CHAPTER

12

Design Methodologies

Take a method and try it. If it fails, admit it frankly, and try another. But by all means, try something.

— Franklin D. Roosevelt

Planning and designing a network can be a daunting task. In the early days of data networking, a network consisted of a handful of nodes. Any addressing schemes were normally manually assigned and maintained. This required human intervention any time a node was moved, removed, or changed in any way. This manual intervention was not that bad, however, due to the fact that there were not that many numbers to keep track of.

In today's LANs, this manual addressing would not work. Networks are changing, technology is changing, and LANs have grown to a size that was not foreseeable 20 years ago. In addition, other concerns exist that were not there 20 years ago, including security, the highs and lows[1] of the LAN, and many others.

LANs can be a simple as a handful of nodes in a remote office to as complex as thousands of nodes in a fully meshed routing environment supporting applications that require as much of the highs and lows as can be squeezed out of the LAN any time the application want to do so. LANs are responsible for supporting multiple protocols running over multiple nodes and multiple media types. Many of these node and media types are from different vendors, all of which can potentially be running some proprietary features that may or may not play nice with the nodes, media, and even protocols that are running the LAN.

[1]These were discussed in Chapter 11 — high throughput, high total bandwidth, and low error rates and delays.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Sounds challenging, doesn't it?[2] And we haven't even gotten to plans for future growth. What is the organization's five-year plan? Are you installing gear that can be upgraded? How do you know how much gear to plan for without getting more than you need? These are just some of the questions you will need to ask yourself if you are going to design a network.

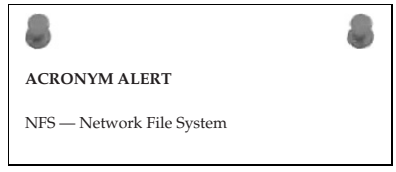
Planning and designing a data network is complex enough from a LAN perspective, and that is the focus of this chapter. For comparison purposes, we may discuss commonalities between the LAN and networks of smaller and larger size. Proper planning and design of the network can be trial and error at times. Sometimes things just don't do what you want them to.[3] But don't get discouraged. When you encounter problems with a design in the network, follow President Roosevelt's advice.

12.1 Your Task Is to Design a Network

By no means will you be a professional network designer after reading this chapter, but that isn't our intention. As with most of the topics in this book, we are trying to teach you the fundamentals. It's important to understand the difference between a network that was planned and designed carefully and one that was thrown together haphazardly, no matter what you end up doing in a networking career.

Careful planning is essential to ensure that your network will support your organization's needs. So what do you want to consider when you are designing a network?

- What are the needs of the business or organization?
- What should be considered in order to meet current and future needs?
- What are the cost considerations (short and long term)?[4]



These are all important questions to consider. You might want to design the most ultra-fantastic network with all the bells and the whistles, but the budget may not cover it. You might also want to build in some features to make life simpler for you, but that may be beyond the scope of the business model or plan.

[2]If you like challenge, you would love a job in data networking.
[3]No matter what the salesperson told you.
[4]This would include costs factored in for network maintenance.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.1.1 Types of Organizational LANs

Following are examples of some of the various network LAN types that are in use. While reading through this list, consider the impact that might occur if these LANs were improperly designed.

- **Hospital LANs** — Life-critical data is delivered to various departments via the computer. Emergency logging is automated. Lives could be in danger if there are any network delays.[5]
- **Banking and financial corporate LANs** — Can you imagine how much money can be lost during the middle of the trading day on Wall Street[6] if the network has delays? What about the delays that could occur in the online trading world? Not to mention all the remote automatic teller machines.
- **Manufacturer LANs** — Production lines in all sorts of different manufacturing environments run with the use of robotics and automation. If there is a data hiccup, thousands of dollars can be lost.
- **Retail LANs** — Retail stores often have a LAN running within them, taking care of inventory and sales along the way. Periodically, the store will connect to the corporate LAN to exchange the data collected. Today, some retail sites run a remote connection into the LAN and are able to provide real-time updates. Imagine the impact if the store is not able to ring sales or communicate as needed with the corporate LAN.
- **Government LANs** — Consider the amount of security that has to be deployed for government LANs. Authentication methods and authorization are of the utmost importance. Consider what might occur if a hacker gains access to a government LAN.[7]

POP QUIZ

Name five businesses or organizations that are not listed above. What do you think the biggest concern would be pertaining to each organizational LAN type?

[5]Getting off topic a bit, here is an interesting tidbit of information. There are hopes that one day a doctor can connect to the hospital from home and perform an operation over a video feed with the use of robotics. Won't that be amazing if it ever happens?

[6]Although based on the days that Wall Street had beginning in late September 2008, maybe the network should fail every time that stocks start to tumble. No network . . . no trading . . . problem solved.

[7]And for any other LAN — security is very important.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

And this is just a small list. Name a business type, and there will be some form of network for it. The network itself may not be optimized,[8] but it will most likely be there. What the design of the network for these organizations looks like all depends on the needs of that organization.

12.1.2 Other Things to Consider

Now that we have an idea of the needs of the business, we still have some work to do. The next thing is to ensure that you have a fair balance between what is available to be considered in the network environment (needs vs. wants) and whether the projected business needs limit what technically is available. You don't want to provide more than is needed for the LAN, but you also don't want unreasonable demands driving design decisions.[9] Another important concern for network planners is to not be too cutting edge. You don't want to deploy a brand new switch, new feature, or new code until it has had time to be field tested.[10] Most products undergo a serious amount of testing, but environments are different and new products often introduce new problems that can take time to iron out.

There are also several external factors:

- Consideration needs to be given to WAN interfacing, as well as interfacings with LANs that are within of your realm of control.
- Make sure you know about any government regulations and are in compliance with them.
- What are your competitors using/doing? What network type would you like to have, and who has done it right? What did they do?
- What is the potential technological growth, and will your proposed design be prepared to support it?

12.1.3 Building the Foundation

Now that you have an idea of the things that need to be considered, you can move on to the planning stage. Before you do so, however, we are going to let you in on a secret. If you have been paying attention to what we have written thus far in the book, guess what? Without knowing it, you already have some of the fundamentals that are necessary to design a network.

[8]This can be for several reasons. The network may be outdated, poorly designed, or simply not maintained properly. If you try modeling yourself based on a similar network type, make sure you model your LAN after one that has been operating a while and proved itself successful.
[9]Just because someone wants something to work a certain way does not mean that it can be done.
[10]Keep in mind that you may be able to make some kind of deal if you are willing to test any or all of these.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

- You have an understanding of networking concepts.
- You have an understanding of the needs of the organization.
- You have an understanding of the hardware types that operate in a LAN.
- You have an understanding of LAN protocols.
- You know the different types of network topologies that are used in today's LANs.
- You know about LAN protocols and MAC and IP addressing.
- You know the seven OSI layers and what functions at each layer.
- You know how to make spaghetti and meatballs!

RANDOM BONUS DEFINITION

aggregator — The entity that performs the operations required to make multiple physical links function as an aggregated link.

Give yourself a pat on the back. You are ready to start planning the network.

12.2 Let's Start Planning

We just realized that there has not been anything really technical about this chapter so far.[11] You will be surprised at how much nontechnical thought is put into the initial planning stages. Don't worry — there is plenty of technical thought left in the upcoming pages.[12]

We already have established that you have been tasked with planning and designing a network. More than likely, you will be given a team to work with to get this project going.[13] The first task you will want to attack is to develop an action plan and project scope.

12.2.1 Development of Scope

```
Main Entry: scope (skōp)[14]
Function: noun

1. The range of one's perceptions, thoughts, or actions.
2. Breadth or opportunity to function.
3. The area covered by a given activity or subject.
```

[11]Then again, when is cooking up some of Mama Bramante's spaghetti a technical task?
[12]Jim is thinking that a nontechnical book might be fun to write, perhaps *The Networker's Guide to Homebrewing Beer*.
[13]At the very least you should insist on access to someone who knows something when and if you have any questions along the way.
[14]The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Developing a project scope is important in the early phases of network design. This is where you gather the information you will need in order to proceed with the project. One of the big considerations is the nature of the organization (the type of network). Do the users only communicate with other users on the network, or is there a need for access to networks outside of your own LAN? Do users need remote access? Do any vendors or customers need access? What applications need to be supported by the network? Finally, it is good to know the budget that is available for the project and the time frame for completion.

The next thing that needs to be addressed is to determine whether the wants and needs are even doable. Is there enough money available to meet the requests? Can the project be completed in the proposed time frame? Will the project's completion keep up with technological growth?

RANDOM BONUS DEFINITION

aging time — This is used in a spanning tree environment — the amount of time a node can be inactive before a dynamic filtering database will remove the node's entry.

Now that the scope has been discussed, and it was determined to probably work, the scope has to be refined even more. The specific services that are to be placed in the LAN need to be determined. Information such as:

- Will the network support voice communications?
- Will the network support data communications?
- Will the network support e-commerce?
- Will the network support video streaming?

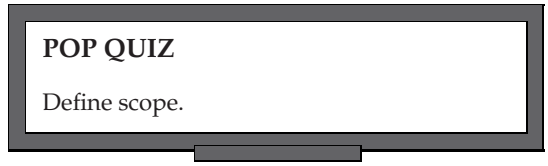
After identifying the services, you must determine what the potential traffic flow will be in such a network. What will be required in the future? Some of these can be answered if you are fortunate enough to have a network you can model yours after. Also, if you have a way to test (or get a vendor to help you out), you can possibly get some traffic analysis data that will give you a good idea of what to look for and expect. But the real test is when you go live. The secret is making sure you have enough, but not too much.

Data traffic patterns are subject to variations and fluctuations. Sometimes this is due to a certain time of day or a particular day of the week. Even the weather can affect data flow. Usually the trends point to an event (Friday night backups, Monday morning end node boot-up, etc.), and you just won't know about all of them until you get the network up and running. In the next chapter, we will be discussing ways to baseline.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.2.2 You Are Not Alone



The great thing about all this is that you are not alone. You can send your scope out to some of the many networking vendors and ask them what they have that will help you do what you want to do. This will get you a lot of information and maybe even some deals along the way. The request for information (RFI) is a standard process used in business to obtain just this type of information from vendors. Once you find what you like, the request for proposal (RFP) is used to seek the best deal.

12.3 A Hierarchical Design Model

There is that word again — *hierarchical*. The hierarchical design model is the most commonly used model in most high-speed LANs today. This model allows for easy expansion. It also makes network management and troubleshooting easier. By breaking nodes in the LAN into three functions, the nodes are able to focus on specific tasks instead of each of them working to perform all tasks. Figure 12-1 shows an example of what we are talking about.

The hierarchical model has the following three different layers, with nodes within each layer performing a specific function:

- Access layer
- Distribution layer
- Core layer

Keep in mind that a model is a recommendation or a guideline more than it is a rule. Sometimes a single node can take care of all the layers itself, sometimes it can't. It's always easier to follow a model, and this one is tried and true.

12.3.1 Access Layer

The access layer is the lowest layer. This is the layer that interfaces with the endpoint nodes. Types of nodes that are found at this layer are wireless access points, hubs, repeaters, bridges, Layer 3 switches, and routers. The access layer is what enables end users to connect to the network. This layer is also responsible for determining when nodes are not allowed access to certain portions of the network.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

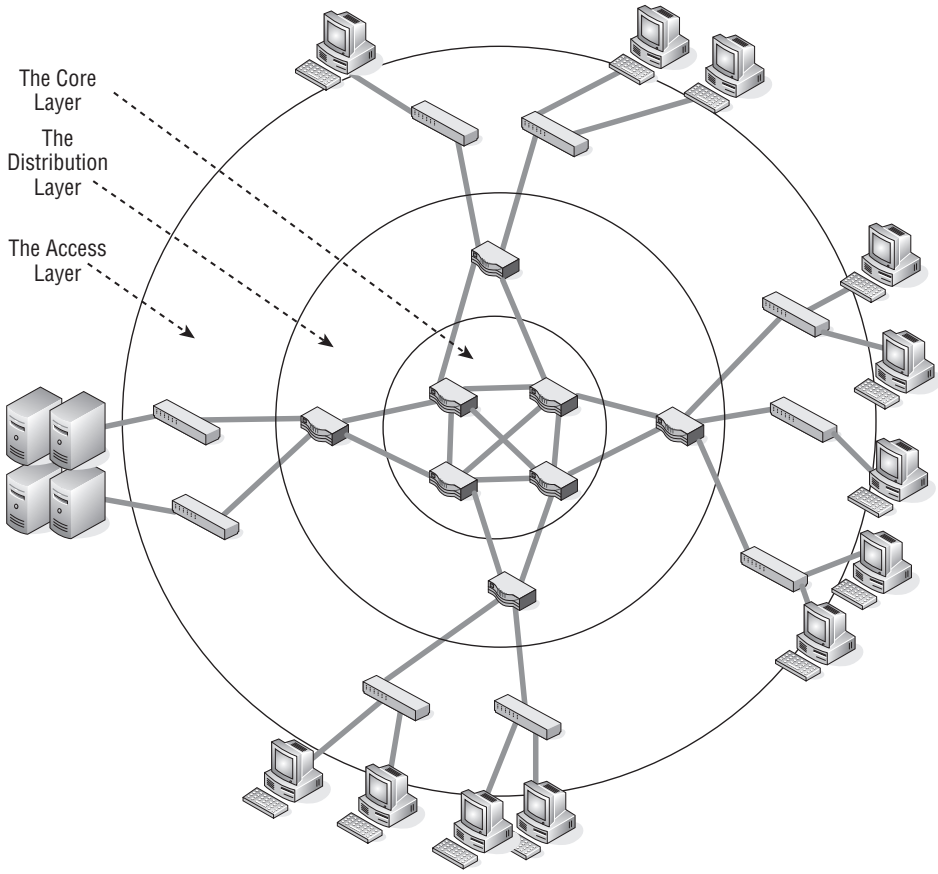


Figure 12-1 A hierarchical approach to LAN design

The access layer can also be the gateway to the LAN for remote users (see Figure 12-2). For this to occur, some form of WAN technology must be used.

Examples of WAN technologies that can be used to connect remote sites to the corporate LAN include:

- Frame Relay
- ISDN
- Leased lines

The access layer can simply be thought of as the endpoint node access to the LAN. It manages the data between the endpoint nodes and the distribution layer. Switched bandwidth and MAC filtering are functions performed at this layer.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

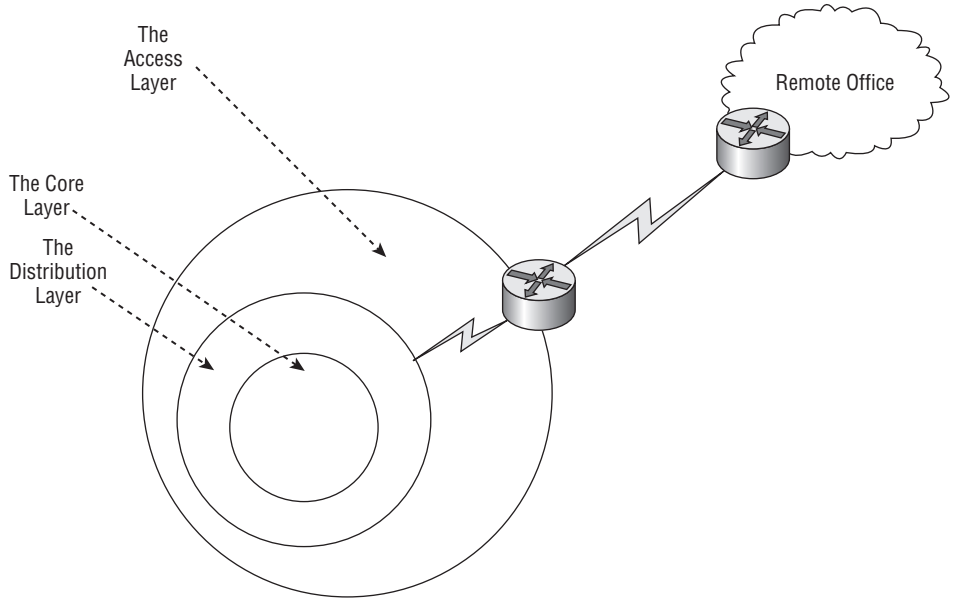


Figure 12-2 Remote relations to the access layer

12.3.2 Distribution Layer

The distribution layer is the middleman between the access layer and the core layer. Data received from the access layer is sent to the core layer to be routed to the destination. Broadcast domains are separated at this layer with the implementation of virtual LANs (VLANs). Security is also a function that is implemented at this layer.

Network access can be implemented at this layer when policy-based connectivity is required. High-performance Layer 3 switches are implemented at this layer. Guarantees that are required at this layer are high performance, high reliability, high availability, and redundancy.

POP QUIZ

Name three WAN technologies that are used to connect to remote sites.

Policy-based connectivity between the other layers is what you get from the distribution layer. Figure 12-3 provides an example of a method of connecting the three layers together.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

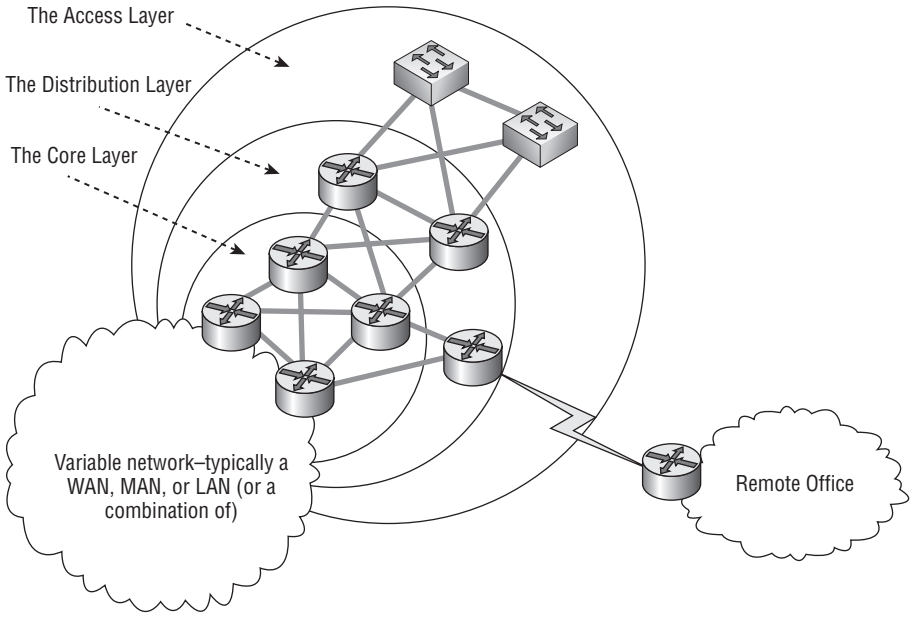


Figure 12-3 Connecting the three layers

Notice that the distribution layer has nodes that aggregate with other nodes in the access and code layers. Additionally, there is a remote connection that is coming from a remote office and accessing the network via the distribution layer.

12.3.3 Core Layer

This is the big daddy layer of this model. The core layer is the backbone of the LAN and often provides connectivity to WANs as well as to Internet services. The core routers[15] are highly available and support redundancy in the connections with the distribution layer nodes. These nodes need to be hefty, as they process data flowing throughout the whole LAN. They have to do that reliably and quickly.

Refer to Figure 12-4 and answer this question: If the drawing represents the physical layout of a network, is this an example of a hierarchical design?

POP QUIZ

What are the layers of the hierarchical design model?

[15]When we say routers, we are referring to any node that can provide network layer services. So, a router may be a router, a Layer 3 switch, etc.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

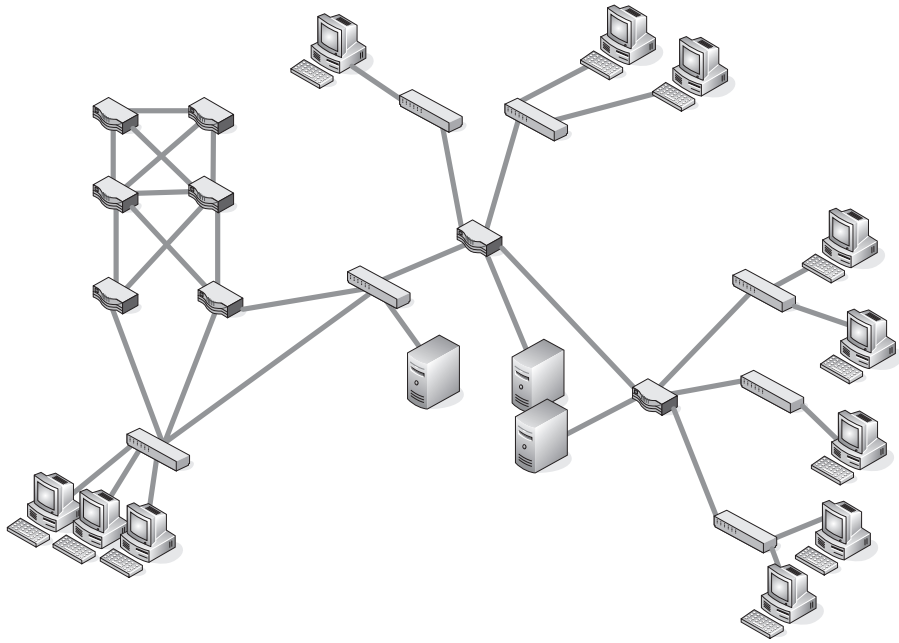


Figure 12-4 An example of a LAN physical layout

The answer to that question is *maybe*. We do not know the logical layout of the network, so it is entirely possible that this figure represents a hierarchical design. Hierarchical in a logical manner, that is; the physical layout is pretty much a moot concern at this point.

AN UNRELATED MOMENT OF PAUSE — BARBECUE CHICKEN NACHOS

We know how easy it can be to get wrapped up in the reading of this book and time can get away from you. Before you know it, you don't have time to make dinner and the last pizza delivery ran 30 minutes ago. This is a super-easy recipe and a really excellent quick fix when you need to fill the void left from skipping dinner.

The layers of the nacho model are as follows:

- **The Determination layer**
- **The Preparation layer**
- **The Application layer**
- **The Thermal layer**
- **The Devour layer**

(continued)

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

AN UNRELATED MOMENT OF PAUSE – BARBECUE CHICKEN NACHOS *(continued)*

The Determination Layer

This is the first layer, in which you decide on the toppings that you want on your nachos. Thanks to this handy reference model, you are not confined to the recipe listed here. Anything goes well on nachos, so if you like it, try it out. For this recipe, we have determined that we will be using the following ingredients:

- **Cheese – Use whatever kind you like (cheddar and/or Monterey jack is good).**
- **Tortilla chips – Any kind will do. We normally use restaurant-style tortilla chips, which make good nacho chips.**
- **Chicken – Chicken breast is the best.**
- **BBQ sauce – At least one bottle of your favorite kind. The ones with the squirt top works well for presentation purposes.**
- **Bacon – One package.**

The Preparation Layer

This layer is where you prepare everything that needs to be prepared. Here are the preparation steps:

1. **In a bowl, place enough cheese to cover the amount of nachos you plan on eating. You can shred it yourself or buy it preshredded.**
2. **The chicken can be boiled and then shredded, or sliced and cooked in a pan; the choice is up to you. Don't add a lot of seasoning to the chicken as it cooks, as you will be gaining flavor in your nachos.**
3. **Fry the bacon and then cut it into small pieces.**

The Application Layer

This is where is you put everything together. Apply all your toppings to your nachos in any way you want – it's hard to mess up nachos. This is what we did; it came out yummy and had a nice presentation.

Use a microwave-safe plate or platter. Put a generous handful of tortilla chips (make sure to cover the plate completely). Now put a layer of cheese and about half of your bacon. Make sure to cover the chips completely with the cheese. Now put on another layer of chips. Next, put the chicken, enough cheese to

(continued)

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

AN UNRELATED MOMENT OF PAUSE – BARBECUE CHICKEN NACHOS *(continued)*

cover the chips, and the rest of bacon. Make sure that you get some cheese on the chicken, but it does not have to bury the chicken. Finally, squirt the BBQ sauce over the whole thing – be creative. The nachos should be in a heap on the plate, but not flowing off of the plate.

The Thermal Layer

Stick all this in the microwave and cook it for about 30 seconds, then pause for about 5 seconds and then another 30 seconds. Keep your eye on it – when the cheese is melted, they are done.

The Devour Layer

Eat the nachos.

12.3.4 Why Hierarchical?

Some of you probably wondering, ''Why hierarchical?'' Well, we have been putting a lot of effort into presenting you with a slew of networking information while making the book as enjoyable to read as possible. So when the recipe was written, we thought it might be funny to present it in a hierarchical model. It worked too. Wait — you were not thinking about the recipe at all, were you? What you are really wondering is what the benefits are of a hierarchical model.

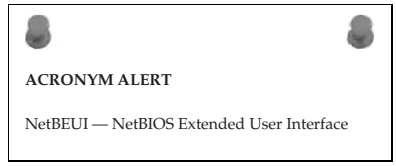
Here are just a few:

- **Design replication** — Once you have a working model, you can simply change the addressing schemes and design the next network expansion based on the way the original design was configured.
- **Expandability** — As the network grows, it is very simple to introduce additional nodes into the topology. Future growth planning is a breeze.
- **Redundancy** — Redundancy from the access layer to the core layer is very important in high-speed LANs. When a node fails, you have to have another node picking up the pieces until the node comes back on line.
- **Better performance** — Nodes that operate in the hierarchical model are able to maintain close to wire speed transmissions to all of the nodes it supports.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

- **Security** — Access control security is provided at the access layer. The distribution layer can support advanced security that meets the security needs of the LAN.
- **Easy to manage and maintain —** Because of the scalability of the hierarchical design model, the network is easy to manage and maintain. A layered approach to troubleshooting helps you find the source of a network connectivity issue. Additional nodes can be installed fairly simply, and configurations can be built from existing configurations, saving you time and money.[16] Over time, the hierarchical model will pay for itself in money saved due to the ease of maintaining and managing the LAN.



And there you have the hierarchical design model in a nutshell. Now let's take a look at a design model that is used in planning Ethernet segments. The next section covers the 5-4-3-2-1 design reference model.[17] It is a nice model to follow when you are planning a network, as it pulls together many tasks that are needed for basic design principles.

THINGS YOU JUST HAVE TO KNOW

Before we move ahead, here are a couple of terms you need to know.

- **Collision domain — A group of nodes, sharing a communication channel, that are all in a group where a collision can occur. These nodes are connected to the same shared medium and are part of the same collision domain. These nodes are not concerned with other collision domains, as they do not have to negotiate for a communication channel bandwidth with them. Collision domains are normally separated by a bridge.**
- **Broadcast domain — A group of nodes that are all within the same broadcast area. The broadcast domain comprises multiple collision domains. Broadcast domains are normally separated by a node that functions at Layer 3 or higher.**
- **Propagation delay — The amount of time it takes to transmit a set number of bytes from endpoint to endpoint in a LAN.**
- **Network segment — A physically related grouping of nodes. Similar in function to a subnet, which is a logical grouping of nodes.**
- **Repeater — A Layer 1 node that connects network segments.**

[16] When it works in one segment, it should work in another.
[17] This is also known as the 5-4-3 rule. Either term is fine, as long as you understand the overall concept.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.4 5-4-3-2-1, Speed Is Not the Big Concern

The rule used for designing a collision domain is known as the *5-4-3-2-1 rule*. This is more of a reference model than it is a rule, providing guidance as to the number of repeaters and network segments that can be on a shared access Ethernet backbone.[18] The 5-4-3-2-1 rule says that between two communication nodes in a shared environment, the following are the maximums that are allowed:

- **5** — This is the total number of segments allowed.
- **4** — This is the number of repeaters used to join the segments together.
- **3** — This is the maximum number of segments that have nodes that are active.
- **2** — This is the maximum number of segments that are not active.
- **1** — This is the number of collision domains.

The 5-4-3-2-1 rule is used in networks that use a tree topology (a combination of a bus and a star topology). The tree topology used groups (segments) that attach to a linear backbone. Figure 12-5 shows an example of this rule.

RANDOM BONUS DEFINITION

backbone — A network used primarily to interconnect other networks.

In a tree topology environment, there can be a maximum of five segments between two communication nodes. Additionally, data can pass through a maximum of four repeaters. Finally, there can be a maximum of three segments that are populated with active nodes. In Figure 12-5, you can see that there are five segments, four repeaters, and no more than three active segments between the source and destination endpoint nodes.

POP QUIZ

What is the purpose of a network's access layer?

By placing these limits on the collision domain, you are essentially ensuring that the propagation delay is decreased (fewer nodes to pass through). This greatly improves the reliability in the collision domain.

[18]Note that this rule only is beneficial in a shared access domain. Switched backbones should consider other methods (most commonly, the hierarchical).

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

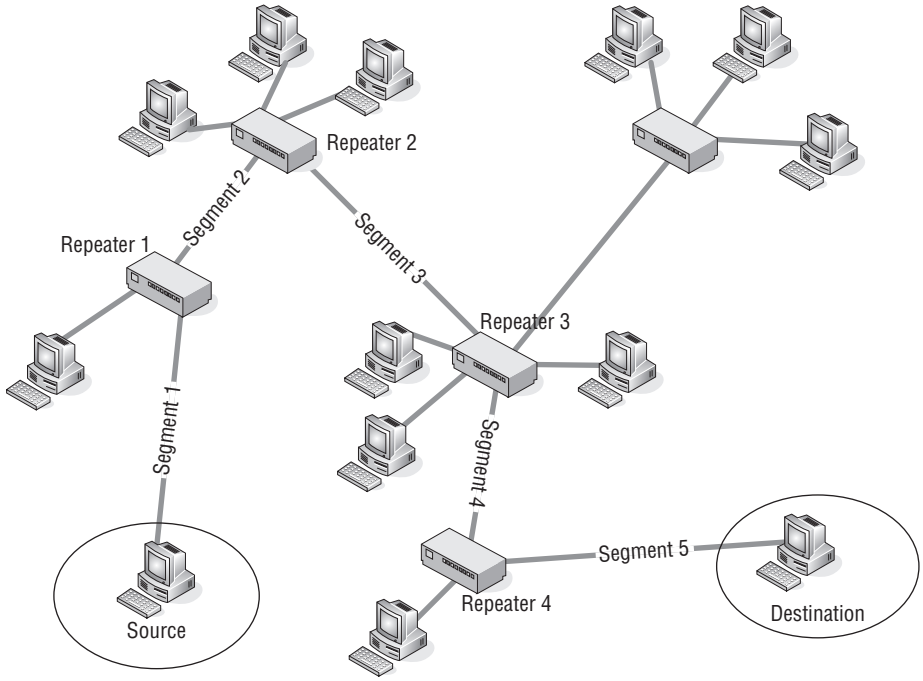


Figure 12-5 The 5-4-3-2-1 rule in action

12.5 Making Determinations

Now that all the preliminary mumbo-jumbo has been taken care of, it's time for you to determine what you will need out of your network. Some things will be contingent on others (for instance, if authentication is going to be used, what will you need to support it?). This is exactly why you will want to review and adjust your plan as you go along.

You have determined the needs and wants of the users of the network. Now you start making determinations on what should be put into the network to support those needs. Be sure to consider potential future growth in your determinations. Some decisions you will make include:

- Which topology are you going to be using?
- Will you be using Ethernet or Token ring?
- How many ports will be needed at each level?
- What is the target transmission speed(s)?
- Which node types are you planning on deploying?

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

- Which end-user applications will be used?
- Which protocols will need to be supported?
- Will remote access be required?
- Which types of WAN protocol options will be used (if required)?
- What are the security concerns?

ACRONYM ALERT

DDP — Datagram Delivery Protocol

In the next few sections, we will discuss some things you should consider when making these determinations.

12.5.1 Determining Which Topology to Use

Deciding on the network topology really depends on the requirements at each level of the network. More than likely you will be using Ethernet (the most popular shared network protocol), so your biggest decision will be the speed and the actual physical layout of the building in which the network is being installed.

Chapter 1 introduced the topology types in most LANs. The three most popular topology types are the bus, the star, and the ring. Let's take a moment to review these.

12.5.1.1 Bus Network Topology

The bus topology is the most often used topology in LANs. In this topology, the nodes connect to a common shared communication channel, referred to as a *bus*. Figure 12-6 shows an example of a network with a bus network topology.

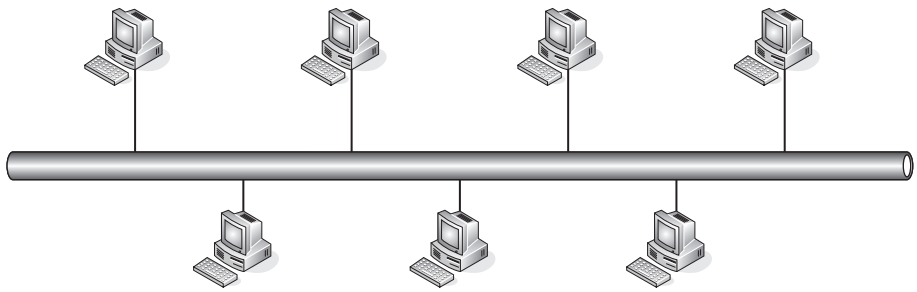


Figure 12-6 The bus topology

So what makes the bus topology the most often implemented?

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Advantages:

- It's easy to install.
- It's easy to extend.
- It's less expensive to implement than other topologies.

Disadvantages:

- There is a limitation to the distance a cable can go without a repeater.
- There is a limit to the number of nodes that can be supported.
- The LAN can experience sluggishness in performance when there are heavy traffic loads.
- Security risks exist because all stations can hear what the others are saying on the shared channel.

The cost and ease of use are the biggest reasons for considering the bus network. However, if there are concerns about speed, performance, reliability, or number of supported nodes, another design might need to be considered.

RANDOM BONUS DEFINITION

blocking state — A stable state in the Spanning Tree Protocol in which a bridge port will receive BPDUs but will neither receive nor transmit data frames.

12.5.1.2 Star Network Topology

The star topology can be divided into two categories. It can be a logical star topology or a physical star topology. Figure 12-7 shows an example of a physical star topology where a central bridge or a hub controls the communications to and from attached nodes.

The advantages of a star topology include:

- It offers better performance.
- It's easy to troubleshoot.
- It offers high scalability of the network through the central node.

The disadvantages of a star topology include:

- There is too much dependency on the central node.
- It can be complex to manage.
- Wiring can become cumbersome.

If neither the bus nor the star topology fit your specific needs, you might want to consider implementing a ring topology.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

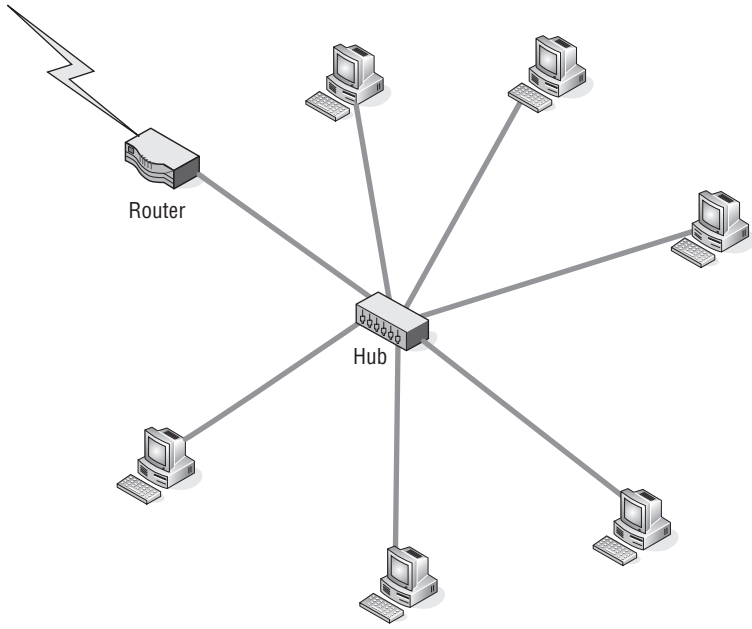


Figure 12-7 The star topology

12.5.1.3 Ring Network Topology

The ring topology is used for Token Ring and FDDI LANs. In the ring topology, a frame is passed from node to node until it reaches its destination. Figure 12-8 shows an example of a network with a ring network topology.

The advantages of a ring topology include:

- There is no need to have a mechanism to ensure collision-free datagram passing.
- It can be expanded to cover a greater number of nodes than some of the other topology types.
- It's fairly simple to maintain.

The disadvantages of a ring topology include:

- A failure with one node on the ring can cause an outage to all connected nodes.
- Any maintenance (e.g., adding a node, making a change to a node, removing a node) affects all the nodes that connect to the ring.
- Some of the hardware required to implement a ring is more expensive than Ethernet network cards and nodes.
- Under normal traffic load, a ring is much slower than other topologies.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

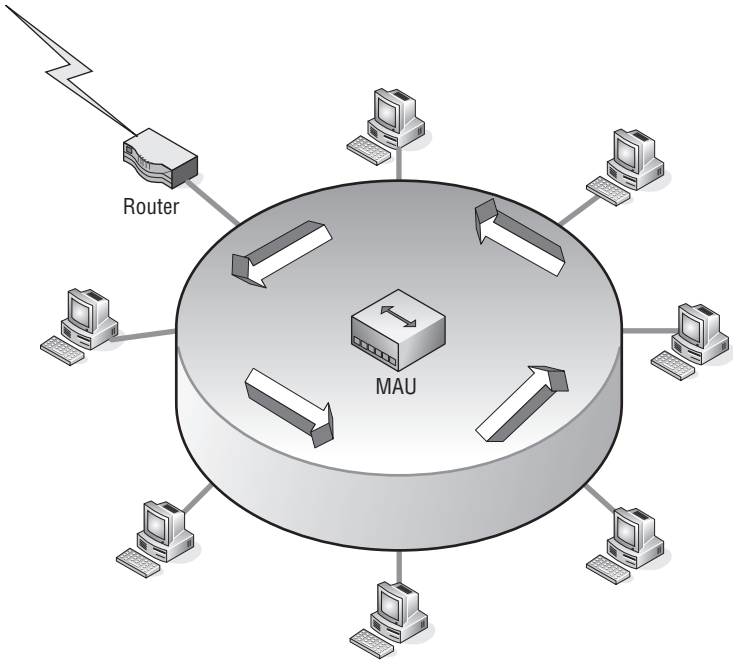


Figure 12-8 The ring topology

Another determination is which nodes to deploy and where to deploy them. The following section discusses some things to consider.

12.5.2 Determining Which Nodes to Use

Traditionally, packet-switched LANs have comprised four main network nodes: concentrators, repeaters, bridges, and routers. For the most part, these traditional nodes are still used and make up various levels of the network. Repeaters and bridges are used heavily in user workgroups, server farms, and in the access layer of hierarchical networks.

ACRONYM ALERT

CST — Common spanning tree

The list of nodes has really grown in the past 20 years. The traditional nodes are still in use, but so many other nodes have been introduced in that time. In addition to the traditional nodes, many networks use Layer 3 switches, Layer 4–7 switches, VPN remote access solutions, etc.

Chapter 3 discussed each of these node types extensively, but here is a quick overview, along with some examples of node deployment.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.5.2.1 Traditional Nodes

The first types of nodes we want to cover are what we will call the *traditional nodes*. These node types are the most often deployed and are found in many home networks. In traditional node networks, each node serves a distinct and specific function. Repeaters and hubs pass data without using any logic at all. Bridges (also known as Layer 2 switches) connect like networks to one another and are able to make correct forwarding decisions. Routers are able to connect different network types to one another and can also make correct forwarding decisions.

Get it? Got it! Good!

12.5.2.1.1 Repeaters

The repeater is a node that simply passes information on. It is used to extend the segment when medium-distance limitations have been reached. Figure 12-9 shows an example of a repeater separating two parts of a network.

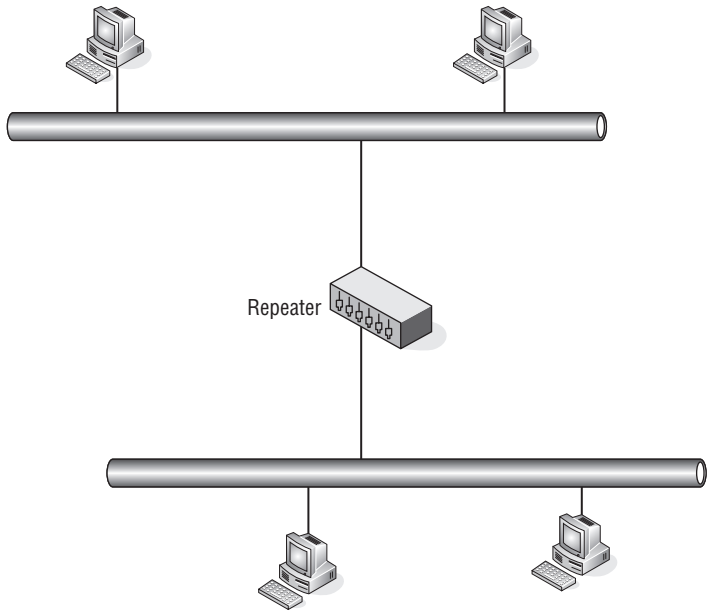
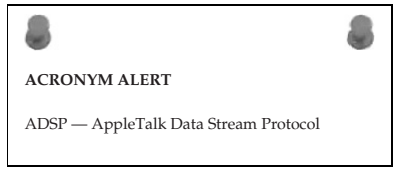


Figure 12-9 A repeater

A repeater amplifies a signal, but that is not its only task. A repeater also filters out any distorted data it has received, and it will not pass that data along. Technically, you can say that the function of the repeater is to amplify good data.



Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.5.2.1.2 Concentrators

The concentrator used within a LAN is either a hub or an MAU that allows the combination of data transmissions for a group of nodes. Figure 12-10 shows an example of a hub deployed in a LAN.

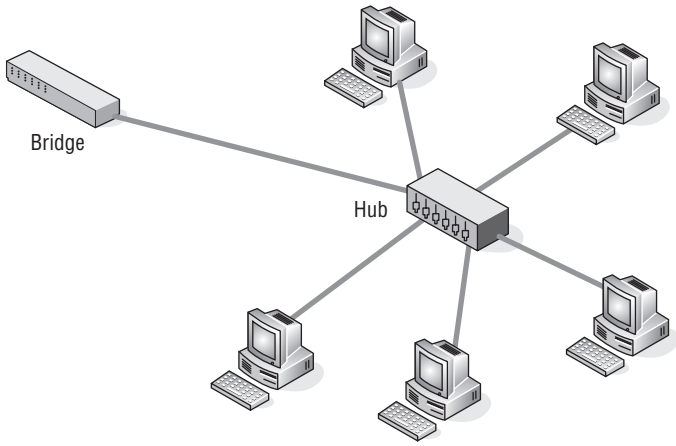


Figure 12-10 A hub

A hub is used to connect segments in a LAN. Hubs have multiple ports, and when data is received on a port, the hub will send the datagram to all of the other ports, so all segments will see all datagrams that are passed through the hub.

An MAU is a type of concentrator that is used to connect nodes within a Token Ring environment. The MAU connects the nodes in a physical star configuration, but the logical operations are Token Ring. The MAU allows the Token Ring to continue operating when a node on the ring breaks. This is much better than the alternative, where a node breaks on a physical ring and the whole ring goes down.

12.5.2.1.3 Bridges

The bridge is a LAN node that operates at Layer 2 of the OSI reference model. The bridge is used to connect different networks to one another. Data received from one network can be forwarded through the bridge to get the data to the correct destination. Figure 12-11 shows an example of bridge deployment.

Bridges are smart enough to know how to send datagrams to a specific port so that not all areas of the network have to receive the data as well. This frees up the other segments to pass data separately, without having to analyze all the datagrams. When a bridge gets the datagram, it passes the data based on the MAC address of the destination node.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

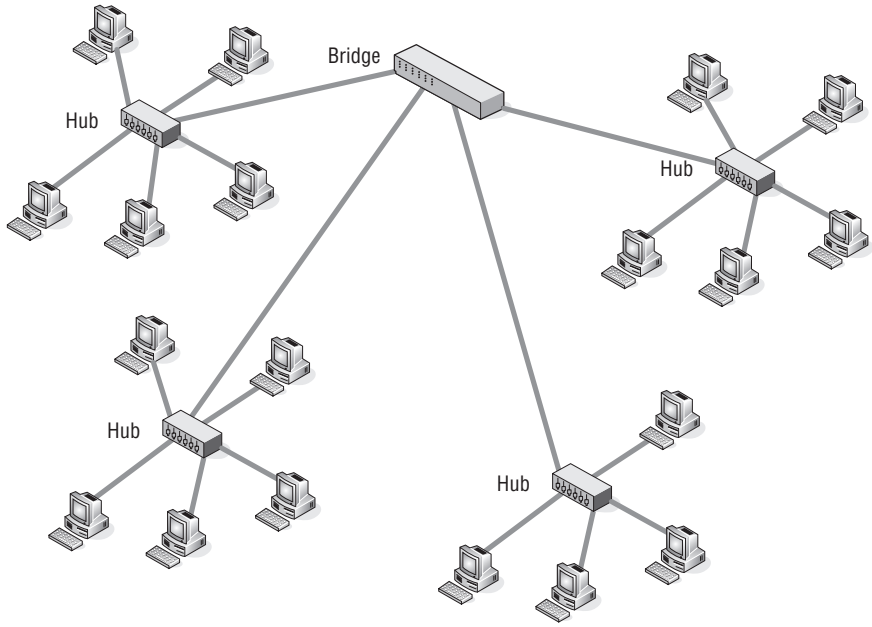


Figure 12-11 A bridge

12.5.2.1.4 Routers

The final node in the traditional node family is the router. Operating at Layer 3, the router is the backbone of most LANs. Routers use IP addresses to route datagrams in a network. Routers support multiple protocols of different types and are able to separate networks of different types because of this. Figure 12-12 is an example of the placement of a router in a LAN.

RANDOM BONUS DEFINITION

coaxial cable — A communications medium used in 10BASE5 and 10BASE2 Ethernet systems.

Routers are still in use in LANs today, but Layer 3 switches are becoming increasingly more popular. The reason for this is simple. The advanced switches are able to function as a router at a much higher speed due to application-specific integrated circuit (ASIC) technology. Additionally, switching hardware is cheaper to replace than traditional router hardware.

Routers are still used as boundaries between the LAN and the Internet.[19] Figure 12-13 shows an example of this. Routers are also often used for remote connectivity for remote offices.

[19]Or other networks that are not controlled by the organization.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

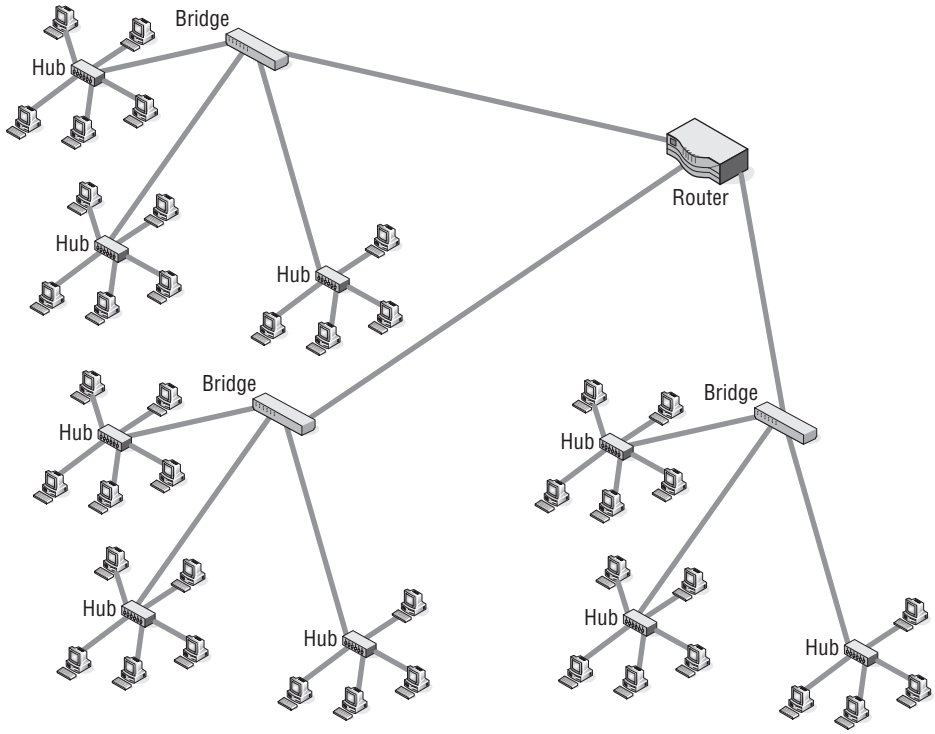


Figure 12-12 A router

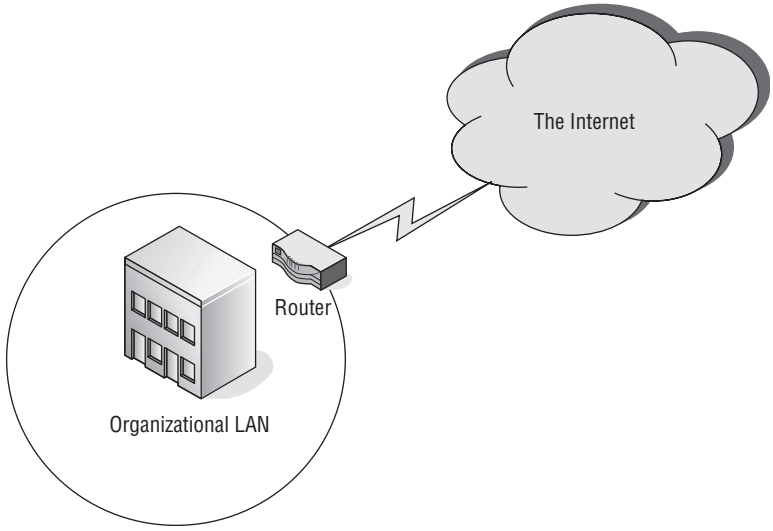


Figure 12-13 Routers connecting a LAN to the Internet

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Routers are used to route data between different networks. Routers control the flow of data in and out of the LAN, often working with a firewall solution to limit and/or control data coming into the LAN, as well as data going out from the LAN to the Internet.

12.5.2.2 Node Evolution

Main Entry: ev·o·lu·tion[20]
Function: noun.

1. A gradual process in which something changes into a different and usually more complex or better form.
2. The process of developing.
3. A movement that is part of a set of ordered movements.
4. Mathematics: The extraction of a root of a quantity.

Networking never stops growing. As a new product is being introduced, there is another product just around the corner that will replace it. Software upgrades and new program implementations also see the same changes and growth. No longer is a modem the standard for accessing the LAN. No longer do we have to rely on filtering and VLAN techniques to authorize and authenticate. There are a lot of nodes out there that do the trick, and a lot of nodes out there that just plain do it better than traditional nodes.

We already have discussed how the term *Layer 2 switch* replaced the term *bridge*, but it is really just a marketing term. As a matter of fact, it was so well received[21] that almost anything networking is a switch now. In this section, we talk about some other switches that are in a lot of LANs. In addition to the switches, we discuss a bit about VPN and wireless nodes.

RANDOM BONUS DEFINITION

congestion — The state where the offered network load approaches or exceeds the locally available resources designed to handle that load

12.5.2.2.1 Layer 3 Switches

Layer 3 switches perform the same task as routers and are deployed in high-speed LANs as well as in WANs. The Layer 3 switch is preferred over a router because routing decisions are hardware-based and thus are able to be performed much faster than traditional routers. Layer 3 switches are also able

[20]The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004.
[21]Well received by the customers or the salespeople. We are not really sure which, but we all know how those sales guys are.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

to perform as Layer 2 switches, giving the best of both worlds. They give you the control of data flow that is offered in a routed network and the speed that is offered in a switched environment. Figure 12-14 shows an example of Layer 3 switch deployment.

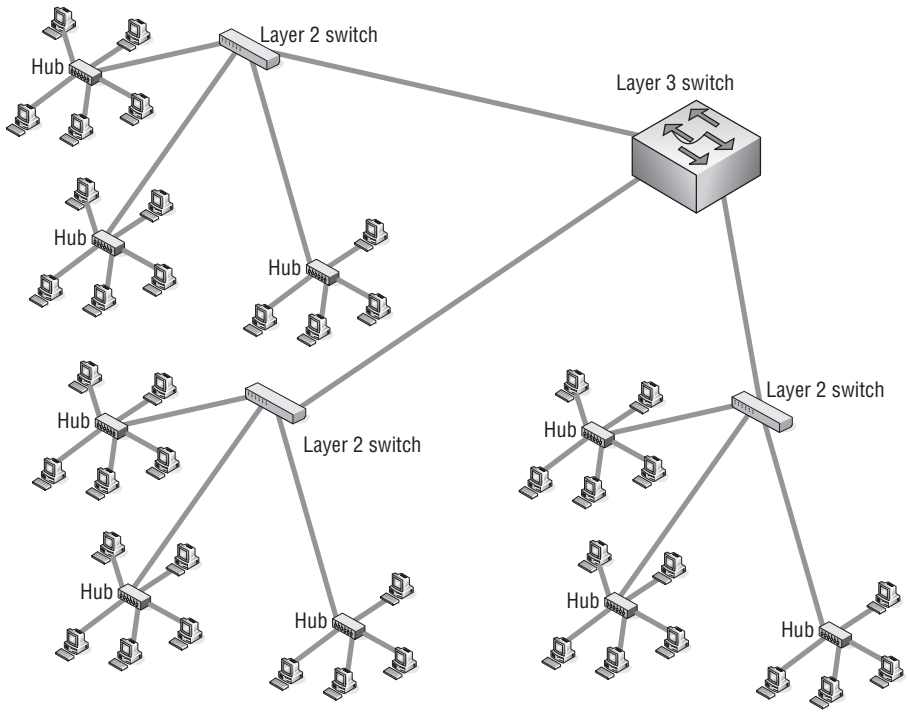


Figure 12-14 A Layer 3 switch deployment

Traditional routers do a great job, but the logic decisions they make are software-based and therefore are a slower process than what is offered by the Layer 3 switches. Layer 3 switches can support the same protocols that are supported by a traditional router and generally cost less than traditional switches.

So what is the hardware feature on the Layer 3 switch? It is the ASIC that makes the Layer 3 switch. A Layer 3 switch can have from one ASIC per chassis up to one ASIC per port.[22]

12.5.2.2.2 Layer 4–7 Switching

Layer 4–7 switching is not traditional Layer 2 switching. Many vendors now market nodes that are able to perform Layer 4–7 functions. It's important to note that even though a node may be labeled a Layer 4–7 switch, multiple

[22]This depends on how badly the vendor wants to make sure that you can get wire speed throughput through the device.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

vendors use the definition loosely, so it may not really be exactly the same between vendors. Some terms you might come across to describe Layer 4–7 switching include:

- Web switch
- Application switch
- Content switch
- VPN switch

Generally, Layer 4 switches are used to assist in balancing data destined for servers within a network. Layer 4 switches operate at the TCP/UDP level and will make decisions about where to send traffic based on information that is stored at the Transport layer. Not all Layer 4 switches actually do transfers based on that information. Web load balancers are often termed Layer 4 switches, as they are able to forward Layer 2 switches based on the MAC address, but are also able to send some MAC address data to multiple physical ports within the load-balancing switch. Some load balancers are able to monitor load on the server ports and can switch requests that are received to the data port that connects to the server with the lightest load.

As we have said, some of these nodes can function at up to Layer 7 of the OSI model. These are used to load-balance traffic among groups of servers. These servers can provide applications such as HTTP, HTTPS, and many others that use TCP/IP to transport traffic via a specified port.

Layer 4–7 switches use Network Address Translation (NAT), often at wire speed, to provide an avenue to allow multiple clients access to multiple host servers without having to know the exact physical server that is handling the request from the individual client. Some Layer 4–7 switches are also able to provide SSL encryption and decryption services so that the servers don't have to, as well as being able to manage digital certificates.

Layer 4–7 switches provide an excellent service — the almost instant, endless, and secure flow of data to end users. This is certainly an improvement for many users who are beginning to expect instant gratification when connecting to a website. The Layer 4–7 switch may not be for everyone, but it does come in handy when a network needs to have it.

12.5.2.2.3 Virtual Private Networks

VPN solutions have changed the way that organizations connect to remote sites. Traditionally, site-to-site connectivity was done over leased lines (such as ISDN, dial-up, etc.). As the Internet grew, and technology grew, so did the way that we connect to remote offices. VPN technology allows remote

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

connectivity over a secure tunnel to the organizational LAN, so it will appear as if the remote user or office is actually geographically located within the LAN. Figure 12-15 provides an example of three uses of the VPN solution.

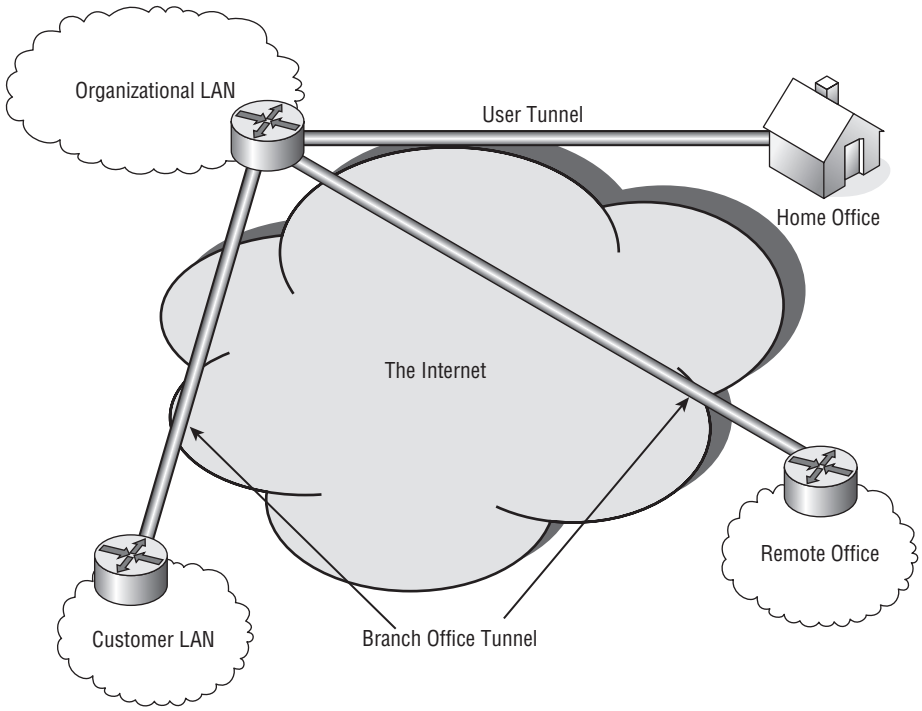


Figure 12-15 Typical VPN deployments

In the figure, you can see that there are three different tunnels going into the corporate LAN. One of these tunnels is a remote user connecting from home through a user tunnel.[23] The other two tunnels connect remote LANs and are known as branch office tunnels. One of the branch office tunnels goes to a remote office for workers in the VPN's organization.[24] The other branch office tunnel is used by customers to connect to the corporate network.[25]

12.5.2.2.4 Wireless Networks

The last topic we will talk about in this node evolution section is wireless networks. Wireless seems to be where networking is really growing. Almost everyone has at least one cell phone, but it does not stop there. You have Bluetooth, infrared, wireless PC connections, etc., almost everywhere you go. We can't tell you the last time we were out and about when there wasn't

[23]This type of VPN is also known as a remote access VPN.
[24]This type of VPN is also known as an intranet VPN.
[25]This type of VPN is also known as an extranet VPN.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

at least one person using some form of wireless device. Thanks to wireless networks, this is all possible.

IEEE 802.11 is the standard that outlines wireless LAN standards. Another standard, called *wireless IP*, allows mobile devices to remain connected, even when they move into an wireless area that has a different IP scheme than the user has. Basically, this standard allows roaming without losing connectivity.

RANDOM BONUS DEFINITION

dedicated bandwidth — A configuration in which the communications channel attached to a network interface is dedicated for use by a single station and does not have to be shared.

Security is a big concern in wireless networks, so encryption and authorization options need to be considered.

12.5.3 LAN Switching Technology

Layer 2 switches changed what we can do in a network. These LAN switches broke up the transitional shared network and converted it into a switched network. This greatly improved the performance of the LAN as a whole. Figure 12-16 shows an example of a small switched network consisting of the switch (of course) and six end users. If this were a shared network connected by a central hub, all the nodes would have to read all the data transmitted, and the end-user nodes would have to negotiate in order to transmit.

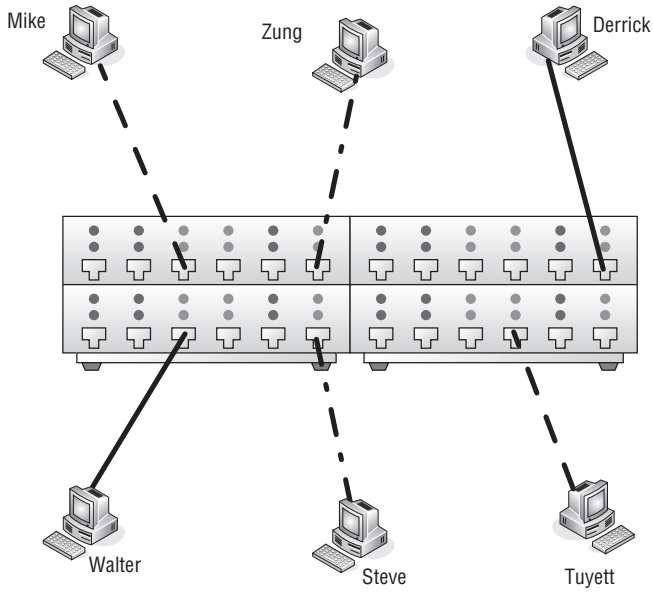


Figure 12-16 A switched network

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

As you can see, there are a total of six end users. Each user is exchanging data with one other node, but each node is communicating with only one node at a time. Notice that there are three simultaneous active connections (Mike to Tuyett, Zung to Steve, and Derrick to Walter) in the example. Try to do that in a shared network!

12.5.3.1 Switch Types

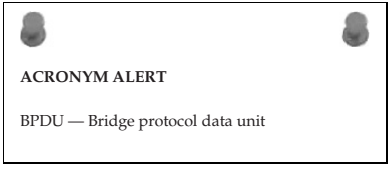
The way that a switch handles the data it receives depends on whether the switch is a *cut-through* type or a *store and forward* type.

- **Cut through** — In cut-through operations, the switch reads the header of the datagram as it is received on a port. Once the switch determines the port that reaches the destination, the datagram is sent to the port and on to its destination. There is no storing of data in a cut-through environment. There are also no options for error checking or control because the cut-through switch only reads the header for an address and sends the datagram on.
- **Store and forward** — In store and forward operations, the switch stores the data and does error checking on the datagram before it sends the datagram off toward its destination port. Although this makes the transfer of datagrams slower than with a cut-through switch, the data is delivered reliably.

12.5.3.2 By All Means, Be Redundant

A well-designed network will be built with plenty of redundancy throughout. The last thing a network administrator needs is a *single point of failure* anywhere in the network. A single point of failure is a location within the network that does not have a backup link of some sort. In other words, if the link fails, the network that is relying on that link will not be able to reach some or all of the LAN. Figure 12-17 shows an example of a single switch that is used to connect LAN 1 to LAN 2.

Consider what would happen in this example if the switch failed, or if one of the links between a LAN and the switch failed. If there were a failure, LAN-to-LAN communication would not happen. Depending on the problem, it could be several hours before service is restored, and in most businesses, there is a financial impact that could be detrimental.



Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

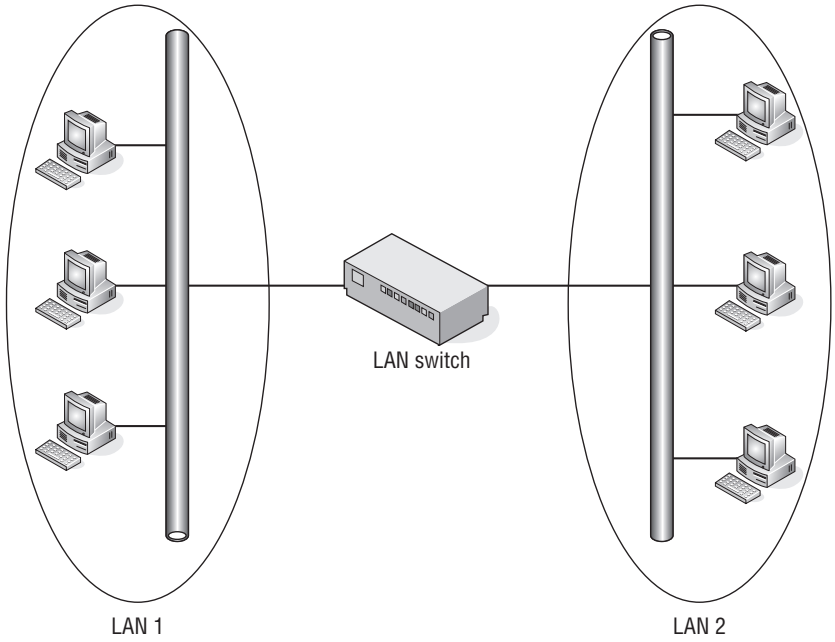


Figure 12-17 A switched network without redundancy

This is why you absolutely want to place redundancy throughout the network. Always have some sort of backup so there is a network convergence to a separate parallel link between endpoints (an example would be the LAN-to-LAN connection in the example we used above). Not only does this improve the reliability of data delivery, but a redundant network in a network diagram also really adds something to the overall picture. Figure 12-18 is an example of a network with redundancy.

So, the problem is resolved, right? Well, technically, yes, the problem of LAN-to-LAN communication being lost when a link goes down is now resolved. But like many solutions in the data world,[26] in resolving one issue, a new issue was introduced. The new issue is a loop, and we discuss it in the next section.

12.5.3.3 I'm Loopy!

We have established that there is a requirement for redundancy if we want our LAN to be reliable. However, in introducing that reliability by adding a second link, we have now created an environment where a loop may occur (see Figure 12-19). We'll now take a different look at the switched network.

[26] This includes both public solutions and proprietary solutions.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

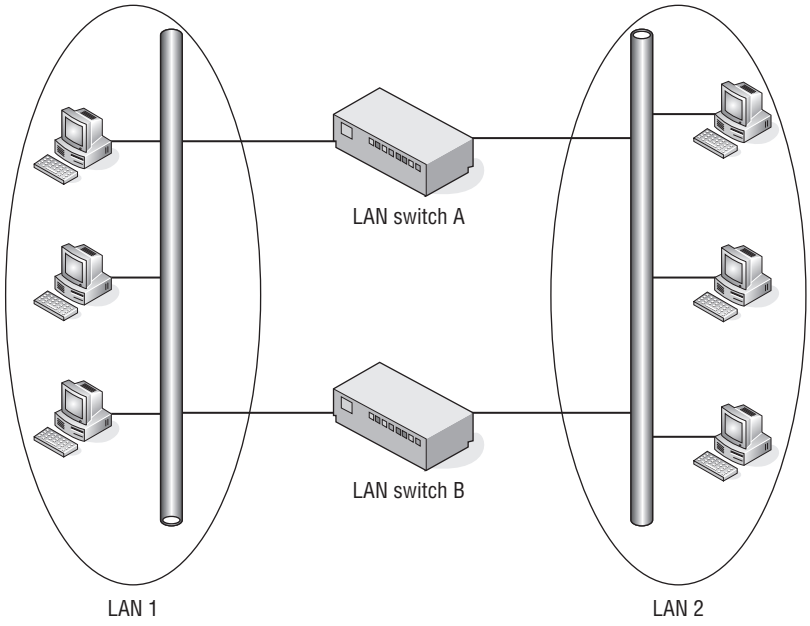


Figure 12-18 A switched network with redundancy

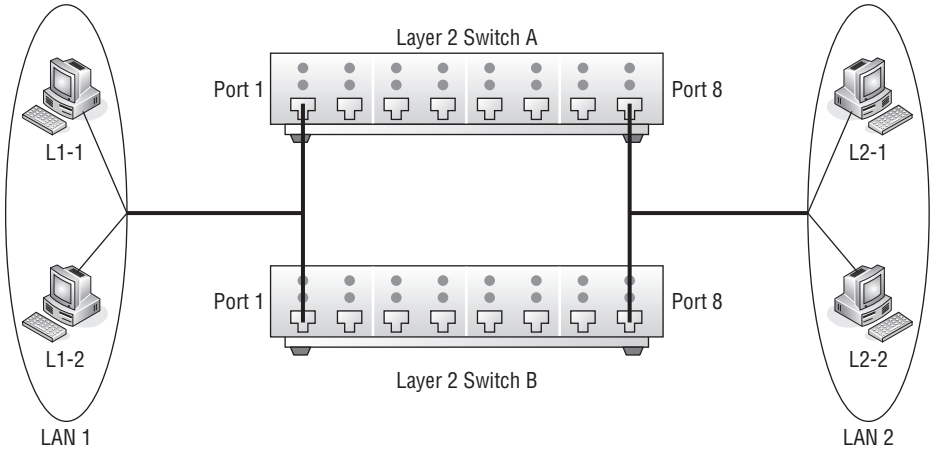


Figure 12-19 A switched network that is vulnerable to a Layer 2 loop

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Assume that both switches are aware of all the endpoints. If node L1-1 sends data to node L2-2, that data will be received on port 1 on both switches and will exit out of port 8 on both switches. The data will be sent to the appropriate node, but that node will get two copies of every datagram it receives. Duplication of effort is never desirable[27] and is a big no-no in a LAN.

So, if the redundant solution caused that kind of problem with the unicast traffic, what will happen with multicast traffic?[28] Believe it or not, this is a much bigger problem.

Let's assume that node L1-2 sends out a frame to a multicast address. The frame will be directed to port 1 on both switches. Once received, the frame will be forwarded to port 8 on both switches. This is where it gets fun. We learned that our LAN switch will receive all data received and will forward the multicasts to all other ports except the one it was received on. This means that both switches will receive the frame on port 8 and will forward it to port 1 on both switches. Port 1 will receive the frame, forward it to port 8, and so on. This multicast frame continues in that same loop indefinitely.

RANDOM BONUS DEFINITION

error detection — A procedure used to detect whether received information contains errors.

Pretty bad, isn't it? Now assume something is plugged into every interface on the switch we used in the example, and that every one of them has multiple loops going on. It does not take long for this condition to saturate the bandwidth and overwhelm the resources of the switches involved.

12.5.3.3.1 Darn that Redundancy Anyway

Now that we have determined that a loop is created when a redundant switch is added to the network, we can let you in on a little secret. Redundant switches are not the only thing that might cause a loop within your switched LAN. Here are a few other things that may be the root cause of a loop on the LAN:

- A configuration error within the LAN
- Introducing a duplicate route
- Introducing an additional node into the LAN

LANs can actually become quite complex (if they were not complex from the outset). The more complex a LAN becomes, the more it can create confusion,

[27] Remember, your job in designing the network is to ensure performance and reliability. Imagine the extra processing that will occur by not only all of the nodes in the domain, but also the upper-layer tasks that are used.

[28] See if you can answer this yourself before continuing on.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

especially if there is incomplete, inaccurate, or missing network documentation. Poor documentation and lack of preparation are leading causes of configuration errors that can lead to a loop in the LAN and can cause disruption in traffic flow, as well as bring portions of the network completely down.

Lack of experience and training is also a problem in many LANs. Sometimes a configuration mistake is made by someone who is not really sure what they are doing.[29] Incorrect provisioning can cause duplicate routes, and duplicate routes can cause loops.

12.5.3.3.2 Loop Resolution

The good news is that there are ways to resolve loops in the LAN and even to prevent them. You can prevent a loop by not making the LAN vulnerable to a loop. In other words, don't do anything that can cause a loop. Although this is the optimal choice, it really isn't practical in today's LANs.[30] The second option is to implement vendor-specific design solutions that manage and eliminate loops. The problem with this choice is that vendor-specific means vendor-specific.[31] The final option is to implement a protocol designed to control loops in LANs. The *Spanning Tree Protocol* (STP) is just that protocol!

12.5.3.3.3 Spanning Tree

The Spanning Tree Protocol (STP) is based[32] on a protocol that was developed by Digital Equipment Corporation (DEC). Many of DEC's bridges were equipped with their version of the protocol, eradicating loops in the DEC environment. As bridge technology grew, the IEEE eventually set up a task force to develop a public version of this protocol, and STP was born. STP is covered in IEEE 802.1D.

[29] When this happens, you can only hope the individual can either fix the issue quickly or be honest about what they did when you are trying to find the solution. Rich and Jim both have network support backgrounds and they can tell stories of troubleshooting issues that would have been resolved a lot faster had the mistake been pointed out early on.

[30] However, it is an open question for some networks where the reliability of data is not the biggest concern. For instance, a mom and pop shop might have a LAN, but really would not suffer if the LAN went down, so the price of redundancy is not worth it.

[31] Although many vendors have proprietary protocols that can interact with another vendor's proprietary protocol, that does not mean they are 100 percent functional in a mixed environment. By implementing a vendor-specific solution, you are effectively tying yourself to that vendor for a while (or will have to wait until the protocol becomes an open standard).

[32] "Based" is the operative word. While the protocols share many similarities, they are not fully interoperable. Therefore, if you are using DEC's version of the protocol, you cannot use the public version in the same network.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Spanning tree[33] uses an algorithm, known as the *spanning tree algorithm*, to make calculations that are used to prevent the dreaded loop. It does this by determining where there are multiple paths to a segment, and then making a calculation that will determine the best bridge to use. Once it determines the best bridge, it will elect that bridge as the *root* bridge. All other bridges in the group will be assigned the title of *designated* bridge when they are participating in forwarding data that the root is sending to a destination. In other words, the designated bridge is the one that is responsible for sending data over the best path. Any bridge that is not the root bridge can be a designated bridge.[34] At the designated-bridge level, there are different port types: the designated port, the root port, and the inactive port. The inactive port can be either a disabled port (a port that is not used) or a port that has been set into a *blocking* status.

Figure 12-20 shows an example of a network containing physical loops (segments A, C, E and segments B, E, D).

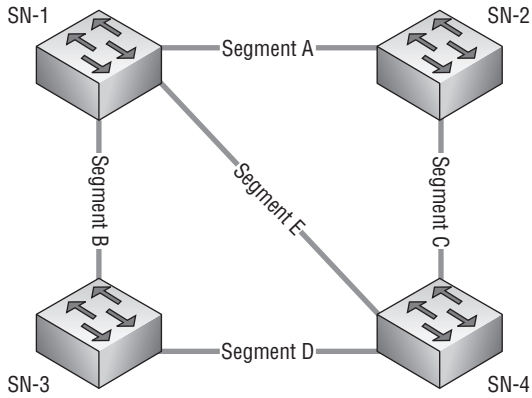


Figure 12-20 A physically looped network

Spanning tree will determine which bridge in the group will be elected to function as the root bridge. The root bridge is always the logical center of the network. The way the root bridge is elected is a process that relies on a data message known as a *bridge protocol data unit* (BPDU).

RANDOM BONUS DEFINITION

globally administered address — A node or interface identifier whose uniqueness is ensured through the use of an assigned organizationally unique identifier (OUI), typically by the manufacturer of the device or interface.

[33]A lot of times instead of calling the protocol STP, network professionals just say ''spanning tree.'' We like spanning tree; it flows better.

[34]We should note that as time goes on and changes happen on the network (adding nodes, removing nodes, etc.), each bridge has the potential of being elected as the root bridge at some point in time.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

The BPDUs are sent by all the bridges that want to participate[35] in the spanning tree. One of the fields in the BPDU contains the bridge identifier of the sending bridge. Once all BPDUs have been compared, the one with the lowest value will be elected the root bridge. Once the root bridge is selected, designated bridges are used to forward data. The main rule the designated bridge needs to follow is that only one bridge can forward data from the root bridge to the destination nodes. This rule ensures that no loops can occur because only one designated bridge is sending data from the root.

BPDUs are sent by spanning tree nodes to a well-known multicast address. This ensures that everyone in the group will receive the data. Spanning tree will decide which designated bridge it will use to forward a frame and will also decide which designated port to use to forward the data away from the root. Another field that is found in the BPDU is the root path cost. The root path cost is a configurable value that is used to set a priority on a preferred link. The port that is identified as having the lowest path cost will become the designated port and is the port that will be used to forward the frame to its destination. Once the spanning tree has determined the designated port, it will prevent traffic from flowing on other links to that destination by putting the ports on the other links into a *blocking* state.

12.5.3.3.4 Spanning Tree Port States

Every port on a bridge that is participating in spanning tree will have one of five possible *port states* assigned to it. A port state is exactly what it sounds like: it identifies the current state of the port. Each port state is important as it will identify the function the port is performing. These port states are as follows:

- **Disabled** — A port in a disabled state is simply that, disabled. There are many reasons why a port may be disabled. It may be a Physical layer problem, a communication problem, may not be used, etc.
- **Blocking** — A port in a blocking state is an active port that is not being used. Any port that is not a designated port or a root port is going to be in a blocking state. A block port listens for BPDUs to determine if it should become active, but does not participate in frame passing when it is in this state.
- **Listening** — A port in a listening state is not forwarding frames, but is listening to, and sometimes sending, BPDUs.
- **Learning** — A port in a learning state is learning paths to destinations and preparing to forward the frame. This state is used on a port that has not built an address table.[36] A learning port

[35]By participate, we mean that the node will use the BPDU to find out about other nodes as well as to receive information that will be used to calculate the spanning tree.
[36]Normally this is due to the port coming up.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

will wait a period of time before it starts forwarding frames.[37] This gives it an opportunity to gather path information.

- **Forwarding** — This is the port state for the active port that is forwarding frames.

12.5.3.4 Link Aggregation

```
Main Entry: ag·gre·ga·tion (ag-ri-gey-shun)
Function: noun.

1. Several things grouped together or considered as a whole.
2. The act of gathering something together.
```

As networks grow and the end application becomes more complex, there is a real need to increase the capacity of a given link. Link aggregation is a method of increasing the capacity of a channel by allowing multiple physical links to act together as a whole. The parallel links make the endpoint nodes think there is a better performing single channel. Figure 12-21 shows an example of two networks; one is using aggregation and one isn't.

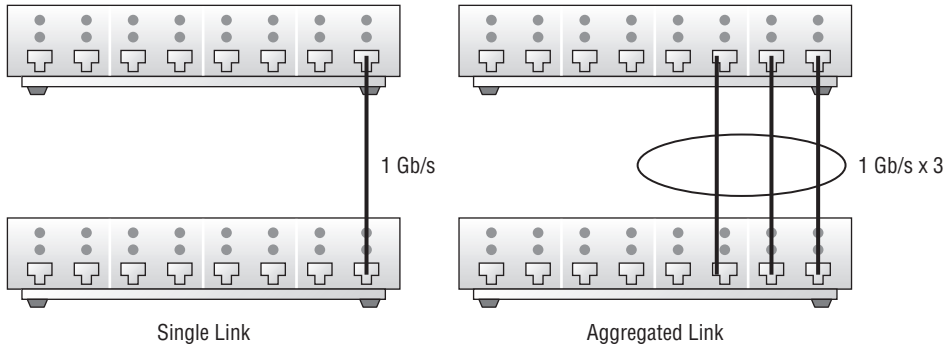


Figure 12-21 The benefits of link aggregation

The standard that covers link aggregation is IEEE 802.1ad, the Link Aggregation Control Protocol (LACP). Most high-speed LANs can support larger data rates, so it makes sense to use link aggregation. In smaller, lower-speed LANs, aggregation may not make sense due to the restrictions of the environment.[38]

The benefits of link aggregation include:

- Increased link capacity
- High link availability
- Often can be done with existing hardware

[37] This is known as "forwarding delay."

[38] Why would you want to aggregate to double your capacity if the network cannot support it?

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

A few disadvantages of link aggregation include:

- Requires additional interfaces on each end[39]
- Higher potential of configuration errors
- May require device driver updates to ensure compatibility with link aggregation

POP QUIZ

What is forwarding delay?

LACP was introduced in 1999 as a standardized way to aggregate multiple gigabit links in a high-speed LAN. As many LANs already supported some proprietary form of aggregation — for instance, Multi-Link Trunking (MLT) for Nortel and Inter-Switch Link (ISL) trunking for Cisco — for lower-speed networks, it was already well known that these were proprietary and did not work with other vendors' equipment. LACP resolved this for the gigabit world, and things have been growing ever since. Link aggregation has been supported from switch-to-switch, router/server-to-router/server, and switch-to-router/server since it came out, but now many NICs support LACP, allowing aggregation to the end-user level. Although it isn't used everywhere and a lot of LANs still use proprietary standards, we predict that it won't be long for this to be the standard of choice. Of course, at the time of this writing, there are a few proprietary solutions that are under standards review, so who knows what tomorrow will bring?

12.5.3.5 Virtual LANs

Early on in this book, we determined that a LAN is a data network that serves a small geographical area. Most of us think of a group of nodes connected to one another as forming a LAN (in other words, a broadcast domain). Larger organizations have an organizational LAN that is made up of several broadcast domains, the extent of the LAN being the area it covers or a distance-limiting factor. With the LAN, the limits remain for as long as the node exists in the LAN. What we mean by this is that within a LAN, the logical topology is limited to the physical topology as well. Figure 12-22 shows an example of this. You can only adjust those limits by having additional nodes to collect the broadcast domains that may be located within the same area. In addition, a router is required to ensure that broadcast domains are separated, reducing the effectiveness of the router.

[39]You may have to buy more equipment, either now or in the future. Not only may you have to purchase more gear now to support this, this also means that you could be consuming empty slots on existing nodes. Although this is great for now, you may have to buy more in the future.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

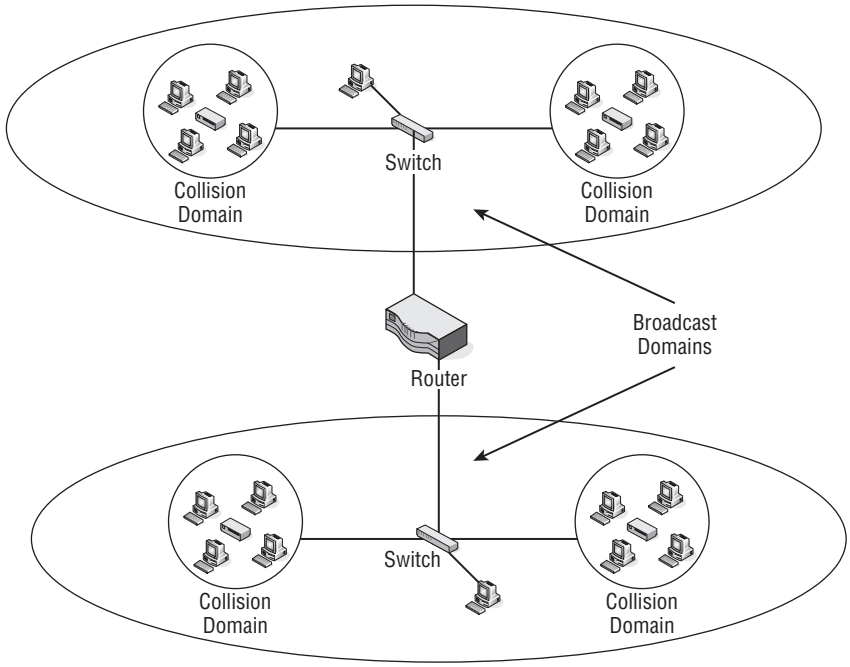


Figure 12-22 A traditional LAN

The virtual LAN (VLAN) was developed to give a LAN bridge the capability to separate these broadcast domains. This not only frees up the router to perform other important functions, but it also allows the network administrator to be flexible in domain configurations. Nodes no longer have to be in the same physical area to participate in a particular broadcast domain. Figure 12-23 shows an example of this. Notice that in each of the VLANs, there are members of each VLAN on each switch. This is a rough example, but the intention is to show that members of VLANs no longer have to be physically together to be in the same broadcast domain.

12.5.3.5.1 Benefits of VLANs

There are a lot of benefits to having VLANs configured in your LAN. Some of these include:

- Better performance. Only VLAN members receive multicasts.
- Members of a group no longer have to physically be located close to the group.
- Administration is easier. Changes to any work area can be done with simple configuration change.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

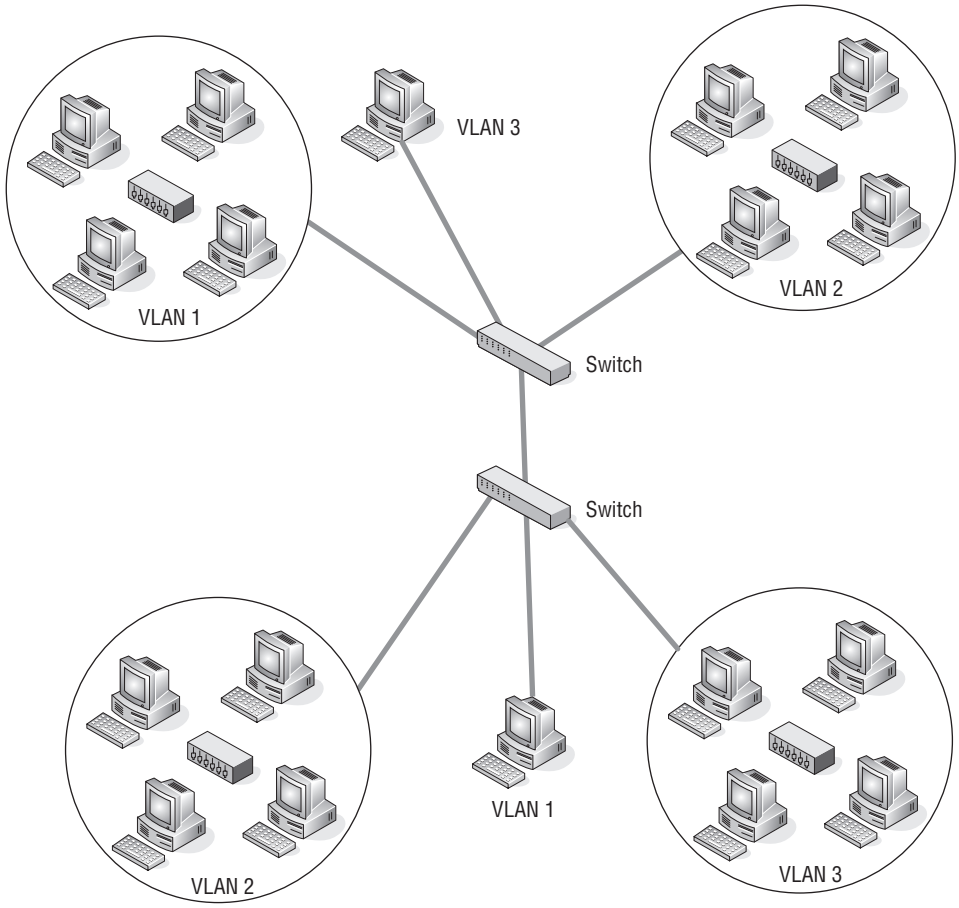


Figure 12-23 A VLAN

- Increased security. Only nodes within a VLAN have access to data.
- No need for a router in order to separate the broadcast domain.

RANDOM BONUS DEFINITION

individual port — A switch port that cannot form an aggregated link with any other port.

12.5.3.5.2 VLAN-Awareness

A node that participates in a VLAN, whether it is a user node or a LAN switch, is known as a *VLAN-aware node/switch*. This simply means that the node is aware of the VLAN rules and is participating in such an environment. VLAN-awareness is the capability to understand that there is an underlying function that allows the mapping of frames to the correct and appropriate

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

destination(s). VLAN-aware switches make forwarding decisions based on the destination address as well as the VLAN to which the frame belongs.

12.5.3.5.3 Tag! You're It!

To determine which VLAN a particular frame is a member of, the VLAN environment uses either implicit tagging or explicit tagging. When the switch receives a frame, it will ''tag''[40] the frame with the VLAN identifier where the data came from. This process is known as *explicit tagging* (commonly referred to as *VLAN tagging*, or simply *tagging*). The other type, *implicit tagging*, is a method of mapping an untagged frame to its associated VLAN by inspecting the contents of the frame.

Information that is contained within the explicit tag can be based on MAC address, port, and any other combination of information, but will always contain the VLAN identifier. VLAN tags can be set by a VLAN-aware node, or they can be assigned to a frame when received on a VLAN-aware switch. When a VLAN-aware switch receives an untagged frame, it applies the VLAN mapping rules and forwards the frame with the tagged bit set.

The implicitly tagged frame is a frame that has no tagging at all. Forwarding decisions are made based on the source address, protocol type, network identifiers, etc.[41]

AN UNRELATED MOMENT OF PAUSE — WHAT IS IN THE WORD "TAG"?

In the preceding section, we discussed an implicit tag and an explicit tag. But what other uses are there for the word "tag"? One of the first things that I thought of was the kids' game tag, as in "Tag! You're it!" It wasn't so much me wanting to relive my childhood, but with five kids under my belt, I have spent many weekends playing tag in the backyard.

The next thought when I think of the word "tag" is my two boys, who outgrew tag long ago. Both of them went through a phase where they were constantly squirting Tag body spray on themselves. I thank goodness that the stampede of women you see on the commercials never came charging at the house.

You can call a small label a tag, although I think that "label" is perfectly fine. Tagging a wall means adding your personal graffiti, which some consider art (I have seen some impressive tagging). Your car has a couple of tags on it: a VIN tag, tax tag, license tag, and so on and so forth. There are tags in computer programming, tags on the shelves in the grocery store — as a matter of fact, I don't know that we could get through life without tags. Seriously, try getting through life without seeing that gas is at $4.00 a gallon. Okay, that's a tag we could all do without.

[40] A tag is a field inserted into a frame that provides an explicit indication of the VLAN association for that frame.

[41] And any such combination that is predetermined.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.5.3.5.4 VLAN Types

Membership to a particular VLAN is based on the following criteria:

- **Port-based VLANs** — Port-based VLANs are determined by the ports that are members of a particular VLAN. This is a Layer 1 decision, as no Layer 2 or 3 data is used to make the membership determination.
- **MAC-based VLANs** — MAC-based VLANs are determined by the MAC address of the nodes that are members of the VLAN.
- **Protocol-based VLANs** — Protocol-based VLANs members are determined based on the protocol type in the header of the Layer 2 frame.
- **IP subnet–based VLANs** — IP subnet-based VLAN members are determined by the subnet address contained in the Layer 3 header. This does not mean that a Layer 3 VLAN can route. It cannot. This means there is a Layer 3 subnet address used for the VLAN membership rules.

POP QUIZ

What is implicit tagging?

12.5.4 Determining What Other Determinations Need to Be Determined

This section discusses a few things you should consider in designing a network. Some of the items are good practice talking points and the rest are provided as a vehicle for thought. Some of the determinations are based on decisions particular for your environment. Will you be using SNMP management? Is there a need for secure remote access? How much documentation is appropriate for your network? These are only a few questions that will be answered in this section.

If there is anything missing from this section that you feel is important, blame Rich![42]

12.5.4.1 Talking to a WAN

With any luck, your LAN won't require a connection to a WAN. Individual dialup sessions can be handled by the users on the network, if they require remote connectivity. This is ideal because the number of security issues that you could potentially have is reduced.[43] If this type of LAN works for you, go for it — it will be a gem to maintain in the long run.

[42]Just kidding! Jim can't help but give Rich a hard time.

[43]If you are not connected to a WAN, then a hacker has no way in, unless he is already in. The majority of security incidents in corporate LANs can be attributed more to physical (human) carelessness (some examples are losing laptops, leaving areas unsecure, not securing passwords, etc.) than to maliciousness.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

The reality is that most of us are going to be working within LANs that do require WAN connectivity, and because of this, there are decisions to be made as to what protocols you want for your LAN-to-WAN connectivity. Examples of options available include:

- Integrated Services Digital Network (ISDN)
- Leased lines
- Synchronous Optical Network (SONET)
- Frame relay
- Asynchronous Transfer Mode (ATM)
- Packet over SONET (POS)
- Point-to-Point Protocol (PPP)
- High-level Data Link Control (HDLC)
- X.25

The protocols and standards used can be determined by you and the service provider. The anticipated bandwidth requirements, type of traffic, costs, and many other items can be (and should be) considered in the decision making. Regardless of the main protocol you choose, it is always a good and effective idea to have a backup plan. For instance, you can use frame relay as a primary method of connecting and have ISDN as a backup. This way, if the frame relay service fails, you can continue to have connectivity.

POP QUIZ

What are the four types of VLANs?

Connectivity doesn't always stop when you meet the WAN. Often there is a reason for remote offices to connect to the LAN. We have discussed the VPN solution,[44] ISDN, and other services that are in use today. But there are times when you do not need continuous remote access. For instance, a retail store may connect one or two times a day to transmit inventory, sales figures, employee data, etc. In cases like this, a simple dialup connection or satellite link is often used. You and only you can determine what you need.

12.5.4.2 Management and Security

Don't kid yourself. Network security and network management are big business. We will be discussing these topics in later chapters of this book (network security in Chapter 14 and network management in Chapter 15). For the purposes of this chapter, it is important to know a little about both of these as you are determining what other determinations need to be determined.

[44]The next best thing to being there!

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.5.4.2.1 Network Security

There is a lot to be said about taking a strong, proactive approach to network security in today's networks. There is a real need to protect the network from not only individuals who are out for a challenge, but also to someone who wants to steal or harm data in the network. The malicious offender is probably a deeper concern, but either type of security breach can cause harm to the network and to the organization's operation and effectiveness.

Network security is important regardless of whether you are connected to a public network. Without security, your network is vulnerable to an outside (and sometimes even an inside) attack.

Security precautions need to be taken to protect the data that is being transmitted in the network. Here is a list of things to consider:

- Antivirus software is a must for every PC in the network. There are too many viruses and worms that can affect not only that end user's node, but also the entire network. These attacks can be introduced to the network through e-mail, web surfing, and even through a software application loaded from a disk to the end user's nodes.
- A firewall is important, as it will help prevent unauthorized access to the network. Some services that are offered by firewalls are spoofing, encryption and decryption, authentication, filtering, and proxy services. Not all firewalls will offer all of these, so you will need to determine what suits your needs.
- Maintain a strong network authentication procedure. Change passwords often, and control the individuals who can access them.
- Do not discount the importance of physical security. Only authorized individuals should have physical access to network equipment. End users need to understand the importance of not leaving their PCs open and available when they are not at their desks. Passwords need to be protected. Laptops and other mobile gear need to be secure, and users must understand the importance of keeping a good eye on the laptop and the data it contains.
- Utilize network management to keep track of operations within the LAN (more on this in the next section).

Again, we discuss network security further in Chapter 14.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

12.5.4.2.2 Network Management

Network management is the process of configuring, monitoring, and maintaining the operations of the entire network. There are two types of network management nodes within a network:

- **Network management agent** — An entity (typically a combination of software and hardware) within a node that is responsible for gathering network management information and reporting it to a network management station as appropriate.
- **Network management station** — A node that communicates with network management agents throughout a network. Typically it comprises a workstation operated by a network administrator, equipped with network management and other relevant applications software.

Security of the network is actually a network management function, but it is such a deep subject that it is often separated from other network management functions. Network management also includes maintaining the reliability of the network as well as keeping track of network overall performance.

We discuss network management in Chapter 15.

12.5.4.3 Choosing Protocols

POP QUIZ

What is a network management station?

You have determined what the network will look like and you have also determined the nodes you plan to ''roll out.'' Some of the protocols you will be using in your LAN are determined by the types of nodes you have decided on.[45] Some of the major protocols (for instance, RIP vs. OSPF) will be easy to select, just based on the design and the needs of the network. On the other hand, some of the protocols that you will want to implement may be proprietary and not interact well with other protocols. Investigate, test, and then make the determination on what you will implement.

In some cases, the de facto standard may not be the optimum choice, and you may want to implement a protocol based on its current availability. In other words, how widely is it deployed? As we discussed early in this chapter, another rule of thumb is to model your design after another network. Often, you will be able to implement the same protocols.

Complex protocols may have a lot of bells and whistles, but may also be well out of scope for your network. There is a principle in professional communities

[45]You would not implement TCP/IP on a Macintosh network.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

known as KISS — Keep It Simple, Stupid.[46] Pick your protocols based on need, but follow the KISS principle at all times.

12.5.4.4 Proactive Thinking

Throughout the design process, it is important to remain as proactive as possible. Not only do you want to try to figure out traffic patterns and future needs in your design decisions, it is also good to keep in mind that no matter how the network is designed, there will be at least one person at some point who will have a real need to understand the network and whether the performance expectations are being met. Here are a few tips:

- Use the KISS principle as often as possible in everything that you plan for the network. Design the network to be easy to configure, easy to maintain, easy to troubleshoot, easy to replicate, etc.
- Always develop an action plan. Have a logical sequence of steps that you take during the design process and on through implementation (see next chapter). Always have a back-out plan, too. Make sure to leave yourself a way to get things back to where they were working before you tried that last thing.
- Always document everything. Keep a record of IP addressing, node name, protocols running on each slot/port in the LAN, and anything else that you come across that might be important. In some cases, when you can't document, make sure you share. Do not keep node administrative passwords to yourself. Share them with at least one person. The more the network is on paper,[47] the better.
- Following very close to the documentation category, the network diagram is a useful tool to have and keep current. When troubleshooting is necessary, it can save a lot of time if you can point out something that is documented, rather than doing it on the fly.

12.6 Network Implementation

Okay, folks, you have the design of the network determined, you have purchased the equipment, and you have had a test running for several weeks now. Vendors are flying in tomorrow, because it's implementation day! Network implementation is the next stop on the way to the end of this book. We don't know about you, but we can taste that beer already.[48]

[46] Although Keep It Simple, Silly, is a bit nicer.
[47] Actually, this will probably be digital, but you get the drift.
[48] That is the beer that we will be drinking when we type the last letter of the book. If you choose to have a beer when you read that last letter, Rich and Jim are hoping that it will be in celebration of a book you enjoyed and not a beer drunk in sadness for the time you wasted. If your opinion is the latter, we hope that those yummy recipes will save us.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

In lucky Chapter 13, we will take all the information that you learned in this chapter and put it to use in several different scenarios.

POP QUIZ

What is the KISS principle?

12.7 Chapter Exercises

1. What are the three layers of the hierarchical design model?
2. In this chapter, we listed six benefits of the hierarchical model. List these.
3. This question is actually broken down into questions about the 5-4-3 rule. Refer to Figure 12-24 for these questions.
   (a) Does this network comply with the 5-4-3 rule?
   (b) Identify what A and B represent in the diagram.

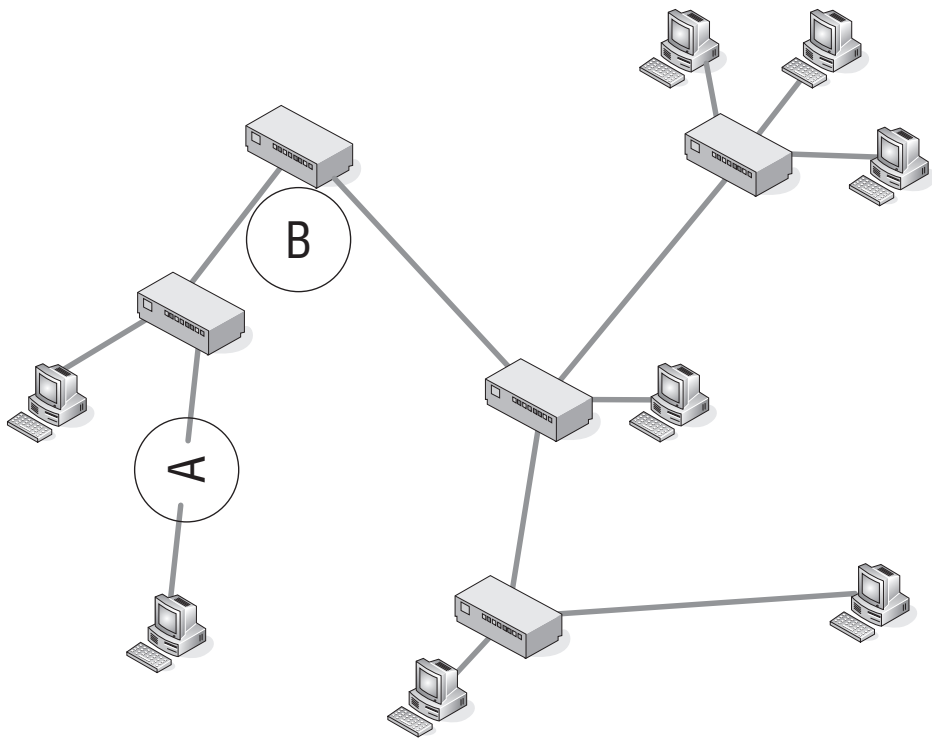


Figure 12-24 An example of the 5-4-3 rule

4. How many possible spanning tree states are there and what are they?

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

5. In this chapter, we discussed that a spanning tree port can be in a learning state. Why do you think that this is required instead of the port becoming active and just forwarding the frame?
6. A port in a _____ state is one that is _____ paths to destinations and is preparing to forward the frame.
7. What is the purpose of the distribution layer of the hierarchical network?
8. True or false: When the switch receives a frame, it will ''tag'' the frame with the VLAN identifier from where the data came from. This process is known as implicit tagging.
9. What are the VLAN types we discussed in this chapter?
10. Take a look at Figure 12-25 and then identify the appropriate layer of the hierarchical design model.

    The letter A in the example represents the _____ layer.

    The letter B in the example represents the _____ layer.

    The letter C in the example represents the _____ layer.

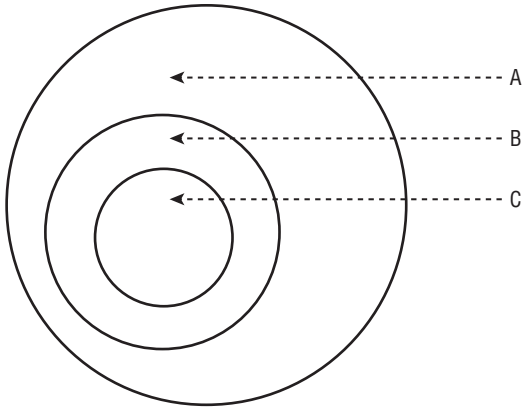


Figure 12-25 The hierarchical model

12.8 Pop Quiz Answers

1. Name five businesses or organizations that are not listed above. What do you think the biggest concern would be pertaining to each organizational LAN type?

   This answer is intended to provoke thought, so there are no right or wrong answers.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

2. Define scope.
   - The range of one's perceptions, thoughts, or actions
   - Breadth or opportunity to function
   - The area covered by a given activity or subject
3. Name three WAN technologies that are used to connect to remote sites.

   In the chapter, we mentioned frame relay, leased lines, and ISDN. Any protocol or implementation standards used to connect to the remote site are good answers as well.
4. What are the layers of the hierarchical design model?
   - Distribution layer
   - Core layer
   - Access layer
5. What is the purpose of a network's access layer?

   This is the layer that interfaces with the endpoint nodes. Types of nodes that are found at this layer are wireless access points, hubs, repeaters, bridges, Layer 3 switches, and routers. The access layer is what allows end users to connect to the network. This layer is also responsible for determining when nodes are not allowed access to certain portions of the network.
6. What is implicit tagging?

   Implicit tagging is a method of mapping an untagged frame to its associated VLAN through the inspection of data contained in the frame.
7. What are the four types of VLANs?
   - Port-based VLANs
   - Protocol-based VLANs
   - MAC-based VLANs
   - IP subnet–based VLANs
8. What is a network management station?

   A network management station is a node that communicates with network management agents throughout a network. Typically it comprises a workstation operated by a network administrator, equipped with network management and other relevant applications software.
9. What is the KISS principle?

   Keep It Simple, Stupid

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.

Copyright © 2009. John Wiley & Sons, Incorporated. All rights reserved.

Edwards, James, and Richard Bramante. Networking Self-Teaching Guide : OSI, TCP/IP, LAN's, MAN's, WAN's, Implementation, Management, and Maintenance, John Wiley & Sons, Incorporated, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/shsbt-ebooks/detail.action?docID=433738.
Created from shsbt-ebooks on 2017-10-09 13:01:37.