40
30
20
10
0
1.0
0.8
0.6
0.4
0.2
0.0
10/21/2011
10/22/2011
10/23/2011
10/24/2011
10/25/2011
10/26/2011
10/27/2011
10/28/2011
10/29/2011
10/30/2011
10/31/2011
11/1/2011
11/2/2011
11/3/2011
11/4/2011
11/5/2011
11/6/2011
11/7/2011
11/8/2011
11/9/2011
11/10/2011
11/11/2011
11/12/2011
11/13/2011
11/14/2011
11/15/2011
11/16/2011
11/17/2011
11/18/2011
11/19/2011

PART 3 - EXECUTION

3.01 DECOMMISION EXISTING SYSTEMS

A. Vendor is responsible for the decommissioning of all existing hardware being upgraded. Decommissioning scope of work to include:

1. Remove existing systems from network and physical racking.
2. Remove existing systems and all miscellaneous hardware no longer required off site each day, or in a timely manner as agreed upon by Palm Beach State College.
3. Provide full data wiping of hardware configurations and all Palm Beach State College data including hidden disk sectors or other hidden digital media.
4. Vendor to provide validation certificate verifying the overwriting procedures were properly executed and completed. Certificate to identify defects log list and bad sectors list that could not be overwritten.
5. Vendor to remove all Palm Beach State College asset tags prior to removing existing network devices from the College campus.
6. Vendor to provide certificate verifying that the hardware has been disposed of in accordance with environmental law and disposal procedures.
7. Vendor to provide an inventory of decommissioned equipment in Microsoft Excel format to include the name of the manufacturer, the equipment part number, the equipment serial number and the College asset-tag number.
8. Vendor shall carry liability insurance to cover all legacy equipment from the time it is disconnected from Palm Beach State College network in addition to data wiping insurance. Vendor to provide copy of insurance policy upon request from Palm Beach State College.

3.02 NETWORK OPERATIONS CENTER

A. The NOC will provide network, server, storage and facility infrastructure monitoring.

3.03 TELEPHONY

A. Palm Beach State College is evaluating Microsoft Lync for Enterprise Voice. If the current product does not fit the needs of the college the evaluation will chose another system in 6 – 18 months. Consequently, Network RFP responses should take VoIP into consideration and support future implementation.

B. There is a small Microsoft VOIP trial base installed on the Lake Worth campus. Future telephony applications may also include unified messaging.

3.04 FUTURE APPLICATIONS

A. Applications that are anticipated to increase the network requirements in the near future include:

1. Internal streaming media services to external consumers
2. Internal streaming media services to internal consumers
3. LiveMeeting services and HD Video for internal web conferencing
4. IP based CCTV security traffic on local network, and over wide area network for monitoring.

3.05 MULTI DATA CENTER ARCHITECTURE

A. Lake Worth Data Center

1. The NOC will continue to be located within the existing campus.
2. Palm Beach State College is moving to a disk-based enterprise data archive solution dividing the storage between Lake Worth and Palm Beach Gardens. Backup traffic will traverse the WAN during off-peak hours.

B. Possible Secondary Data Center

1. There are plans to implement a new secondary data center at the Palm Beach Gardens location. Consideration should be made with respect to the impact of a new secondary data center housing a copy of disk-to-disk backups from the Lake Worth NOC as well as a warm copy of the College ERP and main databases. The anticipated backup traffic is 1TB per day during non-peak non-business hours for incremental backups.
2. The existing NOC will continue to be located in the Lake Worth facility and monitor the critical networks, servers, storage, and facility infrastructures across the enterprise.

END OF SECTION