

Diary of a Network Administrator: The Project Launch.....	1
Diary of a Network Administrator: Project Management	5
Diary of a Network Administrator: Mean People Suck	10
Diary of a Network Administrator: Planning for Success.....	15
Diary of a Network Administrator: Julia Roberts and COM1 Folders	20

Diary of a Network Administrator: The Project Launch

Date: Sep 20, 2002 By [Joseph Phillips](#). Article is provided courtesy of [Que](#).

Source: <http://informit.com/articles/article.asp?p=29390>

Have you ever kept a diary of the work you've dodged or completed? Ever wonder what's in other network administrator's diaries? In this series of articles, Joseph Phillips opens his diary for look into the life of network administrator. In this article covering the project launch, he shares his nightmare experience while creating a network plan for a new client.

As an independent consultant, I'm exposed to many different industries, many different networks, and many different types of aspirin. Don't get me wrong—there's nothing better than a good challenge, but sometimes I wish for my own network, in which I can implement things the right way from the ground up.

Ever hear of being careful for what you wish for? A couple of months ago, I got my wish. A new client invited me to take a look at his network. Not just the servers, routers, and patch panels—the physical network. Let me give you some background.

This company has close to 100 clients on its LAN, a couple of small remote sites, and a T1 line connecting it to the outside world. Its ultimate goal is to upgrade its clients and servers to Windows 2000 on a speedy, acceptable network. The clients are all running (please promise not to giggle...) Windows 95. I know, Windows 95, but this is in Indiana, where we don't participate in daylight savings time so the cows will get milked on time. The five servers are running Windows NT 4 with the latest service pack. More on that later...

As I was saying, the client asked me to look at his network. Starting in the server room, which wasn't more than a closet, I could see that something wasn't quite right. Thirty or so CAT5 cables spilled out of the plenum (the area between the drop ceiling and the floor above) like someone dropped a bowl of spaghetti. Each cable wasn't punched down, but crimped and plugged into stacks of hubs.

Snakes, Holidays, and Insulation

If you've been paying attention, and I know you have, you're wondering where the other 70 cables for the network clients are. As I soon (and occasionally) discovered, throughout this office, there were hubs hidden away like forgotten Easter eggs. Don't like Easter? How about Christmas? Because there were so many collisions, the hubs blinked red and green like a string of lights on Snoopy's doghouse.

Most of the hubs were connected to only one other hub, although a few of the hubs were connected to two or three other hubs. A real mess. As you may be aware, Ethernet uses CSMA/CD, which means that network participants listen before they speak on the network. If two clients happen to speak at the same time, they'll collide and then they'll take a short siesta. The trouble is that when you start daisy-chaining hubs together, especially like this rocket scientist did, collisions increase and the network slows. No fun for anyone.

In the plenum, it reminded me of, well, you ever watch the Discovery Channel during snake week? I've never seen a bigger mess. Whoever had "installed" the cable must have thought CAT5 had a run of 100 inches rather than 100 meters. This joker had clipped and spliced the wires together with line extenders—every 10 feet or so on every cable. One cable had 27 splices from its hub to the client's PC. He might as well have used barbed wire and hoped for the best.

At each client's PC, there wasn't a wall jack. I bet you were guessing this already. The wire popped out of the ceiling, ran through a tube, and connected directly to the client's computer. Above each cubicle, a network cable dropped from the ceiling into the NIC. One fellow had at least decorated his network cable with GI Joe and Batman action figures. I think he got more use out of the network than anyone else did.

How this network actually worked to some level is beyond me. As I climbed down from my ladder, the staff could tell things were not good. I was just thinking that I would need an old priest and a young priest to exorcise this network.

Master of My Domain

The next step of the inspection was to see how the domain was configured. Surely, this couldn't be too bad...it's a relatively small shop. Guess what? I was wrong, wrong, wrong. Whoever installed the Windows NT servers must have been the same guy who ran the network cables. They had five servers, each one acting as a primary domain controller (PDC). Okay, if you're not a Windows NT person that may seem innocent enough. The trouble is that you can have only one PDC per domain. For the math-challenged in the group, that means they had five separate domains. Not exactly ideal for just 100 users. One domain would have sufficed.

Now in the crazy world of Windows NT 4 domains, you have to create a trust relationship between domains to access resources in other domains. For example, if I wanted to borrow 100 dollars from you (wait a minute, the stock market is still down; better make it a twenty). If you agree to loan me a twenty, you'd trust me with your money. You'd trust that I'd spend it on beer and lottery tickets, not something wacky like Enron or WorldCom stock. You would be the trusting partner, because you have the resource. I'd be the trusted partner because I want the resource.

So, if you log into the domain called DOMA and want to print to a printer in DOMB, DOMB must trust DOMA. Additionally, you still need permissions to the printer in DOMB.

There is, however, a sneaky, defeating way around this whole "trust thingy." If there's a user in both domains with the same account name and password, they can bypass the trust business and get onto accessing resources. The trouble here, however, is should the user's password change in either domain then they're out of luck.

My client was using this sneaky, defeating method, rather than the somewhat-preferred "trust thingy." The administrator of these domains created each user account in each domain by hand. No users can ever change their passwords, and their passwords never expire. And what happens when a user forgets their logon password? No problem, they've a list of every user's logon name and password hanging on a bulletin board by the coffee maker. Not exactly Fort Knox, eh?

Mail Servers and Webbed Servers

The next challenge was the Exchange Server. Of course, it was slow as a slug, loved to crash, and was sitting on a PDC. Unfortunately, it was not the same domain all of the users logged into. I would have preferred for the Exchange Server to at least be in the same domain as where the users were originally authenticated. Now, I was having visions of breaking out Microsoft's Move Server Wizard to push the Exchange Server to a new site.

Next on the list was their Windows IIS Server, also installed on a primary domain controller. When you opened this Web address, it could take a minute to load the home page—or just time out. And, no, there's nothing fancy on the page. It's a simple, clean design that's little more than an interactive brochure. As it was discovered, the IIS Server was actually sitting in some guy's office. Anyone from anywhere visiting their Web site passed through the router, the firewall, across the LAN (somehow), to this server.

A few discoveries along the way:

- All clients have a static IP address.
- Every client registers with a WINS Server, but not necessarily the same WINS Server because each server was running WINS.
- The servers are using FAT, and each volume is shared with Everyone=Full Control.
- There are 13 accounts in the Domain Admins groups in every domain. Seem fishy to you?
- Backups are run only on the server in the domain users are logging into.
- There is no support for roaming profiles, but each user has a home folder. The home folder is in a different domain.
- The company does not like or use logon scripts.
- The Exchange Server happily forwards spam for a few porno sites. (Naughty server!)
- This company has good coffee and free bagels on Thursday.

My final inspection, a few days later, was over. Without a doubt, this was one of the worst networks I had ever seen in my life. I felt like a dentist at Halloween: Dreading the upcoming work, but appreciating the invoice.

My proposal to the client was multitiered to reduce the initial expense, and to disrupt as little production work as possible. Too often, technical leaders rush into upgrades, conversions, and remedies without a solid logical plan in place. I like to approach technical implementations as a project manager rather than as a soldier of fortune. This ensures quality, vision, and success in the long run.

Summary of My Plan

1. Backup. A backup schedule must be implemented on each of the servers. Lack of planning or lack of knowledge—it doesn't matter. There are millions of dollars of work just waiting to disappear. An immediate backup of each server is needed. A regular backup schedule must be implemented.
2. Wiring. Properly install Gigabit Ethernet throughout the office. Each office will have a wall jack; each cube will connect to surface-mounted jacks. A central patch panel and switch for the servers will be installed in the server room.
3. Move Exchange Server 5.5. Part of the goal is to upgrade to Exchange 2000. When the domains are flattened, Exchange will have to be moved to a central domain. This client desires Outlook Web

Access because workers are often on the road or want to check email from home. Once the Windows 2000 domain is created, 5.5 can be upgraded to 2000.

4. Flatten the domains. The goal of this large project is to deploy Windows 2000 to the servers. Flattening the domains into a single domain will gather all of the resources under one umbrella and allow for an easier transition to Windows 2000. Not all of these servers need to be domain controllers. File and printer servers should be member servers; Exchange should also be a member server.
5. Windows 2000 Server implementation. This client will be giving up two leased servers and getting two new servers. Once the domains have been consolidated, create the Windows 2000 domain, and upgrade the existing servers to Windows 2000.
6. Clean up. Install DHCP, convert to NTFS, set policies, allow for roaming profiles, confirm the backup schedule under Windows 2000, install service packs, and troubleshoot.
7. Deploy Windows 2000 Professional. Using Sysprep and Ghost, deploy an image to the clients on their new workstations.

As you can see, this was no small project, even for what should have been a simple solid LAN. As a technical consultant, a tour of the office can only reveal who likes Dilbert, where the server room is, and sometimes a list of passwords by the coffeemaker. To really educate ourselves about a network's needs, we need to stick our heads above the drop-ceiling, dive into the servers, and document our discoveries.

In the next few articles, I'll share how this project advanced and the adventures I encountered. In the meantime, get out your ladder, and take a peek at your network.

Diary of a Network Administrator: Project Management

Oct 18, 2002 By Joseph Phillips. Article is provided courtesy of [Que](#).

Source: <http://informat.com/articles/article.asp?p=29755>

All IT implementation needs a solid plan to find success. Far too often, projects spin out of control due to a lack of vision, planning, and technical leadership. In this network administrator diary entry, Joseph Phillips discusses the importance of project management.

So I'm sticking my head into the drop ceiling, insulation is finding its magical way into my shirt, and I'm sweating like Richard Simmons in a pastry shop. As I swivel my flashlight around, I see two red dots just a few feet away from my face.

No, I've not been eating mushrooms. I'm starting a network upgrade project for my new client, and it all begins with planning. Of course, not all of planning is done on white boards, in Microsoft Project, and on the back of napkins. Planning, real planning, requires that you get familiar with all of the work the project entails so you can plan—and price—accordingly.

The first article in this series introduced you to my new client and all the excitement the staff is having with their network. As a reminder, they've got a bunch of NT 4.0 domains, servers that Noah had on the ark, printers by Gutenberg, lousy network cables, and workstations the Smithsonian has inquired about. As you can imagine, their network has more errors than the Tampa Bay Devil Rays.

After my initial review of the network, it was time to create a project plan. A what? If you're like many network administrators (wait, it's not you, it's a friend) you may be tempted to just hop in get to work on any assignment. You can't just yell, "Release the hounds!" and then rush through IT projects. Why?

What starts out as a simple upgrade, or adding a new switch, or configuring some IP properties turns into nights and weekends of agony. Not to mention the time lost to complete the work—and the hours of production time that may be impacted. Production time? Sure. Consider the time lost by your company's employees if your "upgrade" puts them out of work for even 10 minutes. Consider 10 minutes or 10 hours of lost profit.

Welcome to IT Project Management

What needs to happen at the onset of any project is to create an effective yet flexible project plan. This is project management. Project management is the ability to envision the end result of a project, create a plan to reach that vision, and then implement the plan to arrive at the vision.

So what's vision? Vision is the ethereal substance that allows network administrators to see the invisible and to feel the intangible before either exist. I know, I know, after reading that sentence you're convinced I'm eating mushrooms. I promise you I'm not.

Simply put, vision is the ability to see the end result before you begin. Without vision, how can you adequately plan?

My client had a vision not of a Windows 2000 domain, with multiple domain controllers, file and print servers, roaming profiles, and policies, but of a network that just works. Their vision was a day of not

suffering through slow transfers, printer spools hanging, and server crashes. They didn't care what technology got them there—just that they would indeed arrive.

My job (and yours) is to take the vision of clients offer and snap-in the realities of technologies to reach those goals. The only way, okay the best way, is through IT project management.

Research, Research, Research

Dad always said, "When it comes to real estate, it's location, location, location." Okay, he didn't always say that, but the point is, when it comes to projects, it is "research, research, research." Once you've got the vision for the end result of the project you need to begin your research, you can complete your research from a number of different sources:

- Internet (such as InformIT.com)
- Books and magazines (Speaking of books, here's a shameless book plug: Buy my new book...*IT Project Management: On Track From Start to Finish*. Osborne McGraw Hill, 2002. ISBN: 0072223499)
- Personal experiences
- Experiences of others
- Live investigation and experimentation

Research has many different goals, including the following:

- To learn as much as you can about the problem you'll be solving
- To discover a solution (or solutions) to reach a project's vision
- To learn how to implement the discovered solution
- To discover an affordable investment versus a cheap fix

Research is like a first date: You wish it could go on forever, or you can't wait until it's over. On any project you're working on, big or small, you must allot a viable amount of time to research the project.

Back to billable hours.

This is where you joined me in my project. My client knew its network was a mess and had a vision for the deliverables. I then took the vision and applied technology to it. Now I was completing the research phase of this long, massive project.

As I was sayin', I was examining the physical structure of the network when I see two red dots and then it kicks in—those are eyeballs. And those eyeballs are attached to a rat! And then I can see its hairy, nasty body. Ewww! Fortunately, this rat's a few yards away and not breathing on me. Then it occurs to me, if there's one rat hanging out up here, how many more rats are there?

And then it occurs to me again: Guess who'll be moving all over this drop ceiling to pull out the old network cable and properly install the new? You guessed it! My talented cable installer, David. Well, he always makes me help.

In the research phase of this project, I had to check several different areas of the office. This, of course, required me to open several different panels and poke my head into the plenum. I thumped on each panel, quickly slid it out of the way, and then pushed my head into the abyss. All I could think of was that FOX-TV special: "When Rats Attack!"

Plan on Planning

Once my research was done, it was on to creating the project plan. Creating a project plan is not as stuffy as it sounds—at least not in the beginning. To begin creating a project plan, you create what's known as a Work Breakdown Structure (WBS).

To create a WBS, you take the work at hand (in this case, upgrading the network) and you break it into large, chunky phases. This job had three fat phases:

1. Upgrade the network cable.
2. Install and create a Windows 2000 domain.
3. Install Microsoft Exchange 2000 Server.

Then, the work is broken down some more, adding detail and steps under each phase. The new information is technically called work units:

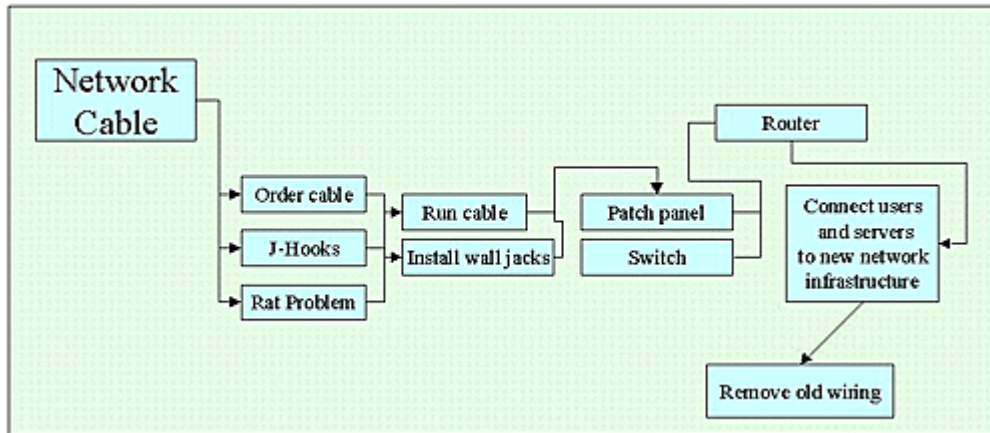
1. Upgrade the network cable.
 - a. Add rat poison and traps.
 - b. Add J-Hooks according to code.
 - c. Run plenum-grade cable throughout office.
2. Install and create a Windows 2000 domain.
 - a. Configure five new servers.
 - b. Configure AD.
 - c. Configure policies.
3. Install Microsoft Exchange 2000 Server.
 - a. Add Exchange services.
 - b. Add and configure SMTP.
 - c. Import user accounts.

You would continue to break down the work units in the list into tasks. When all of the work units have been broken down into manageable and logical tasks, you've got your WBS. At first glance, your task list looks longer than Oprah's shopping list. Look again, though, and see that you've got a detailed checklist of the work to be completed.

Now You Know How Magellan Felt

To get your hands around the project, you need to arrange the tasks into a logical mapping of events. In this map, you identify the phases that can begin simultaneously, the work units within each phase, and the tasks within each work unit. You literally create a map of the work to be completed. This map is called a Project Network Diagram (PND). Depending on the number of people involved in the project, a PND can help you organize your work and visualize the dependent and independent tasks.

Figure 1 is a portion of a PND; it covers just the path of the tasks in the network cable upgrade part of the project. Note that some tasks may begin at the same time, while others are dependent on prior tasks to complete before they can start.



On my assignment, I completed a PND—not only to give myself and staff a plan to follow, but to share with the client so they could visualize the work we'll be completing for them. You may be saying, "Hey, I don't have no stinkin' clients," but if you're a network admin, you do: your boss and your colleagues who use the network you administer.

Time Is Money

Project Network Diagrams also ensure that you've addressed all of the work to be completed, and created a feasible timeline. In practically any project—from creating a Web site to cleaning out your garage—there's going to be unexpected events (like rats in the plenum).

New project managers often bloat the time allotted for each individual task to...frankly...cover their asses. The problem with this ploy, however, is Parkinson's Law. This law states, "Work expands so as to fill the time available for its completion." In English, if you allot a week to install a service pack, it will amazingly take a week to install the damn thing.

So how do we account for all those glitches that eat into the project time? Management Reserve. Management Reserve is a percentage of the total predicted time to complete the tasks within the WBS. A network upgrade like the project I worked on would likely take 160 hours to complete. To account for any unforeseen problems, we'll add 10–15 percent of the total time allotted for the work at the end of the PND. So the 160 hours of actual work is now predicted to take 180 hours for the entire project. Keep in mind: This is all based on your research, experience, and the lunar phases.

As tasks take longer than expected, we apply the overrun in time to the Management Reserve. Of course, some tasks won't take nearly as much time as originally anticipated, so we can apply the extra time back to Management Reserve. Fascinating, huh?

At this point in my project, I completed the WBS and the PND, assigned tasks to team members, and kept the client in the loop regarding timing and anticipated hours. I also provided the client with a project acceptance agreement, which is like a contract, but without the attorneys. It's a checklist of the required deliverables of the project and a target completion date. At project completion, the client and I will revisit this agreement, and we'll go through each required deliverable to prove its existence and quality before the project is closed.

You'll be happy to hear that I did not see any more rats during this project—unless you want to count those Mac users in the design department.

Source: [http://web.wilson.k12.pa.us/buildings/sh/staffpages/mccchr/Cisco/Diary of a Net Admin.doc](http://web.wilson.k12.pa.us/buildings/sh/staffpages/mccchr/Cisco/Diary%20of%20a%20Net%20Admin.doc)

Diary of a Network Administrator: Mean People Suck

Date: Nov 15, 2002 By [Joseph Phillips](#). Article is provided courtesy of [Que](#).

<http://informit.com/articles/article.asp?p=30036>

As a network administrator, you're vital to the success of your organization. Consider all of the people within your company who rely on the technology you support. Your attitude, aptitude, and level of professionalism impact those same people. In this diary entry, Joseph Phillips lists characteristics of good (and bad) network administrators.

Have you seen any good bumper stickers lately? I like the ones with quips like "My kid beat up your honor student" or "My Other Car is a Porsche." And on and on these sticky bits of wisdom go.

As you may have guessed, I travel quite a bit. I teach seminars, consult, and implement technology throughout the country—and I like to drive. Driving lets me think, listen to CDs, and catch up with books on tape. Lately, for some reason, I've been paying attention to bumper stickers. One I've been seeing says, "Mean People Suck."

Maybe these "Mean People Suck" stickers have been around for years. Maybe they have been affixed next to "Nine Inch Nail" logos, Jerry Garcia's dancing teddy bears, and others. But I've not noticed until lately.

So what does this rant have to do with being a network administrator? Unfortunately, quite a bit. Here's the painful truth: Many of us ("us" being network administrators) are jerks.

There. I said it: Too many network admins are jerks.

Now sure, I'm certain there is a huge percentage of us who love our jobs, love the people we support, and love making life better for everyone. But there's another wide percentage of techs who think corporations, organizations, and technology itself wouldn't tick unless they showed up to work their magic.

Know anybody like this? I bet you do. If you're one of the good ones, read on and then slip this article onto some jerk's desk. You can continue to lead by example, but some people need a kick in the pants. Allow me.

God and the Network Administrator

Being a network administrator does not make you God. Being a network admin does mean you likely know more about networks, technology, and NOSs than anyone else within your organization. But chances are, your organization was around long before Ctrl+Alt+Del meant much.

The role of a network admin is a role of support. You exist to make the work of the employees better, more accurate, more productive. Basically, you're hired to help the company make money. Now this may come as a shock, but your organization most likely does not exist to give you something to do.

Too many network administrators have a "god complex." Some admins I've met act like they've just delivered three babies in a helicopter, discovered a method for cold fusion, and explained Notre Dame's "West Coast Offense" to a group of nuns. Please.

Now I admit there's nothing wrong with being confident, taking pride in perfection, and letting management know your projects are all successful, on track, and on budget. An occasional toot on one's own horn is dandy.

My message: If you're unprofessional, you lose respect, impact company morale, and are the proverbial wet blanket on the fire of productivity. Let your accomplishments, your superior network management, and flawless technical execution speak for you. How? Here are a few hints:

Ditch the Cocky Attitude

You may be brilliant, and many of you are, but brilliance is best seen through your work, not your mouth. Shut up, drop the John Wayne swagger, and get some work done.

Develop an Attitude of Servitude

Far too many IT gurus isolate themselves from the rest of the organization. In many companies I visit, there is open contempt for the IT department. Worse yet, the admins have no clue. Why? These admins treat every request as if Mom just asked them to take out the garbage in the middle of Baywatch. Here's sarcasm: You are at work to do this new thing called uh, oh yeah, work.

Quit Being a Demeaning Buffoon

I've witnessed more than one admin dismiss an employee's request with disgust, intended humiliation, and spite. Most professionals are not technical people—they can't do your job, but are dependent on you to do theirs. You might be needed today, but what goes around comes around.

Learn about Your Business

Many network admins are incredibly astute with technology. They can make Microsoft, NetWare, Linux, and more purr like a kitten or roar like a lion, but they can barely explain what their company actually does. Learn about your company: its business requirements and functional requirements. This knowledge, coupled with your technical brainpower, can make your company even more profitable.

Realize You Are Not Indispensable

In today's rocky economy, even the most obstinate admins know their jobs could be in peril. What about admins moving on to other opportunities? Or admins who win the lottery? Or worse? How well documented, organized, and clean are your network infrastructure, topology, file servers, and the rest of the server room? Prepare yourself and your organization for the worst or best that could happen: organize, document, and share the information.

Can You Trust Yourself?

Character is defined by what you do when you know no one would ever find out. As a network administrator, it is incredibly, undeniably easy to do whatever you'd like to anything you'd like, whenever you'd like—on the network, that is.

Want to know how much your boss makes? Click, click: no problem. Want to see the retirement plan of the CEO? Click, click: no problem. Want to read the email of that good-looking receptionist? Click, click: again, no problem.

I have had lengthy heated arguments with admins who feel they are entitled to Full Control permissions on every piece of data within their organization. These admins believe they are entitled to access anything they'd like. Wrong...that's called being above the law, a bit different than autonomy.

Like most things in life, just because you can doesn't mean you should. There is a certain level of trust that goes with being a network admin. I'd venture that management in most companies do not realize the level of power a network admin can wield.

Suggestions for Civility

So what's a mean nerd to do? How about a little restraint for starters? Next, bring it your level of power to management's attention. That's right—by sharing with management what you can do, there's a heightened sense of responsibility. This also spurs you to document your access, permissions, and admin duties to protect your career.

Next, create proper security. Admins should be able to set permissions, but not access resources. Yeah, yeah...you're the admin and can do whatever the hell you want, but try playing by some common rules.

Implement auditing. This can be done electronically to prove who's accessed what and when they accessed it. This not only creates a system of checks and balances, but also can protect the admin from being accused of accessing sensitive data.

If there's more than one network admin in your environment, are you both using the same account to administer the network? You are? Gasp! If all admins are using the same account to administer, how can auditing be effective? How can there be accountability?

Each admin should have their own administrative account to use only when it's time for admin duties. In other words, Susan's not logged on as an administrator while writing a report in Microsoft Word.

Network administrators should not, must not, know the password of users. If you know the password of users, you should be held accountable for the activities users do on your network.

Revenge of the Nerds

Let me share a hypothetical, fictional scenario with you. Let's say there's a company with a very strict Internet access policy: no porno, no job sites, no <http://josephphillips.com>, no chat, and on and on this list of rules go. The trouble is, however, this fictional company has no way of enforcing its policy.

Until now. Now the company has implemented a proxy server that effectively filters out all the unwanted sites: shuts down chat, games, MP3 downloads, and just about anything else they'd like to eliminate—an excellent plan.

But remember, its written Internet policy had not been effectively enforced since Atari was cool. The employees at this company have been using Internet access as their own personal pipe to anything and everything that's available on the Web.

Now these folks are blocked from doing any mischievous Web activities. The admin, however, has a new hobby with this proxy software: watching where people attempt to go on the Web. "Hmm..." this dork thinks, "there are lots of people trying to access porn, job sites, even MP3 sites. I better report this info to all of their bosses." So he does and "it" hits the fan.

You see, what this admin failed to tell management was that these users couldn't actually access the restricted sites—they just attempted to access them. My argument is why is he gunning for these people? They can't get there from here.

Put it this way: If I try to get into a house and the front door is locked, I may try a different door. If that door's locked, I may try a window...and on and on I'll try until I realize I can't get in. The same goes for the people at this company. While I don't agree with the users browsing the Web on company time, human resources should have intervened here, not the network administrator.

What this admin has done is create an "us-against-them" mentality between the employees, management, and the technology department. These employees are embarrassed, written up, and threatened with dismissal. Of course, the admin gets loads of complaints, ill will, and maybe even worse. So what does this fictional admin do? Ah, yes, revenge.

Imagine how easy it'd be for this admin to make it look like anyone is visiting any website in the world. A little password hacking, a little creative IP addressing, and it's "wham-bam-thank-you-ma'am"—you're fired. Don't tell me it hasn't happened.

Oath of an Admin

I propose that companies require their network administrators take a technical oath based loosely on the Hippocratic Oath, to protect and serve the organization's best interest. Here's what I have in mind:

I swear to fulfill to the best of my abilities and judgment this covenant. I will respect the work of the technicians that have gone before me and share the knowledge that I have gained for those that come after me.

I will apply for the well-being, benefit, and good of my organization all measurements that are required to support, implement, and maintain these technologies.

I will remember that there is an art, as well as a science, to technology. I will remember that personality, warmth, sympathy, and empathy may outweigh any technical implementation my abilities allow.

I will not be ashamed to say, "I know not." I will not be ashamed to call for my colleagues when the skill of another is needed for a project's success.

I will respect the privacy of my clients, their work, their email, and their electronic records. My duties as a network administrator are to administer the network and technology without interfering, investigating, or intruding into the work of the clients I support.

I will remember that I do not actually care for a network, implement technology, or administer bits and bytes; but ultimately support a collection of individuals whose careers may be dependent on my abilities as a professional. My responsibilities are great, but I must not play God.

If I do not violate this oath, may I enjoy life. May I be respected while I serve and be remembered with affection thereafter. May I always act with the good of my organization and its employees in mind.

The Golden Rule

As a network administrator, you're vital to the success of your organization. Consider all of the people within your company who rely on the technology you support. Your attitude, aptitude, and level of professionalism impact those same people.

If you want to find success, admiration and respect from the people you serve, follow The Golden Rule: Treat others as you want to be treated.

Technical leaders are superior to mean nerds. Now that's a bumper sticker for my car.

Diary of a Network Administrator: Planning for Success

Date: Feb 28, 2003 By [Joseph Phillips](#). Article is provided courtesy of [Que](#).

<http://informit.com/articles/article.asp?p=31106>

Success is not an accident. Real success comes through ambition, planning, and action. How are your project's plans? Do you have project plans? In this diary entry, Joseph Phillips details his planning process for his client's network, servers, and rats.

My clients, the ones with rats, tangled network cables, and five Windows NT 4.0 domains, are not very happy. They've huffed and puffed their way up and over the learning curve, and they don't like what they've learned. They've found themselves not exactly somewhere over the rainbow.

In case you're new to this series of articles, here's a recap of the adventure and their problems:

- *Network troubles.* The physical network is a disaster. The network cables were mysteriously spliced and joined together every 10 feet or so. Cables were draped across fluorescent lights, wrapped around conduits, dragged over Jimmy Hoffa, and then plopped out of the drop ceiling directly into the NICs. Nice. Yeah, real nice.
- *Network design.* There are roughly 100 users on the network, but there are five servers—each serving as a PDC of its own domain. Not a good solution. The Exchange Server is in a different domain from where users are logging on. As added trouble, their mail server is forwarding porno spam. (Naughty server!)
- *Data backup.* Only one server was being backed up. Unfortunately, this server had a very small amount of data on it. All the other servers had gigs of data waiting to vanish with one grumpy delete key. (Did I mention that the Everyone group had Full Control to everything?)
- *Pet rat.* They have a rat on the loose. Yeah, a real rat. (No Mac user jokes here, I promise.)
- *More sighs.* There's more to this story than what I'm sharing now. My therapist has warned me not to talk about it too much, so you can read the first article [here](#).

Don't Kill the Messenger

Anyway, my clients are not happy. With me? Well, don't kill the messenger. Actually, they're not upset with me, just the news I bring. They're not thrilled with their original "vendor." They're not thrilled knowing that they've been... now how should I put it, er, scammed? Conned? Flimflammed? Bamboozled?

And they're not thrilled with the imminent expense of revamping their network from the ground up. They already had plans to lease new servers and workstations, but had not counted on the expense of the network cabling, patch panels, autoloader tape drives, and network switch. Surprise, surprise: They weren't following or documenting their licensing agreements. (I know you have licenses for all of your applications, each with its own serial number and installed according its respective EULA. You also have Client Access Licenses and are paid up on all your shareware, right? Good; I thought so.)

While we're playing accountant, let's not forget the expense of time. Labor is not cheap. Okay... skilled, knowledgeable labor is not cheap. You can pay for things to be done right the first time or you can pay even

more to correct problems down the road. This was not going to be an inexpensive easy project. If only my new clients had researched their original vendor at the onset, they'd be in better shape now.

Enforcing a Project Management Methodology

Knowing they've been duped once already, my clients wanted to take precautions to make certain that this project would be successful. With that in mind, the clients and I agreed to progress with traditional project management guidelines. So, for starters, we drew up a Project Scope, a Project Charter, a Statement of Work (SOW), and a contract for the clients and me to abide by.

The Project Scope defines the work that will and will not be done, the assumptions that the project team is working under, and a targeted end date for the project. The Project Scope, like a periscope or microscope, restricts and focuses your vision. A Project Scope focuses on the end result of the project. Change requests, deadline issues, or quality assurance issues must also be held against the details specified in the Project Scope.

The Project Charter is the commencement of the project. The Project Charter must come from someone with power in the organization—to authorize the time, resources, and monies to complete the work. In this case, the charter came from the owner of the company and was sent to all of the functional managers, the operating officers, and the building management. This document ensures that the stakeholders know that the Project Manager is working on behalf of the Project Sponsor (the guy with the power and the bucks).

The SOW is a document that clearly defines what the heck you're trying to do. Let's get some detail here. When I first visited with these clients, they didn't care about Novell, Linux, or Windows 2000. All they wanted was a network that would operate without all the hiccups, snafus, and general wackiness they were experiencing. The owner and management had a vision of a sound, reliable network. This is the business portion of the pyramid shown in [Figure 1](#).

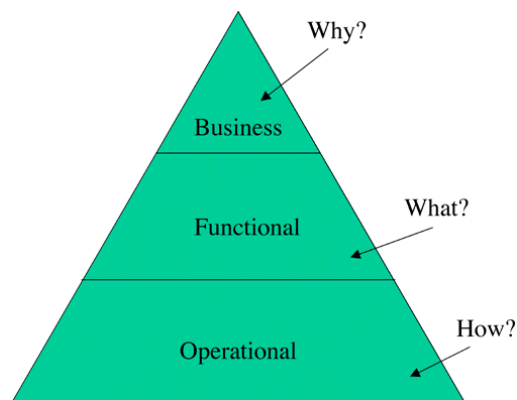


Figure 1 Operations can map to three layers: Business, Functional, and Operational.

Three Queries for Projects

The vision answers the "why" questions: Why is this important to my company? Why do we need technology XYZ?

Next is the functional portion of the pyramid. This is where all the "what" questions are answered: What are we trying to do? What will this technology do for productivity? What will it mean for finances? What can we expect from the solution?

Finally, down where all the Pharaohs hang out at the bottom of the pyramid, is where operations take place. That's you, me, and King Tut. Through the operations layer, we answer the "how" questions. Specifically, we answer how our solution supports the layers of the pyramid above us: the "what" and "why" values assigned by the Executives and Functional Managers. Our solutions must be a foundation to their vision and concerns.

Planning the Work; Working the Plan

So now that my clients had a Statement of Work, a Project Charter, and a contract, I was ready to move on. Well, almost. Next, we needed plenty of planning. To ensure success, to have minimal downtime, and to answer the functional business requirements of the project, we needed a solid plan. Actually, we needed several plans in this project; not just one. All projects need a set of plans before starting work. We needed several support plans to ensure success.

Scheduling Plan: Based on the Work Breakdown Structure and the Project Network Diagram, the schedule could be created to ensure that all the work that needed to be completed was done on time and in the correct sequence.

Risk Response Plan: Within this project, there were several potential areas for risk. We had to identify each of the potential threats, assign Risk Owners, and then mitigate the risks if they were to come to fruition. How? There are two methods: Qualitative Analysis and Quantitative Analysis.

What's the difference? Glad you asked. Qualitative Analysis lists the risks in a matrix, as shown in [Figure 2](#). Each risk is assigned a level of severity multiplied by a level of probability of actually occurring. The risks are ranked according to their score. Based on the ranking, you focus your mitigation efforts on the higher risks.

Risk	Severity	Probability	Score
Losing server data	0.9	0.2	0.18
Impacting production hours	0.6	0.8	0.48
Hardware failure	0.8	0.2	0.16
Mail services stop	0.9	0.3	0.27
Loss of email	0.9	0.2	0.18

Figure 2 A risk matrix can help you plan your mitigation efforts.

Quantitative Analysis focuses on the identified risks through interviews, subject matter experts, and discussion with the project team. This method of risk analysis is harder to complete, can be more subjective depending on whom you are interviewing, and requires ample time to get a true reflection of the risks in the project. Don't discount this method of risk analysis for fluff. Admins and Project Managers must get out of their offices, get into production, and interview the stakeholders of the project.

Communications Plan. This plan details the information that needs to be disseminated as the project progresses—and specifies to whom the info is distributed to. Does this seem like overkill to you? Not really. Although this project was only going to take a couple of months to complete and the company was fairly small, a Communications Plan was needed.

A Communications Plan is a roadmap of what the client expects in the form of reports on the project. In this case, the Project Sponsor wanted weekly summaries of the work completed, open tasks for the upcoming week, and details about any new discoveries that could impact the completion of the project. Our Sponsor wanted this in hard copy, not email. In addition, our Sponsor wanted a biweekly Executive Summary that he could use in his staff meetings to report on our progress. No problem.

Our Communication Plan also included the phone numbers and email addresses of the project team, stakeholders, and building management company. Building management company? Yes, the building owners wanted to get involved when we mounted wall plates for the network connections.

Operations Plan. This plan is needed for the project team. My clients didn't need to see this plan, but we shared it with them anyway. This plan detailed the work my team was about to put into action. We detailed computer nomenclature, IP addressing schemes, and task ownership. This was a playbook to project success.

Authorizing Project Work

In any project, tasks can't be assigned all at once; there must be some logical approach to completing the work. For example, you can't install and configure Exchange 2000 Server until Active Directory has been installed and configured. Everything must be done decently and in order. That's where the Project Manager's organizational skills are paramount. The Work Breakdown Structure (WBS), Project Network Diagram (PND), and our Operations Plans will guide the team through the project somewhat, but the PM needs to be able to record the completed tasks, document their completeness, and then alert the owners of the successor tasks to begin their work.

Now it may seem logical for Susan to just tell Bob she's done with her task and then Bob can start his. The trouble, however, is that you may need to review Susan's work, or you must check for quality, or Bob's away on vacation, or Susan forgets, or yada yada yada. Don't leave projects to chance. Within your plan, create a method of reporting task completeness to launch the next task in the timeline.

So how do I do this? For the most part, I use Microsoft Project, but I still like simple solutions. I don't over-engineer. What I do is create a poster size PND. When tasks are reported as complete, I get out my green marker and color in the tasks to represent where we are in the project. Now I tell Bob he's ready to move forward. If Bob misses the message, or if other team members want to see the status of the project, a quick glance at the PND poster keeps them on track. It's not magic, fancy, or difficult, but it works.

Closing the Project

Project Closure Plan. Another plan? Geez. I know, but this one is really important. It details the conditions to determine whether all the deliverables have been met. In this instance, closure called for an internal audit by my team to guarantee that the deliverables had been fulfilled. The Closure Plan also specified that our Sponsor must audit our work for quality, proof of deliverables, and completion of the SOW. Finally, this plan had a formal sign-off and payment for services rendered. (Aahh, the good part...frosty beverages all around.)

Once my client was happy with our plans, risk mitigation, and quote for completing the project, they gave us the green light to move forward. My team and I followed our Operations Plan with a few exceptions, and we ultimately transformed their lousy network into a speedy, reliable network I'm proud of.

Plans and the Network Admin

Should you implement all these plans into your next project? Maybe not all of them, but I think most of them. You wouldn't take a road trip, build a house, or start a business venture without a plan. Implementing technology shouldn't be any different.

Creating a solid, well-developed plan does not guarantee success. Following the solid, well-developed plan does. In an upcoming article, I'll reveal my Operations Plan for this project and show you how we transformed their network and helped this company become more profitable. In the meantime, consider the projects you've completed. Were the projects finished on time, on track, and on budget? What plan got you to that point? Planning is not a necessary evil, as some believe. Planning is an integral part of the business process.

Diary of a Network Administrator: Julia Roberts and COM1 Folders

Date: Mar 14, 2003 By [Joseph Phillips](#). Article is provided courtesy of [Que](#).

Source: <http://informit.com/articles/article.asp?p=31278>

Julia Roberts is excellent, but I wouldn't want her movies on my server. A hacker created a COM1 folder on a client's server and filled it with videos. In this article, Joseph Phillips shares the thrills of undoing the work of an unscrupulous hacker.

Do you like movies? I do. There's something great about turning off the phone, shutting down email, and dimming the lights for a night of movies. Make a bowl of popcorn, mix in some M&Ms candy, and then press Play. I like spy thrillers, courtroom dramas, and...yeah, I'll admit it, the occasional "chick flick." I am a real sucker for Julia Roberts.

Recently, a client called because his server likes movies, too. Well, I guess his server is impartial to movies, but the guy who hacked into his server? He sure likes movies. This hack filled up a healthy portion of my client's hard drive with a few recent thrillers—including "The Bourne Identity." Too bad that this version of the thriller was dubbed in German.

Truth be known, the hacker wasn't much of a hack. My client, a competent IT director, had accidentally left his FTP server open for anonymous access. But don't start pointing fingers and say, "Serves you right." It was purely an accident, an oversight, and an assumption that nobody would be doing something this wild on his server. Live and learn.

Movies, Apps, and Money

So what's the point of parking movies on servers? And how do hackers find servers that have FTP open anyway? Here's what these jokers are doing: They use a port-scanning tool against a range of IP addresses. This port-scanning utility reports which IP addresses have FTP services available. Next, they test which IP addresses with FTP services have anonymous Write permissions open. Now they've found a home, temporary or long-term, for anything they want to throw on the drive.

The dark corners of the web are full of guys who say, "Pssst...Hey, buddy. \$9.00 will get you tons of free movies, copied software, and other goodies. All you have to do is download them." These crooks copy DVDs, applications, and other copyrighted material to these FTP sites they've exploited—and then sell access to them. Now their paying customers connect to the FTP servers and download the stolen software, movies, and whatnot—all on someone else's bandwidth dime. Nice racket, Tony Soprano.

In the case of my client, the "hacker" parked several movies on the hard drive. The tricky thing here isn't the port scan or the anonymous access to the file system through FTP. The intruder was able to create a deep directory structure that included a folder called COM1. Seems innocent enough, right? COM1 is a reserved name in the family of Microsoft operating systems. You can't create a folder named COM1—at least not with standard Microsoft operating system tools.

COM1 Folders are COM1~1 Folders

As I soon discovered, the COM1 folder actually had a few spaces after the name. Windows doesn't allow folders to end with spaces—it truncates them to the last character. It is possible, through POSIX tools, to create folders with reserved system names. Heck, it's even possible to create folders with spaces only.

This nasty trick allows the intruder to park his MP3s, movie files, photos of his ugly mother, and just about anything else he wants on your hard drive. Keep in mind that you haven't invited the fellow to put his stuff on your server, but you might as well have if you're allowing FTP with anonymous Write access. Which is what my client did. Poor guy.

We've all heard of hacks, phreaks, and warez masters parking all sorts of crap onto servers, but fortunately for me I've not run into this exact problem until now. And here's the rub: I can't delete the COM1 folder. In reality, there are three COM1 folders in three different directories. I can't delete any of them. Well, not just yet...

With strong coffee in hand, I went to work hardening this server. For starters, I took away the anonymous FTP rights through IIS. Next, I added proper NTFS security, checked the event logs, and ran a virus scan. I also checked for any unusual apps that may have been installed to monitor or undo the business I was about to do. After testing for the connection for security and accessibility, I could set about deleting the video files.

The directory structure looked a little something like this:

```
F:\destop>tagged\by\MORON\COM1\
```

Now the structure didn't exactly say MORON—it was some moron's code name. (Note to MORON: ooh, a code name. Cool. Do you have a secret handshake, too?) Anyway. As it turns out "tagged" is similar to the way animals claim their territory. If other hacks stumble onto this open FTP site and see "tagged\by\MORON", they'd know MORON had already claimed this site and they should move along. Fascinating. Where's my "Dungeons and Dragons" set when I need it?

I immediately learned what happens in Explorer when you click, right-click, look at, or even breathe on a folder magically named COM1: Windows Explorer locks up. Ah-hah! I hopped out to a command prompt and tried to navigate through the directory. I can move through the folders until I get to COM1—and then it's Accessed Denied. Okay, so MORON is slightly smarter if not more aggravating than his name.

Deleting is not Easy

I try DIR /X to get a listing of the directory structure with the 8.3 names. Eureka! I can see the COM1 folder as COM1~1. Can I access and delete it now? Nope. Still Access Denied. MORON is smarter than I thought.

Back to Windows Explorer. I took ownership and assigned the local Administrators group Full Control to the parent folder, Tagged. I chose the option to reset permissions on all child objects. Sounds good, right? Wrong. Windows can't traverse the folders to assign Full Control to COM1.

Another cup of coffee later, I'm digging out some POSIX tools myself. There are a host of POSIX tools in the Windows 2000 Resource Kit. Here are the tools I used in my attempt to delete these folders:

- `chmod`—This tool is like `ATTRIB` in DOS. It's used to change the access type to the folder, not necessarily the permission.
- `chown`—This tool is used to change the owner of an object. I had high hopes here.
- `ls`—This tool is like the `DIR` command; it lists the contents of a directory.
- `rm`—This tool is like the `DEL` command. It has some switches to delete files and directories. I couldn't wait to get to use this one.
- `rmdir`—This tool deletes directories. I was hoping to use this one right away.

Unfortunately, none of these tools did much good to gain access to the COM1 folder. I had expectations of RM.EXE. This bad boy allows you to remove directories with POSIX commands. In POSIX, we don't use all the frilly colons and backslashes. C:\Tagged\By\MORON becomes C/Tagged/By/MORON. Specifically, with RM.EXE, it's `rm -r //C/Tagged/By/Moron` to delete the whole directory structure. But (sigh) that COM1 folder won't go away. Next, I try `rm -r //C/Tagged/By/Moron/COM1~1`, but it's back to the Access Denied message. Grrr.

Could it be that the folder is locked because another process is accessing the folder? I doubted it, but I was having little luck. I fired up a great tool from the fine folks at sysinternals.com called Process Explorer. This tool enables you to see what processes are running and the related resources in use. As fine as the tool is, it didn't reveal any open processes on the COM1 folder. Now I was getting mad.

The Right Tools for the Job

It appeared that the problem with deleting the COM1 folder centered on the permissions to access the folder. I can't change the permission to the folder because Windows doesn't allow the folder to exist. I tried XCACLS and CACLS to no avail. I checked out the owner of the parent folder—it is Administrators, as it should be. I can't see the owner of COM1 because Windows freaks out when I even look at the dirty folder. I tried walking around the block to think it over. Nothing.

Later that night, I remembered a tool that's used to take ownership of folders that you can't delete. Here's the deal: Let's say that for experimental purposes you have installed Windows 2000 twice on the same partition: a WINNT folder and a WINNT2 folder. You want to keep one of the 2000 installs and axe the other. If you try to remove all your Windows 2000 directories without formatting the drive, you can't. One of the folders, called /Installer, has some special .MSI files inside.

And along comes takeowner.exe. This gadget allows you, the Administrator, to take ownership of the directory. Unfortunately, when I thought of this hot idea, it was 2 a.m. and my client was probably at home, fast asleep with his three cats. I could hardly wait to get to his server room to try out takeowner.exe.

Sweet Victory: the Delete Key

And guess what? It worked. Within ten minutes I had blown away 3GB or so of worthless data. Well, worthless to me, but not to MORON.

Here's how it all worked out: Through a command prompt, I ran takeown.exe against COM1~1, and the echo reported that ownership had been assigned. Of course, I got to see what was hiding in there, so I could now navigate into the folder. For safety's sake, I renamed the folder to junk. As it turns out, this folder started a tree of folders that each had a COM1 directory inside them. No problem.

I had to run takeown.exe against each subdirectory (using the COM1~1 nomenclature) until I got to the good stuff: movies. On a couple of the subdirectories within the COM1 folder, takeown.exe wouldn't work, and Windows reported that it didn't recognize the file structure. On a hunch, I ran CHKDSK and then takeown.exe again. This solved the problem and I could move on my way.

Now about these movies—they weren't MPEGs; they were sliced-and-diced DVD movies. Their parent folder's name said the film was dubbed in German, but I didn't have a viewer, the desire, or the guts to attempt to open the movie. I was more interested in deleting the files.

Actually, I was imagining some little guy named Deeter hacking into FTP servers from his mom's basement. Sorry, Deeter. After I took ownership of your movies, I went ahead and deleted them. It was great.

Finishing the Work

To be safe, I ran a complete virus scan, ran CHKDSK, and examined the security logs. Fortunately, there were no viruses, but "someone" was still trying to log into the server! Of course, it was a bogus account from the "home.com" network. Nice try, but you now need a valid user name and password to access this FTP server.

As a follow-up, I checked the Administrators, Domain Admin, Server Ops, and Backup Ops groups to be certain that there weren't any bogus accounts lurking around. Next, I confirmed with my client that the firewall was still working and the accounts that needed access to the server could reach their data. Finally, I tried to remotely access the FTP, Web, and server through a variety of tools. I could not access the site without proper credentials—and even then the NTFS permissions were in place.

Have You Been Here?

I'm certain that some of you have had similar attacks. When I searched the web for "FTP and COM1," there are a handful of messages out there about similar incidents. Most of them direct folks to the RMDIR and RM.EXE tools, whereas others said to just format the drive. Formatting the drive was not an option in this case, and I bet it wouldn't be in yours, either. Thanks to the resource kit for takeown.exe, you won't have to.

I encourage you to go have a look at your FTP security. Confirm that anonymous access is turned off. Then, take a look at the amount of free space on your drives. If it looks suspicious, do a search for "Tagged" or drill down through your directory structure. If you find a COM1 folder, you know what to do: Review your security, use the takeown.exe, blow away the directories, and run CHKDSK.

After you're satisfied that your servers are secure, rent yourself a movie starring Julia Roberts. I'm partial to "Pretty Woman," but in remembrance of Deeter and his deleted movies, I rented "Flatliners." Who's got the M&Ms for my popcorn?