CHAPTER 1

Conducting a Network Audit

You bought this book to find out which management data to collect from the network, so why is the first chapter about audits and documentation? Simply put: You can't measure performance and watch for faults effectively without understanding where everything is and how it's connected. No matter how sophisticated the tools you purchase or build may be, the measures and alerts mean nothing without understanding how the network works.

Effective network management begins with a well-designed network. Unfortunately, most people do not have this luxury; if they do have network access, they usually cannot redesign the network to improve their ability to manage the infrastructure. Aside from simplifying the management, starting with good network design or improving existing network design facilitates simpler and quicker resolution of network problems.

In order to implement effective network management, you must begin by learning and documenting the network as it currently exists. This includes documenting the physical and logical makeup of the network and its components, the people involved and their responsibilities, and the processes in place (if any) to enhance and maintain the network. These are the steps that make up a network audit. This chapter describes the primary tasks that are useful for learning and documenting how the servers, network devices, and users are connected. By learning and documenting the physical connectivity and logical configuration of your network, you will simplify the troubleshooting process when problems arise. The resultant information provides the foundation and integrity necessary to proceed with the creation and seeding of the knowledge base described in Chapter 3, "Developing the Network Knowledge Base."

Although not an exhaustive study, this chapter covers the following topics:

- The purpose of network audits
- Why documentation is important
- Conducting a physical inventory audit
- Conducting a connectivity audit
- Conducting a process and personnel audit

The Importance of Network Audits

The purpose of a *network audit* is to accurately assess and document the current state of the network, its components, the people involved, and the human processes used. The audit, in effect, documents the purpose and priorities of the network. Without the audit, you must rely on people's memory, hearsay, and possibly out-of-date or inaccurately documented maps and databases.

Without proper documentation and understanding of how things change in the network, you cannot reliably deploy performance and fault network management. You must determine how all devices are connected to each other—both physically and logically—and where the network components are located. From this information, you can determine which devices, ports, and connections are important for the development of your performance and fault management strategy.

NOTE When you are working with outside consultants for network design or management issues, the network audit should be the first action they initiate. Without understanding the components, people, and processes, an outside consultant cannot accurately determine the state of the network and develop a plan of action. Regardless of your company's level of documentation, the consultant must still verify that the information matches the physical reality.

Without a proper understanding of physical connectivity and the location of network components, it will take longer to isolate network problems and you stand a greater chance of mistakenly introducing faults into the network during moves, adds, and changes.

Although commercial auto-discovery and mapping tools do a good job of drawing logically connected networks, they cannot discover on which floor, building, desk, or closet the devices are located. Trace a cable under the floor or between closets at 3 a.m. and you'll never underestimate the importance of a physical map again!

When a portion of a network goes down or becomes unstable, troubleshooting the source of the outage is done through a process of fault isolation. During an outage or fault, network administrators work as quickly as possible to search out and isolate the source of the problem. In order to do so, they typically begin somewhere in the middle or at the edge of the affected area, and work to reduce the fault domain or area of affected devices. The goal is to get as much of the network operating around the fault domain as possible. With proper documentation, this goal is much easier to achieve. In addition, in a well-documented network, the network manager knows which applications and users are affected by a problem, and can proactively notify the user community.

In a poorly documented network, fault isolation becomes a game of finding a needle in the haystack. The goal of fault isolation is to reduce the affected area; how can you do so if

there is no documentation? Some administrators resort to brute force by splitting networks in half or randomly plugging and unplugging connections until they narrow down the affected areas. This prolongs the time to resolution and increases the chance of introducing additional faults. It also frustrates and angers users (and your boss) as they witness flaky, intermittent service.

All in all, the inconvenience of maintaining useful network documentation will be most appreciated during outages.

If you have not previously documented your network as described in this chapter, you will need to begin the process by auditing the physical network and its connectivity. Through the audit, you will learn and document which devices are in your network, where they are located, how they are connected, and who is responsible for the device. This will be the starting point for your network documentation.

As part of the audit, you will identify those ports that are critical to the successful operation of the network. Critical ports tend to be those with routers, switches, hubs, servers, channel service unit/data service units (CSU/DSUs), and the key users (such as the CEO) connected to them.

Monitoring all ports and connections in a network can be overkill and cause over-management of the network. Monitoring generates traffic load on the network and sucks up network device resources (memory, CPU). Is it really necessary to monitor user ports? Probably not, although you may want to monitor the traffic performance on key user ports in order to use them as a baseline for their floor or workgroup.

TIP If a device or port goes down and nobody cares, don't manage the port any longer. Manage only those devices and ports that are critical to the operation of the network.

In order to select which ports to monitor, you must know how your network is connected, both physically and logically. Without this information, the importance of a port cannot be determined. The network management infrastructure can become crippled with information from devices (such as user PCs) that have no impact on the operation of the network. You must determine where network devices and servers are located, how they are connected, and who is affected if they become slow or unavailable.

The Importance of Documentation

Unless you were lucky enough to build your network from the start, chances are that you inherited an "organically grown" network. Perhaps different independent networks were built years ago and subsequently connected to the corporate net, or different organizations have had control over parts of the network and turned over their control to your

organization. Or perhaps your group has grown the network over the years but has not documented the changes. However your network has grown, trying to manage it without understanding where devices are and how they're connected can be extremely difficult.

Documenting and tracking the physical inventory and logical connectivity will not only simplify the task of implementing effective network management, but it will also greatly enhance the timeliness of problem resolution. With the network being the backbone of corporate data exchange, your group's timeliness in resolving network problems has the ability to affect the enterprise's bottom line.

If a financial firm loses the capability to trade stocks due to a network outage, not knowing where network devices are located and how they are connected ultimately translates into lost revenue for the company. Do you know how much money per hour of downtime your company loses with unplanned outages?

Documentation can be maintained on anything from scraps of papers and napkins to intricate database systems. Ultimately, however it's maintained, the documentation should communicate its contents clearly and should easily be shared by those who need the information. It must also be easy to update and modify by those who need to.

The ultimate test is at 3 a.m. when you are paged out of bed to determine why several buildings dropped off of the network. If you find yourself tracing cables and wondering whether a router is connected to the right switch despite your documentation, perhaps it is time to reconsider your documentation practices.

Please see Chapter 9, "Selecting the Tools," for more details on criteria for tools that can help you with documentation.

TIP

Effective and reliable documentation must contain the following traits:

- A consistent and integrated method for storing information, such as a database or spreadsheet.
- Non-intrusive processes surrounding the maintenance of the documentation. If the docs are too difficult to keep up-to-date, the documentation will be rendered useless.
- Easy online access to the documentation for those who need it. This includes viewing as well as updating the documentation.
- Automation (self-documenting) whenever possible. Automated data collection helps you keep your documentation up-to-date.
- Port standardization and interface description usage (discussed later in this chapter).

It is important to determine the usefulness of each form of documentation and compare it to the organizational cost (that is, the difficulty in maintaining it). Sometimes, organizations

can get documentation paralysis in which the maintenance of a particular piece of documentation overweighs its usefulness. It tends to be a matter of trust with documents because after the users of a particular document or knowledge base find that the information is out-of-date or wrong, they lose trust for the information. And after a couple of attempts that result in the discovery of out-of-date information, the documentation will no longer be used.

Ultimately, there is a natural balance. Too much documentation is difficult to maintain and becomes useless. Not enough documentation results in not having information when you need it.

Part of maintaining accurate documentation is implementing automated methods for updating the information. For instance, in a network made up of Cisco devices, you can automatically discover and track physical connectivity between routers and switches by using the Cisco Discovery Protocol (CDP). Or, the location of Media Access Control (MAC) addresses can be tracked by querying the Content-Addressable Memory (CAM) tables from the LAN switches.

Unfortunately, there are preciously few tools that take advantage of this information to produce a Layer 2 topology. The CDP and CAM tables are available via SNMP, enabling you to build your own applications.

Some things cannot be automated, such as physical wiring termination. For those that cannot be automated, you should work to integrate the documentation of a change into the overall process of making the change.

Take the running of new cables between wiring closets as an example. As part of running the cables, labels that identify the source and the destination of the run should be created and attached to the wiring racks. In addition, labels that identify either end should be attached to the cables themselves.

Whenever a connection is physically modified, the change should be indicated in a knowledge base, which is discussed in Chapter 3, “Developing the Network Knowledge Base.” Thus, the database becomes the source of connection information.

TIP Following are some tips on tracking and documenting moves, adds, and changes. Although these tips describe the best possible tool scenario, they should be used as goals when building and buying software:

- Make changes electronically in a method that allows the change to be automatically documented when the change occurs. Examples include activating a previously unused switch port or switching a user to a different VLAN, and capturing the changes through syslog messages and SNMP traps.
- Integrate the change tools so they populate the knowledge base automatically.

- Integrate the change tools with a change management tool so overlapping or competitive changes are regulated and documented appropriately.
- Make sure that configuration changes can be tracked and logged. Using tools that track user configuration changes and enforce configuration policies will help you prevent and/or track unauthorized and mistaken changes.

Conduct a Physical Inventory Audit

The first step in a network audit is to identify physical network assets. The audit provides a nice side benefit because you can collect the device asset information. If your company requires the collection and reporting of asset information, you'll be able to do both with the same effort.

A physical inventory audit consists of the following:

- Documenting the wiring closet locations
- Documenting the wiring
- Documenting the network devices
- Documenting the servers
- Documenting the key users

Where Are Your Wiring Closets?

It's 2 a.m. and the network is down; do you know where your wiring closets are? Surprisingly, some enterprises would have to answer "no" to this question.

You must document the location of each wiring closet, lab, and raised floor area in which cabling terminates and network devices are located. This is an important step in documenting the network because knowing where the wiring closets are helps you determine where connections terminate. The documentation of wiring closets will become invaluable when fighting network problems and trying to isolate the source of a problem.

You should document the location of each wiring closet in two ways. First, develop and maintain a list of wiring closets that contains the following information about each location:

- Building, floor, and location
- Name of wiring closet
- Key or badge type of access
- Description of purpose (for example, server room, floor 2 wiring, or development test lab)

Second, obtain building engineering documents and mark up the wiring closet locations. By visually representing the wiring closets, such documents aid you in understanding the relationship of the wiring closets to each other.

TIP Scan the plans or save them with a CAD system as JPEG files and put them on a secured website. Link them together so that a person can drill down. Starting with a map of the various corporate sites, drill down to a location, then a building, then a floor—and up pops the appropriate floor plans with the wiring closets highlighted. This procedure can help your operators or anyone else needing access to the wiring closets to quickly drill down and determine the location.

If you are not sure where each of the wiring closets are, this is a perfect opportunity to hunt them down and understand what state of disrepair they may be in. If you end up visiting each of the wiring closets in order to verify their location and purpose, use the opportunity to answer the question raised in the following section.

NOTE While you're out inventorying the wiring closet, make sure you lock them down. It becomes an impossible task to maintain good documentation and integrity with the network when multiple groups of people with possible conflicts of interest have access to the wiring closet.

If someone walks in and moves cables around or switches off a device, you may be ultimately held responsible for their actions.

Where Are Your Wires?

You've got wiring closets spread all over the campus, perhaps all over the world. Fiber between floors, service provider demarcations, cables running under a bridge, copper running between wiring closets—all of these become indistinguishable when you are sitting in a wiring closet or computer center trying to isolate a problem. You must have and maintain accurate schematics of wiring termination and purpose.

The main purpose of a cabling audit is to ensure that connections run where you think they run. This is important when documenting the logical connections.

The easiest method to track connections is by implementing an organized labeling system in the wiring closet by labeling both ends of a cable with the same label. The label should clearly identify the source, destination, and purpose of the cable. Thus, when looking at a cable or a wiring rack, you can clearly understand the purpose and termination of the cable.

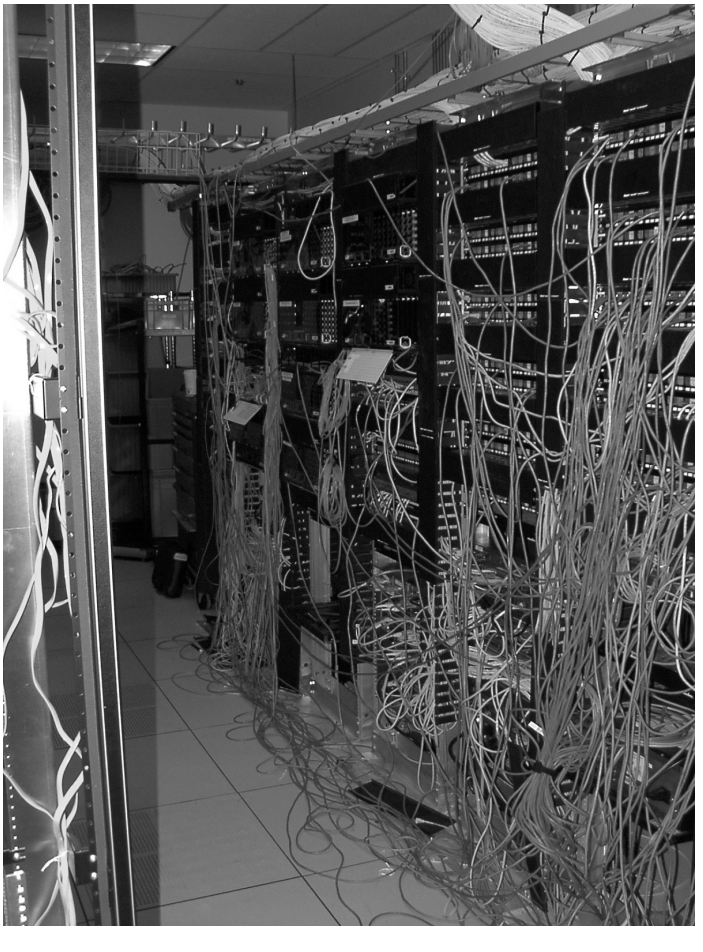
Select a Wiring System that Fits with Your Organizational Needs

There are plenty of vendors who offer organized wiring systems. The goal is to purchase racks that make it easy to snake wires to their connection points and contain labels identifying the wire's purpose or destination at the other end.

Rack systems provide multiple color labeling and connectors, allowing you to color-code the type of connection. For example, you may designate blue to represent servers, red to represent wiring closet connections, yellow to represent user connections, and so on. Using the colored wires that match the colored connectors allows for easy identification of a wiring mistake.

A poorly maintained wiring closet makes troubleshooting become more complicated than it need be. In Figure 1-1, cables are going everywhere (including on the floor), making it very easy to introduce more problems during troubleshooting.

Figure 1-1 *An Example of a Bad Wiring Closet*



Too frequently, network administrators have been shocked to find out that a connection is not what it seems. For example, what they thought was a connection to a new server was actually a redundant link to a switch that happens to have spanning tree turned off. The result: a bridging loop that may cripple the network.

There are standards for organizing wiring and wiring closets, such as structured tested cabling and wiring closet locations. You should review these standards and stick with those that work with you.

Finally, be sure to keep your wiring closets organized. The identification systems in place (such as color-coding) do no good if patch cables are hanging all over the place. Motivate the operators to keep clean wiring closets with cables tucked away properly and everything labeled appropriately. This will greatly simplify the identification of connections while troubleshooting problems.

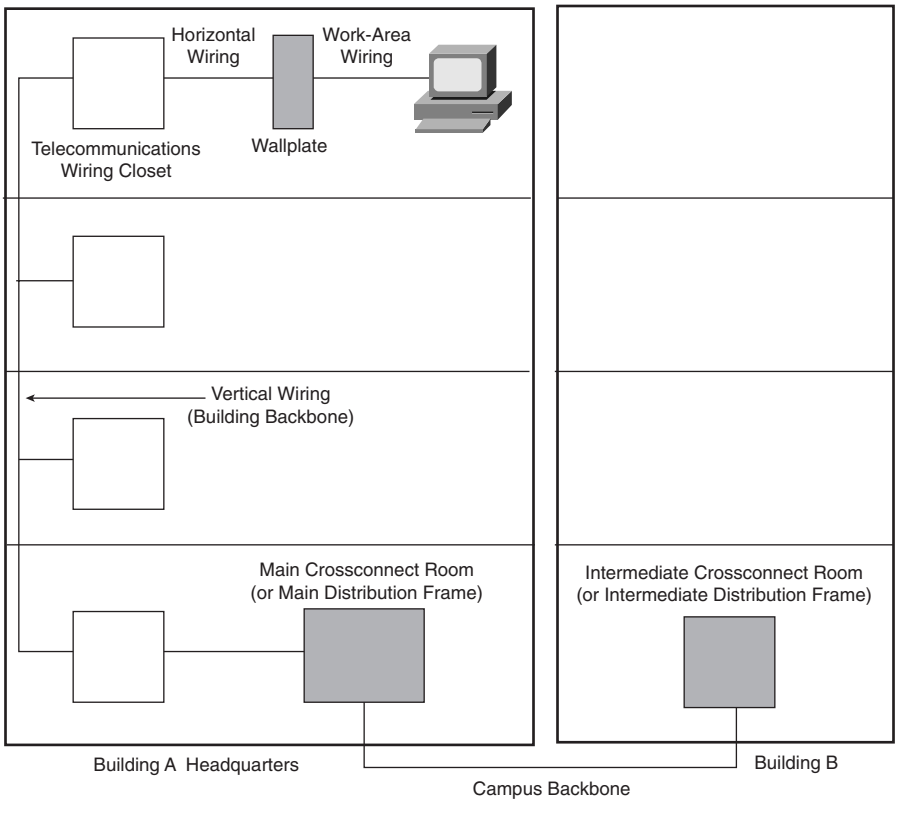
If you haven't tracked physical connections or feel that the current documentation method is out-of-date, you will need to audit each wiring closet and trace where the wiring goes. This can be a tedious process, especially if you have no idea of the state of the cabling.

TIP If you have a third party managing your cable for you, be sure that they maintain the labeling as they make changes. Build incentives into their contract, which are based on the cleanliness and accuracy of the wiring closet.

In addition to cleanly running and maintaining cabling, they should remove cables that run nowhere—that is, cables that once connected network devices that have been removed.

Figure 1-2 is an example of a typical floor wiring diagram.

Figure 1-2 *Example of a Floor Wiring Diagram*



This example represents a typical floor wiring diagram in which the source and destination of wiring is documented. Table 1-1 is used to document the wiring locations and terminations.

Table 1-1 *Example of a Wiring Documentation Table*

Building Name:
Location of telecommunications closets:
Location of cross-connect rooms and demarcations to external networks:
Logical wiring topology (structured, star, bus, ring, centralized, distributed, mesh, tree, or whatever fits):

Table 1-1 *Example of a Wiring Documentation Table (Continued)*

	Coaxial	Fiber	STP	Category 3 UTP	Category 5 UTP	Other
Vertical Wiring:						
Vertical Shaft 1						
Vertical Shaft 2						
Vertical Shaft *n*						
Horizontal Wiring:						
	Coaxial	**Fiber**	**STP**	**Category 3 UTP**	**Category 5 UTP**	**Other**
Floor 1						
Floor 2						
Floor 3						
Floor *n*						
Work-Area Wiring:						
	Coaxial	**Fiber**	**STP**	**Category 3 UTP**	**Category 5 UTP**	**Other**
Floor 1						
Floor 2						
Floor 3						
Floor *n*						

Where Are Your Network Devices?

You've found and documented all of the wiring closets worldwide and implemented a well-documented wiring system with labels. Now, it's time to physically learn and document the location of the routers, switches, hubs, firewalls, and other network-related equipment that make up your network.

You should start by collecting and recording an inventory of the devices and their locations. At a minimum, you should track the following:

- Device name
- Device location

- Device IP address (the IP address to manage the device by)
- Person or group responsible for the device

Note that although manual tracking of information is quite common, you should consider automating the collection of device information and the association of that information with contact information. For instance, use a Layer 3 auto-discovery routine to generate the device list. Then, have a routine query each of the devices to obtain the MIB II sysContact and sysName variables to correlate the device name and contact name. The routine can then use the contact name to look up contact information (phone number, pager).

The final report would then include all information listed previously, but would be generated in an automated fashion. This will save time compared to the manual method as well as increase the chances that the documentation is up-to-date and accurate.

Table 1-2 is an example of a spreadsheet used to track network devices.

Table 1-2 *Example of a Spreadsheet for Tracking Inventory*

Device Name	Device IP Address	Device Location	Contact Information
bb-rtr-01	10.50.50.1	Building 4	Adam Smith
		Floor 2	999-999-9999
			800 page-me1
		Rack 3	afrog@fake.edu
bb-rtr-02	10.50.50.2	Building 4	Adam Smith
		Floor 2	999-999-9999
			800-page-me1
		Rack 4	afrog@fake.edu
bb-sw-11	10.50.50.102	Building 4	Gina Jones
		Floor 2	999-999-8888
			800-page-me1
		Rack 4	jedi@fake.edu

In Table 1-2, the network manager chose to track the minimum amount of device information, as well as the device contact. Typically, the contact is the person who should be called when an incident involves the owned device.

Collecting Other Inventory Information

Inventory information, such as serial number, firmware revs, hardware revs, software and configuration, is extremely useful for the network management process.

Serial numbers are particularly relevant for tracking your assets and working with Cisco support. Unfortunately, some devices do not provide their serial numbers via SNMP (this is mainly because of the way the devices are manufactured). When this is the case, you can set the serial number via SNMP by entering the **snmp-server chassis-id** command and providing the serial number.

Some companies have to march through their wiring closets and server rooms every couple of years to document devices for asset tracking purposes. This usually involves verifying that each device has an asset tracking "brass tag" on it and that the equipment is where it was thought to be.

If this is your experience, you should consider purchasing or developing software that automates the collection of this information. Cisco and other vendors provide software that performs this function.

Where Are Your Servers?

Tracking the location of shared servers and how they are connected into the network is just as important as tracking network devices. Too often, when a user complains of slow response time, the server support teams point the finger at the network support team. By knowing how servers and key applications connect into the network, you will be able to determine definitively whether the source of a slow response problem, for example, is the network or a device connected to it.

Using the methods described in the previous sections, you should document where the servers are physically located and how they connect back to their associated switches or hubs. Server types include the following:

- File and print servers
- Mainframes
- Network infrastructure servers such as DNS/DHCP servers
- Corporate web servers
- Any other shared devices that are considered critical to a particular operation

Table 1-3 illustrates a server tracking spreadsheet.

Table 1-3 *Example of a Server Tracking Table*

Device Name	Device IP Address	Device Location	Switch	Switch Port	Contact Information
mail-02	10.29.30.2	Building 4 Floor 2 Rack 3	Ser-sw-01	4/2	Adam Smith 999-999-9999 800-page-me1 afrog@fake.edu
mail-03	10.29.30.3	Building 3 Floor 2 Rack 1	Ser-sw-01	5/2	Suzie Q 999-999-8888 800-page-me1 suzieq@fake.edu
dns-02	10.40.44.2	Building 3 Floor 2 Rack 1	ny-sw-07	2/7	Adam Smith 999-999-9999 800-page-me1 afrog@fake.edu

Documenting the servers, as shown in Table 1-3, is important when troubleshooting. It also makes a handy reference when performing administrative tasks on the servers.

You may consider working with the server administrators to develop a questionnaire that identifies relevant information concerning each server that would help to understand the server and its application's availability. Examples include the documentation of the following:

- How the server is configured
- What applications run on the server
- What group or business unit owns the server
- Preventive maintenance and backup schedules.

By documenting and keeping accurate the server information, your operations staff will be able to distinguish between planned maintenance and unplanned outages. The server administrators may never offer thanks, but you will impress them when your network documentation actually helps them do their job.

Where Are Your Key Users?

For larger organizations, it can become burdensome to track every network connection for every user. Each managed connection requires a bit more hard disk space and network bandwidth. Only those ports that are considered business-critical should be monitored. This avoids filling event logs with link-down messages when users turn their PCs off for the day. Additionally, monitoring that many ports will generate reams of data that will probably not be used and can complicate the reporting process.

Network performance and server access for a user or group of users can be inferred by measuring the availability and performance of the connecting network devices and servers involved. This conserves the amount of polling to the network devices (because information for every hub or switch port will not be generated) and considerably cuts down the amount of stored data to process.

However, from a management perspective, monitoring certain key users may still be important. It can be helpful to identify a single user out of a group in order to measure their network connectivity and performance. The information from the single user can then be used to infer performance for the rest of the group. For instance, you may choose to monitor the network port for named users from individual groups in order to use the port as a gauge for the availability of the network for the entire group.

It may also make political sense to monitor the ports of certain executives (or "mahogany row") to ensure that you catch performance problems before they occur. With both fault and performance monitoring, it is usually in the network manager's best interest to ensure that the boss's connection is running smoothly. This may seem sneaky or underhanded (it is), but it generally ensures that the executive's view of the network (and, therefore, your company's investment in the network) is as fast and clean as the network infrastructure. You do not want the VP of Sales who is responsible for your network's funding to call in a network down or performance problem with their connection.

You should never sacrifice the performance and availability of network services for a group of people in order to provide greater-than-ordinary access to an executive. Or as Spock once said, "The needs of the many outweigh the needs of the few or the one."

NOTE Sometimes, catering too much to the executive level can backfire. It may be advantageous to have certain executives experience network problems, as felt by the majority users, in order to gain budget. If this is the case, let them feel your pain!

Conducting a Connectivity Audit

Understanding how devices are logically and physically associated with each other is the next step of a network audit. Without tracking this information, you can never be sure what the true source of traffic to a device can be. It makes a huge difference whether traffic coming into a switch is from a server, user, or another switch. When deciding which ports to monitor in the network, you may mistakenly choose not to monitor a particular port because you thought it was a user port, when in fact it was the mainframe connection.

Unfortunately, after the audit is complete, you must maintain the currency of the documentation. The nature of business is that people move (and so do their connections), devices move, and networks undergo change. As a result, the documentation will be good as long as it is accurate. As soon as its accuracy declines, people will learn not to trust the information and eventually find other methods to keep track of network connectivity. Most of the time, the alternative method is guesswork, which leads to unnecessary outages due to mistakes.

Connectivity maps tend to be the most-used pieces of documentation with network operations. Therefore, it is important to integrate appropriate maintenance of the information within the framework of work. Don't let the information get out-of-date.

Documenting network connectivity consists of the following:

- Standardization
- Layer 2 Automation
- Layer 3 Automation

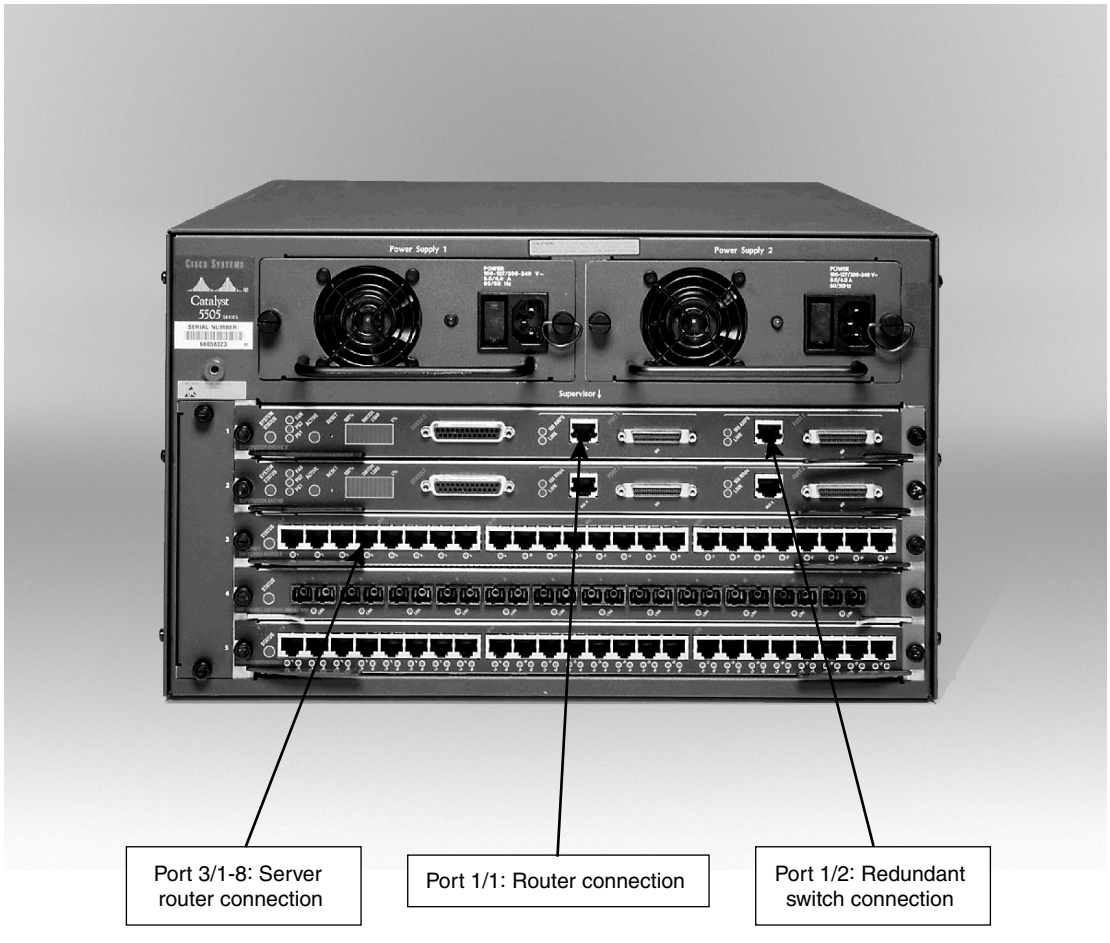
Standardization

Standardization involves setting up standard methods for naming, connecting devices, and locating equipment. Develop a naming scheme that will allow people (and automated tools) to quickly identify the type and use of a device. Use DNS names, hostnames, and interface descriptions to implement the naming. Interface description usage is especially helpful because the description can be obtained both from the device configuration file as well as SNMP.

Another form of standardization involves consistently using physical ports on devices to identify the type of device connected. For instance, the first port of the first card on a Catalyst 5000 could be used exclusively for connecting building routers.

Figure 1-3 provides an example of port standardization. In this case, port 1/1 is used for connection back to the backbone router, whereas port 1/2 is always used to connect to a redundant switch.

Figure 1-3 *Example of Port Standardization*



You should also indicate the purpose of the port in the configuration of the port name or interface description. For example, the switch in Figure 1-3 might have port names such as *bb-rtr-2* for port 1/1 and *redun-flr1-sw-2* for port 1/2.

Finally, you can standardize on IP address assignment. For instance, for each subnet, the following host portions would be reserved:

- .1–.9 are reserved for routers, switches, and RMON probes
- .10–.20 are server addresses

So, if you see a problem with an address such as 172.26.10.6, you would know that it is a router, switch, or RMON probe, as opposed to a user workstation or server.

Documentation Using Data Exchange

Network administrators typically begin documenting physical network and connection information using spreadsheets. With spreadsheets, it's quite easy to quickly create something for tracking IP address assignments, wiring schemes, and just about anything else. Spreadsheets are quick and easy to set up, but do not work well when trying to build an interconnected and automated knowledge database.

If you determine the need to move beyond spreadsheets, you should consider software built upon a relational database that will allow the tracking of assets and how they're connected. Chapter 3, "Developing the Network Knowledge Base," describes the selection and building of a knowledge database.

Regardless of your approach, you should strive to implement a software solution that can integrate with other database systems such as your network monitoring, element management, and HR database systems (for contact information). Data exchange among various systems will allow the presentation of a more unified system to its users.

Layer 2 Connectivity

The next stage of a connectivity audit involves learning and documenting the physical relationships between devices. In this context, the physical relationships include the following:

- The physical locations of the devices
- How the devices are connected together
- The name of one device's port that connects to the name of its neighbor's port (for example, switch 1 port 2/1 connects to switch 2 port 1/1)
- Redundant paths (for example, HSRP router peers and redundant bridged paths, port channels)

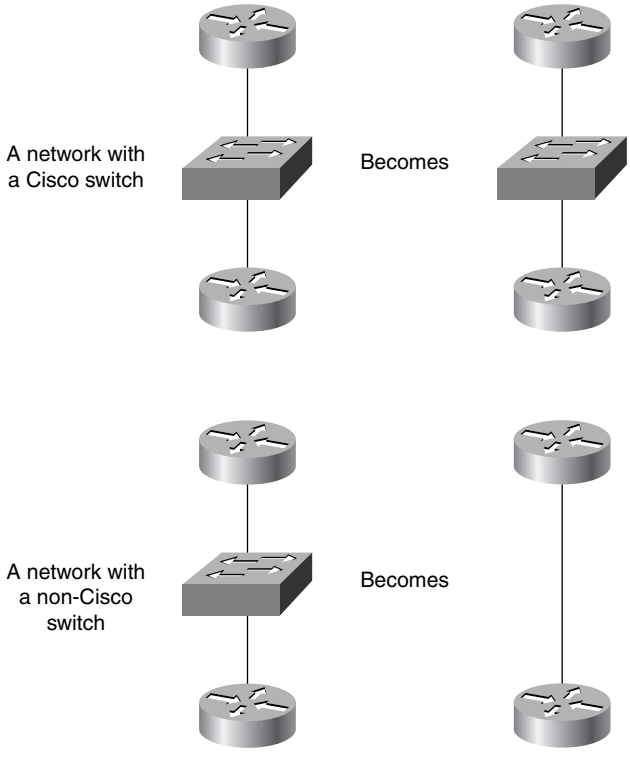
Network management software from Cisco and other vendors provides Layer 2 discovery in which given a particular switch, Layer 2 and physical relationships between switches and routers can be discovered. The software can be used to seed your documentation with the current connectivity of devices, which generally requires the use of proprietary protocols. This is because there is no standard method for network devices to learn and report their Layer 2 neighbor relationships.

With Cisco devices, the Cisco Discovery Protocol (CDP) is used. CDP runs on each Cisco device and allows it to track those Cisco devices connected off of each of its ports. CDP works well in an all-Cisco network for documentation and troubleshooting, but becomes

less useful in a multi-vendor network because non-Cisco devices do not participate in CDP, and thus will not be known by their neighbor.

Figure 1-4 compares the CDP discovery of Cisco devices with a Cisco and a non-Cisco device in-between. If a Catalyst 5000 connects two Cisco routers, a CDP discovered map would display the proper relationship. However, if two Cisco routers are connected by a hub or switch from another vendor who does not participate in CDP, the map will simply display the routers as directly connected without a switch in-between.

Figure 1-4 *CDP Discovery with a Cisco Switch and a Non-Cisco Switch*



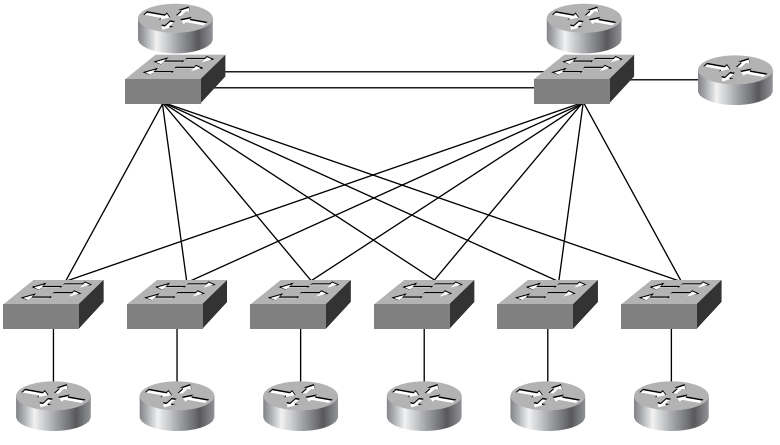
A CDP discovery application generally requires the specification of a starting, or seed device. The seeding involves manually entering a device name or IP address, community strings, and possibly Telnet passwords for each device of interest. This provides the auto-discovery routine with enough information to be able to interrogate the device for more information. The downside of this approach is that if devices are swapped out, moved around, or reconfigured, the changes must manually be tracked.

Given the seed device, the application queries the device's CDP neighbor table. Once discovered, the application can continue to track the changes that occur in the network. The discovered network can then be displayed or printed in map form.

The map displays the physical connectivity relationship between network devices. For each device, there is a line that connects to each of its physically adjacent network device peers.

Figure 1-5 provides an example of a map that was discovered using CDP. Notice that the map is able to display the Layer 2 and Layer 3 relationships of Cisco devices.

Figure 1-5 *Example of a Hypothetical Map Discovered Using CDP*



By using CDP, the application can determine how each device is physically connected, down to the port/interface number. Unfortunately, auto-discovering the physical relationships among multi-vendor networks is considerably more difficult because of the complete lack of standard neighbor discovery protocols.

Cisco has submitted the CDP standard to the IETF.

Layer 3 Connectivity

Unlike physical connectivity, Layer 3 connectivity is easier to auto-discover and map. This is mainly due to public domain methods and MIBs to collect the necessary information.

Logical connectivity maps demonstrate the distribution and relationship of network layer addresses. There are multiple methods for documenting logical connectivity (as mentioned for physical connectivity), including auto-discovering network management software, spreadsheets, and databases.

The data/reports should then be made available to those who need it. You could generate reports or capture screen shots and place them on an internal web server. Or you could simply print them out and distribute. (Don't forget to date them so people know whether they've got the latest version.)

In addition, DNS and DHCP servers can be used to capture and enforce the distribution of addressing. Network management products that auto-discover logical networks can also be used as reference documentation.

TIP Never allow network devices to dynamically learn their network addresses. You should always assign a static address so that the device is definitively known by that address.

Automatic discovery of logical connectivity is relatively commonplace in today's network management tools. By parsing through each router's routing table, an auto-discovery routine can determine the neighbor router for each learned route. The routine then can query the routing table from the neighbor and discover the neighbor's neighbors.

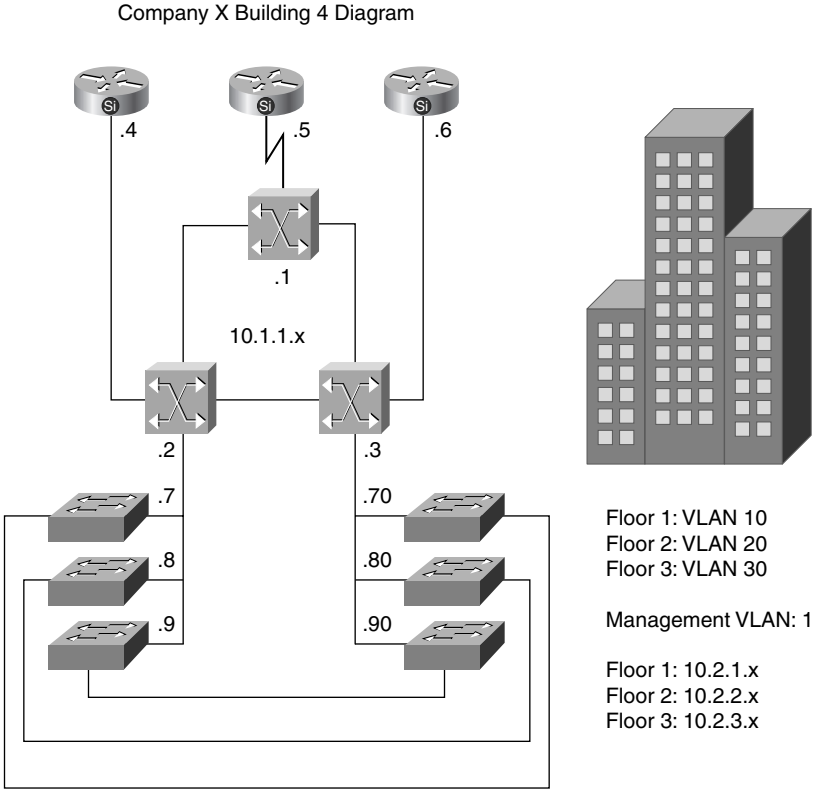
TIP You can take certain preventive steps to help auto-discovery routines more accurately discover your network and in general provide you with a cleaner network to manage:

- Ensure that the network management software is installed with the latest patches. This will help prevent bugs that may exist with the base release of the software.
- Ensure that the IP addresses for each network device are consistently and appropriately named across your DNS servers. Problems can arise when two DNS servers refer to the same IP address with different names. Also, problems can arise when an IP address has multiple names associated with it, the reverse lookup name doesn't match the forward lookup name, or finally two IP addresses are associated with the same name. Ensure that there are no duplicate IP addresses in the network. This situation, aside from causing more general connectivity issues, causes difficulty for network management software. Software vendors must take special cases into consideration when writing their software (for example, fault-tolerant features such as HSRP).
- Use consistent SNMP community strings across all devices and network management software. When the strings vary from device to device, some network management software might not be capable of handling the differences. Some network management software might have to wait for the use of the first incorrect community string to time out before trying the second correct community string. This causes unnecessary delays. Inconsistent community strings occur frequently when different groups in an organization manage different types of devices.

There are third-party tools available that allow you to draw the network connectivity as it makes sense to your organization. One method for mapping the logical network is to draw maps that display the physical network and identify the IP addresses and networks between network devices. You may also choose to incorporate connecting port and server information as well. You may also choose to store MAC addresses in the system.

Typically, hybrid maps will evolve in which logical and physical information is displayed together. This is the kind of information that people will print out and store in their notebooks or pin up on the wall. Figure 1-6 provides an example of a hybrid map.

Figure 1-6 *Example of a Hybrid Connectivity Map*



In this map, notice how physical connectivity, physical device traits, logical addressing, and VLAN information are displayed on the same map. Notice the following:

- The IP addressing is indicated for each of the network interface.
- A picture of a building provides a quick visual cue that we are talking about the building network infrastructure versus a floor or campus.

- The pictures of the devices themselves provide visual cues as to the type of device.
- VLANs are indicated by color, thereby weaving in the Layer 2 element of the topology.

Who Is Responsible for the Devices?

For larger organizations, tracking-device responsibility is the next step in a network audit. Typically, this type of tracking involves matching a device name or device type with a particular person or group. Some companies take this to the next step by linking the person or group with an HR database, and thus being able to associate a device with the location, phone, and beeper of responsible parties.

Tracking device responsibility becomes important when determining what types of performance reporting to produce and who should have access to the reporting.

Process Analysis

The final step of conducting your audit is process analysis. Process analysis means learning the various processes used to design, maintain, and troubleshoot the network. By understanding how things get done in your organization, you will be able to more effectively make process changes to help document your network.

Specifically relevant to this chapter, the following will help determine how effectively you can maintain the information gathering:

- Is there a change control process? If so, is it adhered to?
- How does each form of documentation get updated?
- How does a fault get created and tracked?
- How are the causes of outages determined and documented?
- How is customer satisfaction tracked?

The study of organizational processes is not for the faint of heart. There are plenty of resources and consultants available to assist you with this process. Kornel Terplan provides an excellent discussion on process analysis for a network management organization in *Benchmarking for Effective Network Management* (see “References”).

Summary

You must first learn and document your network before introducing performance and fault management. Tracking and documenting network devices and their connectivity is vital when analyzing performance data, as well as during fault isolation.

When determining what and how to document, be sure to track the information in a timely and correct manner. Otherwise, the documentation will become less reliable over time, and it will cause operators to look elsewhere for their information.

Understanding device ownership and processes in place to manage leads to the effective implementation of low-impact and maintainable documentation.

After you have documented the network as described in this chapter, you will be prepared for the next chapter, "Policy-Based Network Management," in which you conduct a baseline analysis of the network.

References

Books

Leinwand, A. and K. Fang Conroy. *Network Management: A Practical Perspective*. Reading, MA: Addison-Wesley, 1996.

Stallings, W. *SNMP, SNMPv2, and RMON: Second Edition*. Reading, MA: Addison-Wesley, 1996.

Terplan, Kornel. *Benchmarking for Effective Management*. New York, NY: McGraw-Hill, 1995.

Terplan, Kornel. *Communication Networks Management*. Upper Saddle River, NJ: Prentice Hall, 1992.

Paper

Berthet, Gerard and Paul Della Maggiora. "Cisco Network Monitoring And Event Correlation Guidelines." *Cisco White Paper*, 1998.

Internet Resource

Cisco Discovery Protocol MIB

http://www.cisco.com/public/mibs/v2/CISCO-CDP-MIB.my