VOLUME 1

CCNA CERTIFICATION

Understanding Cisco™ Networking Technologies

Read BEFORE the CCNA Certification Study Guide, Volume 2

EXAM 200-301

Covers the core elements of the CCNA certification:

- Understand the fundamental principles of computer networking
- Learn about network components, services, and infrastructure
- Prepare for the next steps toward Cisco certification

TODD LAMMLE

SYBEX
A Wiley Brand

Volume 1

Understanding

Cisco® Networking Technologies

Exam 200-301

Volume 1

Understanding

Cisco® Networking Technologies

Exam 200-301

Todd Lammle

SYBEX
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-65902-0
ISBN: 978-1-119-65906-8 (ebk.)
ISBN: 978-1-119-65903-7 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2019953035

10 9 8 7 6 5 4 3 2 1

Acknowledgments

There were many people that helped me build these new CCNA books. First, Kenyon Brown helped me put together the direction for the books and managed the internal editing at Wiley, so thank you, Ken, for working diligently for many months keeping these books moving along. The editors that I personally used in this first book in the CCNA series were Troy McMillan, who read each chapter in the full series multiple times, making amazing discoveries both technically and editorially and Todd Montgomery who also read through every chapter and helped with the technical edits with a sharp detailed eye. Also, Monica Lammle read and re-read each chapter and really helped me keep the voicing in place throughout the editorial process, which isn't an easy thing to do! Thanks also to Christine O'Connor, my production editor at Wiley for well over a decade now, and Louise Watson, proofreader at Word One.

About the Author

Todd Lammle is the authority on Cisco certification and internetworking and is Cisco certified in most Cisco certification categories. He is a world-renowned author, speaker, trainer, and consultant. Todd has three decades of experience working with LANs, WANs, and large enterprise licensed and unlicensed wireless networks, and lately he's been implementing large Cisco Security networks using Firepower/FTD and ISE.

His years of real-world experience are evident in his writing; he is not just an author but an experienced networking engineer with very practical experience from working on the largest networks in the world at such companies as Xerox, Hughes Aircraft, Texaco, AAA, Cisco, and Toshiba, among many others.

Todd has published over 90 books, including the very popular *CCNA: Cisco Certified Network Associate Study Guide*, *CCNA Wireless Study Guide*, *CCNA Data Center Study Guide*, *SSFIPS (Firepower)*, and *CCNP Security*, all from Sybex. He runs an international consulting and training company based in Colorado, where he spends his free time in the mountains playing with his golden retrievers.

You can reach Todd through his website at `www.lammle.com`.

Contents at a Glance

Contents

Introduction

Welcome to the exciting world of internetworking and your path towards Cisco certification. If you've picked up this book because you want to improve yourself and your life with a better, more satisfying, and secure job, you've chosen well!

Whether you're striving to enter the thriving, dynamic IT sector or seeking to enhance your skill set and advance your position within it, being Cisco certified can seriously stack the odds in your favor to help you attain your goals. This book is a great start.

Cisco certifications are powerful instruments of success that also markedly improve your grasp of all things internetworking. As you progress through this book, you'll gain a strong, foundational understanding of networking that reaches far beyond Cisco devices. And when you finish this book, you'll be ready to tackle the next step toward Cisco certification.

Essentially, by beginning your journey towards becoming Cisco certified, you're proudly announcing that you want to become an unrivaled networking expert, a goal that this book will help get you underway to achieving. Congratulations in advance for taking the first step towards your brilliant future!

NOTE

To find your included bonus material, as well as Todd Lammle videos, practice questions and hands-on labs, please see `www.lammle.com/ccna`.

Cisco's Network Certifications

It used to be that to secure the holy grail of Cisco certifications—the CCIE—you passed only one written test before being faced with a grueling, formidable hands-on lab. This intensely daunting, all-or-nothing approach made it nearly impossible to succeed and predictably didn't work out too well for most people.

Cisco responded to this issue by creating a series of new certifications, which not only created a sensible, stepping-stone-path to the highly coveted CCIE prize, it gave employers a way to accurately rate and measure the skill levels of prospective and current employees. This exciting paradigm shift in Cisco's certification path truly opened doors that few were allowed through before!

Way back in 1998, obtaining the Cisco Certified Network Associate (CCNA) certification was the first pitch in the Cisco certification climb. It was also the official prerequisite to each of the more advanced levels. But that changed in 2007, when Cisco announced the Cisco Certified Entry Network Technician (CCENT) certification. Then again, in May 2016, Cisco proclaimed new updates to the CCENT and CCNA Routing and Switching (R/S) tests. Today, things have changed dramatically again.

In July of 2019, Cisco switched up the certification process more than they have in the preceding 20 years! They've announced all new certifications that began in February 2020, and probably the reason you are reading this book!

For starters, the CCENT course and exam (or ICND1 and ICND2) are no more, plus there are no prerequisites for any of the certifications at all now, meaning for example, that you can go straight to CCNP without having to take the new CCNA exams.

The new Cisco certification process will look like Figure I.1.

FIGURE I.1 The Cisco certification path

Entry Starting point for individuals interested in starting a career as a networking professional.	Associate Master the essentials needed to launch a rewarding career and expand your job possibilities with the latest technologies.	Professional Select a core technology track and a focused concentration exam to customize your professional-level certification.	Expert This certification is accepted worldwide as the most prestigious certification in the technology industry.	Architect The highest level of accreditation achievable and recognizes the architectural expertise of network designers.
CCT	DevNet Associate	DevNet Professional	CCDE	CCAr
	CCNA	CCNP Enterprise	CCIE Enterprise Infrastructure CCIE Enterprise Wireless	
		CCNP Collaboration	CCIE Collaboration	
		CCNP Data Center	CCIE Data Center	
		CCNP Security	CCIE Security	
		CCNP Service Provider	CCIE Service Provider	

First, the listed entry certification of CCT is just not worth your time. Instead, you'll want to head directly to CCNA after this foundational book, and then straight to the CCNP of your choice.

This book is a powerful tool to get you started in your CCNA studies, and it's vital to understand that material in it before you go on to conquer any other certifications!

What Does This Book Cover?

This book covers everything you need to know to solidly prepare you for getting into your CCNA studies. Be advised that just because much of the material in this book won't be official Cisco CCNA objectives in the future doesn't mean you won't be tested on it. Understanding the foundational, real-world networking information, and skills offered in this book is critical to your certifications and your career!

So as you move through this book, here's a snapshot of what you'll learn chapter by chapter:

Chapter 1: Internetworking In Chapter 1, you'll learn the basics of the Open Systems Interconnection (OSI) model the way Cisco wants you to learn it.

Chapter 2: Ethernet Networking and Data Encapsulation This chapter will provide you with the Ethernet foundation you need in order to understand the CCNA and CCNP material. Data encapsulation is discussed in detail in this chapter as well.

Chapter 3: Introduction to TCP/IP Chapter 3 provides you with the background necessary for success on the CCNA/NP exams, as well as in the real world, with a thorough presentation of TCP/IP. It's an in-depth chapter that covers the very beginnings of the Internet Protocol stack and moves all the way to IP addressing. You'll gain an understanding of the difference between a network address and a broadcast address before finally ending with valuable network troubleshooting tips.

Chapter 4: Easy Subnetting Believe it or not, you'll actually be able to subnet a network in your head after reading this chapter! Success will take a little determination, but you'll find plenty of help in this chapter as well as at: `www.lammle.com/ccna`.

Chapter 5: Troubleshooting IP Addressing Here, we'll continue on from Chapters 3 & 4 and begin covering how to troubleshoot basic IP issues. You'll also test your understanding of the previous two chapters.

Chapter 6: Cisco's Internetworking Operating System (IOS) Chapter 6 introduces you to the Cisco Internetworking Operating System (IOS) and command-line interface (CLI). In it, you'll learn how to turn on a router and configure the basics of the IOS, including setting passwords, banners, and more.

Chapter 7: Managing a Cisco Internetwork This chapter provides you with the management skills needed to run a Cisco IOS network. Backing up and restoring the IOS and key router configuration skills are covered, as are the troubleshooting tools necessary to keep a network up and running well.

Chapter 8: Managing Cisco Devices This chapter describes the boot process of Cisco routers, the configuration register, and how to manage Cisco IOS files. It wraps up with a section on Cisco's new licensing strategy for IOS.

Chapter 9: IP Routing This is a super fun chapter because in it, we'll begin building a Cisco network and actually adding IP addresses and route data between routers. You also learn about static, default, and dynamic routing. The fundamentals covered in this chapter are probably the most important in the book because understanding the IP Routing process is what Cisco is all about! It's actually assumed that you solidly possess this knowledge when you get into the CCNA & CCNP studies.

Chapter 10: Wide Area Networks This is the last chapter in the book. It covers multiple protocols in depth, especially HDLC and PPP for serial connections. We'll also discuss many other technologies such as cellular, MPLS T1/E1, and cable. I'll guide you through strategic troubleshooting examples in the configuration sections—don't even think of skipping them!

Chapter 1

Internetworking

Welcome to the exciting world of internetworking! This chapter is essentially an internetworking review, focusing on how to connect networks together using Cisco routers and switches. As a heads up, I've written it with the assumption that you have at least some basic networking knowledge.

Let's start by defining exactly what an internetwork is: You create an internetwork when you connect two or more networks via a router and configure a logical network addressing scheme with a protocol such as IP or IPv6.

I'm also going to dissect the Open Systems Interconnection (OSI) model and describe each part of it to you in detail because you really need comprehensive knowledge of it. Understanding the OSI model is key to the solid foundation you'll need to build upon with the more advanced Cisco networking knowledge gained down the line.

The OSI model has seven hierarchical layers that were developed to enable different networks to communicate reliably between disparate systems. Since this book is centering upon all things CCNA, it's crucial for you to understand the OSI model as Cisco sees it, so that's how I'll be presenting the seven layers to you.

NOTE To find your included bonus material, as well as Todd Lammle videos, practice questions and hands-on labs, please see `www.lammle.com/ccna`.

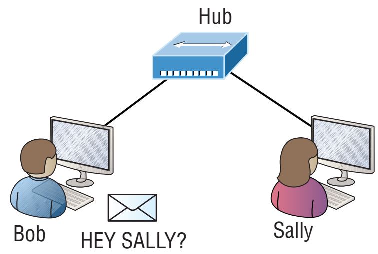
Internetworking Basics

Before exploring internetworking models and the OSI model's specifications, you need to grasp the big picture and the answer to this burning question: Why is it so important to learn Cisco internetworking anyway?

Networks and networking have grown exponentially over the past 20 years, and understandably so. They've had to evolve at light speed just to keep up with huge increases in basic, mission-critical user needs (e.g., the simple sharing of data and printers) as well as greater burdens like multimedia remote presentations, conferencing, and the like. Unless everyone who needs to share network resources is located in the same office space, which is increasingly rare, the challenge is to connect relevant networks so all users can share the wealth of whatever services and resources are required, on site or remotely.

Figure 1.1 shows a basic *local area network (LAN)* that's connected using a *hub*, which is basically just an antiquated device that connects wires together. Keep in mind that a simple network like this would be considered one collision domain and one broadcast domain. No worries if you have no idea what I mean by that because we'll go over that soon. I'm going to talk about collision and broadcast domains enough to make you dream about them!

FIGURE 1.1 A very basic network



Things really can't get much simpler than this. And yes, though you can still find this configuration in some home networks, even many of those as well as the smallest business networks are more complicated today. As we move through this book, I'll just keep building upon this tiny network a bit at a time until we arrive at some really nice, robust, and current network designs—the types that will help you get your certification and a job!

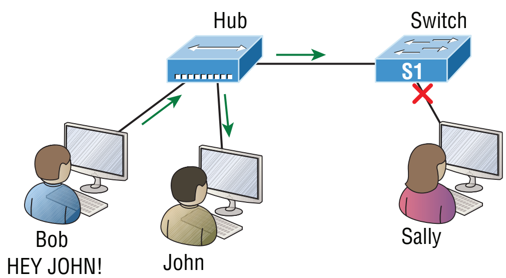
But as I said, we'll get there one step at a time, so let's get back to the network shown in Figure 1.1 with this scenario: Bob wants to send Sally a file, and to complete that goal in this kind of network, he'll simply broadcast that he's looking for her, which is basically just shouting out over the network. Think of it like this: Bob walks out of his house and yells down a street called Chaos Court in order to contact Sally. This might work if Bob and Sally were the only ones living there, but not so much if it's crammed with homes and all the others living there are always hollering up and down the street to their neighbors just like Bob. Nope, Chaos Court would absolutely live up to its name, with all those residents going off whenever they felt like it—and believe it or not, our networks actually still work this way to a degree! So, given a choice, would you stay in Chaos Court, or would you pull up stakes and move on over to a nice new modern community called Broadway Lanes, which offers plenty of amenities and room for your home plus future additions all on nice, wide streets that can easily handle all present and future traffic? If you chose the latter, good choice…so did Sally, and she now lives a much quieter life, getting letters (packets) from Bob instead of a headache!

The scenario I just described brings me to the basic point of what this book and the Cisco certification objectives are really all about. My goal of showing you how to create efficient networks and segment them correctly in order to minimize all the chaotic yelling and screaming going on in them is a universal theme throughout my Cisco series books. It's just inevitable that you'll have to break up a large network into a bunch of smaller ones at some point to match a network's equally inevitable growth, and as that expansion occurs, user response time simultaneously dwindles to a frustrating crawl. But if you master the vital technology and skills I have in store for you in this series, you'll be well equipped to rescue your network and its users by creating an efficient new network neighborhood to give them key amenities like the bandwidth they need to meet evolving demands.

And this is no joke; most of us think of growth as good and it can be. But as many experience daily when commuting to work, school, etc., it can also mean your LAN's traffic congestion can reach critical mass and grind to a halt! Again, the solution to this problem begins with breaking up a massive network into a number of smaller ones—something called *network segmentation*. This concept is a lot like planning a new community or modernizing an existing one. More streets are added, complete with new intersections and traffic signals, plus post offices are built with official maps documenting all those street names and directions on how to get to each. You'll need to effect new laws to keep order to it all and provide a police station to protect this nice new neighborhood as well. In a networking neighborhood environment, all of this infrastructure is managed using devices like *routers, switches*, and *bridges*.

So let's take a look at our new neighborhood now.... Because the word has gotten out, many more hosts have moved into it, so it's time to upgrade that new high-capacity infrastructure that we promised to handle the increase in population. Figure 1.2 shows a network that's been segmented with a switch, making each network segment that connects to the switch its own separate collision domain. Doing this results in a lot less yelling!

FIGURE 1.2 A switch can break up collision domains.



This is a great start, but I really want you to make note of the fact that this network is still one, single broadcast domain, meaning that we've really only decreased our screaming and yelling—not eliminated it. For example, if there's some sort of vital announcement that everyone in our neighborhood needs to hear about, it will definitely still get loud! You can see that the hub used in Figure 1.2 just extended the one collision domain from the switch port. The result is that John received the data from Bob but, happily, Sally did not, which is good because Bob intended to talk with John directly. If he had needed to send a broadcast instead, everyone, including Sally, would have received it, possibly causing unnecessary congestion.

Here's a list of some of the things that commonly cause LAN traffic congestion:

- Too many hosts in a collision or broadcast domain
- Broadcast storms
- Too much multicast traffic

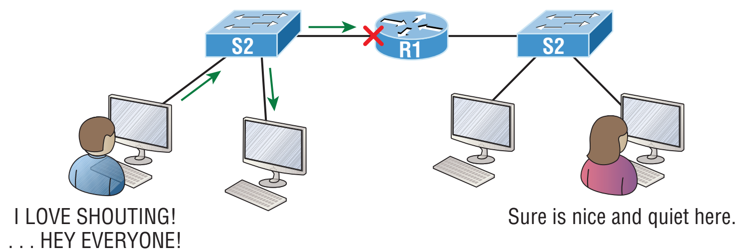
- Low bandwidth
- Adding hubs for connectivity to the network
- A bunch of ARP broadcasts

Take another look at Figure 1.2 and make sure you see that I extended the main hub from Figure 1.1 to a switch in Figure 1.2. I did that because hubs don't segment a network; they just connect network segments. Basically, it's an inexpensive way to connect a couple of PCs, and again, that's great for home use and troubleshooting, but that's about it!

As our planned community starts to grow, we'll need to add more streets along with traffic control and even some basic security. We'll achieve this by adding routers because these convenient devices are used to connect networks and route packets of data from one network to another. Cisco became the de facto standard for routers because of its unparalleled selection of high-quality router products and fantastic service. So never forget that by default, routers are basically employed to efficiently break up a *broadcast domain*—the set of all devices on a network segment, which are allowed to "hear" all broadcasts sent out on that specific segment.

Figure 1.3 depicts a router in our growing network, creating an internetwork and breaking up broadcast domains.

FIGURE 1.3 Routers create an internetwork.



The network in Figure 1.3 is actually a pretty cool little network. Each host is connected to its own collision domain because of the switch, and the router has created two broadcast domains. So now Sally is happily living in peace in a completely different neighborhood, no longer subjected to Bob's incessant shouting! If Bob wants to talk with Sally, he has to send a packet with a destination address using her IP address—he cannot broadcast for her!

But there's more… Routers provide connections to *wide area network (WAN)* services as well via a serial interface for WAN connections—specifically, a V.35 physical interface on a Cisco router.

Let me make sure you understand why breaking up a broadcast domain is so important. When a host or server sends a network broadcast, every device on the network must read and process that broadcast—unless you have a router. When the router's interface receives this broadcast, it can respond by basically saying, "no thanks," and discard the broadcast without forwarding it on to other networks. Even though routers are known for breaking up broadcast domains by default, it's important to remember that they break up collision domains as well.

There are two advantages to using routers in your network:

- They don't forward broadcasts by default.
- They can filter the network based on layer 3 (Network layer) information such as an IP address.

Here are four ways a router functions in your network:

- Packet switching
- Packet filtering
- Internetwork communication
- Path selection

I'll tell you all about the various layers later in this chapter, but for now, it's helpful to think of routers as layer 3 switches. Unlike plain-vanilla layer 2 switches, which forward or filter frames, routers (layer 3 switches) use logical addressing and provide an important capacity called *packet switching*. Routers can also provide packet filtering via access lists, and when routers connect two or more networks together and use logical addressing (IP or IPv6), you then have an *internetwork*. Finally, routers use a routing table, essentially a map of the internetwork, to make best path selections for getting data to its proper destination and properly forward packets to remote networks.

Conversely, we don't use layer 2 switches to create internetworks because they don't break up broadcast domains by default. Instead, they're employed to add functionality to a network LAN. The main purpose of these switches is to make a LAN work better—to optimize its performance—providing more bandwidth for the LAN's users. Also, these switches don't forward packets to other networks like routers do. Instead, they only "switch" frames from one port to another within the switched network. And don't worry, even though you're probably thinking, "Wait—what are frames and packets?" I promise to completely fill you in later in this chapter. For now, think of a packet as a package containing data.

Okay, so by default, switches break up collision domains, but what are these things? *Collision domain* is an Ethernet term used to describe a network scenario in which one device sends a packet out on a network segment and every other device on that same segment is forced to pay attention no matter what. This isn't very efficient because if a different device tries to transmit at the same time, a collision will occur, requiring both devices to retransmit, one at a time—not good! This happens a lot in a hub environment, where each host segment connects to a hub that represents only one collision domain and a single broadcast domain. By contrast, each and every port on a switch represents its own collision domain, allowing network traffic to flow much more smoothly.

NOTE

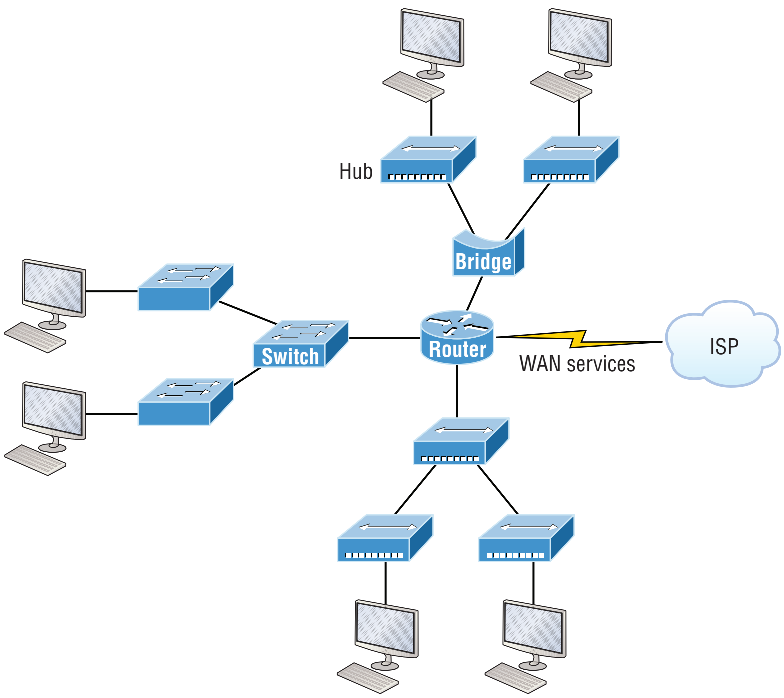
Switches create separate collision domains within a single broadcast domain. Routers provide a separate broadcast domain for each interface. Don't let this confuse you.

The term *bridging* was introduced before routers and switches were implemented, so it's pretty common to hear people referring to switches as bridges. That's because bridges and switches basically do the same thing—break up collision domains on a LAN. Of note is that you cannot buy a physical bridge these days, only LAN switches that use bridging technologies. This does not mean that you won't still hear Cisco and others refer to LAN switches as multiport bridges now and then.

But does this mean that a switch is really just a multiple-port bridge with more brainpower? Actually, pretty much, but there are still some key differences. Switches do provide a bridging function, but they do it with greatly enhanced management ability and features. Plus, most bridges had only two or four ports, which is severely limiting. Of course, it was possible to get your hands on a bridge with up to 16 ports, but that's nothing compared to the hundreds of ports available on some.

Figure 1.4 shows how a network would look with all these internetwork devices in place. Remember, a router doesn't just break up broadcast domains for every LAN interface, it breaks up collision domains too.

FIGURE 1.4 Internetworking devices



Looking at Figure 1.4, did you notice that the router has the center stage position and connects each physical network together? I'm stuck with using this layout because of the ancient bridges and hubs involved. I really hope you don't run across a network like this, but it's still really important to understand the strategic ideas that this figure represents.

See that bridge up at the top of our internetwork shown in Figure 1.4? It's there to connect the hubs to a router. The bridge breaks up collision domains, but all the hosts connected to both hubs are still crammed into the same broadcast domain. That bridge also created only three collision domains, one for each port, which means that each device connected to a hub is in the same collision domain as every other device connected to that same hub. This is really lame and to be avoided if possible, but it's still better than having one collision domain for all hosts! So don't do this at home…it's a great museum piece and a wonderful example of what not to do, but this inefficient design would be terrible for use in today's networks. It does show us how far we've come though, and again, the foundational concepts it illustrates are really important for you to get.

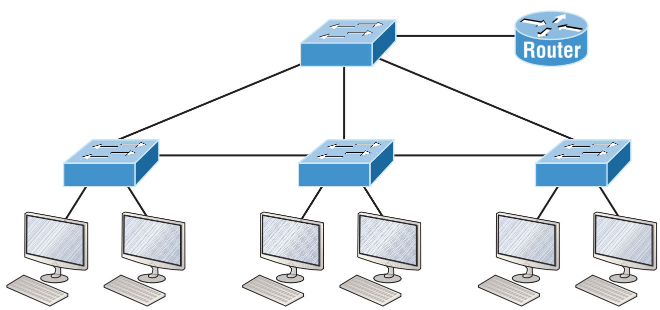
And I want you to notice something else: The three interconnected hubs at the bottom of the figure also connect to the router. This setup creates one collision domain and one broadcast domain and makes that bridged network, with its two collision domains, look much better by contrast!

Don't misunderstand… Bridges/switches are used to segment networks, but they will not isolate broadcast or multicast packets.

The best network connected to the router is the LAN switched network on the left. Why? Because each port on that switch effectively breaks up collision domains. But it's not all good—all devices are still in the same broadcast domain. Do you remember why this can be really bad? One, because all devices must listen to all broadcasts transmitted. Two, if your broadcast domains are too large, the users have less bandwidth and are required to process more broadcasts. Network response time eventually will slow to a level that may cause riots and strikes, so it's important to keep your broadcast domains small in the vast majority of networks today.

Once there are only switches in our example network, things really change a lot. Figure 1.5 demonstrates a network you'll typically stumble upon today.

FIGURE 1.5 Switched networks creating an internetwork



Here I've placed the LAN switches at the center of this network world, with the router connecting the logical networks. If I went ahead and implemented this design, I'll have