Journal of VALIDATION TECHNOLOGY®

An Approach To Network Qualification

BY ART KOZEL AND RUBEN ARMAS

INTRODUCTION

Qualification and validation activities in a Good Manufacturing, Laboratory, or Clinical Practice (GXP) environment traditionally have been about ensuring that a system has been designed and implemented as intended. This is typically achieved by employing good practice requirements - gathering, designing, and building the system - then performing a series of tests that independently verify the system has been installed properly, operates as expected, and performs as designed. During these activities, the systems requirements, design, and testing are all documented.

Today's applications are distributed applications that follow a client server model where multiple users on different workstations generate and access data that is stored in a centralized data repository. The diagram in *Figure 1* illustrates typical, distributed GXP applications.

The client server model has increased the dependence of applications on the network infrastructure making the network infrastructure an integral part of the application. This paper provides an approach for qualifying a network infrastructure. Servers and workstations are purposely omitted from this paper for the sake of clarity and to specifically focus on the network hardware and cabling infrastructure.

Network 101

There are many possible network components and network configurations. In general terms, a network interconnects multiple host computers through some medium. In most corporate networks, copper cabling connects workstations, servers, printers, and other network devices to a network concentrator. Data is sent from one host to another via the network concentrator.

One of the most prevalent network technologies in use today is Ethernet. Ethernet uses hubs or switches as network concentrators, but in very different ways. Ethernet hub technology is analogous to a room full of people all trying to communicate with each other; only one person can speak at a time. It is an inefficient way of communicating and it is being phased out in favor of network switches.

The network switch model is analogous to the telephone system in which a call is established between two individuals. Additionally, most enterprise-level network switches can be managed. In other words, the switch will have a user interface that allows the network administrator to configure features, such as routing schemes, diagnostic alerts, network connectivity, and fault tolerance, just to name a few. These features are specific to the vendor and the feature set purchased. Hubs and some lower end switches cannot be managed and are rarely used within the corporate environment.

Oftentimes in corporate networks, there are a large number of switches spread across the facility. The facility contains network closets, strategically located, each with a set of switches serving a specific area of the facility. This design accommodates the limitation of Ethernet running over copper cabling, which has a practical limitation of 300 feet. All users must be within 300 feet of the network closet or they will experience a variety of network errors and performance issues. The switches within each closet are interconnected using either copper cabling or fiber cabling. Additionally, the closets themselves must be interconnected and can use copper if the network closets are within 300 feet or they can use fiber if the closets are within 2000 feet.

Network Interface Cards (NICs) are used to connect all

network devices to the network switch. The NICs inside the device have a port for the network cable. The cable is used to connect the network device to the network outlet on the wall. The outlet on the wall is connected to a network cable that goes back to a patch panel in the network closet. The patch panel is a board where all the cables are terminated. From the patch panel, another cable is used to connect (patch) the panel port to the actual network switch.

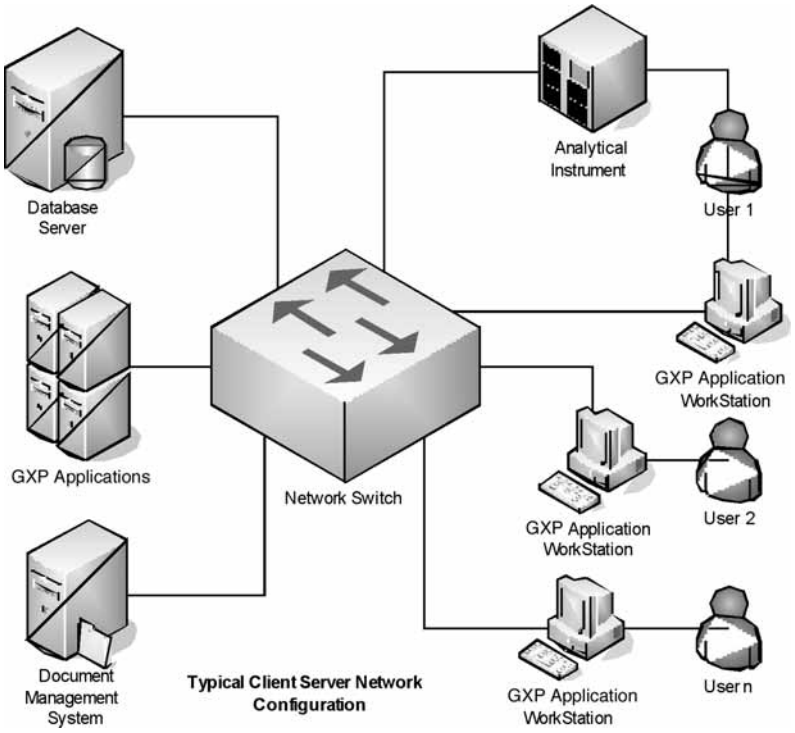
Depending on the networking protocol being used, the network protocol will have some kind of network addressing scheme. Typically, most corporations use Transmission Control Protocol/Internet Protocol (TCP/IP) as their base protocol - although they may use other protocols in addition to TCPIP. TCPIP is the same protocol used exclusively on the Internet. The TCPIP configuration is a very important aspect of the network because network devices must have the correct TCPIP configuration to communicate with each other. Moreover, administrators may segregate traffic using TCPIP address schemes and Virtual Local Area Networks (VLANs) to improve the performance of the overall network. Routers and special network switches, called layer three switches, are used to route network traffic from one VLAN to another.

Another aspect of a network is the speed at which a network transmits data. Modern day equipment is capable of transmitting data at least 10 megabits, and up to 1000 megabits per second. When connecting network devices, the devices must be able to negotiate a common speed at which they can communicate. Most switches will be backward compatible, which means that a switch may be capable of speeds of 1000 megabits per second and will also support older devices capable of only 10 megabits per second.

This section is meant to describe a typical corporate network infrastructure and provide a common understanding of the different network components. There are other varieties of network types and protocols still in use today. Qualification of the network must be customized to the network currently in use. In addition, there are Wide Area Networks (WANs) that use local Internet Service Providers (ISP) to interconnect the different geographically dispersed sites that are not discussed here. WANs are available in many varieties and the reader is referred to the IEEE website at http://www.ieee.org for more information.

Figure 1

Typical Client Server Network Configuration



Network Analysis and Lifecycle

Whether implementing a new corporate network or retrospectively qualifying an existing network, there must be a complete network systems analysis performed. The network analysis must investigate and document all aspects of the network configuration. The easiest way of performing such an analysis is by following the natural procession of the network lifecycle.

Networks, just as traditional software applications, follow a lifecycle that includes requirements, design, testing, maintenance, and eventually, retirement. The documentation of each of these components is crucial to maintaining the qualified state of the network infrastructure. Moreover, the documentation can also be used to troubleshoot issues, make smart decisions about network reconfigurations, determine which components would need to be re-qualified during upgrades or changes, and ensure that all network engineers have the documentation necessary to understand and maintain the corporate network.

Requirements

In general terms, the requirements phase documents what needs to be accomplished and not how it will be accomplished. In addition, the requirement phase documents the minimum specifications that must be met when purchasing, installing, and configuring a network device. These requirements outline the minimum performance parameters such as negotiated speeds, network interfaces, error handling, reporting mechanisms, cabling requirements, and maximum network segment size, as well as any specialized requirements.

An important aspect of any requirement is that it must be testable and verifiable. Vague requirements cannot be tested and will, therefore, cause problems during the testing phase. As a rule of thumb, a good requirement is one that can always answer the question "How will this requirement be tested?"

McCabe breaks down requirements into three different categories, User Requirements, Application Requirements, and Device Requirements [McCabe, 2003]. User requirements are those requirements that address user needs to accomplish the assigned tasks. These requirements include the ability of a user to retrieve and transfer data to and from a server, logical and physical security, and network accessibility.

Applications will also have a minimum set of requirements. Applications that use multimedia components, such as video or voice, must have a predictable capacity and delay that is required. The devices used to access the network and run the different applications have their own set of requirements as well. These requirements will include items such as network interfaces needed to interconnect devices. For example, network switches that are used to connect network closets may require fiber interfaces as opposed to copper interfaces, and servers may require a per second connection of 1000 megabits, while workstations may only need a 100 megabits per second connection.

Requirements specifications must be customized to the particular corporate environment. The items mentioned here are not a complete and exhaustive list of requirements, but are intended to provide a general understanding of what should be included in a network requirements specification.

Design

Design documentation provides the detailed documentation that informs network engineers how requirements are to be implemented, and more importantly, describes the network architecture. Network designs typically have both a textual and graphical description of the network being qualified. For example, a general network topology diagram is a view of the network that illustrates how all the network backbone devices are interconnected. A different view of the network may include a topology diagram that illustrates how the different hosts and network devices, such as printers, connect to the network backbone.

The topology diagrams should also include details such as IP addresses, subnets, gateways, VLAN names, interconnecting media, and device names. Moreover, a textual description of the network components and configurations should also accompany the network topology diagram.

Device configurations are another piece of documentation that should be added to the design documentation. Configuration reports of all devices should be included in the design documentation, whenever possible, to document the current state of the network device. For example, Cisco devices have a command that displays the current running configuration of the network device. The running configuration should be copied and documented as part of the network design documentation.

To streamline the documentation change process, each network device should have its own document with its own device change history. This avoids the complications that occur when many changes must be made to single governing documents for multiple devices and by different people.

Agreeing on the best method of setting up the documentation is a decision that must be made in conjunction with the corporate Quality Assurance (QA) group and, as needed, with the document systems group. Additionally, there are many tools available to help with the documentation and administration of a network infrastructure. Examples of these tools include: Cisco's CiscoWorks, Fluke's Optiview Console, and Computer Associate's Unicenter.

When managing and implementing a corporate network, it is best to maintain consistency among the network devices whenever possible. Therefore, a network equipment standard should be developed that outlines the model numbers of the different network switches and network routers, as well as possible alternatives. The following section lists some of the benefits of standardizing infrastructure equipment:

- Maintaining a few select pieces of equipment allows the user to have more comprehensive education and knowledge about the products and mitigates the chance of error during maintenance.

- Interoperability of the network components of a single vendor reduces complications that could occur with the interoperability of devices from multiple vendors.

- Support of network devices by a single vendor is usually better than that provided by multiple vendors, because it avoids the 'blame game' where one vendor points to the other as the cause of a problem.

- Pricing is usually more advantageous when purchasing in volume from a single vendor.

The most important reason for companies to standardize equipment is to make the qualification process easier.

Fewer testing scripts need to be developed that address standardized network components. For example, if the corporation standardizes on Cisco 3650 switches, then each time a new switch is added or replaced on the network, the same testing script can be used. This approach will avoid confusion because the scripts will be standardized. Only new features or specialized configurations would need new test scripts and these can be added as optional addenda to the standard script while the base configuration is kept the same.

Cabling is another aspect of the network infrastructure that should be standardized. The design documentation should specify a cabling system to be used throughout the facility. Cabling systems are actually a suite of components that include the cable, the jacks, and the patch panels. The components in a cabling system are designed to work together and to consistently deliver the cable's rated performance. Furthermore, since there are different types of cables that can be used for interconnecting devices, the design documentation must document the type of cable that will be used (i.e.: Fiber, Cat 6, Cat 5e, etc.).

This does not mean that a facility must forever remain with a single cabling standard. When a decision to upgrade to a new standard is made, the decision must be documented in a corporate standard and all new cabling must comply with the new corporate standard. Moreover, the new cabling system and the type of cabling used must also comply with the Telecommunications Industry Association (TIA)- Electronic Industries Alliance (EIA) 568 cabling standard. The TIA-EIA 568 cabling standard is the document that sets the specifications for all the cabling used for voice and data regardless of vendor. For more information and parameter calculations, the reader should review the TIA-EIA 568 B standard.

The network-addressing scheme is another aspect that must be documented. In the case of TCPIP, it is important to understand what address space is used for each network segment. For example, if a network is segmented into VLANs, each VLAN will have a unique address space. If two VLANs have the same address space, the network devices will not know where to send the data, causing data to be dropped and applications to fail. The documentation of the network-addressing scheme is useful for both new and existing network engineers responsible for maintaining the network.

There are different ways of labeling network cable drops and naming network devices. The labeling or naming convention for all network devices and network cabling should be included in the design documentation. Each device should have a code that identifies the location of any device or network cable within the facility. Furthermore, a floor plan illustrating the location of all the data cables should be developed and maintained. The floor plan should clearly identify the cable termination port in the facility and the location of the network closet with the patch panel where the other end of the cable terminates.

Testing

There are different ways of testing a network, but for the sake of clarity, it is easiest to follow the well-established model of Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ). The primary purpose of the testing phase is to ensure that the network performs as designed and that it meets all specified requirements.

Network IQ

In general terms, the IQ provides objective evidence that the network equipment and cabling have been installed properly. The cable vendor tests and certifies that the cabling has been installed according to the TIA-568 standard. Generally, manufacturers offer a 25-year warranty that their cable will be able to transmit data at the rated speed regardless of technology.

A caveat in the certification process: manufacturers have individual cable specifications that will most often conform to the TIA 568 standard, but since the TIA specifications are a function of frequency, the testing parameters may, at a certain point, exceed the TIA standard, therefore, care must be taken that a cable is certified to the TIA standard.

The network equipment installation is tested against manufacturer installation recommendations. The IQ visually verifies that the network equipment is bolted to the rack properly and that the equipment is grounded properly. Every manufacturer specifies the environmental parameters for all their equipment. This typically includes temperature and relative humidity, which may be tested by monitoring the temperature and humidity with a calibrated temperature probe and a chart recorder over a 24-hour period. Manufacturers will also specify the electrical requirements such as voltage and frequency that may be tested with a calibrated voltage meter.

Network OQ

Operational Qualifications are specifically geared toward ensuring that network devices have been configured correctly and operate properly. The easiest way of accomplishing this is to design tests around the specific features being employed to meet the needs of the specified requirements. For example, if the requirement states that the network interface on the network switch must be capable of negotiating speeds of 10, 100, and 1000 megabits per second, then the appropriate feature on the network must be tested.

Switches will often have an option to statically or dynamically set the bandwidth speed of the interface. If the switch is configured to auto-negotiate the speed, then you can test by connecting network cards that are able to run at 10, 100, 1000 megabits per second. By listing all the features normally utilized, a simple and straightforward test script can be developed.

Identifying and grouping equipment along family lines that have the same feature sets and use the same command sets is extremely beneficial, because it allows the test script to be used over and over again. Additionally, explicitly turning off features not being used may avoid issues such as incorrect packet routing or packet filtering during testing or normal operations.

Ping and Trace Route are valuable diagnostic tools within the TCP/IP suite. The Ping sends a ubiquitous data packet to a remote host computer, where the command checks for connectivity. The host computer then replies to the computer that made the request. The Trace Route displays the route the packet takes through the network. This is important, because a device incorrectly configured, may not route the packets correctly or may route the traffic in an inefficient manner, thereby wasting resources and leading to poor network performance. Both of these diagnostic tests must be included in the network OQ, but should be customized to the network environment and design.

Network PQ

The Performance Qualification deals with how well the network is able to transfer data. The network's ability to transfer data is directly related to a set of parameters that provide the current health of the network. This paper addresses the health parameters that deal specifically with Ethernet, since it is one of the most widely used technologies. Ethernet breaks up data into smaller discrete packets. These packets contain the data payload, the source address of the sender, and the destination address of the recipient in every packet.

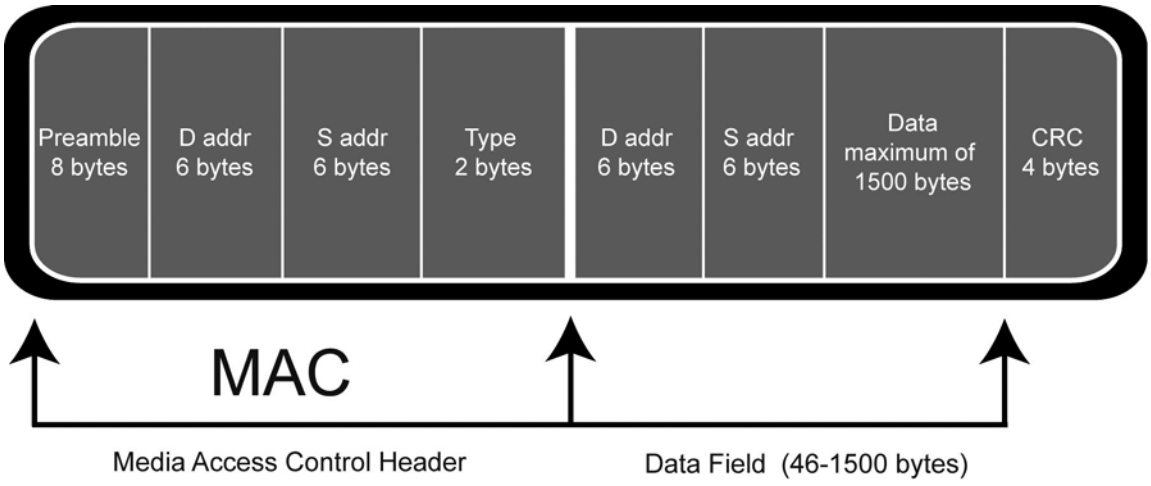
The diagram in *Figure 2* illustrates the format of an Ethernet packet with a brief description of each field:

- Preamble Field: Used for synchronization, 64-bits
- Destination Address: Ethernet address of the destination host, 48-bits
- Source Address: Ethernet address of the source host, 48-bits
- Type of Data Encapsulated, e.g., IP, ARP, RARP, etc., 16-bits.
- Data Field Data area, 46-1500 bytes, which has:
  - ➢ Destination Address - Internet address of destination host
  - ➢ Source Address - Internet address of source host
- CRC (Cyclical Redundancy Check): Used for error detection

Incorrect hardware configurations, faulty network interface cards, or cabling that exceeds the maximum length, are a few sources of errors that can be introduced into the network causing network performance to suffer. The PQ testing must verify that the percentage of network errors is small when compared to the overall traffic. Additionally, PQ testing must verify that bandwidth utilization is not consistently high, because switches will drop packets that cannot be processed. The following are a list of parameters to be verified with some suggested limits:

- End to end loss of Ethernet packets. This usually occurs when the network is being over utilized and frames cannot be processed fast enough or when frames are corrupted. When frames are lost, the transmitting end may resend the frame, but this will degrade network performance.

Figure 2



The maximum throughput expected on a network switch is between 80% and 95% of the available bandwidth. Therefore, the maximum sustained bandwidth utilization should be at 80% to avoid packet loss and retransmissions. Occasional packet loss may occur, but should not exceed 2% of the total network traffic.

- Ethernet packets have certain rules regarding packet size. Depending on the Ethernet packet type, frame sizes can range from 64 bytes to 1,518 bytes in length. A short or ghost packet is any packet smaller than 64 bytes. It is possible for an NIC, transceiver, or even a corrupted LAN driver to generate long and short frames. The cause is usually isolated to a failing network interface card. Captured long or short packets may not include reliable address fields. These packet size errors are often referred to as long, short, or ghost packets and these types of errors should be less than 3% of the total network traffic.

- A collision is the mechanism used by Ethernet to control access and allocate shared bandwidth among stations that want to transmit at the same time on a shared medium. Because the medium is shared, a mechanism must exist to detect that two stations want to transmit at the same time. This mechanism is collision detection.

  Late Collisions are input errors due to a collision that occurs after a station has been transmitting for some period of time. Late Collisions indicate that the time to propagate the signal from one end of the network to another is longer than the time to put the entire packet on the network; therefore, the two devices that cause the Late Collision never detect that the other station is sending data until after both stations put entire frames on the network.

  The proliferation and almost exclusive use of switches in modern day networks has virtually eliminated collision errors, however, cables that exceed their maximum rated length, or faulty network interface cards, may cause collisions. Therefore, these types of errors may occur, but should be less than 3% of the total network traffic.

- A Cyclic Redundancy Check (CRC) "validates" each Ethernet packet. If the packet has been corrupted by the physical network or was sent out with a bad CRC in the first place, the CRC field given will not match one that is computed. CRC errors are also called "Checksum errors" or "Frame Check Sequence (FCS) errors." There can be many causes for FCS errors, including incorrect in-room wiring, faulty Ethernet cards, and cables that exceed their maximum rated length. These types of errors may occur, but should be less than 3% of the total traffic.

- Jabber occurs when garbled bits of data are emitted within the frame sequence in a continuous transmission fashion. The packet length is usually more than 1,518 bytes and can be identified by a protocol analyzer as a CRC error. When nodes detect collisions, they emit a normal JAM signal on the network segment to clear transmission. Sometimes certain nodes attempt to keep jamming the network due to excessive high collision rates, which can be caused by overloaded traffic levels.

> If the bandwidth-utilization levels are normal or low for the particular Ethernet segment, it is possible that the collision detection pair of a jamming node's NIC or transceiver cannot hear the network signal and may not know a collision has stopped. If this occurs, it continues to jam the network. Jabber errors may occur with faulty network interface cards and should not exceed 3% of the total network traffic.

The best way of monitoring the network's performance is by employing the Simple Network Management Protocol (SNMP). SNMP is a set of protocols used for managing networks by sending status messages called Protocol Data Units or PDUs. These messages are stored on the SNMP network device in the Management Information Bases and are provided to authenticated requestors.

Network Analyzers are designed to exploit the SNMP messages by periodically querying the network device and trending the data to provide the current state of the network. SNMP does utilize a small percentage of the network bandwidth, but it is negligible in the overall traffic. The network analyzer is a powerful tool and is used to capture the network health parameters by performing a series of tests.

The first test is a baseline test. The baseline test monitors the network activity over a period of 24 to 48 hours to ensure that the network parameters are within acceptable limits. The second is a load test. In theory, the network can be loaded with dummy data to utilize all the available bandwidth. In practice, this is not realistic since it would bring the network to a halt. Instead, you can simulate a load test on the network by maximizing the application utilization. For example, if there is a Laboratory Information Management System (LIMS) that is configured with five chromatographic analyzers and three user workstations, then a test may include a 24 to 48 hour chromatographic sample run on all five instruments while users perform data analysis on existing data over a limited period of time. The network health parameters can then be monitored as all the instruments generate and transfer data across the network while users perform data analysis functions concurrently. In this scenario, you are testing that the network can handle the maximum load of the application in addition to all the other network traffic.

A third test is a stress test that shows that data can be transferred across the network even when the network utilization reaches the 80% limit. Here again, it is not feasible to stress the entire network, so, instead, the network analyzer can be configured to generate enough data to reach 80% utilization on a specific port on the network switch. This kind of traffic is called unicast traffic and it can be directed at ports on a switch. The 80% utilization of the available bandwidth on a particular port simulates the worst-case conditions allowed by the network health parameter limits without affecting the entire network. If data is successfully transferred from one machine to another, even if the utilization reaches 80%, then this shows that the network is capable of handling the occasional spikes in network traffic.

During the stress test, the unicast traffic can be pointed to the port that connects a data-acquiring device, such as a chromatography instrument. Then the network analyzer can monitor the network health parameters as the instrument generates and transfers data to the server. In a successful test, the network switch does not drop any packets and the data should be acquired successfully, even if the utilization exceeds 80%.

Traceability Matrices are one of the best ways of ensuring that all requirements and design aspects of the system have been tested. The traceability matrix is a table that lists references to each requirement and matches them to the corresponding design element. In some cases, there will be design elements that do not directly correspond to a requirement, because it may be some needed function required to manage the system. In these cases, the design element is still listed on the traceability matrix, but is not linked to a requirement. Test cases are then developed to address every requirement and design element in the matrix. The test case is given a unique identifier and linked to the particular set of requirements and design elements. This tool provides a reference to all testing that was done on the system and is an invaluable tool during an audit.

Maintenance

Keeping the network in a qualified state can seem like an overwhelming task, because it is difficult to keep track of all the computers that are connected to the network. This is especially true with mobile notebook computers that can be connected to the network from different locations within the facility. The easiest way of maintaining a network in a qualified state is to take the metrology concept and apply it to the network.

A network analyzer can be added to the network to monitor traffic and send out alerts when established thresholds are exceeded. If all the network health parameters are within their limits despite the attached computers or the data being transmitted, then the network is functioning as designed. Most modern day network analyzers are capable of providing standard and customized reports on a daily, weekly, and monthly basis. These reports can then be submitted as objective evidence that the network is

functioning within specifications. Additionally, the same network analyzers have the added benefit of maintaining a network inventory list and are capable of providing real time network topology diagrams. These features can be used to detect problems, identify rogue networks, and maintain the network in a qualified state.

The retirement of a network device is also a part of the maintenance phase. When a device replaces a retiring device that performs the same functions and the new device comes from the same vendor, then all that is needed is a qualification of the device that is tested by the standard test script.

One caveat to this approach is that most commands may be the same in the device's operating system, but there may be some commands that have been deprecated and replaced by others. In such cases, it is recommended that a dry run of the qualification protocol be performed on the network device prior to replacing the old device to identify any issues with the test script. If a discrepancy between the test script and the device is found, then new steps can be added to either the addendum or a new family test script can be created.

CONCLUSION

Network qualifications may seem like an ominous task, but in reality, with the right tools, and an understanding of how the networking technology works, this task is both manageable and straightforward. ❑

SUGGESTED READING

1. "*Commercial Building Telecommunications Cabling Standard TIA/EIA-568-B.*" TIA/EIA Standard, (May). 2001
2. FDA. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*
3. FDA. *Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application*
4. Fields, T. "Establishing a Sound IT Infrastructure in a GXP Environment." *Journal of Validation Technology*, Vol 9, No. 3 2003, pp. 229-234
5. Haudahl, J. S., Network Analysis and Trouble Shooting. Addison-Wesley: Upper Saddle River, 2000, pp 357.
6. Hay, D. C., Requirements *Analysis: from Business Views to Architecture.* Prentice Hall PTR: Upper Saddle River, NJ, 2003, pp xxxvi, 458.
7. McCabe, J. D., *Network, Analysis, Architecture, and Design*. Elsevier Science San Francisco, USA. 2003, pp 501.
8. Neal, C., "Prerequisites for Successful Validation," *Journal of Validation Technology*, Vol 9, No. 3 (May), 2003, pp. 240-245.
9. Tracy, D. S. and Nash, R. A., "A Validation Approach for Laboratory Information Management Systems," *Journal of Validation Technology*, Vol 9, No. 1, (November), 2002, pp. 6-14.

Article Acronym Listing

CRC	Cyclic Redundancy Check
EIA	Electronic Industries Alliance
FCS	Frame Check Sequence
GXP	Good Manufacturing, Laboratory, and Clinical Practice
IQ	Installation Qualification
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NIC	Network Interface Card
LIMS	Laboratory Information Management System
OQ	Operational Qualification
PDU	Protocol Data Unit
PQ	Performance Qualification
QA	Quality Assurance
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TIA	Telecommunications Industry Association
VLAN	Virtual Local Area Network
WAN	Wide Area Network