PLANNING FOR A WEB CAST

Four Months before the event:

1. How many cameras/angles will you web cast?
2. Will you web cast live audio, or a prerecorded music track?
3. Will the event also be recorder for future viewing?
4. What quality of video is expected?
5. Determine & diagram basic camera layout.
6. Determine what equipment & services are required to web cast.
7. What internet connection is available at the venue?

Three to Four Months before event:

1. Write formal letters requesting permission/changes to venue's network.
2. Start designing signs & website for the event.
3. Start gathering required equipment.

Two Months before event:

1. All major equipment should be obtained by now.
2. Setup equipment and run through a test web cast (Intranet).
3. Purchase domain name & setup DNS records.
4. Go live with website.

Six Weeks before event:

1. Make list of volunteer positions needed for the web cast & start filling them.
    a. Webmaster
    b. Web cast monitoring position
    c. Camera crew
    d. Sound Tech. (Audio Mixing/Level Control)
2. Distribute Flyers.

One Month before event:

1. Send reminder email about the required setting changes to the venue's network.
2. All equipment should be obtained at this time.

Two to Three Days before event:

1. Setup and do a final test web cast.
2. Prepare volunteers for their part in the web cast.
3. Creates Ghost image backups of all servers.

use MMS to stream content to computers running Windows Media Player for Windows® XP or earlier. You can implement MMS through the WMS MMS Server Control Protocol plug-in in Windows Media Services Administrator. This plug-in is enabled by default.

Using HTTP

- If ports on your firewall cannot be opened, Windows Media® Services can stream content by using Hypertext Transfer Protocol (HTTP) over port 80. HTTP can be used to deliver streams to all Windows Media Player versions. You can implement HTTP through the WMS HTTP Server Control Protocol plug-in in Windows Media Services Administrator. This plug-in is not enabled by default. If another service, such as Internet Information Services (IIS), is using port 80 on the same IP address, you cannot enable the plug-in. For more information about HTTP streaming concurrently with other services, see Windows Media Services Help.

- HTTP can also be used to do the following:
    - Distribute streams between Windows Media servers.
    - Source content from Windows Media encoder.
    - Download dynamically generated playlists from a Web server.

Data source plug-ins must be configured in Windows Media Services Administrator to support these additional HTTP streaming scenarios. For more information, see Windows Media Services Help.

About Protocol Rollover

If clients that support RTSP connect to a server running Windows Media® Services using an RTSP URL moniker (for example, rtsp://) or an MMS URL moniker (for example, mms://), the server uses protocol rollover to stream the content to the client to provide an optimal streaming experience. Automatic protocol rollover from RTSP/MMS to RTSP with UDP-based or TCP-based transports (RTSPU or RTSPT), or even HTTP (if the WMS HTTP Server Control Protocol plug-in is enabled) may occur as the server tries to negotiate the best protocol and provide an optimal streaming experience for the client. Clients that support RTSP include Windows Media Player 9 Series or later or other players that use the Windows Media Player 9 Series ActiveX control.

Earlier versions of Windows Media Player, such as Windows Media Player for Windows XP, do not support the RTSP protocol. However, the MMS protocol also provides protocol rollover support for these clients. Thus, when an earlier version of the Player attempts to connect to the server using an MMS URL moniker, automatic protocol rollover from MMS to MMS with UDP-based or TCP-based transports (MMSU or MMST), or even HTTP (if the WMS HTTP Server Control Protocol plug-in is enabled), may occur as the server tries to negotiate the best protocol and provide an optimal streaming experience for these clients.

To make sure that your content is available to all clients that connect to your server, ports on your firewall must be opened for all of the connection protocols that might be used during protocol rollover.

You can force your Windows Media server to use a specific protocol by identifying the protocol to be used in the announcement file (for example, rtspu://*server*/*publishing_point*/*file*). However, to provide an optimal streaming experience for all client versions, we recommend that the URL use the general MMS protocol. If clients connect to your stream using a URL with an MMS URL moniker, any necessary protocol rollover occurs automatically. Be aware that users can disable streaming protocols in the property settings of Windows Media Player. If a user disables a protocol, it is skipped during rollover. For example, if HTTP is disabled, then URLs will not roll over to HTTP.

Allocating Ports for Windows Media Services

- Most firewalls are used to control "inbound traffic" to the server; they generally do not control "outbound traffic" to clients. However, ports in your firewall for outbound traffic may be closed if a more stringent security policy is

implemented on your server network. This section describes the default port allocation for Windows Media® Services for both inbound and outbound traffic (shown as "In" and "Out" in the tables) so that you can configure all ports as needed.

In some scenarios, outbound traffic may be directed to one port in a range of available ports. Port ranges shown in the tables indicate the entire range of available ports; however, you can allocate fewer ports within the port range. When deciding how many ports to open, balance security with accessibility by opening just enough ports to allow all clients to make a connection. As a starting point, determine how many ports you expect to use for Windows Media Services and then open 10 percent more to account for overlap with other programs. After you've established this number, monitor your traffic to determine if adjustments are necessary.

Port range restrictions potentially affect all remote procedure call (RPC) and Distributed Component Object Model (DCOM) applications that share the system, not just Windows Media Services. If the allocated port range is not broad enough, competing services such as IIS may fail with random errors. The port range must be able to accommodate all potential system applications that use RPC, COM, or DCOM services.

To make firewall configuration easier, you can configure each server control protocol plug-in (RTSP, MMS, and HTTP) in Windows Media Services Administrator to use a specific port. If your network administrator has already opened a series of ports for use by your Windows Media server, you can allocate those ports to the control protocols accordingly. If not, you can ask the network administrator to open the default ports for each protocol. If opening ports on your firewall is not possible, Windows Media Services can stream content by using the HTTP protocol over port 80. For more information, see the Windows Media Services Help.

Delivering a unicast stream

Application Protocol	Protocol	Port	Description
RTSP	TCP	554 (In/Out)	Used for accepting incoming RTSP client connections and for delivering data packets to clients that are streaming by using RTSPT.
RTSP	UDP	5004 (Out)	Used for delivering data packets to clients that are streaming by using RTSPU.
RTSP	UDP	5005 (In/Out)	Used for receiving packet loss information from clients and providing synchronization information to clients that are streaming by using RTSPU.
MMS	TCP	1755 (In/Out)	Used for accepting incoming MMS client connections and for delivering data packets to clients that are streaming by using MMST.
MMS	UDP	1755 (In/Out)	Used for receiving packet loss information from clients and providing synchronization information to clients that are streaming by using MMSU.
MMS	UDP	1024-5000 (Out)	Used for delivering data packets to clients that are streaming by using MMSU. Open only the necessary number of ports.
HTTP	TCP	80 (In/Out)	Used for accepting incoming HTTP client connections and for delivering data packets to clients that are streaming by using HTTP.

To make sure that your content is available to all client versions that connect to your server, open all ports described in the table for all of the connection protocols that might be used during protocol rollover. If you are running Windows Media Services on a computer that is running Windows Server™ 2003 Service Pack 1 (SP1), you should add the Windows Media Services program (wmserver.exe) as an exception in Windows Firewall to open the default inbound ports for unicast streaming, rather than opening ports in the firewall manually. For more information, see Using Windows Firewall.

Streaming from an encoder

Application Protocol	Protocol	Port	Description
HTTP	TCP	8080 (In) 1-65535 (Out)	The Windows Media® server uses the TCP In port to accept the incoming encoder connection when the encoder "pushes" the stream to the server. The Windows Media server uses the TCP Out port value that is specified in the encoder to "pull" the stream from the encoder. Port 8080 is used by default.

A Windows Media server can be configured to stream live content directly from an encoder source. For a broadcast publishing point to stream a live encoding session, the content path must be set so that the encoder "pushes" the content through the firewall to the server or the server "pulls" the content through the firewall from the encoder.

When pushing a stream, the encoder initiates an HTTP connection with the server through port 8080. On the other hand, when pulling the stream from the encoder, the server initiates the connection, and port configuration for the outbound port is usually not required unless the encoder administrator specifies a different port (other than port 8080). If a different port is used, you must specify the same port when you identify the encoder connection URL for the Windows Media server and when opening the port on your firewall.

If the encoder is pushing the content, the WMS HTTP Server Control Protocol plug-in must be enabled in Windows Media Services Administrator so that the encoder can successfully connect to the server. If you are pulling the stream from the encoder, set the publishing point path to reference the URL of the encoder from which you want to stream content (for example, http://*encoder*:*port*).

Distributing content

Application Protocol	Protocol	Port	Description
RTSP	TCP	554 (Out)	The Windows Media distribution server uses this TCP Out port to establish an RTSP connection to the origin server.
RTSP	UDP	1024-5000 (In)	The Windows Media distribution server uses a port within this UDP In port range to receive data packets from the origin server.
RTSP	UDP	5005 (Out)	The Windows Media distribution server uses this UDP Out port to send correction-oriented control messages to the origin server.
HTTP	TCP	80 (Out)	The Windows Media distribution server uses this TCP Out port to establish an HTTP connection to the origin server.
MSB	UDP	1-65535 (In)	The Windows Media distribution server uses a port within this UDP In port range when receiving a multicast stream from the origin server. The UDP In port number on the distribution server must match the UDP Out port number of the origin server that is delivering the multicast.

A *distribution server* publishes content that is received from another streaming source (called the *origin server*), such as another Windows Media server. Any computer that runs Windows Media Services can operate as a distribution server. The origin server is the source of the content that the distribution server streams. Distribution servers are located between the origin server and the client in the content stream. Clients connect to the distribution server as if it were the origin server.

A distribution server can be placed inside your network firewall and source from an origin server that is outside your firewall, providing clients inside your firewall with access to the content without opening additional ports. Alternatively, a distribution

server can be placed outside the network firewall and source from an origin server that is inside the firewall, providing clients that are outside the firewall with access to your content.

Note If the Windows Media distribution server is receiving a multicast stream from the origin server, the port value that is specified must match the port value that is specified in the multicast information (.nsc) file. In addition, you must allow packets that are sent to the IP multicast address that is specified in the .nsc file to come through your firewall.

Administering the server remotely

Application Protocol	Protocol	Port	Description
HTTP	TCP	8080 (In/Out)	The Windows Media server uses this TCP port to communicate with Windows Media Services Administrator for the Web by using HTTP.
HTTPS	TCP	443 (In/Out)	The Windows Media server uses this TCP port to communicate with Windows Media Services Administrator for the Web by using HTTP over Secure Sockets Layer (HTTPS).
RPC	TCP	135 (In)	The Windows Media server uses this TCP port to accept the incoming remote connection to the Service Control Manager (SCM), which provides RPC-based services for DCOM.
RPC	UDP	135 (In/Out)	The Windows Media server uses this UDP port for communication between the remote computer and the SCM.
DCOM	TCP	1025-65535 (In)	DCOM dynamically allocates one TCP port per process within this port range. You can restrict the port range, or specify specific ports, by creating a registry key. For more information, see Firewall and Registry Settings for DCOM.
DCOM	UDP	1025-65535 (In/Out)	DCOM dynamically allocates one UDP port per process within this port range. You can restrict the port range, or specify specific ports, by creating a registry key. For more information, see Firewall and Registry Settings for DCOM.
SNMP	UDP	161 (In/Out)	Allows remote administration and monitoring using Simple Network Management Protocol (SNMP).
SMB	TCP	445 (In/Out)	Allows remote administration and monitoring using Windows Management Instrumentation (WMI).

You can administer a Windows Media server behind a firewall by using the following interfaces:

- **Windows Media Services Administrator for the Web**. This interface makes remote administration of your server easy through the use of a Web browser. Using a Web interface allows you to administer Windows Media Services over a firewall, on a low-bandwidth network connection, or in a non-Windows environment. You connect Windows Media Services Administrator for the Web from a remote location to the Web services running on the Windows Media server by using HTTP over port 8080, which is not blocked by most firewalls. For example, you might use the URL http://*server*:8080/default.asp.
- **Windows Media Services snap-in**. This interface enables you to use Microsoft Management Console (MMC) to manage your Windows Media server. You can add the snap-in to MMC on any computer running Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition operating systems, or you can access the snap-in by using a Remote Desktop connection.

Both administrative interfaces require that you have access permission to the Windows Media Services service through DCOM. To enable access, you must open the TCP In and UDP In/Out ports in the firewall for RPC endpoint mapping and DCOM. By default, DCOM is free to use any port between 1025 and 65535 when it dynamically selects a port for an application. To create a higher level of security, you can configure a registry key that restricts the range of ports that DCOM will use to assign to applications. For more information, see Firewall and Registry Settings for DCOM.

If you use a network management console, such as Hewlett Packard HP OpenView, Compaq Insight Manager XE, and Dell OpenManage, you can receive events through SNMP and Windows Management Instrumentation (WMI). With these events, you can keep apprised of server activity and react quickly to situations as they arise. To enable receipt of SNMP and WMI events, you must open UDP port 161 and TCP port 445 in your firewall.

Note If you are running Windows Media Services on a computer that is running Microsoft Windows Server 2003 (SP1) or later, the Windows Firewall service and DCOM may deny access if the remote computers and accounts that are used for remote connections are not configured properly. For more information, see the Connecting Through Windows Firewall Web page.

If you remotely administer the Windows Media server from a computer running Windows® XP with Service Pack 2 (SP2), be aware that DCOM restrictions in Windows XP with SP2 are different from DCOM restrictions in earlier versions of Windows. You may encounter problems when you use remote access to administer the Windows Media server from your Windows XP SP2-based computer. For more information, see article 875605, "How to troubleshoot WMI-related issues in Windows XP SP2," in the Microsoft Knowledge Base.

Using Windows Firewall

Windows Firewall in Windows Server™ 2003 (SP1) or later is a host firewall technology that replaces Internet Connection Firewall (ICF). Windows Firewall provides stateful inspection of incoming IPv4 and IPv6 traffic and is designed to protect you from network attacks that pass through your perimeter network or originate inside your organization, such as Trojan horse attacks, port scanning attacks, and worms. You should run Windows Firewall on each of your Windows Media® servers, thereby extending your defense-in-depth strategy to the innermost layer of your security architecture.

When it is enabled in its default configuration, Windows Firewall blocks all unsolicited incoming network traffic on all network connections. While blocking unsolicited incoming traffic reduces your attack surface and increases your level of security, it can cause Windows Media Services to not work properly. For this reason, you will need to configure Windows Firewall so that unsolicited incoming traffic is allowed for Windows Media Services.

To allow Windows Media Services to receive unsolicited traffic through Windows Firewall, you need to add the Windows Media Services program (wmserver.exe) to the Windows Firewall exceptions list or use this document to determine which inbound ports the program uses and add them to the Windows Firewall exceptions list. You should always add programs to the exceptions list before you try to add ports; add ports to the exceptions list only as a last resort. The reason for this is that, when you add a program to the exceptions list, Windows Firewall dynamically opens the required ports for the program. When the program is running, Windows Firewall allows incoming traffic through the required ports; when the program is not running, Windows Firewall blocks any incoming traffic that is sent to the ports. In contrast, when you add a port to the exceptions list, Windows Firewall allows incoming traffic through the port, regardless whether there is a program or system service listening on the port for incoming traffic.

In addition, Windows Firewall automatically prompts you to add new programs to the program exceptions list. By default, Windows Firewall displays a **Windows Security Alert** dialog box (called a *notification*) when a program attempts to listen for unsolicited incoming traffic. If you are a member of the Administrators group on the computer, the notification gives you the ability to add the program to the exceptions list. If you are not a member of the Administrators group on the computer, the notification informs you that the program attempted to listen for incoming traffic but was blocked. You cannot add the program to the exceptions list if you are not a member of the Administrators group on the computer.

Windows Firewall does not display a notification when a system service, such as Windows Media Services, attempts to listen for incoming traffic on a port. This is also true for any program that runs like a system service. However, you can use the security event log to determine whether a system service, or a program that runs like a system service, attempts to listen for incoming traffic. To do this, you must enable the **Audit process tracking** policy and the **Audit policy change** policy. When you do this, Windows Firewall will write a Failure Audit with Event ID 861 to the security event log any time a program or system service attempts to listen for incoming traffic.

For information about Windows Firewall in Windows Server 2003, see the Windows Firewall Web page on the Microsoft

Windows Server 2003 TechCenter Web site.

Configuring Windows Firewall for Windows Media Services

If you install Windows Server 2003 (SP1) with Windows Media Services, the necessary exception for Windows Media Services is not created automatically in Windows Firewall. You must open Windows Firewall ports manually by doing the following:

1. Click **Start**, point to **Control Panel**, and then click **Windows Firewall**.
2. On the **Exceptions** tab, click **Add Program**.
3. In the **Add a Program** dialog box, click **Browse**.
4. In the **Browse** dialog box, navigate to *%systemroot%*\system32\windows media\server.
5. Click **WMServer.exe**, and then click **Open**.

Note If using Windows Server 2003 (SP2), the necessary exception for WMS is created automatically in Windows Firewall; therefore, this procedure is not required.
To perform this procedure, you must be logged on as a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
On Windows Server 2003, Windows Firewall is turned off by default and the Windows Firewall/Internet Connection Sharing service is disabled by default. You might have to start the Windows Firewall/Internet Connection Sharing service if you try to perform this procedure and you have never started Windows Firewall before.

Firewall and Registry Settings for DCOM

DCOM dynamically allocates one port per process. You need to decide how many ports you want to allocate to DCOM processes, which is equivalent to the number of simultaneous DCOM processes through the firewall. You must open all UDP and TCP ports corresponding to the port numbers you choose. You must also open TCP/UDP port 135, which is used for RPC endpoint mapping. Finally, you must edit named values for the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet to tell DCOM which ports were allocated. (This key may need to be created in the registry.)

The following example tells DCOM to restrict its port range to 10 ports:

```
          HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet
Name: Ports
Type: REG_MULTI_SZ
Data (one port/port range per line):
135
3001-3010

Name: PortsInternetAvailable
Type: REG_SZ
Data: Y

Name: UseInternetPorts
Type: REG_SZ
Data: Y
```

For more information about configuring DCOM to work through a firewall, see the Using Distributed COM with Firewalls Web page.

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system.
Note You must restart your computer any time you make changes to registry settings in order for them to take effect.

To have a web cast the basic requirements are:

1. A camera
2. Video capture card or Firewire card if digital video camera *
3. Computer running streaming software
4. Encoder*
5. High Speed Internet Connection

* These items can be replaced with a Tricaster (~$8000), gives professional results, but extremely expensive.

List of Equipment:

1. Camera - can be either analog or digital video
2. Video capture card – card must have the appropriate interface for the type of camera. Ex. Firewire for digital, or RCA for analog
3. Media Server – Used to stream the content (can also act as the encoder computer)
   Dual 2.4GHz, 1GB Ram, 10/100 LAN, 36GB HDD for Operating system, 50GB for captured video
4. Web Server – Used to hold the link to the media stream and place current rankings, scores, etc.
   1GHz, 515MB Ram 10/100 LAN, 40GB HDD
5. KVM Switch – Used to share a single keyboard mouse monitor between multiple computers
6. Firewall Router
7. Laptop – Used to monitor the web cast (Optional)
   1GHz, 512MB Ram, 10/100 LAN or WIFI, 40GB HDD
8. Capture Card – Connects video/Audio to the Encoder Computer
9. Encoder Software – Encodes the feed from the capture card Ex. Windows Media Encoder 9
10. A/V switch – Needed if multiple cameras are being used
11. Audio Mixer – Mixes multiple audio inputs into a single output
12. Patch Cables – Six or more if additional computers used
13. Wireless Access Point – Connects computers wirelessly
14. Audio & Video Cables
15. A/V Adapters – Ex. 1/8 to ¼, 1/8 to RCA, RCA to RCA Couplers
16. Misc - Power Cords, Surge Strips, Keyboard, Mouse, Monitor(LCD or CRT), Camera Power Adapters

List of Services:

1. Domain Name – Links your Public IP address to an easier to remember name
2. Access to High Speed internet Ex. T1, T3, Microwave, Optical Carrier Line
3. Ability to open/forward required ports
4. Volunteers to assist in the running of the web cast
   Possible positions:
   a. Webmaster – updates the webpage with current rankings, scores, alliance pairings
   b. One person per camera (unless stationary camera angle)
   c. Video Tech – Switches the camera feed, watches the encoder computer (works TriCaster if used)
   d. Person checking the web cast on the laptop, and controls audio levels of the web cast

Equipment Sources:

Possible sources to obtain this equipment from are:

1. School – High School, College
2. Donation
3. Local Store – Radio Shack, Wal*Mart, Circuit City, Best Buy
4. Online Store or Auction - eBay.com, newegg.com, tigerdirect.com
5. Team – Student, Mentor, Engineer, Alumni

Cost:

An estimate of the equipment cost based on eBay and best buy/circuit city prices is ~$2200 (non TriCaster option) for the entire system with a single camera and a one year domain name registration.

My configuration:

Firewall Ports were opened & forwarded to the media server as highlighted above. The server hosting the stream was placed in the DMZ of the router.

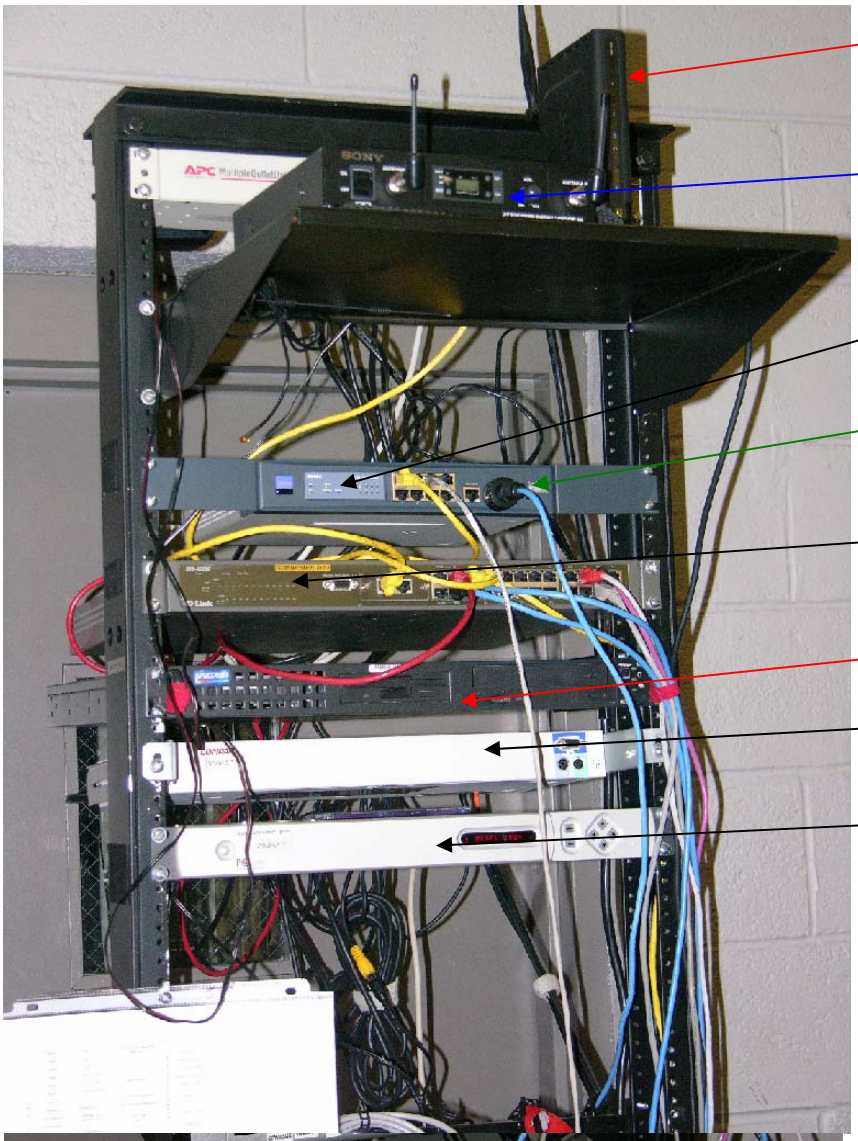
The announce file was formatted as follows:

http://encoder-server/publishingpiont

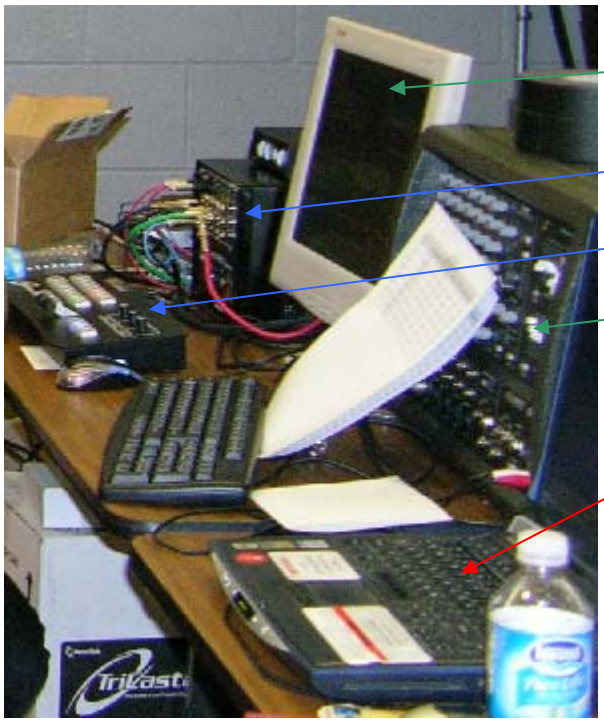
Example: http://nishinsei.shinraikon.com/PARCX

What I used this year is:

1. A server class computer (IBM x345) with dual 2.67Ghz HT CPUs, 1GB ECC Ram, 4 18.2GB HDDs in a striping RAID (combines all drives to act as a single drive; faster read write times to drive) running windows 2003 Enterprise (Streaming server is an option as a server role)
2. Hardware Encoder/Video Mixer (Newtek Tricaster Pro)
3. 24-Port Ethernet Switch
4. Audio Mixer (Behringer 2442-FX)
5. 3 Video Cameras (Recording studio type)
6. My own domain name that dynamically links to my current IP (dynamic DNS client running on server) http://EditDNS.net
7. Soft switch, to redirect page request based on requested domain-name. http://octagate.com
8. Wireless Microphone for Announcer


Wireless Router
Wireless Microphone Receiver
VPN Firewall
Internet Connection
24-Port Switch
Web Server & Soft-Switch
KVM Switch
Video Scan Converter


Media Server



Monitor for servers & TriCaster

Newtek TriCaster

TriCaster Control Keyboard

Audio Mixer

Laptop (used to monitor the web cast)