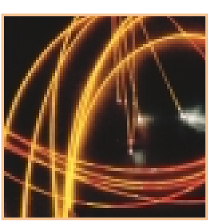
IMAGING NETWORKS IN A DIGITAL WORKFLOW – Keeping The Traffic Flowing.

The ability to successfully move image files while maintaining their integrity is a far more daunting challenge than moving data files. It must be remembered that infrastructure and components that work well for data may not be optimal for images.

The challenge for professional labs is clear-cut. The average image file size can be more than 100 times greater than a typical data file. While problems with a lab's data network can be a real nuisance by slowing or interrupting internal business communications, lab production can be adversely affected or even come to a screeching halt if the network prevents the actual image files from moving through the digital workflow. And this digital output is the professional lab's business!

An image network is not unlike a major highway whose size and configuration will greatly determine the volume of traffic it can handle, as well as the speed of the traffic flow. It's important to consider that the network not only enables the image workflow, it must be fully optimized to exploit the maximum capability of each input and output device.

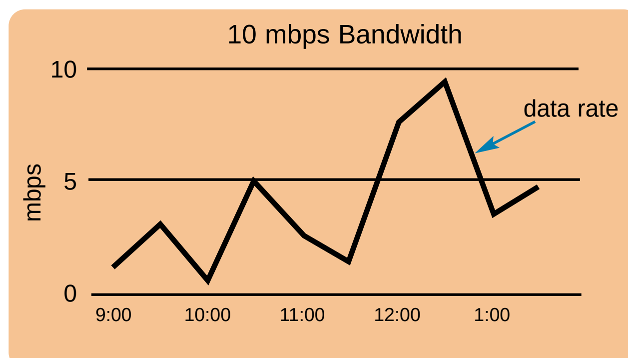


■ Asking A Lot Of The Network.

In a digital workflow, the network must have the bandwidth (capacity for carrying data) to support all production, color management, operating system and image enhancement software applications – as well as the device drivers for lab scanners, workstations, printers, storage systems and other networked devices.

Bandwidth is measured in bits per second (bps) and is the maximum rated capacity of throughput between any two nodes on a network. This rate is only a capacity, not an actual measurement of throughput, which is called the "data rate." The relationship between the bandwidth and data rate provides a measurement of bandwidth "utilization", shown as a percentage.

For example, if a 10 mbps network has an average data rate of 4 mbps, the utilization is 40%, but the bandwidth remains 10 mbps.



Theoretically, if this same "data rate" information was captured on a 100 mbps network, the utilization would be 10 times less (or 9.2% at a throughput of 9.2 mbps, rather than 92% for a 10 mbps network)

Networking

Moving images among devices, and between lab and studio without diminishing the performance of the system, are no easy tasks. Labs that are accustomed to being self-sufficient in implementing optical workflow strategies may find that it is beyond their in-house skill sets to address the increasing complexity of image network infrastructure solutions, unique technological standards/requirements, and network security issues. Labs should consult with a firm that has these specialized capabilities.

Five Touchpoints Of Effective Network Design.

Despite the technical complexity of the subject matter, labs can help ensure the image network can exploit the full capabilities of the lab's existing and future hardware and software purchases by addressing the following key elements of network design:

1 Bandwidth Aggregation

Think of it this way. You're about to enter a multi-lane superhighway designed to speed you to your destination, only to find yourself caught behind a long line of motorists inching their way up to the only open toll booth.

In an image network, the pinchpoint (or bottleneck) is often a networked device (such as a printer) whose network interface card, cabling, or network workflow design is incapable of simultaneously handling the aggregate input from multiple devices (workstations). This can be a result of improper network design, device configuration, or both.

It's important to remember that throughput of networked devices aren't only limited by device specifications, but also by the capacity of the network to deliver the required input from multiple sources.

2 Segregation

Think of the advantages of building separate highways for tractor-trailers and automobiles that would simplify life for all drivers. In a lab environment, network configuration modifications can achieve similar benefits by segregating image and data files into separate workgroups on the network to optimize workflows. Remember, high-bandwidth networks can be very costly to implement for all users. It's much more cost effective to isolate traffic and supply high bandwidths only to those devices that really need it.

3 Security

In a networked lab environment, security becomes an immediate issue as soon as files are shared between the lab and studio, lab and studio's or third-party's Internet site, or lab and satellite lab location for load balancing.

A network must be designed to conform with a lab's security policy. If one doesn't exist, a policy should be adopted for networking purposes, alone. It's common knowledge that the Internet provides a tremendous potential for intrusion. Numerous strategies and techniques can be employed to control access to transmitted images, and these implementation costs widely vary.

A Virtual Private Network (VPN) is essentially a private highway through the Internet. Only approved resources can gain access to the VPN, and the data that resides on the devices connected to it.

A firewall is another device that acts as a buffer between private and public networks.

These security solutions utilize a number of methods to ensure security, including access control lists, encryption, authentication, and authorization of trusted resources.

Networking

4 Installation

Not only must the tangible assets of networking meet specifications established by regulatory agencies, installation must conform to standards to prevent a significant erosion of performance that can severely compromise network integrity.

Category 5 cabling, a common standard for current network installations, must be installed in compliance with a list of category 5 specifications.

For example, when installed with too much tension or improper punchdown techniques, measurable degradation of the network's performance will occur. Even the length of the cabling is a factor. (Category 5 installations can be no longer than 90 meters). Any deviation from accepted installation practices can jeopardize a lab's entire networking investment.

5 Monitoring And Trends Analysis

Effective network management requires an ongoing monitoring of resources, utilization, and errors – (especially during peak load periods – to help predict how the network will perform as image file volumes increase over time). From a practical standpoint, it would be difficult to determine the relative need for device or network enhancements without this data. For example, installing a network printer that can handle twice the output volume does little good if the network is not capable of handling the increased traffic flow. Empirical data is required to support decisions to add imaging device or network enhancements. Monitoring and trends analysis provide this data.

What To Do With An Existing Network.

Labs looking to protect the investment they have made in their current network infrastructure, while meeting future requirements for both data and images, should start with a network audit to document all devices on the network.

This audit is designed to identify all high-capacity requirements, while providing a connectivity map with bandwidth utilizations and protocols for all existing components. This is virtually impossible without the proper use of network protocol analysis tools.

Labs that do not have access to these tools are advised to seek out reputable vendors to supply this service. Analysis tools provide a baseline of data to support network design decisions. With this baseline, labs can determine the existence of any problem that needs to be fixed in the redesign.

At this point, it can then be determined what new components and general resource requirements must be added to accommodate current and future needs.

Networking