THE NETWORK AND ITS ROLE IN DIGITAL IMAGING AND COMMUNICATIONS IN MEDICINE IMAGING

DENNIS BALLANCE

The elements of a digital imaging system are bound together by the network, so careful attention must be paid to this essential component. Networking hardware and cable choice will affect the speed of image transmission between devices within a network. Wireless networking offers convenience at the expense of speed and potentially, security. If a facility allows its network to connect to the Internet, security precautions are essential. Firewalls prevent unauthorized and destructive access to the network; virtual private networks allow encrypted communication with the network; and email and web browser encryption allow data transmitted from the network to other users on the Internet safely. This article presents an overview of this broad array of technologies. Readers are encouraged to seek additional depth as needed to address individual networking needs.
Veterinary Radiology & Ultrasound, Vol. 49, No. 1, Supp. 1, 2008, pp S29–S32.

Key words: digital radiography, PACS, TCP/IP, teleradiology, veterinary.

Introduction

TYPICAL DIGITAL IMAGING departments are composed of image acquisition devices (e.g., digital radiography, computed tomography), viewing workstations, a Picture Archiving and Communication System (PACS) server, and back-up systems or off-site storage facilities. The piece that is most frequently ignored or undervalued is the network that binds these components together. The network is essential for a PACS to operate and for the practice workflow to move in an efficient manner, but it is also the primary gateway for electronic intrusion and data theft. The Digital Imaging and Communications in Medicine (DICOM) standard describes both the structure of images and image data, and the communication mechanisms that two devices use to share this data and information. Proper network design and careful planning are essential for achieving adequate or superior PACS performance, and for ensuring adequate security. Additional information about image acquisition devices,[1] DICOM,[2] viewing workstations,[3] PACS,[4] and back-up systems or off-site storage facilities[5] are found in this Supplement.

Broadly, the primary considerations when planning a network are as follows:

1. Hire a network engineer or qualified consultant to plan and implement a network. Most people not employed in Information Technology (IT) probably do not have enough recent knowledge to adequately plan an effective, secure, and scalable network.
2. Be willing to invest in high-quality (and thus high speed) commercial-grade network switches and routers.
3. If the network is connected to the Internet, acquire a dedicated professional-grade hardware firewall. Software firewalls should also be used on each individual computer.
4. If access to image data is necessary from off-site, either provide a Virtual Private Network (VPN) or use a third-party hosting system that uses Secure Sockets Layer (SSL) to encrypt file transfers.

Network Protocol

Over the past 30 years many different networking protocols (i.e., network languages computers use to communicate) were developed. Each protocol shares data in a different way that allows computers to communicate with others that understand that protocol. The most popular commercial protocol today is TCP/IP, a combination of the Transmission Control Protocol and the Internet Protocol that were initially developed by the Defense Advanced Research Projects Agency for military networks. Fundamentally, TCP/IP transmits data by encapsulating data itself and information about where it is headed into packets that are transferred from node to node until these data reach their destination.[6]

TCP/IP is the protocol used by the Internet, and is also used by the vast majority of modern PACS servers, image acquisition devices, and viewers for transmitting image data.

Network Performance and Bandwidth

In imaging, the network is frequently the greatest bottleneck to smooth and efficient workflow. Consider

From the School of Veterinary Medicine, University of California, Davis, CA 95616.

Address correspondence and reprint requests to Dennis Ballance, at the above address. E-mail: dwballance@ucdavis.edu
doi: 10.1111/j.1740-8261.2007.00330.x

this example: a typical uncompressed DICOM Digital Radiography image is 10–12 megabytes (MB). Transferring one such file between two computers in an office with a 10 megabit/s (Mbps) network requires 12–15 s. 1 (Mbps) means 1 million bits, or 0.12 MB, are transmitted each second. Transferring this file to a computer on an outside network (such as the Internet) via a fast DSL connection (1 [Mbps], though many are 750 Kbps/s or less when uploading) would take 10 times as long, or 2–3 min. Thus an exam that contained 10 or more images could require a couple minutes on a fast internal network, and the better part of an hour at typical broadband speeds. In a busy practice environment, this level of performance is just not practical.

One solution for reducing or eliminating long delays in image transfer is to increase the speed of the network. One hundred megabit/s network switches allow data to be moved in 1/10th the time of a 10 Mbps network (that 10-image study in 10–15 s). Similarly, 1 gigabit/s (Gbps) is 10 times faster (or a blazing 1.5 s). Performing this kind of upgrade within an office is often fairly easy, though it may require cable upgrades (specifically, Category 5 cable is required for 100 Mbps throughput, and Category 5e is required for 1 Gbps). While increasing bandwidth between the office network and the Internet can be done by upgrading to the fastest available service (and is advised if off-site image transfer is needed), increasing the upper limits is determined by the Internet Service Provider. Fortunately, as network technology advances, transfer speeds will become less of an issue.

As speeding up the network is often not possible, many PACS vendors provide a lossless wavelet-type compression (based on the JPEG 2000 image compression standard) that, when coupled with an image viewer that understands that specific compression, allows the viewer to retrieve only the portions of the images actually being displayed. As the user pans or zooms on the image, and more image content is required, the complete data set for the panned or zoomed area is retrieved from the server. The effect is that the display comes up quickly at first, but some delay is encountered when making adjustments. Generally, this delay is much less than the delay imposed by waiting for a complete study to transfer.

Key to network performance is the hardware (i.e., switches and routers) that route network packets from one place to another. Small networks may only have one such device, but that number can grow as wiring or computer placement needs change and the network, or even the building, enlarges. In general, equipment marketed for home use (such as what one might find at a consumer electronics store) is insufficient for business networking needs. Commercial grade hardware is generally more tolerant of environmental conditions (heat, cold, dust), provides more remote management tools (configuration, traffic analysis, error tracking, identification of new devices), is better equipped for expansion (greater number of ports, chaining), and can weather outages better (redundant ports, dual power supplies). A forward-thinking network plan will include equipment that can scale with the facility's needs.

Wireless Networking

In today's imaging networks, wireless transfer speeds are still slow enough that wireless networking cannot adequately serve the backbone imaging network needs. The fastest current wireless technology, 54 (Mbps) for 802.11 g, is considerably slower than the current wired network connections. Additionally, wireless network access points create entry points for outside equipment. Warddriving is the practice of driving around a neighborhood with network sensing gear and high-gain antennas, looking for unsecured access points.[7] Once an unauthorized individual has a connection through an access point, he can perform illegal network activities using that connection and they can scan and potentially interact with equipment on the subscriber's network, completely bypassing any firewall that may exist between the subscriber's network and the Internet.

Security built into most wireless access points is generally weak and easy to break with the right tools; today, only Wifi-Protected Access (WPA2) is effective.[8] Without this technology, the broadcast between a wireless computer and the access point is unencrypted, allowing a listener to extract any data broadcast between the two. Older wireless access points should be replaced or upgraded to support WPA2.

An additional security measure to limit unauthorized wireless access is to create restrictions on the access point such that only known devices (via their Media Access Control, or MAC, address, a unique code assigned to every network device) can connect. Not all access points support this capability.

Firewalls

A firewall is a hardware device or software program that controls the access one computer has to another. Any software that expects to be contacted by another computer will be listening on a specified, numbered network port for a series of network packets to be sent to it. Many of these programs were never intended to be contacted by computers outside the local network, so a firewall looks for unsolicited or inappropriate connection requests to these ports and blocks them.

Firewalls are used between networks to prevent unknown computers from one network (such as the Internet) from attempting to communicate with computers on another network (typically the local network). Firewalls are an essential part of computing today, and no network should

be without one. This is especially true for mission critical systems such as PACS servers, not only because damage or disruption of a PACS computer would slow the practice's workflow and be costly to repair, but also because the medical information contained on the system could be both highly valuable and destructive if used incorrectly.

Any computer on a network should only have specific services approved by the system administrators exposed to the Internet, and those services must be updated consistently to ensure that vulnerabilities do not exist.

Generally, hardware firewalls are more robust and capable than software firewalls. Some viruses (such as might be delivered via email or by visiting a malicious web page) will specifically target the computer's software firewall to bypass or disable it. Commercial hardware firewalls generally have friendly interfaces for configuration and management, and can be configured to allow special access for certain computers. Note that any system that connects to the network behind the hardware firewall can then have free access to the other computers also connected behind the firewall. This means that a virus or rogue computer that gets past the firewall would have unrestricted or trusted access to the other computers behind the firewall. To help mitigate this, software firewalls on each individual machine are recommended even when a hardware firewall is in use.

Network Address Translation (NAT)

NAT is a security mechanism typically associated with firewalls that allows several computers or devices to share a single publicly visible network IP address (Fig. 1). The devices can communicate between each other, and if they request data from outside their isolated network, the NAT router can send the information back to the computer that requested it. To any machine outside the NAT, all communication appears to be from the router. Thus, it is impossible to tell how many devices are being hidden by the NAT router, and no way to talk to the other devices directly or even to detect those devices without them initiating contact. NAT provides tremendous security to the protected devices.

NAT has special relevance for PACS because PACS servers and many DICOM devices (especially acquisition modalities) use IP addresses for establishing identity. In general, all devices that need to communicate with the PACS server should be on the same side of the NAT router, otherwise it may be difficult or impossible to establish reliable communications between the various devices.

Data Security

Because veterinary medicine is not bound by human Health Insurance Portability and Accountability Act requirements, the veterinary profession may be more lax about medical data security. This could change, and the profession needs to be prepared if it does.

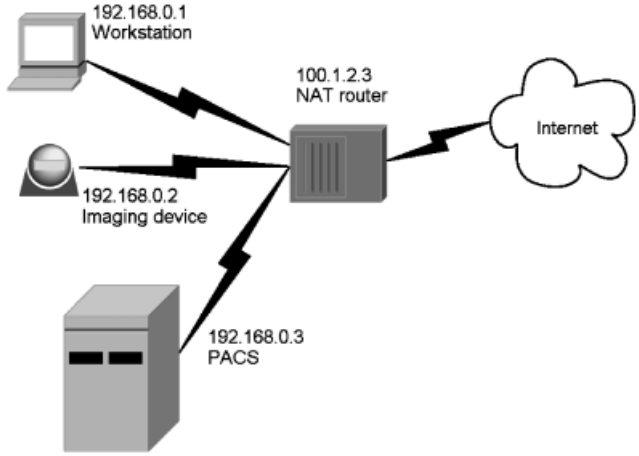

FIG. 1. Diagram representing a Network Address Translation router and how it interfaces between the devices on either side. In this example, the Workstation, Imaging device, and Picture Archiving and Communication System server all appear to have the Internet Protocol 100.1.2.3 to all systems on the Internet.

Medical images are an important part of a patient's medical record, and should be kept as safe and secure as any other part of the patient record. Any user viewing a medical image should be required to enter a username and password, as this will prevent unauthorized users from viewing sensitive images. Ideally, when any image is viewed, that information should be logged, allowing a network administrator to track down an information leak if one should happen.

Image data may be subject to manipulation without adequate security. Tampering with files on the PACS server could result in altered diagnostic information, or even loss or substitution of images. Recently the DICOM standard became more secure with the addition of a Digital Signature specification.[9] A signature is created by performing a mathematical transform on image data, in such a fashion that altering any amount of the file would result in creation of a different signature. PACS software available now or in the near future may include digital signature capability.

VPN

A VPN is an encrypted connection between one computer and a remote network. The encryption allows the computer to communicate securely over a public network (such as the Internet) as if it were physically connected to the remote network, without fear of having the data it is sharing with that network being legible to anyone on the public network. VPNs are commonly used by companies or organizations that need to provide secure, remote access to their network and online resources. There are several types of encryption used in VPNs, with IPsec,

SSL/TLS, and PPTP being the most common.[10,11] Consulting a knowledgeable IT security consultant is probably the best way to get a reliable recommendation on a specific product or implementation.

SSL

SSL is one type of Transport Layer Security (TLS). In addition to being used to encrypt a VPN connection, SSL can also encrypt individual data transmissions, such as uploads to a web server. If your practice or business uses imaging software or data transfer mechanisms that do not involve a VPN, ensure that an SSL connection is present every time data is transferred.[12]

Email

The DICOM standard includes a Multi-purpose Internet Mail Extensions encoding specification, and DICOM images can be successfully sent via email. However, due to the number of images often associated with a study, and the size of each image, email message sizes are quite large. Attempting to email messages with DICOM attachments frequently exceeds the recipient's email storage limits and prevents delivery of additional messages. As a courtesy to email recipients, the sender should avoid using email for sharing DICOM images.

Email encryption is an important topic. Email messages are not encrypted as they move through the Internet. Many email hosts allow the user to maintain an encrypted connection between the personal computer and the email server, but the encryption ends there. Additionally, email is often cached at each waypoint, meaning multiple copies of your message may live in logs or caches throughout the Internet. The only way to ensure that no individual except the recipient does not see the contents of a message is to employ some type of message encryption, such as Pretty Good Privacy.[12] This requires both the sender and recipient to have encryption keys. Fortunately, modern email programs make use of encryption fairly simple.

DICOM Connectivity

While the DICOM standard addresses elements of networking, data transmission, and data security, the fundamental security model in DICOM is unencrypted full-file transfer between two devices on the network. Additional considerations like user-level access control, encryption, digital signatures, and partial image transfer (such as via wavelet streaming) are added by software vendors to their specific packages. For this reason, it is common for packages to include PACS server, remote archiving, and viewing software bundled together. The DICOM committee is working toward making some of these elements part of the standard, which will make it easier to separate some of these components (for instance, to allow one vendor's viewer to retrieve wavelet-compressed images from another vendor's server).

Conclusions

As this document demonstrates, the network is an essential and complicated piece of the digital imaging puzzle. A solid understanding of these fundamentals is required to make informed decisions about network topography and security.

Disclosure of Conflicts of Interest: The authors have declared no conflicts of interest.

REFERENCES

1. Widmer WR. Acquisition hardware for digital imaging. Vet Radiol Ultrasound 2008;49:S2–S8.
2. Wright M, Ballance D, Robertson I, et al. Introduction to DICOM for the practicing veterinarian. Vet Radiol Ultrasound 2008;49:S14–S18.
3. Puchalski SM. Image display. Vet Radiol Ultrasound 2008;49:S9–S13.
4. Robertson I. HIS, RIS, and PACS. Vet Radiol Ultrasound 2008;49:S19–S28.
5. Wallack S. How to store digital images and comply with medical record keeping standards. Vet Radiol Ultrasound 2008;49:S37–S41.
6. Hauben R. A study of the ARPANET TCP/IP Digest, 1998.
7. Ryan P. War, peace, or stalemate: wargames, wardialing, wardriving and the emerging market for hacker ethics. Virginia J Law Ethics 2004;9.
8. Frankel S. Establishing wireless robust security networks: a guide to IEEE 802.11i. National Institute of Standards and Technology, 2007.
9. Oosterwijk H. DICOM basics, 2nd ed. OTech Inc., 2002.
10. VPN Consortium. VPN technologies: definitions and requirements. VPN Consortium, 2006.
11. Hamzeh K. Point-to-point tunneling protocol. Network Working Group RFC 2637, 1999.
12. Freiser O. The SSL Protocol, Version 3.0. Transport Layer Security Working Group, 1996.