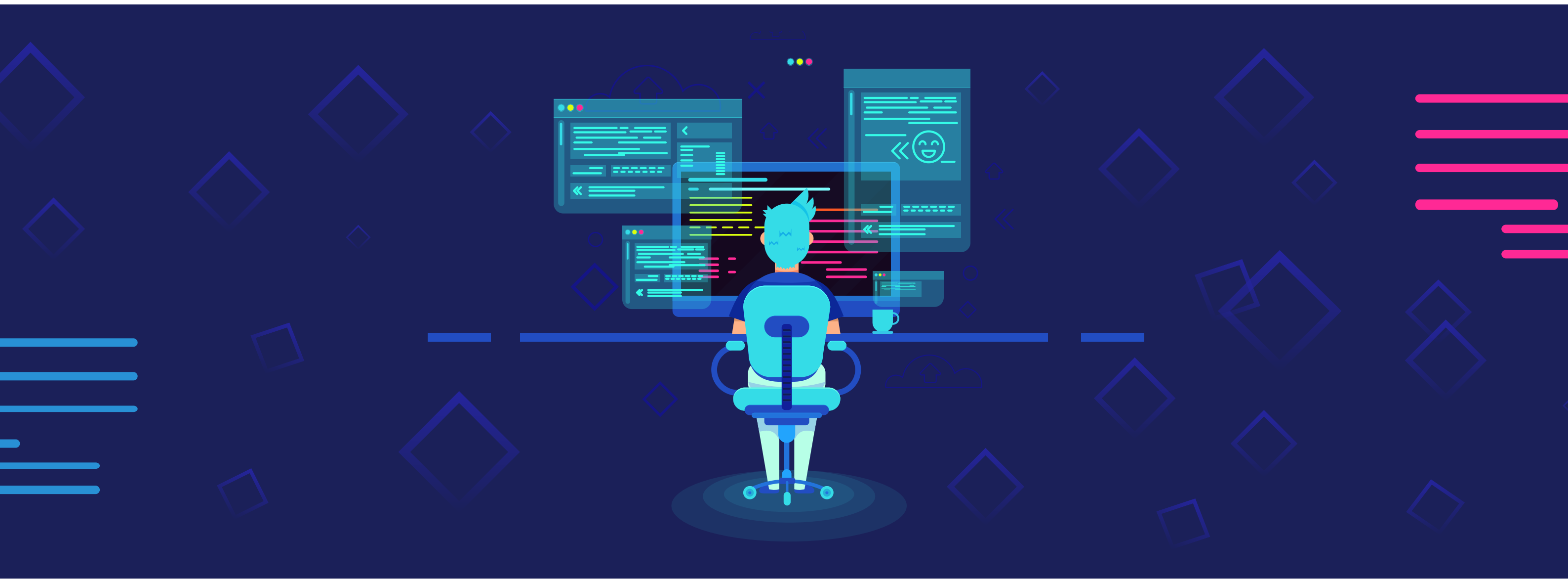


E-BOOK

Network Admin Handbook:

Basics, Subnets, IP Addressing, Hardware and Security Considerations

TABLE OF CONTENTS

Introduction 2
Network Hardware 2
Network Services Basics: DCHP and DNS 4
DHCP 4
DNS 5
Guide to Subnets and IP Addressing 7
What Is a Subnet? 7
VLANs 8
Virtual Private Networks 9
Conclusion 9
Guide to Network Mapping 10
Wireless Networks 11
Wireless Networks Security Considerations 11
Wireless Speeds 11
Network Security Best Practices 12
Physical Security 12
User Authentication 13
Firewalls and Protection Software 14
Network Firewalls 14
PC Software 14
When to Forbid Outbound Access 14
Conclusion 15

Introduction

A network is a lot like a community. Both a network and a community are made up of hosts. In a community, we're talking about homes and other buildings; in a network, it's PCs, servers, and other devices. The roads that deliver traffic between these hosts in the network world are generally Ethernet, although they may include other types of cables. Each community host has an address. In a network, each host has an IP address. Traffic intersections are handled by switches and routers.

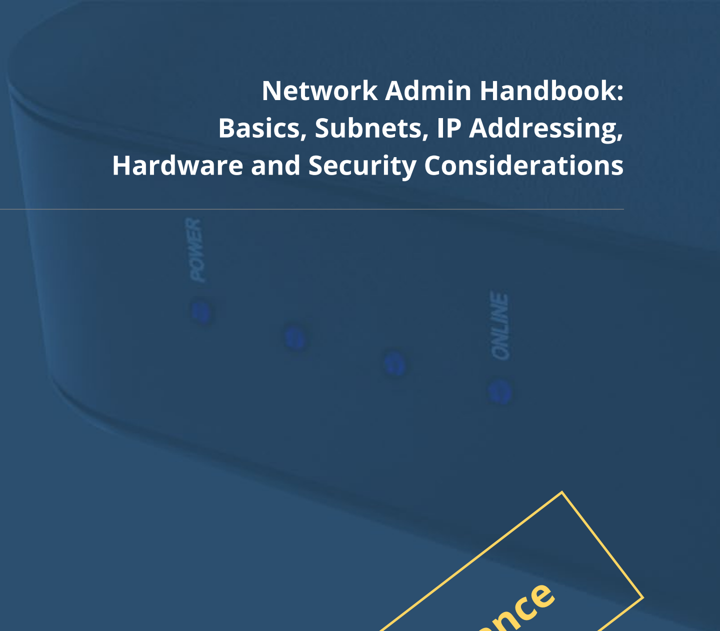
This example can be carried on and expanded upon, but the point is clear. A properly functional network, just like a community, should be designed properly. A network is only as effective as each of its parts. If just one of these items isn't fully functional, a bottleneck is created and the entire network is negatively affected.

With that challenge in mind, this e-book provides an overview of how to design an efficient and effective network. Keep reading for tips on network hardware selection, setup, security, and more.

Network Hardware

A network, in its most basic form, is hardware connected by wires. This hardware can include PCs, servers, routers, and switches. Most of the wires on a modern network are Ethernet cables. Other types, such as coaxial and fiber, can be found as well.

When designing a network, the biggest considerations to take into account with regard to hardware are your routers and switches. First, the appropriate configuration level should be chosen. Next, certain specifications should be considered, and a cost-based analysis should be carried out. Finally, model and manufacturer choices can be explored as well.



Choosing the router

Outbound traffic should be routed

THROUGHPUT
(how much speed do you need?)

CONFIGURABILITY
(VPN configurations, port forwarding, etc.)

SECURITY FEATURES
(content filtering, gateway AV, intrusion prevention, firewall)

⚠ Plan expansion in advance

Choosing the switch

Handling local communications

UNMANAGED SWITCH
(for simple networks)

→ **Non-configurable**
(basically, you add additional ethernet ports to network)

MANAGED SWITCH
(for complex networks with need for custom configuration)

→ **Configurable**
(either CLI or web interface port speed, VLAN, redundancy port mirroring, etc.)

Main switch characteristics

Handling local communications

TYPICAL SPEEDS
(the speed at which your network will operate)

- **10-100 mbps**
  (used on older networks)
- **1 Gbps**
  (used on most new networks)
- **10 Gbps**
  (used in enterprise environments)

NUMBER OF PORTS
(how many devices you can connect to the network)

- **5-48 ports to network**

Network Services Basics: DCHP and DNS

Network administrators utilize services every day to make their lives easier. These network services run on the application layer of the OSI model, as well as on top of it. Services, when configured and administered correctly, can automate administrative processes and do work that may in the past have had to be done manually.

Of all of the different services that administrators work with, DHCP and DNS are integral to every network. Almost every business-class router offers settings for both of these servers. Every PC technician knows how to configure these settings on individual PCs.

DHCP is used to automatically assign IP addresses to devices on your network. DNS is used to convert domain names to associated IP addresses. Every modern business network should have a server for each of these services. Administrators who take advantage of both of these services have an inside track on the configuration of their network.

DHCP

DHCP (or Dynamic Host Configuration Protocol) servers hand out IP addresses to devices that don't have them statically assigned. A network without a DHCP server must have static assignments on all existing hosts. Some network administrators feel that they have more control of their network by manually configuring each device's network card. However, most modern business networks have a DHCP server.

Overview

DHCP server management appears fairly simple initially, but the devil is in the detail. Distinctions need to be made based on your server and how static IP addresses are handled. Here's an overview of what DHCP offers.

Software or hardware-based servers

In many cases, DHCP servers are installed on physical machines running server operating systems. In simpler cases, these servers can be managed from a router. Almost every router available today offers a DHCP server. While software DHCP servers may be more configurable and offer more options, a router-based server will meet the needs of most businesses.

Static assignments over manual configurations

There are some devices on every network that need to keep the same IP address at all times. This can be done in two ways: manual configurations at the device level, or static reservations configured in the DHCP server. Using static reservations simplifies the process by keeping all of the IP address information, both static and dynamic, in one place.

Best Practices

Following a few best practices regarding DHCP will keep your network running at its best. You need to make sure you have appropriately sized DHCP scopes. You should also be sure that those scopes aren't overlapping IP addresses that are already being used.

Have an appropriate number of established IP addresses

You need to have a good idea of the number of IP addresses that you are going to need to assign. It's important to remember that, in today's networks, we're talking about more than just computers. Other devices that may be requesting IP addresses are VoIP phones and mobile devices, to name just a few. On top of all that, your DHCP scope should leave room for future growth as well.

Avoid overlapping static addresses

While you can use DHCP server settings to assign static reservations to most devices, there will still be some devices on your network that need to keep the same IP address via manual configuration. When creating your DHCP scope, make sure you are aware of any IP addresses that are already in use.

Keep security in mind

You need to make sure that you are not allowing unwelcome devices to infiltrate your network. Here's where to start:

- Keep your business networks and guest networks separate.
- If you are using a managed switch, be sure to disable unused ports.
- Generate alerts from your DHCP server when an unrecognized device sends a DHCP request.

DNS

DNS (or Domain Name System) is a service used primarily for translating domain names to IP addresses. In reality, this is just part of what DNS does. For our purposes - the role that DNS plays on a local network - we only need to consider this basic function. Very often, the DNS settings on a local server are ignored. Administrators who want more control of their network are able to take advantage of these options.

Overview

With a little bit of work, you can configure a local DNS server to make your job as a network administrator easier. This involves setting up local naming on the network for easier device lookups, and using DNS for content filtering or blocking ads.

Global DNS servers or local servers

There are a number of popular, widely respected global DNS servers available to do most of your translation for you. Here are the most popular ones out there today:

- Google. 8.8.8.8, 8.8.4.4, and 4.4.4.4.
- OpenDNS. 208.67.222.222 and 208.67.220.220.
- Level 3. 4.2.2.1 through 4.2.2.6.

While administrators should avail themselves of the advantage of having their own local DNS server, requests for domain name translation for websites on the internet should be sent to one of these global DNS servers.

Local network naming

When we consider domain name resolution, oftentimes we are thinking about resolving domain names for websites on the internet. One of the best uses of DNS, however, is resolving hostnames on your local network. Instead of having to memorize the IP addresses of your servers, use hostnames. Additionally, you can use your local DNS server to set up multiple names to resolve to a specific IP address.

There are a number of different devices on your network for which using a local DNS server will make things simpler. These include the following.

- Printers. Printer selection can be made clearer with descriptive hostnames, rather than memorized IP addresses.
- Terminal servers. Connect to your servers by name.
- PCs. Recognize and identify problem computers instantly.

Having devices such as printers, servers, and PCs named accurately helps administrators do their job more efficiently.

Can be used for content filtering or ad blocking

Administrators can take advantage of DNS server settings for security purposes as well. With a few different third-party tools, you can use DNS to filter web content and block ads.

Administrators can use services such as OpenDNS to filter web content. In this case, your DNS server can be configured to send website resolution requests to the OpenDNS servers (208.67.222.222 and 208.67.220.220). Configurations can be made to block requests (by category or by domain name) from specific source IP addresses.

Linux administrators can install a PiHole server on their network to utilize DNS to block ads on websites. Your PiHole server will check in with a central database to recognize domain names and IP addresses that are used by web advertisers and block requests to them.

Best Practices

There are a number of different things to consider, and here we cover a few of them.

Use descriptive hostnames on local networks

The larger your network grows, the more confusing things get. You need to make sure you use a logical naming scheme for all of the devices on your network. The hostnames that you assign your devices should be easily recognized for troubleshooting and configuration purposes.

A typical naming scheme could include device location, purpose, and a numerical value. Here are a few examples:

- A PC in the accounting office: ACCTPC01
- The second server in the communications room: COMMSERV02
- The printer in the branch office in Springfield: SPRINGPRINT001

The main point is that it should be descriptive enough to save you time when the device needs to be recognized.

Forbid untrusted DNS servers

Ideally, all of the devices on your network are provided with DNS server settings via DHCP. Even so, there still may be devices on your network that use manually configured DNS servers for resolution requests. As a security measure, you should have a list of DNS servers that are allowed to perform resolution requests, and forbid all others.

Some DNS servers aren't updated fast enough and won't be able to translate all requests. Other, more malicious DNS servers will intentionally direct traffic to hostile websites for the purposes of infiltrating your network.

Allowing outbound access for requests to these servers creates a security loophole that you want to keep closed.

Guide to Subnets and IP Addressing

Subnets are a fundamental part of the basic infrastructure of computer networks. Designing subnets properly requires a fair amount of planning and foresight.

Here, we offer tips for designing subnets and assigning IP addresses to them in a way that will allow you to simplify network management and grow the network when it's needed. In addition, we discuss different classes of subnets and how they can be used.

What Is a Subnet?

Local networks are made up of IP address subnets. A subnet is a range of IP addresses allocated to a specific network or virtual LAN. The subnet selection process may seem trivial, but there are a number of things to keep in mind when making the decision.

Selecting a Subnet

Selecting the best subnet for your network is important, no matter how simple it seems. Ideally, a subnet is allocated at the time a network is first designed. Occasionally, networks need to be re-addressed. This could be due to a network that has outgrown its allotment of IP addresses. Other times, networks have to be re-addressed due to improper subnet selection, such as a non-private scheme.

Classified Private IP Addressing

There are three different, large "super-subnets" from which every local subnet should be chosen. In order to avoid conflicts with local networks, these subnets are never used on the public internet. Each subnet is classified into one of three classes: A, B, or C. Administrators are free to create smaller local subnets by subdividing these original subnets. Here are the three classified subnets:

- Class A: 10.0.0.0/8 (10.0.0.0 – 10.255.255.255)
- Class B: 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
- Class C: 192.168.0.0/16 (192.168.0.0 – 192.168.255.255)

Network Considerations

When choosing the specific subnet for your network, you need to consider a few different things.

- Size of the subnet. Your chosen subnets should fit the network of which they are a part. It's also a good idea to leave room for additional devices.

- Popular consumer subnets. There are a number of subnets that come as the default subnets on many routers. The two most popular, for example, are 192.168.0.0/24 and 192.168.1.0/24. These subnets should be avoided. For maximum uniqueness, use a Class A subnet.

Multiple Subnets

While picking the right subnet is important, subnet selection for multiple networks brings another level of complexity. There are a few different ways that your different networks may interact, including VLANs and VPNs. With VLANs, multiple subnets on the same local network are considered. Different networks in different locations interact over a VPN. It's not uncommon to have to configure both VLAN and VPN subnets in the same project.

VLANs

VLANs (or virtual local area networks) are a way to segregate your network for efficiency and security. Before subnets are selected, a few items need to be verified. Although this is a slight divergence from the topic of subnet selection, it's very important to have a good understanding before making any other decisions, including choosing IP address schemes. You need to know that you have the proper hardware for the job, understand the reasons why you are creating VLANs, and know how you want to configure each port.

- Proper hardware. To set up VLANs on your network, your network infrastructure must support it. You need to have a router that is capable of creating VLANs and assigning VLAN IDs to different networks. You must also have a network switch that is manageable and allows for port configuration.

- Security needs. It's very important to know WHY you are creating VLANs and to have a concrete plan for how you will use them. Too often, administrators use VLANs to carve up their network without an end goal, with the result being confusion and complications. VLANs are a great way to separate corporate data from guest traffic, wired and wireless networks, and telecom communications from the rest of your network. VLANs should be used to streamline information, not to over-complicate things.

- Port configuration. You need to understand how you want to configure each port. Here are a couple of key terms to be aware of:

- Trunk port. This port is configured to communicate with all of the other ports and VLANs on your switch. Only a few ports, such as the uplink port from your router, should be configured as a trunk port.

- **Tagged.** Tagged VLAN ports, like the trunk port, are able to communicate with other VLANs on your switch. There should be only one tagged VLAN, often referred to as the management VLAN.

- **Untagged.** Untagged ports only give access to a single VLAN. Most of the ports on your switch should be on tagged VLANs.

Generally, you can use similar, sequential schemes between subnets. If you want to have one subnet substantially stand out from the rest, you can use a subnet of a different class for that case.

Here's a general example of how you can allocate subnets to a business with separate management, wired, wireless, and telecom VLANs. In this example, we're using a larger subnet for the wired network due to the number of devices, and putting the telecom devices in a different subnet class for clarification.

- Management VLAN: 10.0.0.0/24
- Wired VLAN: 10.0.4.0/22
- Wireless VLAN: 10.0.8.0/24
- Telecom VLAN: 192.168.150.0/24

Virtual Private Networks

A business with multiple locations spread out over a wide area may use virtual private network (or VPN) technology to join its networks together. Distinguishing different networks may be simpler in this scenario than with VLANs, but there are some considerations here as well.

- Keep everything unique. Overlapping subnets will not be able to interact with each other over a VPN. Be sure to keep everything unique.
- Use larger "super-subnets". Assign each of your locations a large subnet that can be divided up for VLAN purposes, if needed.
- Leave room for growth. In the future, there may be additional subnets that you need to connect to. Be prepared for that by setting aside a few subnets for future use.

Here's an example of a small business with three different locations, connecting via VPN.

- Location 1: 10.0.0.0/16
  - Management VLAN: 10.0.0.0/24
  - Wired VLAN: 10.0.4.0/22
  - Wireless VLAN: 10.0.8.0/24
- Location 2: 10.1.0.0/16
  - Management VLAN: 10.1.0.0/24
  - Wired VLAN: 10.1.4.0/22
  - Wireless VLAN: 10.1.8.0/24
- Location 3: 10.2.0.0/16
  - Management VLAN: 10.3.0.0/24
  - Wired VLAN: 10.3.4.0/22
  - Wireless VLAN: 10.3.8.0/24

Conclusion

Subnet selection is critical when setting up a new network. Proper subnet configuration offers a number of benefits. Clean subnets reduce the chances of IP address conflicts. Organized subnets make life easier for administrators trying to manage a network or troubleshoot issues. When networks are configured in the right way, administrators are better prepared for network growth in the future.

Hopefully, this information helps to show how important proper subnet selection is. It can seem very trivial, but when it's done in the right way, the benefits are definitely there. If you are the administrator of a mess of a network, try to redesign the subnets if you can. And if you are creating a new network from scratch, save future administrators a headache by doing it right the first time!

Guide to Network Mapping

Throughout history, people have created and used maps for navigation. Maps help us understand where destinations are located and how to reach them. To communicate this information effectively, maps need to be drawn correctly and labeled accurately. It's also important that maps be kept up to date, because terrain often changes.

In the networking world, we use maps for similar purposes. Maps help administrators perform do their jobs more efficiently thanks to having properly organized data at their fingertips. When the control of a network is transferred to a new administrator, network discovery becomes much easier with the help of an efficiently designed network map.

Why mapping a network?

EASIER TO MANAGE

EASIER TO PLAN EXPANSION

EASIER TO TROUBLESHOOT

Network map consists of

RECORD OF IP ADDRESSES IN USE

INVENTORY OF HARDWARE ASSETS

Devices to include on the network map

PCS

- IP assignment (static or dynamic)
- Wired or wireless
- Software inventory
- Hostname

PRINTERS

- IP assignment (static or dynamic)
- Physical location
- Manufacturer and model
- Tray assignments

VOIP PHONES

- Extension number
- VLAN ID
- Physical location

NETWORKING EQUIPMENT

- Number of connections and ports
- Connection speeds
- Uplink information

Wireless Networks

More and more, network administrators are seeing wireless networks move from being an ancillary part of the network to one that is just as important as the wired network. Administrators should have a good understanding of wireless coverage through their network via mapping. Additionally, they should take into consideration speed and security.

Wireless Networks Security Considerations

Because your wireless network naturally increases the vulnerability of your infrastructure, security must be taken extremely seriously. Here are a number of suggestions for securing your wireless network.

- Security keys. All networks with corporate-level access must be encrypted and force users to use a key to authenticate. For increased security, guest networks can be password-protected as well.
- Network segmentation. Your guest network should be separated from your corporate network. This could be done in a number of ways, including VLANs, router configuration, or even separate internet connections. If your corporate wireless network doesn't need the same access as the wired network, these networks should be segmented as well.
- MAC address filtering. Administrators can use MAC address filtering on corporate networks to provide additional verification for devices to connect. For devices to be able to access a filtered network, not only do users need to know the wireless key, but the administrator must add the device's MAC address to a list of allowed devices. Keep in mind, however, that attackers can easily "spoof" MAC addresses (by making a device appear to have a valid MAC address in order to connect), so you should not rely on this safeguard alone to secure your wireless network.

Wireless Speeds

As wireless technology develops, speed capabilities have become faster and faster. With the growing demands of wireless networks in a business setting, it's almost always worth investing in the fastest infrastructure possible. There are three different speed classifications that most administrators work with today.

- 802.11ac. As of today, this is the fastest speed classification available. Network administrators who are purchasing new access points should be sure that the equipment they shop for supports this technology.
- 802.11n. While this specification is quite fast, it is nevertheless slower than 802.11ac technology. Existing infrastructure running at these speeds doesn't necessarily need to be replaced, but it should not be purchased for new installations.
- 802.11b/g. This specification is now quite old, and fairly slow. Network administrators should be actively replacing equipment that communicates at these speeds.

Network Security Best Practices

Keeping your network secure is paramount to your business's success. In fact, if your security systems fail, it may cost you everything. Because of this, you should take network security as seriously as any other business function.

At the forefront of every security policy should be the sanctity of your clients' business premises and the location of the network infrastructure. The users should be required to authenticate at every level and follow strict guidelines while accessing your business's data. The devices should be locked into security policies, too.

Physical Security

The most basic dimension of network security is "protecting your castle". This concept is simple, but important. You don't want to allow the general public where they don't belong. If an intruder does make it past the gates, you need to do everything that you can to make it harder for them to get what they want. Here's a breakdown of securing the physical side of every part of your network.

Secure Your Premises

The building you protect should be divided into separate levels of access. Access should only be given to those who need it, and no one else. Here are three levels of access that should be included:

- Public access. At some level, the public should be separated from the rest of your business. If your area of business doesn't involve face-to-face communication with clients, access should be locked down at the front door. Retailers and other customer-facing businesses should separate the areas where customers are welcome from those where only employees are allowed.
- Employee-only access. The "employees only" area of your building should require some sort of authentication for access. As employees come and go, access should be adjusted in real time. When employees quit or are let go, their access to private areas should immediately be revoked. There are some additional areas, such as your network closet, where only specific employees should be granted access.
- Network administrators. The locations within your business that should be kept the most secure are the rooms that contain your networking infrastructure. The only people that should be allowed into these rooms are network administrators. Access in and out should be recorded, so that when security issues arise, those who have had direct access can be identified.

While physical building security isn't specific to networking, the two levels of security go hand-in-hand and need to be considered. A tiered access system is the best way to make sure that the right people are given access to the correct locations.

Port Configurations

There are security measures to be taken with regard to intruders who make it past your initial levels of security. One effective way to help secure these systems is to disable all unused ports. Disabling these reduces the surface area of attack on your network.

On your managed network switches, disabling unused ports will prevent intruders from plugging a device in and accessing the network. Turning off unused USB ports on your servers and workstations will prevent attackers from stealing data with USB sticks. Similarly, preventing foreign devices from connecting to your access points and stealing data locks down a wireless “port” into your network.

User Authentication

Gone are the days when you could get away with not asking for a password. More and more, user access systems are hacked and exploited. Fortunately, it’s quite easy to minimize the risks of your accounts being compromised. The following are best practices for your user authentication policy.

Force Logins at Every Level

At every level of network access, your employees should be forced to have a username and password. It’s no longer acceptable to choose not to activate password protection on your PC, no matter how relaxed the work environment is. In addition to this, authentication should not be shared between users. Every employee needs to have his or her own individual username and password.

Enforce a Password Policy

Having a simple but logical password policy helps to prevent security issues. There are a few standard password policy rules to follow.

Use complex passwords. Passwords should have a minimum length requirement of at least eight characters. Each password should require at least one number, one letter, and one special character.

Change your password periodically. Your users should be changing their passwords frequently. Forcing users to pick a new passphrase every two months is a good rule to follow.

Don’t use the same passwords over and over. The best practice is to use a different password for every place that you log in to. To make things simpler, there are a few different secure software packages that can help you keep track of your passwords across systems.

Following these rules will sharply reduce vulnerabilities. In a domain environment, these policies can be enforced with your Active Directory server.

Manage Authentication Properly

As users enter and leave your business, it’s important to follow a few key rules to stay on top of authentication security.

- New employees should go through proper security training before receiving access. As new hires come in, you need to know that everyone is on the same page. Proper, uniform security training will help your new employees understand the company’s security standards.
- Principle of minimal privilege. Most of your users will need minimal access to the entirety of your company’s data. You shouldn’t give employees access to what they don’t need. Limit access to what is essential.
- Departing employees should have access revoked immediately. Employees who leave, especially those who are fired, should be rendered unable to access data immediately upon being removed from the

building. You don't want a disgruntled employee using your data against you.

At all times, your IT staff should be aware of all of these rules. They are the ones who will be responsible for enforcing them.

Firewalls and Protection Software

You've secured your network and user authentication processes. Now it's time to make sure that traffic in and out of your system is being monitored. All incoming traffic should meet a gateway firewall before being allowed to enter your network. Once it is allowed through, there should be a second level of protection at the device level.

Network Firewalls

Every network should be protected by a robust firewall. Here's an overview of the standards that each firewall should follow.

Block all inbound access by default. When your firewall is first set up, all traffic hitting your router should be blocked by default. As requests come in for open access, ports can be opened, one at a time.

When possible, restrict inbound access by source address. Eventually, you'll have to allow traffic in. If possible, find out where traffic is coming from and restrict it to certain host IP addresses. In some situations, such as VoIP phone systems, this may not be possible.

Limit outbound access as much as possible. In general, your network is going to need to leave a lot of ports open for outbound access. If possible, block outbound ports that you know you won't be using.

Network firewalls, when combined with PC firewalls, offer a very secure layer of protection for your network.

PC Software

All of your PCs should be running protection software. The Windows operating system offers a few different options, including Windows Firewall and Windows Defender. Network administrators can add an extra layer of security by using centrally managed third-party protection software. These software packages can be managed from a central server, maintaining system updates and other aspects.

When to Forbid Outbound Access

On the occasions in which devices on your network fail security protocols, steps should be taken to secure your network. The most effective way to do this is to deny these devices outbound access. The following are a few situations in which this is effective.

- Devices using unfamiliar DNS servers. A list of allowed DNS servers should be kept within your internet gateway. Devices that aren't using these DNS servers should be denied outbound access. Compromised DNS servers could cause a security risk by diverting traffic to risky websites, rather than the intended destinations.
- Devices using protection software that has gone out-of-date. Threats on the internet change a lot. There are new vulnerabilities being discovered daily. Because of this, your devices should check for updates and new virus definitions daily. Overlooking these updates can create a security hole in your network.

Devices running insecure operating systems. Security updates to your operating system are crucial. PCs should be forced to stick to up-to-date, actively supported operating systems and be current with security updates.

Once security issues have been resolved, these devices can once again be allowed outbound access. If these issues were caused by user error, it's good practice to explain the situation to the user and let them know how to prevent it from happening again.

Conclusion

A logically and intelligently designed network helps businesses communicate and operate with minimal interruption. To enjoy the benefits of such a network, you need to build these elements into the design stage.

Not only should the proper hardware for the network be purchased, but it should also be configured in a way that best fits the network. An appropriate IP address scheme should be selected, with provisions made for additional networks and VLANs. Network services, such as DHCP and DNS, should be configured to best fit your specific network. Security considerations should be addressed for all areas of your network as well.

Your network, like any other community of hosts, works best when it is designed intelligently.

About MSP360™

Established in 2011 by a group of experienced IT professionals, MSP360™ (formerly CloudBerry Lab) provides cloud-based backup and file management services to SMBs.

MSP360's offerings include powerful, easy-to-use backup management capabilities and military-grade encryption using customer-controlled keys. Customers can choose to store their backup data with all the major cloud storage providers, including Amazon S3, Microsoft Azure, Google Cloud, Wasabi, and others. MSP360™ also partners with thousands of VARs and MSPs to provide them with turnkey, white-label data protection services.