FilmCompany

FINAL PROPOSAL

John Glass

Table of Contents

EXECUTIVE SUMMARY

Project Goal

Overall Project Goal Statement:

The proposed network upgrade will allow FilmCompany to achieve its overall goals of providing better service to its customers, increase its share of the sports event video market, customer support services, and profit margin through the following:

- Better performance for existing applications
- Integration of voice and video networks
- Additional improvements to security and network availability
- Increase the speed of processing and response time
- Improved processing and delivery of video content across the network
- Ability for improved flexibility in meeting customer needs

Financial Goals:

- Obtain a positive cash flow from the stadium contract within six months
- Increase gross revenue by 75% within 18 months
- Reduce production costs by 15% over six months - 20% over twelve months

Job Management Goals:

- Provide network connectivity and bandwidth for projected new hires, up to six temporary and part-time production staff, plus at least one IT and communications technician
- Provide a fast reliable link between Film Company and the Stadium Company
- Consolidate all staff and facilities into Building F
- Implement a highly available secure network

Customer Communication Goals:

- Survey the customer monthly
- Provide customer satisfaction measure of at least four on a scale of five within four months after upgrade
- Respond to 90% of customer non-live media productions requests within 12 hours
- Respond to 100% of customer non-live media productions requests within 18 hours
- Meet Survey customer live media production targets 97.5% of the time

Project Scope

Scope Statement:

The scope of this project is to upgrade the existing LAN and WAN to accommodate the network expansion requested by Film Company, specifically as follows:

- Adding VLANs
- Increase bandwidth and security for wireless coverage
- Implement new network security measures
- Addition of firewalls
- Addition of a core layer
- Adding redundancy links and equipment
- Upgrade bandwidth to remote sites

Items that are out of Scope:

- Installing IP telephony system
- Replacing any infrastructure wiring
- Addition of servers to the existing server Farm
- Implement QoS to support the video applications

Summarization

- Significant upgrade
- To increase the business by 70%
- Data traffic to increase by 80%
- Reduces unit cost by 15% over 6 months and 20% over 12 months
- To respond to 90% of customer non-live media production request within 72hrs and 100 within 18 hrs.
- Meet customer live media production targets 97.5% of the time
- Film Company plans to consolidate all their staff and resources in one building.
- Increase in staff
- A fast reliable network link to the stadium
- Pre and post-production work on premises using communication link from stadium
- Wireless connection at both location and office
- To reuse at least 75% of existing network components
- Network is in full production meeting the deadlines

NETWORK REQUIREMENTS

Business Goals:

Business goals described by Kevin Lim in the initial interview:

Business Goals Prioritized For FilmCompany

	BUSINESS GOAL
1	Upgrade the existing network to support and handle 80% additional traffic
2	Provide a reliable and fast link between the StadiumCompany network and the FilmCompany facilities.
3	Ensure and implement a highly available network
4	Continue to support and enhance wireless access at the FilmCompany facilities (all)
5	Design and implement QoS to support all voice and video applications
6	Design and implement network security and monitoring

Success Criteria:

- Achieve positive cash flow from the stadium contract within 12 months.
- At least 75% of the existing network components are reused.
- Reduce unit production costs by 15% over 6 months and 20% over 12 months.
- Increase gross revenue by 75% within 18 months.
- Respond to 90% of customer non-live media production requests within 12 hours and 100% within 18 hours.
- Achieve a customer satisfaction measure of at least four on a scale of five within four months after upgrade.
- Meet customer live media production targets 97.5% of the time.
- Support an increase of 80% in media data volume within 2 months of upgrade completion.
- Unauthorized network intrusions are intercepted, prevented, logged, and reported.
- Reliable network performance is maintained under load conditions.

Scalability:

- Support up to 80% additional traffic on the FilmCompany network
- Support additional growth of the proposed network in wireless coverage and access area.

Availability:

- Support meeting customer live media production targets 97.5% of the time on a consistent basis
- Support target of responding to 90% of customer non-live media production requests within 12 hours or less
- Support target of responding to 100% of customer non-live media production requests within 18 hours or less
- Support 24/7 network availability and security applications across the entire network

Security:

- Provide wireless security
- Centralize network management
- Improve security with addition of filtering, DMZ, and firewalls

Manageability:

- Maintain the new network architecture with at least one IT and Communications Technician
- Maintain the new network architecture with the existing personnel and up to six new temporary and part-time production staff
- Provide and implement reporting and management tools

Current Network Rating:

Network Ratings	Lowest				Highest
	1	2	3	4	5
Hierarchical network design			X		
Firewall location	X				
Server location			X		
Bandwidth			X		
Quality of wiring				X	
Network equipment suitability					X
Wireless security	X				
Suitability for advanced services like IP phones or video (QoS)		X			
Redundancy and availability	X				
Failure domain size	X				
Physical security					X

User Group Requirements:

The different user groups and their access requirements are listed.

- Customers
- Vendors
- Team personnel
- Remote workers
- On-site management company personnel

Each of these groups may have specific requirements for network services. It is important to document these requirements so that they are considered in the network design.

Application Requirements:

The network traffic characteristics and requirements of various applications affect the design of the network. This section of the document describes the types of applications the network must support. Any specific network traffic requirements are listed as well.

CURRENT NETWORK ENVIRONMENT

Current Network Equipment:

- 2 Cisco 1841 routers (FC-CPE-1, AC-1)
- 3 Cisco 2960 switches (FC-ASW-1, FC-ASW-2, ProductionSW)
- 1 Network and Business server
- 1 Linksys (Cisco) WRT300N wireless router (AC-AP)
- 1 ADSL modem (Internet access)
-

Physical and Configuration State:

- Located in two buildings (Building F, Building A)
- Network LAN cabling in both offices is CAT5e Ethernet
- Combined infrastructure is not optimized at all
- Flat network without redundancy
- 1 small WLAN used by a few project managers and guests
- Remote access through an ADSL, inadequate for growth
- Off-site access from office at the stadium used by two staff members
- Addressing and naming are inconsistent and poorly structured
- 2 configured VLANs (General & Production)
- 3 user PCs and a printer connected to each switch in Building F (FC-ASW-1 and ProductionSW)
- 3 user PCs and a printer connected to switch in Building A (FC-ASW-2)
- 3 servers located in each building (Connected to FC-ASW-1 and FC-ASW-2)
- 2 PCs connected via wireless router (AC-AP)

Network Addressing Scheme:

The General VLAN uses this Addressing:

- Network 10.0.0.0/24
- Gateway 10.0.0.1
- Hosts (dynamic) 10.0.0.200 – 10.0.0.254
- Hosts (static) 10.0.0.10 – 10.0.0.20

The Production VLAN:
Serves the production suites and provides networking for the media development and storage. It consists of 9 high-performance workstations, 5 office PCs, and 2 printers. The Production VLAN uses this addressing:

- Network 10.10.0.0/24
- Gateway 10.10.0.254
- Hosts (dynamic) 10.10.0.100 – 10.10.0.200
- Hosts (static) 10.10.0.1 – 10.10.0.99

Strengths of the Existing Network:

- Adequate space for data center
- Quality of wiring
- Can reuse existing Equipment
- Network equipment suitability
- Current models
- Physical security
- Bandwidth

Weaknesses of the Existing Network:

Weakness	Impact	Possible Fix
Flat Network Design	No scalability - network cannot grow without impacting performance	Create routed hierarchy
Flat Network Design	No network segmentation - cannot filter or isolate traffic creating security risks	Create segmentation with VLANs Apply traffic filters
No Redundancy	Large failure domains - link and device failures affect large areas of the network	• Create smaller failure domains • Use redundancy where possible
Distributed Servers	Servers at risk - no controlled environment, power backup or redundant connectivity	Move servers to data center server farm
Distributed Servers	Servers not available - no high speed links to servers	Install gigabit links to servers, centrally locate
Limited Fiber Availability	Limits the possible redundancy in the network	Stack switches and add high speed uplinks
No Stateful Firewall	Filtering only, does not prevent all unauthorized or unwanted traffic	Use IOS stateful firewall features
Firewall Only at the Edge of Network	Internal devices vulnerable - no protection from internal attacks	• Create layered firewall and filtering mechanisms • Add IDS at data center

*** Current Physical and Logical Topology – APPENDIX A**
*** Existing Device Tables – APPENDIX B**
*** Strengths and Weaknesses – APPENDIX C**

PROPOSED PHYSICAL DESIGN

Constraints:

FILMCOMPANY CONSTRAINTS		
CONSTRAINT	**GATHERED DATA**	**COMMENTS**
Budget	• Tight budget. • Need to reuse 75% of the existing network components (prefer all of it).	• Limited budget. Will affect any proposed new equipment. • Existing equipment may not support the proposed traffic with the stadium.
Policy	• Planning to consolidate staff and facilities into Building F. • Temporary staff not permitted to access other accounts. • Payroll/accounting not accessible by other departments • Physical access to equipment is limited to IT personnel • Training needed for new hires on company security policy.	• Equipment will need to be consolidated into one location. • Redundancy needs to be added. • Cabling may not support 70% future growth. • Older equipment doesn't have an SLA and may not be covered in the event of a failure.
Schedule	• Project must be completed within 4 months of project start. • Maintenance windows are between 2am and 6am Monday through Friday.	• Less than 4 months to get the project completed.
Personnel	• Looking to hire 6 temporary and part-time production staff and at least 1 IT technician. • Training on new equipment for IT personnel is needed.	• Looking to hire 6 temporary and part-time production staff and at least 1 IT technician. • Training on new equipment for IT personnel is needed.

Availability Strategies

Modules and redundant power supplies to increase availability for switches:

- Cisco RPS2300 Redundant Power System
- Cisco EtherSwitch Service Module Switch – 16 Ports
- Cisco Catalyst Inline Power Patch Panel

The Cisco® Redundant Power System 2300 (RPS 2300) increases availability for converged data, voice, and video networks. The system delivers power supply redundancy and resiliency for a variety of power requirements, including Power over Ethernet (PoE). It helps ensure uninterrupted operation and protection against device power supply failures by providing seamless failover for Cisco switches like the Cisco Catalyst®2960 Series.

Backup Hardware:

- Cisco 1841 Integrated Router (Model 1841)
- Cisco Security Firewall Bundle (ASA5505-SEC-BUN-K9)
- Cisco Intrusion Detection System AIM for Model 1841
- Cat5e Cabling and Patch Cables (Various)

Hot-swappable cards and controllers:

- Cisco 100Base-FX Fast Ethernet Hot-Swappable Card SFP
- Cisco 1X1000 Base BX10 SFP Mini GBIC

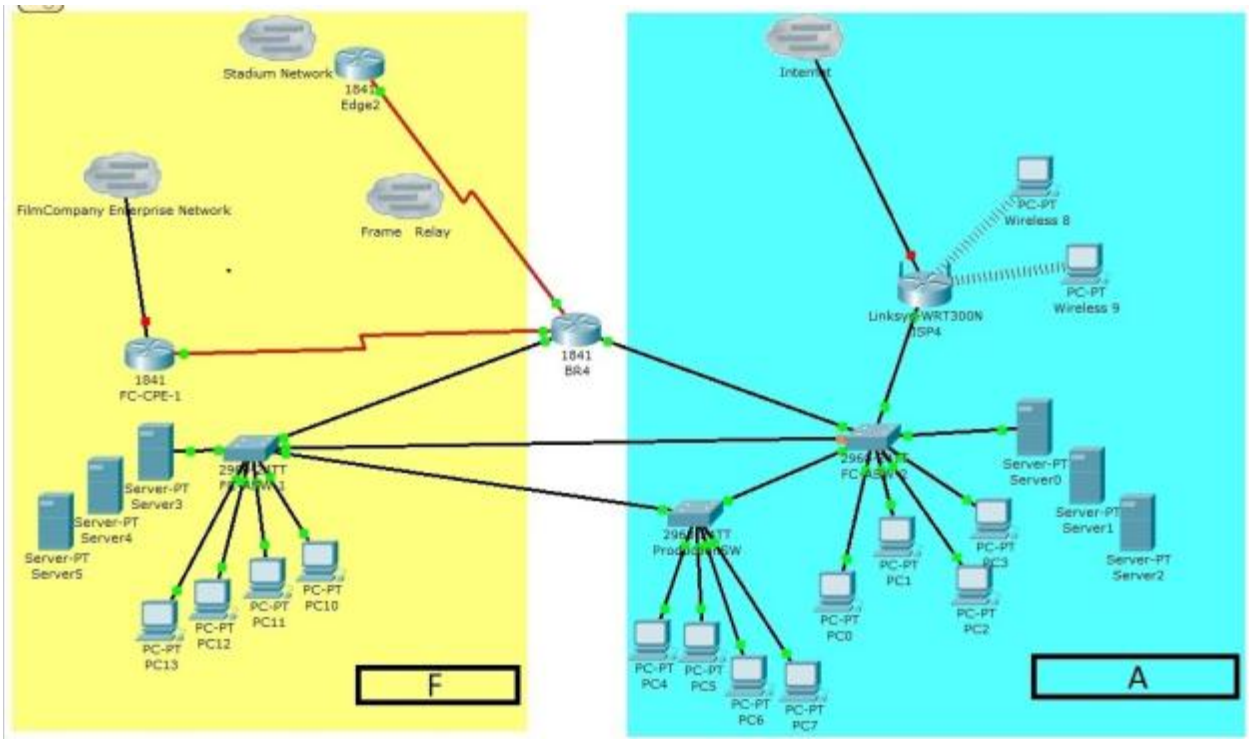
UPS Devices Suitable for Networking Devices:

- Eaton Corporation Eaton PW9130L2500R-XL2U
- APC Smart-UPS 750 LCD-UPS (rack mountable)

Redundant/Uninterrupted Power Supply Option:

- APC Smart-UPS XL SUA3000RMXL3U 3000VA 120V 3U Rack Mount UPS System

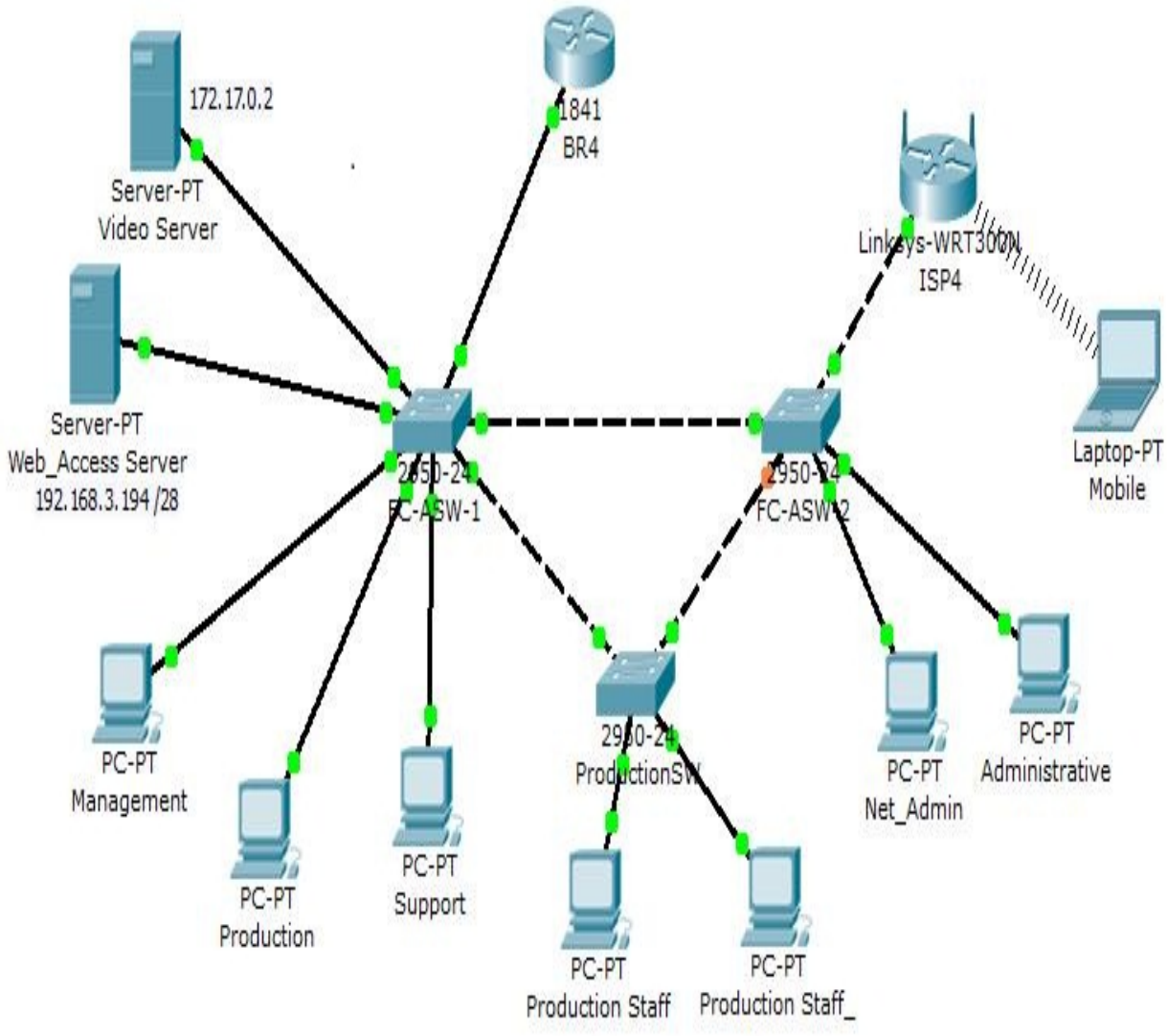
Proposed Physical Design (Building A&F):



***Availability Strategies (Equipment) – APPENDIX D**
*** Security Strategy (Equipment) – APPENDIX E**

PROPOSED LOGICAL DESIGN

Prototype Test Topology:



Proposed IP Addressing Plan:

IP Address Plan

Device Name	Interface	IP Address	Subnet Mask
Web Access Server	Fast Ethernet (100)	192.168.3.194	**255.255.255.240**
Video Server	Fast Ethernet (80)	172.17.0.2	**255.255.0.0**
PC Management	Fast Ethernet (20)	192.168.3.226	**255.255.255.240**
PC Production	Fast Ethernet (50)	192.168.1.129	**255.255.255.128**
PC Support	Fast Ethernet (40)	192.168.1.1	**255.255.255.128**
PC Production Staff	Fast Ethernet (50)	192.168.1.130	**255.255.255.128**
PC Production Staff_	Fast Ethernet (50)	192.168.1.131	**255.255.255.128**
PC Net_Admin	Fast Ethernet (70)	192.168.3.242	**255.255.255.240**
PC Administrative	Fast Ethernet (30)	192.168.3.1	**255.255.255.192**
PC Mobile	Wireless (60)	192.168.3.67	**255.255.255.192**
FC-ASW-1	VLAN 1	192.168.3.210	**255.255.255.240**
FC-ASW-2	VLAN 1	192.168.3.211	**255.255.255.240**
ProductionSW	VLAN 1	192.168.3.212	**255.255.255.240**
BR4	FA0/0.1	192.168.3.209	**255.255.255.240**
BR4	Fa0/0.20	192.168.3.225	**255.255.255.240**
BR4	Fa0/0.30	192.168.3.1	**255.255.255.192**
BR4	Fa0/0.40	192.168.1.1	**255.255.255.128**
BR4	Fa0/0.50	192.168.1.129	**255.255.255.128**
BR4	Fa0/0.60	1982.168.3.65	**255.255.255.192**
BR4	Fa0/0.70	192.168.3.241	**255.255.255.240**
BR4	FA0/0.80	172.17.0.1	**255.255.0.0**
BR4	FA0/0.100	192.168.3.195	**255.255.255.240**
ISP4	**Fast Ethernet 1**	**192.168.3.66**	**255.255.255.192**

Proposed VLAN Plan:

Switch	VLAN Names and IDs	IP Address Range	Group
All	default	192.168.3.208/28	**1**
All	Management	192.168.3.224/28	**20**
All	Administrative	192.168.3.0/26	**30**
All	Support	192.168.1.0/25	**40**
All	Production	192.168.1.128/25	**50**
All	Mobile	192.168.3.64/26	**60**
All	Net_Admin	192.168.3.240/28	**70**
All	Servers	172.17.0.0/16	**80**
All	**Web_Access**	**192.168.3.194/28**	**100**

Basic Connectivity Test:

A baseline test to verify that the test topology is up and running with the proper protocols and features.

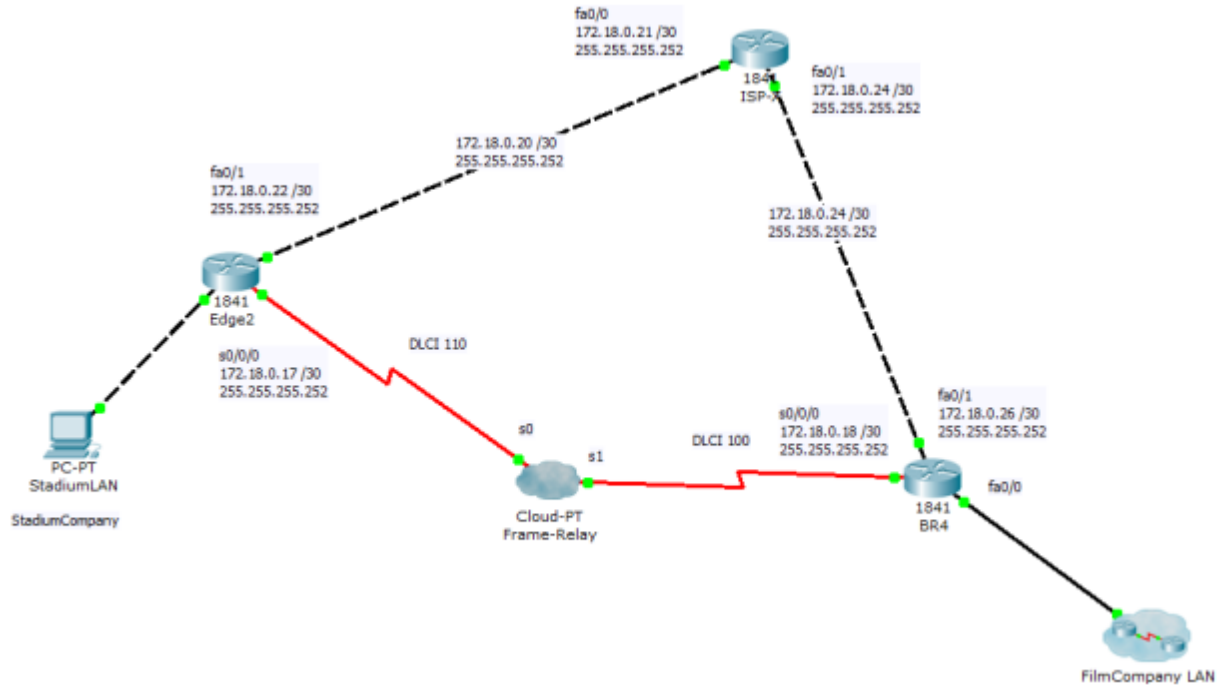
VLAN Configuration Test:

Test the creation of separate networks for the different groups at the FilmCompany. Demonstrate that VLANs will isolate traffic.

VLAN Routing Test:

Test the routing between VLANs. Test that the router is correctly configured to route between VLANs.

Proposed WAN Topology:



Proposed Security Strategies:

- Ensure that physical security measures are in place to prevent unauthorized access to network devices and facilities.
- Prevent network intrusions and attacks by deploying intrusion prevention systems. These systems scan the network for harmful or malicious behavior and alert network managers.
- Control Internet threats by employing defenses to protect content and users from viruses, spyware, and spam.
- Manage endpoint security to protect the network by verifying the identity of each user before granting access.
- Secure Wireless Access Points (WAP) and deploy wireless
- Create secured communications by using VPNs to encrypt information before it is sent through third party or unprotected networks.
- Use firewalls to separate all levels of the secured corporate network from other unsecured networks, such as the Internet. Configure firewalls to monitor and control the traffic, based on a written security policy.

Proposed Security Policies:

1. Remote users must be able to access the Production Server in order to view their schedules over the web and to enter new orders.
2. Remote users must be able to FTP files to and from the Production Server.
3. Remote users can use the Production Server to send and retrieve email using IMAP and SMTP protocols.
4. Remote users must not be able to access any other services available on the Production Server.

5. No traffic is permitted from individual workstations at the main office to remote worker workstations. Any files that need to be transferred between the two sites must be stored on the Production Server and retrieved via FTP.
6. No traffic is permitted from workstations at the remote site to workstations at the main site.
7. No Telnet traffic is permitted from the remote site workstations to any devices, except their local switch.

*** VLAN Design and LAN Addressing Scheme – APPENDIX F**
*** LAN Design Test Plan – APPENDIX G**
*** LAN Testing Result and Conclusions – APPENDIX H**
*** Security Policy Access Control Lists – APPENDIX I**

IMPLEMENTATION PLAN

The FilmCompany network upgrade is to be performed as a "Phased" implementation installation to comply with the FilmCompany stated requirements:

- The company network services must be available during the upgrade. The company network services must be available during the upgrade.
- Existing equipment must be used in the new network design. Existing equipment must be used in the new network design.

This type of implementation plan will minimize downtime, security risks, and service outages to customers. It consists of the following four phases:

Phase 1 – 45 Days

Install the Distribution and Core Layer equipment.	15 days
Configure new IP addressing & VLAN scheme.	15 days
Configure routing and access control lists	5 days
Testing and Troubleshooting	10 days

Phase 2 – 18 Days

Install Server Farm devices.	5 days
Configure IP addressing and apply the needed VLANs to the Server Farm.	3 days
Configure Routing and ACLs used in the Server Farm	5 days
Testing and Troubleshooting	5 days

Phase 3 – 20 Days

Upgrade the WAN connectivity with security configured.	5 days
Extend the network to the remote site.	5 days
Configure Access Control Lists & security policies.	5 days
Testing and Troubleshooting	5 days

Phase 4 – 6 Days

Install and configure the wireless network, equipment and associated mobility using IP addressing and VLAN information from the LAN Test Plan.	3 days
Testing and Troubleshooting	3 days

- Following the implementation of the new network there will be three to five weeks of training for FilmCompany's IT. Baselines will also be recorded and documented during this period.

Network Connectivity Test Form – APPENDIX J
Timeline for Four Phases – APPENDIX K

COST PROPOSAL

Bill of Material Estimate:

Part No.	Item Description	Qty	Cost	Total Cost	Vendor	Notes
CISCO 1841	1841 Router with 64 MB flash 256-MB DRAM	1	$829.85	$829.85	Cisco	Software Support 12.3(8). Backup router
CISCO PS5855	EtherSwitch Service Module 16-ports-PoE	3	$989.48	$2968.44	Amazon	
ASA5505-SEC-BUN-K9	Cisco Security Firewall Bundle	1	$1975.12	$1975.12	Cisco	
CISCO	Intrusion Detection	1	$1842.87	$1842.87	Cisco	For Enterprise

	System (IPS)					Applications
WIC-1DSU-T1	One-Port T1 CSU/DSU WIC	1	$659.00	$659.00	Cisco	
CON-SNTP-VPKG7	Cisco SMARTnet Maintenance 1-year 24x7x4 for Cisco 1841	3	$457.00	$1371.00	Cisco	Purchase contract on same date equipment order is placed
C2960-24TT	C2960 Switch	1	$726.99 + 4yr warranty $134.99	$861.98	Cisco	Backup switch
CISCO	Catalyst Inline Power Patch Panel	3	$127.50	$382.50	Cisco	
CISCO 100BFX-SW-CP	100Base-FX Fast Ethernet Hot Swappable Card SFP	3	#229.85	$689.55	Amazon	
CISCO GLC-BX-U-AO	1X1000Base BX10 SFP Mini GBIC card	24	$564.00	$13536.00	Amazon	16 GBIC for existing switches for redundant links.
WS-X4013+10GE-RF	Cisco Supervisor Engine II-Plus-10GE	1	$7987.00	$7987.00	Cisco	Optional. Recommended for XYZ
53959KX	APC Smart-UPS 750 LCD	1	$4335.00	$4335.00	CompSource	Use for switches
SUA3000RMXL3U	APC Smart-UPS XL 3000VA 120V 3U Rack mount UPS system	1	$1423.31	$1423.31	APC	Use for routers
PWR-RPS2300	Cisco RPS 2300 Redundant Power Supply	3	$595.95	$17857.85	Commercecetel	Use for switches
PW9130L2500R-XL2U	Eaton	2	$1346.29	$2692.58	Eaton Corp.	Use for server farm

Estimated Total Hardware and Warranty:

- **Cost =** $63,412.05

Estimated Labor Cost: 650 hrs. X $100.00 /hr:

- **Cost =** $65,000.00

Recommended Anti-virus Software:

- Trend Micro Worry-Free Business Security Advanced 7
- **Cost** = $7593.00 (50 users/3 years)

Estimated Cabling Cost:

Fiber-Optic Cabling $36.50 per 100 ft. $775.00 installation & labor	**Cat6** $29.00 per 100 ft. $575.00 installation & labor
Cat5e $19.75 per 100 ft. $490.00 installation & labor	**RJ45** $1.75/ea. RJ45 $1.75/ea. RJ45 end $8.50 to install on each end $12.50 cable installation

Warranty and Maintenance Support:

Cisco 1841 Router:

Cisco Warranty	**1 Year Limited HW**
Duration	1 year
Hardware Replacement	10-day AR
Software Replacement	Media Only
TAC Technical assistance	No
OS Software Updates	No
Software Application Updates/Upgrades	No
Online Technical Resources	No
Remote Monitoring, Diagnostics, & Alerts	No

Cisco C2960-24TT Switch:

Cisco Warranty	**1 Year Limited HW**
Duration	1 year
Hardware Replacement	10-day AR
Software Replacement	Media Only
TAC Technical assistance	No
OS Software Updates	No
Software Application Updates/Upgrades	No
Online Technical Resources	No
Remote Monitoring, Diagnostics, & Alerts	No

TERMS AND SIGNATURES

This is a contract entered into by **A&J Computing Solutions** (hereinafter referred to as "the Provider") and **FilmCompany (AnyCompany)** (hereinafter referred to as "the Client") on this date, May 3, 2012.
The Provider's place of business is **64 Commons, Hwy 64E & Hwy 42S Asheboro, NC 27205** and the Client's place of business is. **1313 Mockingbird Land, Madison Heights, CA 98765**
The Client hereby engages the Provider to provide services described herein under "Scope and Manner of Services." The Provider hereby agrees to provide the Client with such services in exchange for consideration described herein under "Payment for Services Rendered."

Scope and Manner of Services

Services to Be Rendered By Provider:

1. The Provider will purchase, install, setup equipment, design new network topology utilizing all required services, test the network, setup and test all computers and printers and design and setup Frame Relay with backup routing.
2. All construction and electrical per approved final blueprint.
3. All security policies and VLAN operation configured and tested.
4. Windows 7 Professional, Office 2010 Professional, Mac OSX, Windows 2008r2 Server and any software needed for daily business purposes.
5. On-site service contract for 1 year from completion of all work, with a revolving clause to renew each year at pricing of **A&J Computing Solutions.**

Payment for Services Rendered

The Client shall pay the Provider for services rendered according to the Payment Schedule within 15 calendar days of the date on any invoice for services rendered from the Provider. Should the Client fail to pay the Provider the full amount specified in any invoice within 15 calendar days of the invoice's date, a late fee equal to 20% shall be added to the amount due and

interest of 10 percent per annum shall accrue from the 15th calendar day following the invoice's date.

Applicable Law

This contract shall be governed by the laws of the **County of Randolph** in the **State of North Carolina and State of California,** and any applicable Federal law.

Signatures

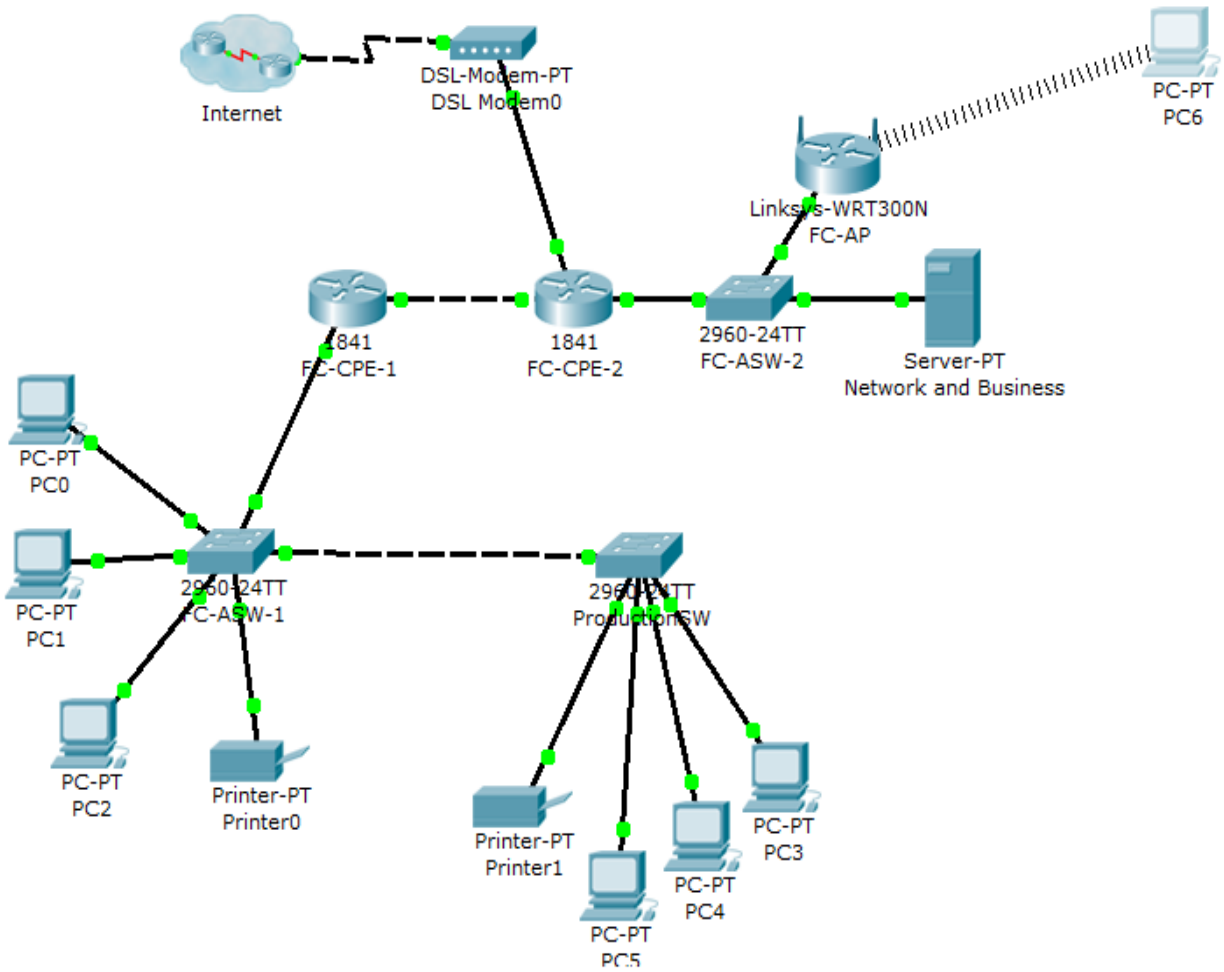
In witness of their agreement to the terms above, the parties or their authorized agents hereby affix their signatures:

_____	_____
(Printed Name of Client or agent)	(Printed Name of Provider or agent)
_____	_____
(Signature of Client or agent) (Date)	(Signature of Provider or agent) (Date)

APPENDIX A – Current Topologies

Current Physical Topology:

Current Logical Topology:



APPENDIX B – Existing Device Tables

Existing Device Tables:

Switch

Hostname: FC-ASW-1
Model: WS-2960-24TT
IOS Version: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
IP Address: Not Configured
Subnet Mask: Not Configured
Default Gateway: Not Configured

Trunk Ports	Fa0/1
Connects to Device	FC-CPE-1
Connects to Interface	Fa0/0
Local Interface Port	Fa0/2
Connects to Device	PC0
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/3
Connects to Device	PC1
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/4
Connects to Device	PC2
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/5
Connects to Device	Printer
Connects to Interface	JetDirect
Local Interface Port	Gog1/1
Connects to Device	ProductionSW
Connects to Interface	Gig1/1
Local Interface Port	
Connects to Device	
Connects to Interface	
VTP	Server Domain Name – Film Password – Not Configured
Port Security	None Listed
STP Information	Enabled Priorities – 32769 Not Root Bridge
Active Access Ports	Fa0/1 – FC-CPE-1 Fa0/2 – PC0 Fa0/3 – PC1 Fa0/4 – PC2 Fa0/5 – Printer0 Gig1/1 - ProductSW
VLAN Number	1
VLAN Name	default

2960 Switch Version Information

IOS Version: 12.2(25)
Name of the system image (IOD) file: C2960-LANBASE-M
IOS feature set: LANBASE
Date of code build: Compiled Wed 12-Oct-05 22:05 by pt_team
Type of processor board and processor: Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory
Number of Fast Ethernet interfaces: 24 FastEthernet/IEEE 802.3 interface(s)
Number of Gigabit Ethernet interfaces: 2 Gigabit Ethernet/IEEE 802.3 interface(s)
Amount of NVRAM: 32768K bytes of flash-simulated non-volatile configuration memory
Amount of flash memory: 32514048 bytes
Configure register: 0xF

Flash Information

Amount of flash memory available and used: 28098511 bytes available– 4415537 bytes used
The size of the IOS file: 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

Physical Location	MDF & POP Room
Configured with Static or Dynamic Routing	Dynamic
ACL's Used	None
Username	None
Accounts	None

Switch

Hostname: FC-ASW-2
Model: WS-C2960-24TT
IOS Version: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
IP Address: Not Configured
Subnet Mask: Not Configured
Default Gateway: Not Configured

Trunk Ports	None
Local Interface Port	Fa0/1
Connects to Device	FC-CPE-2
Connects to Interface	Fa0/0/0
Local Interface Port	Fa0/2
Connects to Device	FC-AP
Connects to Interface	Fa0/0

Local Interface Port	Fa0/3
Connects to Device	Network and Business Server
Connects to Interface	Fast Ethernet
Connects to Device	
Local Interface Port	
Connects to Interface	
Active Access Ports	Fa0/1 – FC-CPE-2 Fa0/2 – FC-AP Fa0/3 – Network and Business Server
VLAN Number	1
VLAN Name	Default
VTP	Server Domain Name – Null Password – Not Configured
Port Security	None Listed
STP Information	Enabled Priorities – 32769 Root Bridge (Only Switch)

2960 Switch Version Information

IOS Version: 12.2(25)FX
Name of the system image (IOD) file: C2960-LANBASE-M
IOS feature set: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Date of code build: Compiled Wed 12-Oct-05 22:05 by pt_team
Type of processor board and processor: Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory
Number of Fast Ethernet interfaces: 24 FastEthernet/IEEE 802.3 interface(s)
Number of Gigabit Ethernet interfaces: 2 Gigabit Ethernet/IEEE 802.3 interface(s)
Amount of NVRAM: 32768K bytes of flash-simulated non-volatile configuration memory
Amount of flash memory: 32514048 bytes
Configure register: 0xF

Flash Information

Amount of flash memory available and used: 28099127 bytes available– 4414921 bytes used
The size of the IOS file: 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

Physical Location	MDP & POP Room
Configured with Static or Dynamic Routing	Dynamic
ACL's Used	None

Username	None
Accounts	None

Switch

Hostname: ProductionSW
Model: WS-C2960-24TT
IOS Version: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
IP Address: Not Configured
Subnet Mask: Not Configured
Default Gateway: Not Configured

Trunk Ports	Gig1/1
Connects to Device	FC-ASW-1
Connects to Interface	Gig1/1
Local Interface Port	Fa0/1
Connects to Device	PC3
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/2
Connects to Device	PC4
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/3
Connects to Device	PC5
Connects to Interface	Fast Ethernet
Local Interface Port	Fa0/4
Connects to Device	Printer1
Connects to Interface	JetDirect
Local Interface Port	
Connects to Device	
Connects to Interface	
Active Access Ports	Fa0/1 – PC3 Fa0/2 – PC4 Fa0/3 – PC5 Fa0/4 – Printer1 Gig1/1 – FC-ASW-1
VLAN Number	1
VLAN Name	default

VLAN Number	10
VLAN Name	Production
VTP	Not Configured
Port Security	None Listed
STP Information	Enabled Priorities – 32778 Root Bridge (By MAC Address)

2960 Switch Version Information

IOS Version: 12.2(25)FX
Name of the system image (IOD) file: : C2960-LANBASE-M
IOS feature set: Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Date of code build: Compiled Wed 12-Oct-05 22:05 by pt_team
Type of processor board and processor: Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory
Number of Fast Ethernet interfaces: 24 FastEthernet/IEEE 802.3 interface(s)
Number of Gigabit Ethernet interfaces: 2 Gigabit Ethernet/IEEE 802.3 interface(s)
Amount of NVRAM: 32768K bytes of flash-simulated non-volatile configuration memory
Amount of flash memory: 32514048 bytes
Configure register: 0xF

Flash Information

Amount of flash memory available and used: 28098511 bytes available– 4415537 bytes used
The size of the IOS file: 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

Physical Location	Production Wiring Closet
Configured with Static or Dynamic Routing	Dynamic
ACL's Used	None
Username	None
Accounts	None

Router

Hostname: FC-AP
Model: WRT300N (Linksys)
IOS Version: N/A

Interface	Fa0/2
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Connects to Device	FC-ASW-2

Connects to Interface	Fa0/2

Router

Hostname: FC-CPE-1
Model: 1841 (Revision 5.0)
IOS Version: 12.3(14)T7

Interface	Fa0/0
IP Address	None (Has Virtual LANs)
Subnet Mask	None
Connects to Device	FC-ASW-1
Connects to Interface	Fa0/1
Interface	Fa0/1
IP Address	10.20.0.254
Subnet Mask	255.255.255.0
Connects to Device	FC-CPE-2
Connects to Interface	Fa0/0

1841Router Version Information

CISCO IOS Version: 12.3(14)T7
Name of the system Image (IOD) file: C1841-IPBASE-M
CISCO IOS feature set: IPBASE
Date of code build: 15 May 06 14:54 by pt_team
Where the router IOS image is booted from: flash:c1841-ipbase-mz.123-14.T7.bin
Type of processor board: ID: FTX0947Z18E
Amount of DRAM: 131072K bytes
Number of Ethernet interfaces: 2
Number of Serial interfaces: None (Module Capable)
Amount of NVRAM: 191K bytes
Amount of flash memory: 32768K bytes Processor Board System Flash (Read/Write)
Configuration register: 0x2102

Flash Information

The amount of flash memory available: 18682016 bytes available
The size of the IOS file: 1 13832032 c1841-ipbase-mz.123-14.T7.bin

Physical Location	MDF & POP Room
Configured with Static or Dynamic Routing	Static
ACL's Used	None
Username	None
Accounts	None
SSH	SSHV1 & SSHV2 (Not Running)

Telnet	5 VTY Connections (0,1,2,3,4 – None Open)
VLAN	VLAN1 - Shutdown

Router

Hostname: FC-CPE-2
Model: 1841 (Revision 5.0)
IOS Version: 12.3(14)T7

Interface	Fa0/0
IP Address	10.20.0.253
Subnet Mask	255.255.255.0
Connects to Device	FC-CPE-1
Connects to Interface	Fa0/1
Interface	Fa0/1
IP Address	172.16.0.2 (DHCP)
Subnet Mask	255.255.0.0
Connects to Device	DSL Modem0
Connects to Interface	Fa0
Interface	Et0/0/0
IP Address	10.40.0.254
Subnet Mask	255.255.255.0
Connects to Device	FC-ASW-2
Connects to Interface	Fa0/1

1841Router Version Information

CISCO IOS Version: 12.3(14)T7
Name of the system Image (IOD) file: C1841-IPBASE-M
CISCO IOS feature set: IPBASE
Date of code build: 15 May 06 14:54 by pt_team
Where the router IOS image is booted from: flash:c1841-ipbase-mz.123-14.T7.bin
Type of processor board: ID: FTX0947Z18E
Amount of DRAM: 131072K bytes
Number of Ethernet interfaces: 2 FastEthernet & 1 Ethernet
Number of Serial interfaces: None (Module Capable)
Amount of NVRAM: 191K bytes
Amount of flash memory: 32768K bytes Processor Board System Flash (Read/Write)
Configuration register: 0x2102

Flash Information

The amount of flash memory available: 18682016 bytes available

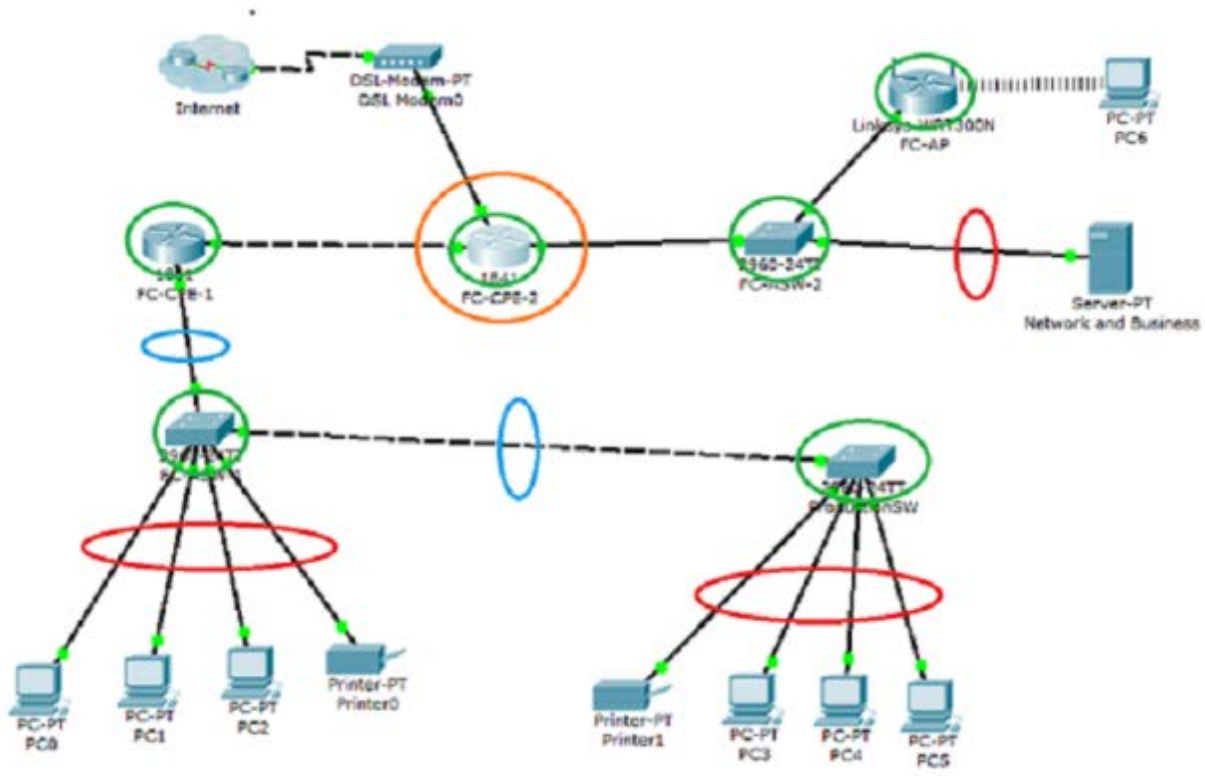
The size of the IOS file: 1 13832032 c1841-ipbase-mz.123-14.T7.bin

Physical Location	MDF & POP Room
Configured with Static or Dynamic Routing	Static
ACL's Used	None that are applied (For ip nat) (access-list 1 permit 10.0.0.0 0.255.255.255)
Username	None
Accounts	None
SSH	SSHV1 & SSHV2 (Not Running)
Telnet	5 VTY Connections (0,1,2,3,4 – None Open)
VLAN	VLAN1 - Shutdown

APPENDIX C – Strengths & Weaknesses

Strength and Weaknesses

Logical Diagram:



Legend:

- **Green**: Can Reuse Equipment (Strength)
- **Red**: Adequate Wiring (Strength)
- **Blue**: No Redundancy (Weakness)
- **Orange**: No Stated Firewall (Weakness)

APPENDIX D – Availability Strategies

Availability Strategies:

Modules and redundant power supplies to increase availability for switches:

I. **Cisco RPS2300 Redundant Power System PWR-RPS2300 for Switches 1U- $457.00**
http://www.commercetelcom.com/pwr-rps2300.html

The Cisco® Redundant Power System 2300 (RPS 2300) increases availability for converged data, voice, and video networks. The system delivers power supply redundancy and resiliency for a variety of power requirements, including Power over Ethernet (PoE). It helps ensure uninterrupted operation and protection against device power supply failures by providing seamless failover for Cisco switches like the Cisco Catalyst®2960 Series.

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps7148/ps7130/prod_bulletin0900aecd805bbf09.html

II. **Cisco EtherSwitch Service Module Switch - 16 ports –PoE- $989.48**
http://www.amazon.com/Cisco-EtherSwitch-Service-Module-NME-16ES-1G-P/dp/B0009NSH5I

Cisco® EtherSwitch® network and interface card modules are innovative solutions that can reduce total cost of ownership for customers by optionally integrating switch ports within a router. This integration allows network administrators to manage a single device utilizing the router command-line interface (CLI) for LAN and WAN management needs. This approach reduces network complexity, IT staff training needs, equipment sparing requirements, and maintenance costs.

http://www.cisco.com/en/US/prod/collateral/routers/ps5855/product_data_sheet0900aecd8028d15f.html

III. **Cisco Catalyst Inline Power Patch Panel- $127.50**
http://www.supplysale.com/Item.aspx?sku=0048366426OP&sgd=330d314d318d312d314

The Catalyst Inline Power Patch Panel enables inline power for Cisco multiservice enabled Catalyst switches. This product supports a new feature called inline power. Inline power is 48-volt DC power provided over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters. Instead of requiring wall power, terminal devices such as IP telephones can utilize power provided from the Catalyst Inline Power Patch Panel. This capability gives the network administrator centralized power control, which translates into greater network availability. By deploying Catalyst gear with uninterruptable-power-supply (UPS) systems in secured wiring closets, network administrators can ensure that building power outages will not affect network telephony connections.

The Catalyst Inline Power Patch Panel extends the features and functionality c the award-winning Catalyst family of switches.

http://www.cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet09186a00800a9ea3.html

Hot-swappable cards and controllers:

I. **Cisco 100Base-FX Fast Ethernet Hot-Swappable Card SFP- $229.85**
http://www.amazon.com/Cisco-100Base-FX-Ethernet-100BFX-SW-CP/dp/B0065P8IYE

Manufacturer Part Number: GLC
The Cisco 100BASE-FX Small Form-factor Pluggable (SFP) is a hot-swappable input/output device that plugs into a Fast Ethernet port or slot, linking the port with the network.

Specifications:
Application/Usage: Data Networking
Product Type: SFP
Data Transfer Rate: 100 Mbps
Compatibility - Switch or Module:
Catalyst 6500 Series
Catalyst 4500 Series
Cisco ME 3400
Catalyst 2960 Series
Cisco ME 2400

http://www.cisco.com/en/US/prod/collateral/modules//product_data_sheet0900aecd804e8cf6.html

II. Cisco 1X1000BASE BX10 SFP Mini GBIC- $564.00
http://www.amazon.com/Cisco-GLC-BX-D-1000BASE-BX-Sfp-1490NM/dp/B000GYI0A2

Manufacturer Part Number: GLC-BX-U-AO
ACP's industry-standard SFP is a hot-swappable input/output device that plugs into a Gigabit Ethernet slot, linking the port with the fiber-optic network

Specifications:

Application/Usage Data Networking Product Type SFP
Depth Interfaces/Ports: 1 x 1000Base-BX
Interfaces/Ports Details: 1 x LC 1000Base-BX
Data Transfer Rate: 1 Gbps Gigabit Ethernet
Connectivity Media: G.652 m Single-mode Fiber 1000Base-BX
Number of Ports/Channels: 1
Compatibility:
Cisco ME 2400
Catalyst 2960 series
Cisco ME 3400
Catalyst 3560 series
Catalyst 3750 series
Catalyst 4500 series
Catalyst 4900 series
Catalyst 6500 series

http://www.cisco.com/en/US/docs/interfaces_modules/csbna/mgb/quick_start/guide/Optical_Module_QSG_en-US.pdf

UPS devices suitable for networking devices:

I. Eaton Corporation Eaton PW9130L2500R-XL2U- $1346.29
http://www.provantage.com/eaton-pw9130l2500r-xl2u~7EPW9120.htm

Manufacturer Part Number: PW9130L2500R-XL2U
The Eaton 9130 UPS eliminates all types of utility power problems to supply clean, continuous power to connected equipment. With its rugged design, the 9130 UPS regulates both voltage and frequency to provide the highest grade of UPS protection available. Incorporating more than 40 years of UPS expertise, the 9130 UPS delivers essential power protection for rack-based IT and networking data center equipment, medical systems and manufacturing process control. It is also ideal for PBX and VoIP telecommunication equipment. The 9130 UPS is part of the Powerware series.

http://www.server-rack-online.com/pw9130l2500r-xl2u.html

II. **APC Smart-UPS 750 LCD - UPS (rack-mountable) - $4,335.00**
http://www.compsource.com/ttechnote.asp?part_no=53959KX&vid=201&src=F

Manufacturer Part Number: 5395-9KX

The IBM® 11000VA LCD 5U Rack Uninterruptible Power Supply (UPS) optimizes for both efficiency and performance, providing the right level of power protection for the moment.

Specifications:

VA/Watts rating: 11000 VA/1000 W
Nominal output voltage (Vac): 208V/230 Output: 11000 VA (normal and high efficiency modes) 5500 VA (double conversion mode) Output power capacity in watts: 10000 W (normal and high efficiency modes) 5000 W (double conversion mode) Load segments Two Output connections: Eight IEC 320 C19 Circuit breakers
Four two-pole output breakers rated at 20 A
Battery mode: 90%
Run time on batteries 100% load: 35mins

http://www-03.ibm.com/systems/x/options/rackandpower/ups11000va/

Redundant/Uninterrupted power supply option:

I. **APC Smart-UPS XL SUA3000RMXL3U 3000VA 120V 3U Rackmount UPS System- $ 1423.31**
http://www.prosecuritys.com/apc-e9sua3000rmxl3u.html

Manufacturer Part Number: SUA750RMI2U
APC Smart-UPS XL protects your data by supplying reliable, network-grade power and scalable runtime in tower or rack-mount form factors. Customers can configure up to 10 matching battery packs for runtimes exceeding 24 hours, if needed. Typical applications requiring longer runtime include critical application servers and storage, IP and PBX based voice networks, and enterprise network switches and hubs. Included PowerChute management software provides IT administrators the comfort of safe system shutdown and advanced UPS management. Additional manageability is available through the SmartSlot, an internal accessory slot that allows installation of optional accessories to enhance performance. Engineered with the same standards as the award-winning Smart-

UPS, the Smart-UPS XL adds the advantage of unsurpassed runtime capability for those business applications that demand continual uptime.

Specifications:
VA/Watts rating: 480 Watts / 750 VA
Input 230V / Output 230V
Interface Port DB-9 RS-232
SmartSlot
USB
Rack Height 2 U

http://www.apc.com/resource/include/techspec_index.cfm?base_sku=SUA3000RMXL3U

APPENDIX E – Security Strategies

Security Strategies:

The "Hardware Firewalls" and "Integrated Service Routers" to be used for security:

I. Cisco 1841 Integrated Router, Model 1841:

Features: The Cisco 1841 Integrated Services Router provides the following support:

- Wire-speed performance for concurrent services at T1/E1 WAN rates
- Enhanced investment protection through increased performance and modularity
- Enhanced investment protection through increased modularity
- Increased density through High-Speed WAN Interface Card Slots (two)
- Support for over 90 existing and new modules
- Support for majority of existing WICs, VWICs, and VICs (data mode only)
- Two Integrated 10/100 Fast Ethernet ports
- Security:
  On-board encryption
  Support of up to 800 VPN tunnels with the AIM-EPII-PLUS Module
  Antivirus defense support through Network Admission Control (NAC)
  Intrusion Prevention as well as stateful Cisco IOS Firewall support and many more essential security features

Cisco 1841 Integrated Services Router

Price: $ 829.85

II. Cisco Security Firewall Bundle, ASA5505-SEC-BUN-K9 :

Features: ASA 5500 Series adaptive security appliances are solutions that combine best-of-breed security and VPN services with the Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a core component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity.

- Connectivity technology- Wired
- Data link protocol- Ethernet, Fast Ethernet
- Network / transport protocol- IPSec
- Performance- Firewall throughput : 150 Mbps VPN throughput : 100 Mbps
- Capacity- IPSec VPN peers : 25 SSL VPN peers : 2 Concurrent sessions : 10000
- Features- Firewall protection, DMZ port, VPN support, VLAN support, wall mountable.

Price: $ 1975.12

The "Intrusion Detection System (IDS)" to be deployed in the FilmCompany project:

I. Cisco IPS AIM for 1841-2800 and 3800. Deploy network-based intrusion prevention that identifies, classifies, and stops known and unknown threats with the Cisco Intrusion Prevention System (IPS).
As an essential part of the Cisco Secure Borderless Network, Cisco IPS is one of the most widely deployed intrusion prevention systems, providing:

- Protection against more than 30,000 known threats
- Timely signature updates and Cisco Global Correlation to dynamically recognize, evaluate, and stop emerging Internet threats
-

Cisco IPS includes industry-leading research and the expertise of Cisco Security Intelligence Operations Cisco Security Intelligence Operations. Cisco IPS protects against increasingly sophisticated attacks, including:

- Directed attacks
- Worms
- Botnets
- Malware
- Application abuse

Cisco guaranteed coverage for IPS provides peace of mind with guarantees for coverage, response-time, and effectiveness for Microsoft, Cisco and critical enterprise application vulnerabilities.

Cisco IPS also helps your organization comply with government regulations and consumer privacy laws. It provides intrusion prevention that:
Stops outbreaks at the network level, before they reach the desktop

- Prevents losses from disruptions, theft, or defacement
- Collaborates with other network components, for end-to-end, network-wide intrusion prevention
- Supports a wide range of deployment options, with near-real-time updates for the most recent threats
- Decreases legal liability, protects brand reputation, and safeguards intellectual property

Price: $ 1842.87

II. Recommended Anti-virus software for the FilmCompany: Trend Micro Worry-Free Business Security Advanced 7

For businesses with mail servers, file servers, and multiple PCs and Mac computers
This single solution is designed for businesses with limited IT resources so it's easy to install and doesn't require expertise to use. The latest Advanced Edition keeps business information private by locking down USB drives and other storage devices. Also, it stops

data loss through email, blocks spam both before and on the Exchange Server, and secures both Macs and PCs.

Fast

- Identifies and blocks new and emerging threats before they impact your business
- Protects without affecting your performance or speed
- Virus scans run in the background so your computers are unaffected

Effective

- Stops viruses, spyware, spam, phishing attacks, and other web threats before they can reach your business
- Data loss prevention stops private business information from being shared via USB drives and other attached storage devices as well as in email messages
- URL filtering keeps employees from inappropriate and infected websites

Simple

- Specifically designed for businesses with limited IT staff
- Easy to install and use, no IT expertise required
- Security status at-a-glance and easy-to-read security reports

Price - $ 7593.00 (24 Month Maintenance Agreement)

APPENDIX F – Detailed VLAN & Addressing

VLAN Design and LAN Addressing Scheme:

FilmCompany VLAN Design				
VLAN Number	**Network Name**	**Number of Hosts**	**Predetermined Network Address**	**Description**
1	Default	14	192.168.3.208/28	Default VLAN for the Layer 2 devices
10	Voice	254	192.168.0.0/24	Voice VLAN to support Voice over IP
20	Management	14	192.168.3.224/28	Management hosts and secure peripherals (payroll printer)
30	Administrative	62	192.168.3.0/26	Administrative hosts
40	Support	126	192.168.1.0/25	Support hosts
50	Production	126	192.168.1.128/25	High performance production workstations (stationary)
60	Mobile	62	192.168.3.64/26	Mobile production hosts
70	Net_Admin	14	192.168.3.240/28	Network support
80	Servers	65534	172.17.0.0 /16	Servers to support video services and storage
90	Peripherals	62	192.168.3.128/26	Peripherals for general use (printers,scanners)
100	Web_Access	14	192.168.3.192/28	VLAN for servers that are publicly accessible
120	Future	126	192.168.2.0/25	VLAN for future services
999	Null	126	192.168.2.128/25	VLAN for terminating unwanted or suspicious traffic
NA	NAT Pool	6	209.165.200.224/29	Addresses for NAT pool for BR4 or interface to ISP4 (Can hit a Public Address and then translate to private address)
NA	DSL_Link	2	192.0.2.40 /30	DSL link to the ISP
NA	Frame_Link	2	172.18.0.16/30	Address of the FR link to the stadium

FilmCompany LAN Addressing Scheme				
Network Names	**Network Address**	**Lowest Host Address**	**Highest Host Address**	**Broadcast Address**
voice	192.168.0.0 /24	192.168.0.1	192.168.1.254	192.168.1.255
support	192.168.1.0 /25	192.168.1.1	192.168.1.126	192.168.1.127
production	192.168.1.128 /25	192.168.1.129	192.168.1.254	192.168.1.255
future	192.168.2.0 /25	192.168.2.1	192.168.2.126	192.168.2.127
null	192.168.2.128 /25	192.168.2.129	192.168.2.254	192.168.2.255
administrative	192.168.3.0 /26	192.168.3.1	192.168.3.62	192.168.3.63
mobile	192.168.3.64 /26	192.168.3.65	192.168.3.126	192.168.3.127
peripherals	192.168.3.128 /26	192.168.3.129	192.168.3.190	192.168.3.191
web_access	192.168.3.192 /28	192.168.3.193	192.168.3.206	192.168.3.207
default	192.168.3.208 /28	192.168.3.209	192.168.3.222	192.168.3.223
management	192.168.3.224 /28	192.168.3.225	192.168.3.238	192.168.3.239
net_admin	192.168.3.240 /28	192.168.3.241	192.168.3.254	192.168.3.255

APPENDIX G – LAN Test Plans

LAN Design Test Plan:

Test 1: Description: Basic Connectivity Test

Goals of Test:
The goal of the baseline is to verify that the test topology is up and running with the proper protocols and features.

Data to Record:
Configurations
Interface status
Routing Tables
CPU & Memory
Ping Test Output

Estimated Time:
90 minutes total
60 minutes build
30 minutes test

Test 1: Procedures

1. Build the topology according to the Design and Topology Diagram. Assign IP addresses according to the IP address plan.
2. Create a basic configuration on each device. Include applicable passwords, device names, default routes, default gateways, and activate interfaces.
3. Console into one of the devices in the topology and ping all of the other devices in the topology. Record any anomalies.
4. Telnet to each device in the configuration and verify that each is reachable.
5. Copy the output of the ***show running-config***, ***show ip route***, ***show processes cpu sorted***, ***show interfaces***, and the first few lines of ***show memory*** and paste into a document using a text editor such as Notepad. Repeat for all devices in the topology

Test 1: Expected Results and Success Criteria

1. All networking devices are connected and accessible through Telnet.
2. Hosts can ping successfully to other hosts on the network.

FilmCompany Connectivity Test				
Source (VLAN)	IP Host Source	Destination (VLAN)	IP Host Destination	Ping Test Result
Mobile (60)	192.168.3.67	Web_Access Server (100)	192.168.3.194	Successful
Mobile (60)	192.168.3.67	Management (20)	192.168.36.226	Successful
Mobile (60)	192.168.3.67	Production (50)	192.168.1.130	Successful
Mobile (60)	192.168.3.67	Support (40)	192.168.1.2	Successful
Mobile (60)	192.168.3.67	Net_Admin (70)	192.168.3.242	Successful
Mobile (60)	192.168.3.67	Video Server (80)	172.17.0.2	Successful
Administrative (30)	192.168.3.2	Web_Access Server (100)	192.168.3.194	Successful
Administrative (30)	192.168.3.2	Production Staff (50)	192.168.1.131	Successful
Administrative (30)	192.168.3.2	Mobile (60)	192.168.3.67	Successful
Administrative (30)	192.168.3.2	Production Staff_ (50)	192.168.1.132	Successful
Administrative (30)	192.168.3.2	Management (20)	192.168.3.226	Successful
Support (40)	192.168.1.2	Video Server (80)	172.17.0.2	Successful
Support (40)	192.168.1.2	Net_Admin (70)	192.168.3.242	Successful
Support (40)	192.168.1.2	Mobile (60)	192.168.3.67	Successful
Support (40)	192.168.1.2	Production Staff (50)	192.168.1.131	Successful
Net_Admin (70)	192.168.3.242	Web_Access Server (100)	192.168.3.194	Successful
Net_Admin (70)	192.168.3.242	Mobile (60)	192.168.3.67	Successful
Net_Admin (70)	192.168.3.242	Management (20)	192.168.3.226	Successful
Net_Admin (70)	192.168.3.242	Production Staff (50)	192.168.1.131	Successful
Production Staff (50)	192.168.1.131	Web_Access Server (100)	192.168.3.194	Successful
Production Staff (50)	192.168.1.131	Support (40)	192.168.1.2	Successful
Production Staff (50)	192.168.1.131	Video Server (80)	172.17.0.2	Successful
Production Staff (50)	192.168.1.131	Mobile (60)	192.168.3.67	Successful
Web_Access Server (100)	192.168.3.194	Production Staff_ (50)	192.168.1.132	Successful
Web_Access Server (100)	192.168.3.194	Support (40)	192.168.1.2	Successful
Web_Access Server (100)	192.168.3.194	Administrative (30)	192.168.3.2	Successful
Web_Access Server (100)	192.168.3.194	Video Server (80)	172.17.0.2	Successful

Test 2: Description: VLAN Configuration Test

Test the configuration of VLANs and VTP. Test the creation of separate networks for the different groups at the FilmCompany. Demonstrate that VLANs will isolate traffic.

Data to Record:
VLAN Configurations
STP Configuration
CPU & Memory
Ping Test Output

Estimated Time:

60 minutes total
30 minutes configure
30 minutes test

Test 2: Procedures

1. Telnet or console to each switch in the configuration.
2. Create VLANs according to the VLAN plan.
3. Create trunk links between the switches.
4. Configure a switch to be the root bridge (FC-ASW-1).
5. Start a log file and record the output of the ***show*** commands.
6. Configure both PC's with the appropriate IP addresses for one of the VLANs.
7. Configure the ports attached to the PC's to be members of the same VLAN.
8. Ping one PC from the other PC and record the results.
9. Configure the ports attached to the PC's to be members of different VLANs.
10. Configure the PC's with the appropriate IP addresses for the VLANs.
11. Ping one PC from the other PC and record the results.

Test 2: Expected Results and Success Criteria

VLANs will exist on all of the switches. PCs in the same VLANs will communicate over the trunk links, PCs in different VLANs will not be able to communicate with each other.

Test 3: Description: VLAN Routing Test

Goals of Test:
Test the routing between VLANs. Test that the router is correctly configured to route between VLANs.

Data to Record:
Router Configuration
IP Routing Table Information
CPU & Memory
Ping Test Output

Estimated Time:
20 minutes total
10 minutes configure
10 minutes test

Test 3: Procedure

1. Console or telnet to the router in the configuration.
2. Create an 802.1q trunk link between the router BR4 and the attached switch FC-ASW-1.
3. Verify the operations of the trunk link.
4. Configure the IP addresses on the router sub-interfaces for the appropriate VLANs.

5. Configure the static routes to route between the VLANs.
6. Start a log file. Record the output of the show running-configuration, show interfaces, and show ip route commands on the router.
7. Record the output of the ***show running-configuration, show interfaces***, and ***show ip route*** commands on the router in a text file using a text editing program such as Notepad.
8. Configure the ports attached to the PCs to be members of different VLANs.
9. Configure the PCs with the appropriate IP addresses for the VLANs.
10. Ping PCs on same VLAN from the other PC's on the same VLAN. Record the results.
11.

Test 3: Expected Results and Success Criteria

Router is correctly configured to route between VLAN's, and a PC in one VLAN can successfully ping a PC in another VLAN.

APPENDIX H – LAN & WAN Testing Results

LAN Testing Result and Conclusions:

LAN

FC-ASW-1 (C2960-24TT)

Show VLAN Brief for FC-ASW-1

```
FC-ASW-1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
--
1    default                          active    Fa0/24
20   VLAN0020                         active    Fa0/4, Fa0/5, Fa0/6
30   VLAN0030                         active    Fa0/7, Fa0/8, Fa0/9
40   VLAN0040                         active    Fa0/10, Fa0/11, Fa0/12
50   VLAN0050                         active    Fa0/13, Fa0/14
60   VLAN0060                         active
70   VLAN0070                         active    Fa0/15, Fa0/16, Fa0/17
80   VLAN0080                         active    Fa0/18, Fa0/19, Fa0/20
100  VLAN0100                         active    Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Show Running Configuration for FC-ASW-1

```
FC-ASW-1#sh run
Building configuration...

Current configuration : 2572 bytes
!
```

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname FC-ASW-1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1,20,30,40,50,60,70,80,100 priority 4096
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.4373.3E34
!
interface FastEthernet0/5
 switchport access vlan 20
!
interface FastEthernet0/6
 switchport access vlan 20
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.21DD.815E
!
interface FastEthernet0/11
 switchport access vlan 40
!
interface FastEthernet0/12
 switchport access vlan 40
!
interface FastEthernet0/13
 switchport access vlan 50
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.A342.AA68
!
interface FastEthernet0/14
```

```
 switchport access vlan 50
!
interface FastEthernet0/15
 switchport access vlan 70
!
interface FastEthernet0/16
 switchport access vlan 70
!
interface FastEthernet0/17
 switchport access vlan 70
!
interface FastEthernet0/18
 switchport access vlan 80
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0010.11A1.A29A
!
interface FastEthernet0/19
 switchport access vlan 80
!
interface FastEthernet0/20
 switchport access vlan 80
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.0FDD.CC15
!
interface FastEthernet0/22
 switchport access vlan 100
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 192.168.3.210 255.255.255.240
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
end


FC-ASW-1#
```

Show VTP Status for FC-ASW-1

```
FC-ASW-1#sh vtp status
VTP Version                     : 2
Configuration Revision          : 8
```

```
Maximum VLANs supported locally : 255
Number of existing VLANs        : 13
VTP Operating Mode              : Server
VTP Domain Name                 : filmcompany
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x15 0xCB 0x86 0x45 0x04 0xB6 0x48 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:18
Local updater ID is 192.168.3.210 on interface Vl1 (lowest numbered VLAN
interface found)
FC-ASW-1#
```

Show Spanning Summary for FC-ASW-1

```
FC-ASW-1#sh spanning summary
Switch is in rapid-pvst mode
Root bridge for: default VLAN0020 VLAN0030 VLAN0040 VLAN0050 VLAN0060
VLAN0070 VLAN0080 VLAN0100
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      5         0        0          3          8
VLAN0020                      4         0        0          4          8
VLAN0030                      5         0        0          3          8
VLAN0040                      4         0        0          4          8
VLAN0050                      4         0        0          4          8
VLAN0060                      5         0        0          3          8
VLAN0070                      5         0        0          3          8
VLAN0080                      4         0        0          4          8
VLAN0100                      4         0        0          4          8

---------------------- -------- --------- -------- ---------- ----------
9 vlans                      40         0        0         32         72
```

FC-ASW-2 (C2960-24TT)

Show VLAN Brief for FC-ASW-2

```
FC-ASW-2#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
--
1    default                          active    Fa0/1
20   VLAN0020                         active    Fa0/4, Fa0/5, Fa0/6
30   VLAN0030                         active    Fa0/7, Fa0/8, Fa0/9
40   VLAN0040                         active    Fa0/10, Fa0/11, Fa0/12
50   VLAN0050                         active    Fa0/13, Fa0/14
60   VLAN0060                         active    Fa0/24
70   VLAN0070                         active    Fa0/15, Fa0/16, Fa0/17
80   VLAN0080                         active    Fa0/18, Fa0/19, Fa0/20
100  VLAN0100                         active    Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
```

```
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Show Running Configuration for FC-ASW-2

```
FC-ASW-2#sh run
Building configuration...

Current configuration : 2051 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname FC-ASW-2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
spanning-tree mode rapid-pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
!
interface FastEthernet0/6
 switchport access vlan 20
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0030.A375.AC92
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 40
!
interface FastEthernet0/11
 switchport access vlan 40
!
interface FastEthernet0/12
 switchport access vlan 40
!
interface FastEthernet0/13
 switchport access vlan 50
```

```
!
interface FastEthernet0/14
 switchport access vlan 50
!
interface FastEthernet0/15
 switchport access vlan 70
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.8545.908A
!
interface FastEthernet0/16
 switchport access vlan 70
!
interface FastEthernet0/17
 switchport access vlan 70
!
interface FastEthernet0/18
 switchport access vlan 80
!
interface FastEthernet0/19
 switchport access vlan 80
!
interface FastEthernet0/20
 switchport access vlan 80
!
interface FastEthernet0/21
 switchport access vlan 100
!
interface FastEthernet0/22
 switchport access vlan 100
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
 switchport access vlan 60
!
interface Vlan1
 ip address 192.168.3.211 255.255.255.240
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
end
```

Show VTP Status for FC-ASW-2

```
FC-ASW-2# sh vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 13
VTP Operating Mode              : Client
VTP Domain Name                 : filmcompany
```

```
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x15 0xCB 0x86 0x45 0x04 0xB6 0x48 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:18
```

Show Spanning Summary for FC-ASW-2

```
FC-ASW-2#sh spanning summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      4         0        0          1          5
VLAN0020                      4         0        0          1          5
VLAN0030                      3         0        0          2          5
VLAN0040                      4         0        0          1          5
VLAN0050                      4         0        0          1          5
VLAN0060                      3         0        0          2          5
VLAN0070                      3         0        0          2          5
VLAN0080                      4         0        0          1          5
VLAN0100                      4         0        0          1          5

---------------------- -------- --------- -------- ---------- ----------
9 vlans                      33         0        0         12         45
```

ProductionSW (C2960-24TT)

Show VLAN Brief for ProductionSW

```
ProductionSW#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
--
1    default                          active    Fa0/1, Fa0/24
20   VLAN0020                         active    Fa0/4, Fa0/5, Fa0/6
30   VLAN0030                         active    Fa0/7, Fa0/8, Fa0/9
40   VLAN0040                         active    Fa0/10, Fa0/11, Fa0/12
50   VLAN0050                         active    Fa0/13, Fa0/14
60   VLAN0060                         active
70   VLAN0070                         active    Fa0/15, Fa0/16, Fa0/17
80   VLAN0080                         active    Fa0/18, Fa0/19, Fa0/20
100  VLAN0100                         active    Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Show Running Configuration for ProductionSW

```
ProductionSW#sh run
Building configuration...

Current configuration : 2028 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ProductionSW
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
spanning-tree mode rapid-pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
!
interface FastEthernet0/6
 switchport access vlan 20
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 40
!
interface FastEthernet0/11
 switchport access vlan 40
!
interface FastEthernet0/12
 switchport access vlan 40
!
interface FastEthernet0/13
 switchport access vlan 50
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.B073.DBDD
!
interface FastEthernet0/14
 switchport access vlan 50
 switchport mode access
```

```
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.F979.D0C0
!
interface FastEthernet0/15
 switchport access vlan 70
!
interface FastEthernet0/16
 switchport access vlan 70
!
interface FastEthernet0/17
 switchport access vlan 70
!
interface FastEthernet0/18
 switchport access vlan 80
!
interface FastEthernet0/19
 switchport access vlan 80
!
interface FastEthernet0/20
 switchport access vlan 80
!
interface FastEthernet0/21
 switchport access vlan 100
!
interface FastEthernet0/22
 switchport access vlan 100
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 192.168.3.212 255.255.255.240
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Show VTP Status for ProductionSW

```
ProductionSW#sh vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 13
VTP Operating Mode              : Client
VTP Domain Name                 : filmcompany
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x15 0xCB 0x86 0x45 0x04 0xB6 0x48 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:18
```

Show Spanning Summary for ProductionSW

```
ProductionSW#sh spanning summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      2         0        0          2          4
VLAN0020                      2         0        0          2          4
VLAN0030                      2         0        0          2          4
VLAN0040                      2         0        0          2          4
VLAN0050                      0         0        0          4          4
VLAN0060                      2         0        0          2          4
VLAN0070                      2         0        0          2          4
VLAN0080                      2         0        0          2          4
VLAN0100                      2         0        0          2          4

---------------------- -------- --------- -------- ---------- ----------
9 vlans                      16         0        0         20         36
```

WAN

BR4 (Cisco 1841)

Show Running Configuration for BR4

```
BR4#sh run
Building configuration...

Current configuration : 1996 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BR4
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!

!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.3.209 255.255.255.240
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.3.225 255.255.255.240
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.192
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.1.1 255.255.255.128
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.1.129 255.255.255.128
!
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.3.65 255.255.255.192
!
interface FastEthernet0/0.70
 encapsulation dot1Q 70
 ip address 192.168.3.241 255.255.255.240
!
interface FastEthernet0/0.80
 encapsulation dot1Q 80
 ip address 172.17.0.1 255.255.0.0
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 192.168.3.193 255.255.255.240
!
interface FastEthernet0/1
 ip address 172.18.0.26 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 description primary link to Edge2
 no ip address
 encapsulation frame-relay
!
interface Serial0/0/0.100 point-to-point
 ip address 172.18.0.18 255.255.255.252
 frame-relay interface-dlci 100
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 network 172.18.0.0
 network 192.168.0.0
```

```
 network 192.168.0.0 0.0.3.255
 no auto-summary
!
ip classless
ip route 172.18.3.0 255.255.255.0 172.18.0.25 130
!
!
no cdp run
!
banner motd ^CUnauthorized use prohibited^C
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
end
```

ISP-X (Cisco 1841)

Show Running Configuration for ISP-X

```
ISP-X#sh run
Building configuration...

Current configuration : 808 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP-X
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
 description link to Edge2
 ip address 172.18.0.21 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description link to BR4
 ip address 172.18.0.25 255.255.255.252
 duplex auto
 speed auto
!
```

```
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.0.0 255.255.252.0 FastEthernet0/1
ip route 172.18.3.0 255.255.255.0 FastEthernet0/0
!
!
banner motd ^CUnauthorized use Prohibited^C
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
end
```

Edge2 (Cisco 1841)

Show Running Configuration for Edge2

```
Edge2#sh run
Building configuration...

Current configuration : 1058 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Edge2
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
 ip address 172.18.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.18.0.22 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 description primary link to BR4
 no ip address
 encapsulation frame-relay
!
```

```
interface Serial0/0/0.110 point-to-point
 ip address 172.18.0.17 255.255.255.252
 frame-relay interface-dlci 110
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 network 172.18.0.0
 no auto-summary
!
ip classless
ip route 192.168.0.0 255.255.252.0 172.18.0.21 130
!
!
banner motd ^CUnauthorized us Prohibited^C
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
!
End
```

APPENDIX I – Security & ACLs

Security Policy Access Control Lists:

I. **Security Policy 1:**

Remote users must be able to access the Production Server to view their schedules over the web and to enter new orders.

Firewall Rule:

Permit users on the 10.1.1.0/24 access to the Production Server (172.17.1.1) on TCPport 80.

Access List statement(s):

(access-list #) permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 80

Access List placement:

Inbound on router SR1 Fa0/1 (remember that extended ACLs should beplaced close as possible to the **source** of the traffic).

ACL Application:

SR1
en
conf t
int fa0/1
ip access-group (#) in

II. Security Policy 2:

Remote users must be able to FTP files to and from the Production Server.

Firewall Rule:

Permit users on the 10.1.1.0/24 access to the Production Server (172.17.1.1) on TCPports 20 and 21.

Access List statement(s):

(access-list #) permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 20
(access-list #) permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 21

Access List placement: Inbound on router SR1 Fa0/1

ACL Application:

SR1
en
conf t
int fa0/1
ip access-group (#) in

III. Security Policy 3:

Remote users can use the Production Server to send and retrieve email using IMAPand SMTP protocols.

Firewall Rule:

Permit users on the 10.1.1.0/24 access to the Production Server (172.17.1.1) on TCPports 143 and 25

Access List statement(s):

(access-list #) permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 25
(access-list #) permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 143

Access List placement: Inbound on router SR1 Fa0/1

ACL Application:

SR1
en
conf t
int fa0/1
ip access-group (#) in

IV. Security Policy 4

Remote users must not be able to access any other services available on theProduction Server

Firewall Rule:

Deny all other IP protocols between users on the 10.1.1.0/24 network to theProduction Server (172.17.1.1)

Access List statement(s):

(access-list #) deny ip 10.1.1.0 0.0.0.255 host 172.17.1.1

Access List placement: Inbound on router SR1 Fa0/1

ACL Application:

SR1
en
conf t
int fa0/1
ip access-group (#) in

V. Security Policy 5:

No traffic is permitted from individual workstations at the main office to remote workerworkstations. Any files that need to be transferred between the two sites must be stored on theProduction Server and retrieved via FTP.

Firewall Rule:

Deny all IP protocols from users on the 10.3.1.0/24 to the 10.1.1.0/24 network.

Access List statement(s):

(access-list #) deny ip 10.3.1.0 0.0.0.255 10.1.1.0 0.0.0.255

Access List placement: Inbound on router BR4 Fa0/1

ACL Application:

BR4
en
conf t
int fa0/1
ip access-group (#) in

VI. Security Policy 6:

No traffic is permitted from workstations at the remote site to workstations at the mainsite.

Firewall Rule:

Deny all IP protocols from users on the 10.1.1.0/24 to the 10.3.1.0/24 network.

Access List statement(s):

(access-list #) deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255

Access List placement: Inbound on router SR1 Fa0/1

ACL Application:
SR1
en
conf t
int fa0/1
ip access-group (#) in

VII. Security Policy 7:

No Telnet traffic is permitted from the remote site workstations to any devices,except their local switch.

Firewall Rule:
Deny all TCP traffic from users on the 10.1.1.0/24 network on port 23.

Access List statement(s):
(access-list #) deny tcp 10.1.1.0 0.0.0.255 any eq 23

Access List placement: Inbound on router SR1 Fa0/1

ACL Application:
SR1
en
conf t
int fa0/1
ip access-group (#) in

VIII. Extended ACLs for FilmCompany

Placement: Inbound on router SR1 Fa0/1
Inbound on router BR4 Fa0/1

Access Control List Statements

Placed on SR1, Interface: Fa0/1,Direction: Inbound:

access-list 100 permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 80
access-list 100 permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 20
access-list 100 permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 21
access-list 100 permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 25
access-list 100 permit tcp 10.1.1.0 0.0.0.255 host 172.17.1.1 eq 143
access-list 100 deny ip 10.1.1.0 0.0.0.255 host 172.17.1.1
access-list 100 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
access-list 100 deny tcp 10.1.1.0 0.0.0.255 any eq 23

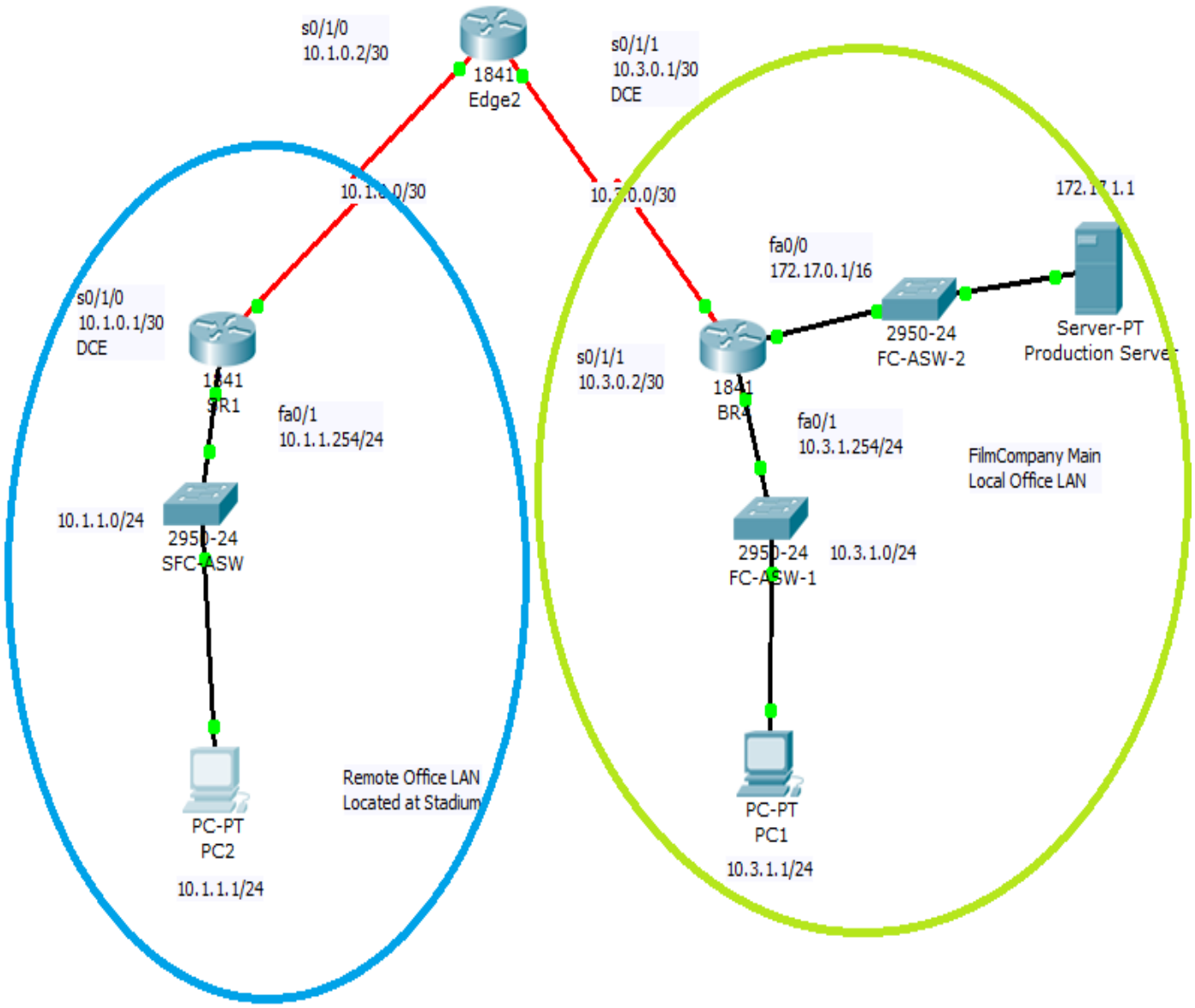
ACL Application:
SR1
en
conf t
int fa0/1
ip access-group 100 in

Access Control ListStatements

Placed on BR4,Interface: Fa0/1,Direction: Inbound:
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 101 permit ip any any

ACL Application:
BR4
en
conf t
int fa0/1
ip access-group 101 in

Logical Diagram ACLs



APPENDIX J – Connectivity Test Form

FilmCompany Connectivity Test				
Source (VLAN)	**IP Host Source**	**Destination (VLAN)**	**IP Host Destination**	**Ping Test Result**
Mobile (60)	192.168.3.67	Web_Access Server (100)	192.168.3.194	
Mobile (60)	192.168.3.67	Management (20)	192.168.36.226	
Mobile (60)	192.168.3.67	Production (50)	192.168.1.130	
Mobile (60)	192.168.3.67	Support (40)	192.168.1.2	
Mobile (60)	192.168.3.67	Net_Admin (70)	192.168.3.242	
Mobile (60)	192.168.3.67	Video Server (80)	172.17.0.2	
Administrative (30)	192.168.3.2	Web_Access Server (100)	192.168.3.194	
Administrative (30)	192.168.3.2	Production Staff (50)	192.168.1.131	
Administrative (30)	192.168.3.2	Mobile (60)	192.168.3.67	
Administrative (30)	192.168.3.2	Production Staff_ (50)	192.168.1.132	
Administrative (30)	192.168.3.2	Management (20)	192.168.3.226	
Support (40)	192.168.1.2	Video Server (80)	172.17.0.2	
Support (40)	192.168.1.2	Net_Admin (70)	192.168.3.242	
Support (40)	192.168.1.2	Mobile (60)	192.168.3.67	
Support (40)	192.168.1.2	Production Staff (50)	192.168.1.131	
Net_Admin (70)	192.168.3.242	Web_Access Server (100)	192.168.3.194	
Net_Admin (70)	192.168.3.242	Mobile (60)	192.168.3.67	
Net_Admin (70)	192.168.3.242	Management (20)	192.168.3.226	
Net_Admin (70)	192.168.3.242	Production Staff (50)	192.168.1.131	
Production Staff (50)	192.168.1.131	Web_Access Server (100)	192.168.3.194	
Production Staff (50)	192.168.1.131	Support (40)	192.168.1.2	
Production Staff (50)	192.168.1.131	Video Server (80)	172.17.0.2	
Production Staff (50)	192.168.1.131	Mobile (60)	192.168.3.67	
Web_Access Server (100)	192.168.3.194	Production Staff_ (50)	192.168.1.132	
Web_Access Server (100)	192.168.3.194	Support (40)	192.168.1.2	
Web_Access Server (100)	192.168.3.194	Administrative (30)	192.168.3.2	
Web_Access Server (100)	192.168.3.194	Video Server (80)	172.17.0.2	

APPENDIX K - Timeline for Four Phases

:

Task Name	Duration	Start	Finish	Assigned To
Phase 1 - FilmCompany	20 days	Thu 5/3/12	Wed 5/30/12	
Upgrade the WAN connectivity with security configured	5 days	Thu 5/3/12	Wed 5/9/12	John, Allen
Extend the network to the remote site	5 days	Thu 5/10/12	Wed 5/16/12	John, Allen
Configure Access Control Lists & security policies	5 days	Thu 5/17/12	Wed 5/23/12	John, Allen
Testing and Troubleshooting	5 days	Thu 5/24/12	Wed 5/30/12	John, Allen
Phase 2 - FilmCompany	18 days	Thu 5/31/12	Mon 6/25/12	
Install Server Farm devices.	5 days	Thu 5/31/12	Wed 6/6/12	John, Allen
Configure IP addressing and apply the needed VLANs to the Server Farm	3 days	Thu 6/7/12	Mon 6/11/12	John, Allen
Configure Routing and ACLs used in the Server Farm	5 days	Tue 6/12/12	Mon 6/18/12	John, Allen
Testing and Troubleshooting	5 days	Tue 6/19/12	Mon 6/25/12	John, Allen
Phase 3 - FilmCompany	20 days	Tue 6/26/12	Mon 7/23/12	
Upgrade the WAN connectivity with security configured	5 days	Tue 6/26/12	Mon 7/2/12	John, Allen
Extend the network to the remote site	5 days	Tue 7/3/12	Mon 7/9/12	John, Allen
Configure Access Control Lists & security policies	5 days	Tue 7/10/12	Mon 7/16/12	John, Allen
Testing and Troubleshooting	5 days	Tue 7/17/12	Mon 7/23/12	John, Allen
Phase 4 - FilmCompany	6 days	Tue 7/24/12	Tue 7/31/12	
Install and configure	3 days	Tue 7/24/12	Thu 7/26/12	John,

the wireless network, equipment and associated mobility using IP addressing and VLAN information from the LAN Test Plan				Allen
Testing and Troubleshooting	3 days	Fri 7/27/12	Tue 7/31/12	John, Allen

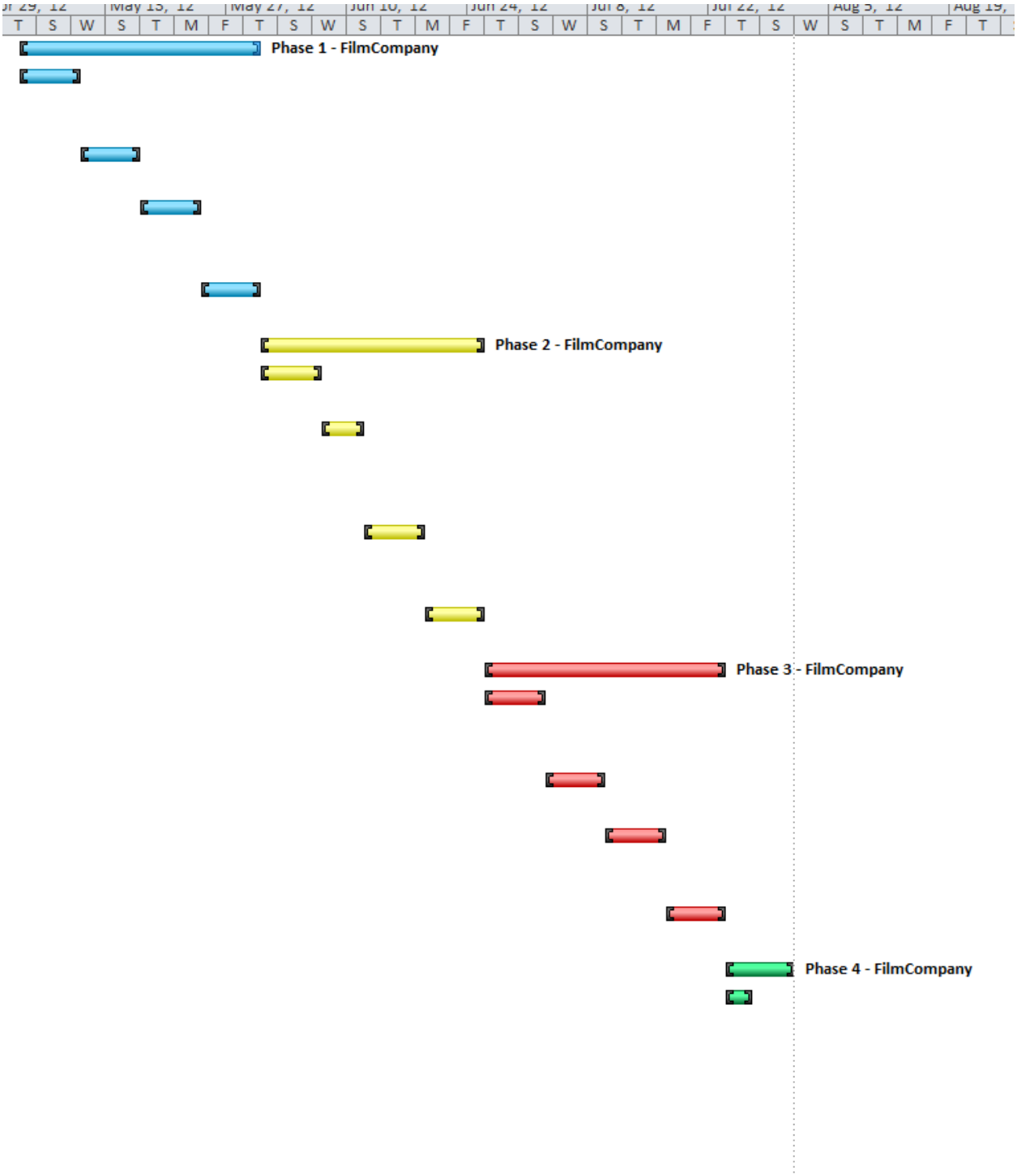


Table Legend:

Step/Phase	Color
Phase 1	Blue
Phase 2	Yellow
Phase 3	Red
Phase 4	Green