IT Fundamentals

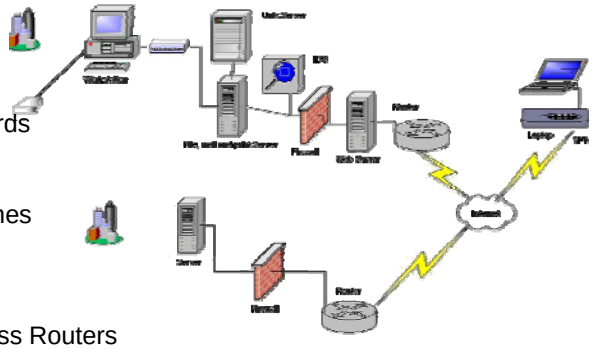
Chris Nowell

www.chrisnowell.com

For more IT and IT security presentations, information, and tools, please visit http://www.chrisnowell.com

Agenda

- Introduction
- History
- Network Interference
- Network Media
- Network Interface Cards
- Workstations
- Servers
- Repeaters and Switches
- Routers
- Firewalls
- Network Diagrams
- Introduction to Wireless Routers
- Tour



www.chrisnowell.com

Today, we're going to see

click

where the networking and the IT fundamentals we're going to cover support business processes *click*

Then we'll take an exciting tour through the life of the Internet and Modern Networks *click*

We'll talk a bit about Network interference, which will set us up for the hands on part of our session *click*

Starting with network media *click*

NICs *click*

A brief overview of Workstations *click*

And Servers *click*

Then we'll get into the nity gritty of repeaters and switches *click*

We'll talk a little about routers *click*

firewalls *click*

And network diagrams like the one you see here

We'll then talk about the part you all want to know about *click*

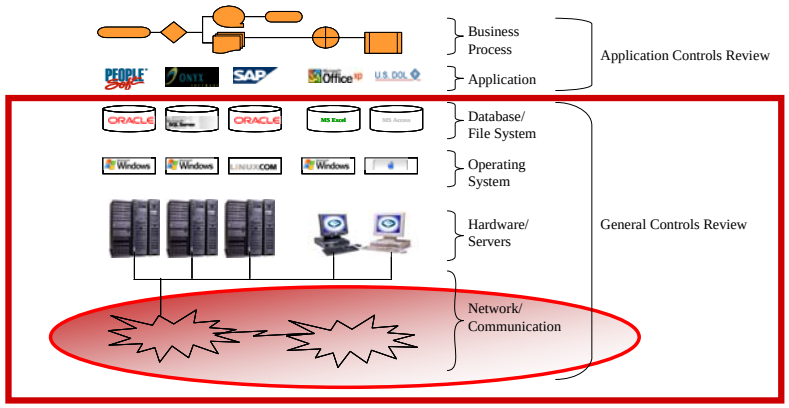
Wireless Routers *click*

And we'll end with a Tour.

This simplified network diagram may seem a little imposing right now, but I will do my best to make you feel at ease with it by the end of this session.

Introduction

- IT Layers



www.chrisnowell.com

Several IT layers support typical business processes

click

Our goal today is to try to gain an understanding of the first level

click

and introduce concepts related to the following levels..

The network is a nuts and bolts area where we could go into great detail. But I will try to not give so much detail that I loose anyone. If what I am saying is not making sense please stop me and let me know.

History of Modern Networks

- Sputnik scared the Americans into creating the **A**dvanced **R**esearch **P**rojects **A**gency
- ARPANET linked Universities and Military
- 1983: TCP/IP
- Growth
- Security

www.chrisnowell.com

It's probably best to start talking about networks with a brief history lesson. Can anyone tell me what triggered the start of the Internet and networks as we know them today?

(It was the Cold War.)

click

Networks and the Internet as we know them today owe their existence to the launch of Sputnik.

The Americans got scared, and created the Advanced Research Projects Agency to fight the Soviets.

click

ARPA created ARPANET, which initially linked UCLA, Stanford, UC Santa Barbara, and U of Utah and then branched out, but was limited to the military and academia.

click

The US wanted to control its nuclear weapons in the case of a nuclear attack, and wanted to be able to link its networks so if one communication path went down, another route would be available. Vinton Cerf and Bob Kahn created the Transmission Control Protocol/Internet Protocol (or TCP/IP) to meet this goal, and in 1983, the networks that started with ARPANET were connected to 562 networks using TCP/IP. This protocol suite (or group of rules for computers to talk to each other) is what powers most modern day networks, and is why we need all the other things we're going to talk about today.

click

By '84, 1024 networks were connected. 10 years after the conversion to TCP/IP, over 2 Million networks were connected. Shortly after the graphical web browser came on the scene, private Internet Service Providers opened up the Internet to everyone.

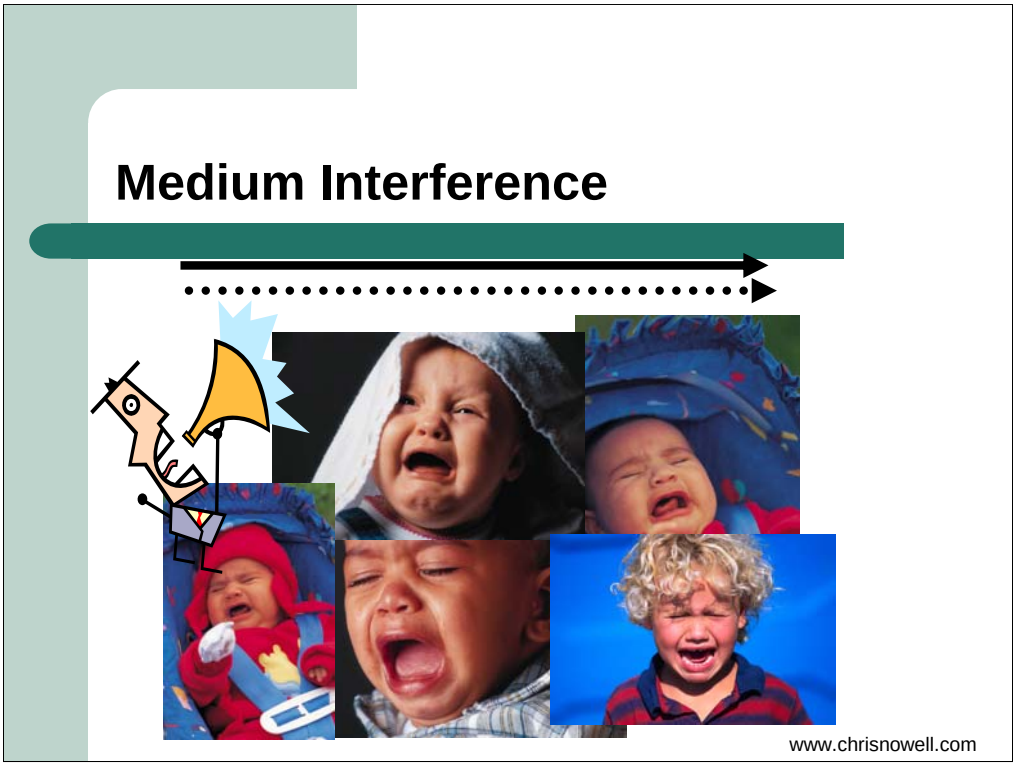
click

When TCP/IP was released, the developers assumed that it would be redesigned later on. Their goal was to add features and make it reliable. Sadly, it was too reliable. As Vinton once said, "once it was deployed, it just kept spreading". Remember that the precursor of the Internet was intended exclusively for trusted academics and the military.

click

Security wasn't an issue. When the Internet exploded in popularity, people started taking advantage of the lack of security, and … well… I guess I should be thankful since part of my job is to make sure that systems are protected from these people

Now that we've endured a history lesson, let's have a quick theory lesson to help us understand network media. *click*



We've all encountered communication interference.

click

This is when one person tries communicating, but the surrounding noise drowns him out or makes him hard to understand.

While we see this problem in wireless networks (including voice conversations we try having at the mall), we also see it in wired systems.

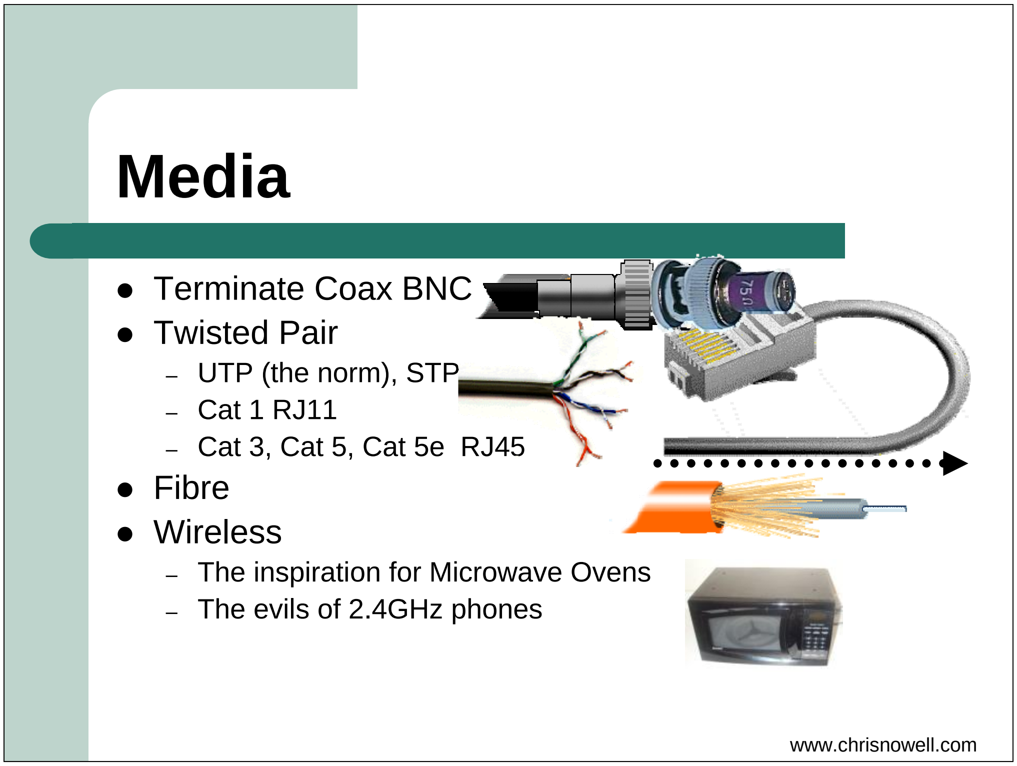
click

When a current is applied to a wire,

click

It will induce a current into a parallel wire. If the second wire contains data sent through electricity, the two will start to interfere, and neither will be very effective.

Now that we understand medium interference, network media will be easier to understand. *click*



A medium is required to communicate in networks.

click You have probably all seen the coaxial cables that connect to your home cable TV.

These coax cables were popular in business networks ten years ago. They consist of a copper core insulated with plastic with a copper mesh on top.

click They had BNC connectors that enjoyed falling off and needed to be terminated,

click which means that caps had to be put on top at the ends of the network. Coax was difficult to install or centralize, but didn't have many interference issues. (185 or 500m)

click The most common medium nowadays is this stuff, [hand out example] twisted pair. (100m)

click UTP, or unshielded twisted pair, is easy to work with and is made up of a bundle of twisted pairs of wire. The twists in the wire mean that the wires aren't parallel, so don't interfere with each other as much. Shielded twisted pair is also available and protects from outside interference, but is harder to work with.

click we see twisted pair everywhere. Your first experience with it was probably with a plain old telephone system line with an RJ11 connector. Cat 1 isn’t always twisted and can’t support very fast communication.

click with computers, we used to use cat 3, which allowed for speeds a tenth of what is common today. We now use cat 5 or 5e. 5e allows speeds up to 10 times what is common today. The ends of cat 3,5,and 5e cables plug into an RJ45 jack.

In general, the more twists per inch, the less interference, and the faster data can travel. Signals sent by twisted pair can still be picked up using the principle of

click induction that we talked about earlier. It is also limited in distance due to the copper's electrical resistance.

click Fiber optics have very little resistance and do not have interference problems

click they consist of a pure glass core, surrounded by a reflective material, which is surrounded by protective material. it's difficult to handle and install, but is very speedy.

click another medium is air.

click Does anyone know what the inspiration was for microwave ovens?

click legend has it that someone discovered that he got hot standing in front of an early microwave generator like the one in this picture.

click It turns out that 2.4GHz is a great frequency to excite water molecules and heat up food and people.

click it's also the frequency of the

click cordless phones that came on the market a couple years ago.

Like crying babies, they interfere with Wireless networks.

click

Network Interface Cards

- Unique MAC address (each manufacturer has own block) Ipconfig/all
- IP Addresses ipconfig
- NICs now usually built-in to *workstations*, *servers*, *printers and other network devices.*

www.chrisnowell.com

A Network Interface Card (or NIC) is a computer's adapter that provides a physical connection to a network.
*click*The first NIC could have been a telegraph
*click*This is a picture of an old NIC with RJ45 and BNC jacks
*click*before they were integrated into laptops, we used to use cards that used dongles like this. They frequently broke, got lost and were generally annoying.

Nowadays, they look like this

[pass around]

click

All network interfaces (such as RJ 45 jacks) have unique MAC address. They help TCP/IP find the right computers within the local network but aren't sent between networks. This is the MAC address of this computer

[run ipconfig/all]

click

All interfaces also have at least one IP address, which is sent with all communications over modern networks like return and to: addresses.

click

NICs are now usually built into devices like the one on the side of your laptop.

Workstations

- Dumb terminals to powerful workstations
  - Tower / Desktop 
  - Notebook 
  - Thin Clients 
- Lockdown and Backup issues

www.chrisnowell.com

While we don't often show NICs on a network diagram, we do show workstations. They can be represented as computers, monitors, or a combination

click

In the good ol' days, computer processing was performed exclusively on big powerful central servers that workers accessed through dumb terminals, which did little more than provide a screen and keyboard to interact with the server.

click

As computers got smaller, and workers had greater power on their desktops, they started doing more work on their own towers and desktop workstations. This also meant that more people knew more about computers and more people had the knowledge to threaten IT security. Users now have machines that they can infect with viruses and misconfigure. They can also save their work on thousands of machines that don't have a central backup system.

click

As notebooks became more prevalent, workers began saving sensitive information on machines that can be easily stolen or lost. Notebooks can be easily taken out of the secure office environment and connect to unsafe networks and bring new viruses and other threats to the secure office environment.

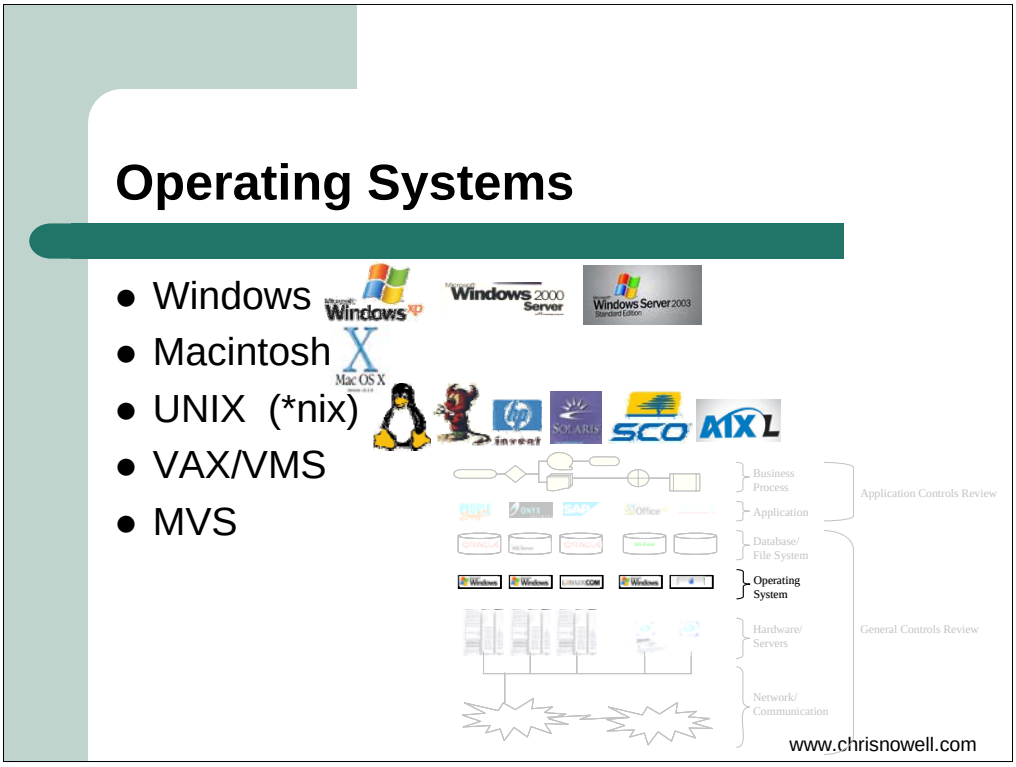
click

Thankfully, we are now seeing a return to thin clients. Thin clients serve the same role as dumb terminals. The processing again takes place on a central application server, and thin clients don't store much more than hard-to-access- configuration information and are not as vulnerable to viruses and other risks.

click

Now that users have tasted the power of desktops and notebooks, it's difficult to lock them down. IT tries to prevent users from being able to install programs that could cause harm to their computers or the network and keep protective applications, such as antivirus solutions, from being disabled. They must do this while trying to keep their actions as transparent as possible to prevent users from thwarting their efforts. We are also seeing a return to central file stores that can be easily backed up.

click



Notebooks and desktops today typically run one of three major operating systems

click

Windows is the dominant operating systems on laptops and desktops.

click

Mac OS X powers modern Apple computers and is now based on UNIX. It's very stable and reliable and is a favourite for graphics, music, and desktop publishing.

click Linux is gaining popularity. It is based on UNIX and is powerful, reliable, and in some cases free. If you'd like to learn more about Linux, please come to our session on

Servers can also run on these three operating systems, but Macintosh servers have yet to gain much popularity.

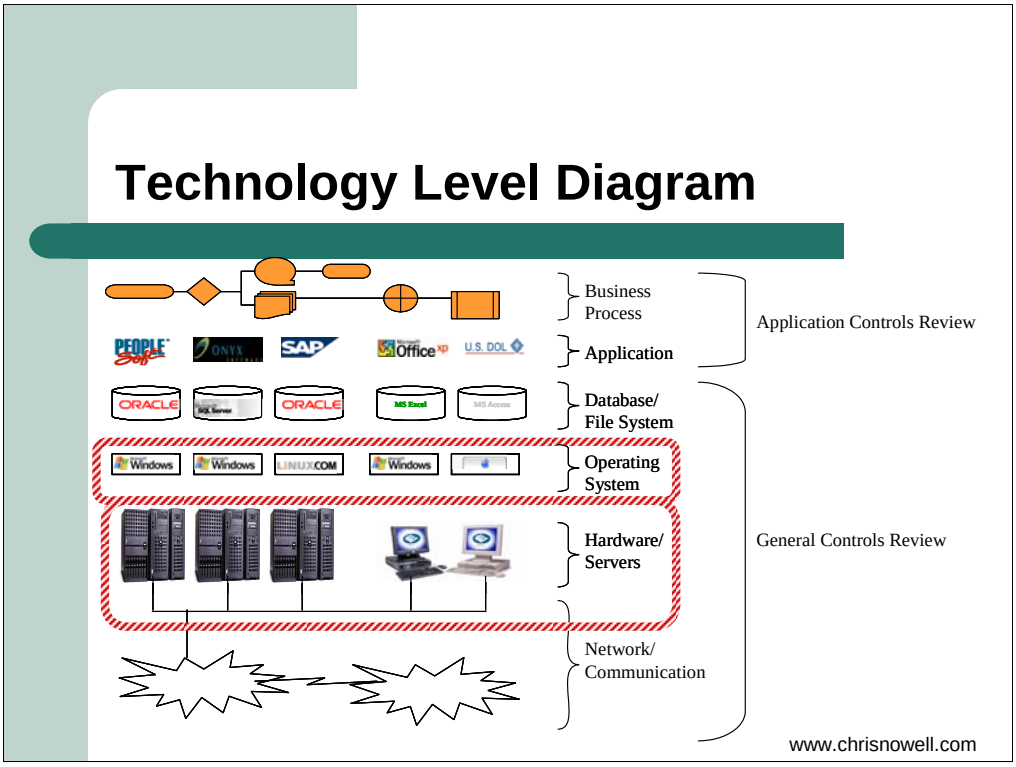
click Windows 2000 Servers are quite common

click However, many of the entities we audit are presently migrating towards Windows Server 2003.

click Linux, and other variants of Unix (sometimes called "star-nix") such as
click BSD
click HP-UX
click Solaris and SunOS
click SCO UNIX
click And IBM's AIX
are all heavy hitters as server operating systems due to their stability and security.
click VAX/VMS is an old and fading operating system. It was reliable, secure, but … slow.

click MVS runs IBM mainframe computers. It has a reputation for being powerful and reliable.

click



While we're talking about servers, let's take a look at this diagram again.

click

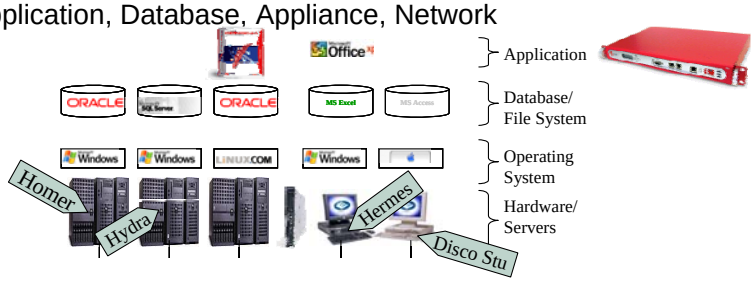
We've already seen that servers run

click

Operating systems and are quite similar to workstations

Servers

- Can be indistinguishable from workstations
- May not look like a PC (rack-mounted, blade)
- Obscure names preferred
- Application, Database, Appliance, Network



www.chrisnowell.com

click In fact, workstations can be used as servers

click But they are typically rack mounted and very thin since we often need to fit many servers in one server room. The thinnest servers are 1 U and are sometimes called blades depending on their housing

click They can also be 2 Us or 4Us thick

click IT used to provide their servers with useful names like “UNIX_Library_server”. But to an attacker, this reads “This is a critical server that houses library resources. If you’d like to attack me, try well-known UNIX attacks first.” Nowadays, we find that most servers have obscure names. The Simpsons and Greek Mythology tend to be favoured sources.

click Servers provide many roles. We just talked about Application servers with thin clients.

Servers are frequently central repositories for databases, which hold vast amounts of related information for structured access. Some common databases we see are

click SQL Server 2000, which runs on Microsoft Windows

click Oracle, which usually runs on Unix, Linux or another star-nix

click And windows

click Less powerful databases such as Microsoft Access, can be run on workstations, and servers of many types

click To an extent, Microsoft Excel can even be used as a database by those daring enough to live without constraints and controls.

If you’d like to learn more about databases, please come to our database session.

Some servers have very specialized roles, such as

click filtering emails for viruses. These are sometimes provided from the vendor as a pre-configured unipurpose device. These are called

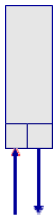
click Appliances.

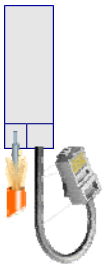
Others have dedicated network roles, such as translating the www.oag.ab.ca to the IP address of 199.214.36.13. These are DNS servers.

While most devices have one IP address, some servers (such as routers) have many network interfaces; each one has its own IP address. Other servers (such as web servers) have one or two network interface, but with dozens of IP addresses, each responsible for its own service, such as a website

Repeaters

- Repeaters
- Converter





www.chrisnowell.com

Servers are great, but we have to find a way to connect workstations to them.

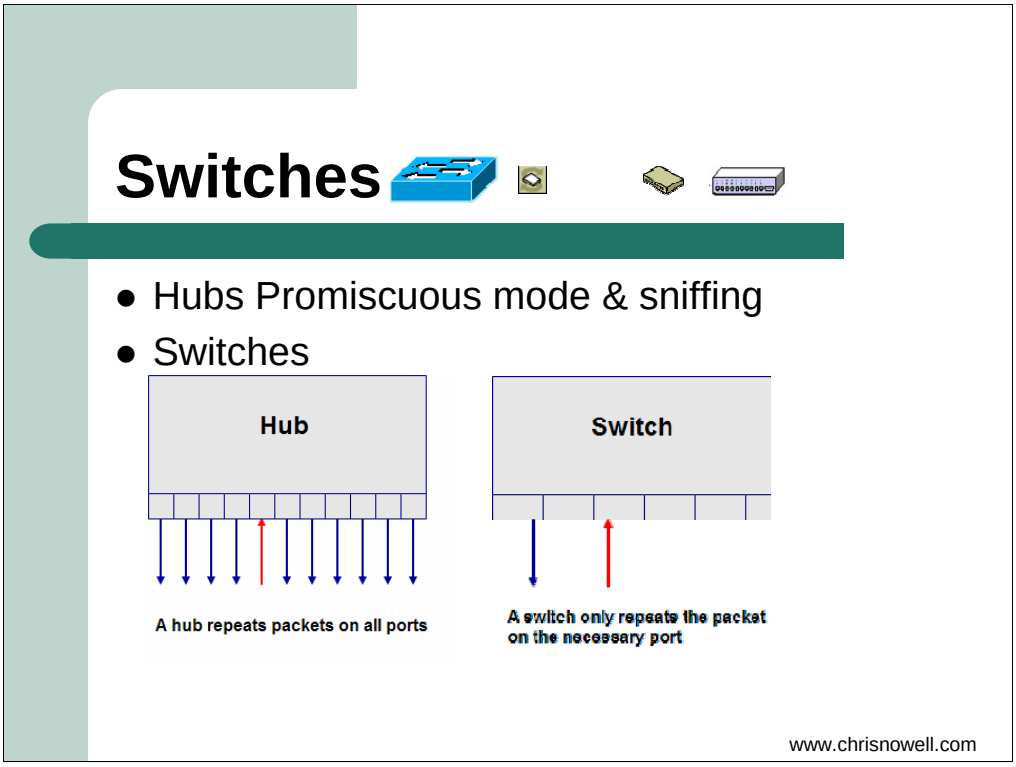
As I said earlier, signals tend to degrade over distances due to resistance in the medium. Repeaters were invented to boost the signal back up so it could continue along its path.

click

A related device is a media converter

click

which accepts data in one medium and repeats it in another.



click

Hubs are basically repeaters that repeat data sent in to multiple ports. This means that if many computers are connected to the same hub, they will be bombarded with traffic intended for one computer. While most computers politely ignore data that isn't intended for them, malicious users can set their computers to use "promiscuous mode" to "sniff" and capture all of the traffic. As you can probably imagine, hubs not only slow down data flow, but also present a security risk.

click

Switches are like hubs, except they repeat traffic only to the port on which the intended recipient is connected using the MAC addresses we discussed earlier. This significantly decreases network traffic and provides greater confidentiality.

Routers

- Connects multiple networks
- Can connect LANs to the Internet for example.
- Make a few IP addresses go a long way
- Interfaces
  - Each connection is called an interface
  - Sometime more than two networks (Internet, Trusted and Untrusted) so more than 2 interfaces

www.chrisnowell.com

A router is used to

click

connect multiple networks and provide paths between computers.

click

Many home users, for example, use a router to connect their local area network (or LAN) to the Internet.

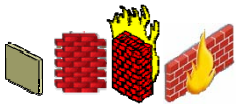
click

A special feature in some routers, called Network Address Translation or NAT, which can assign private addresses to computers inside the LAN. This allows you to use the one address that Shaw or Telus provides on many computers that can be invisible to computers on the other side of the router. (for those techies out there, this isn't a true definition of NAT, but is adequate for those configuring consumer routers)

click

Routers can also separate networks into different groups. For example, we want our web server to be visible to the Internet, but we don't want anyone on the Internet to see patient health records. Routers are employed to accomplish this feat.

Firewalls



- A firewall is a filter
- *Rules* permit or deny traffic based on port, address, or protocol
  - Appliance style (dedicated hardware)
  - Software style (A PC with multiple NICs)

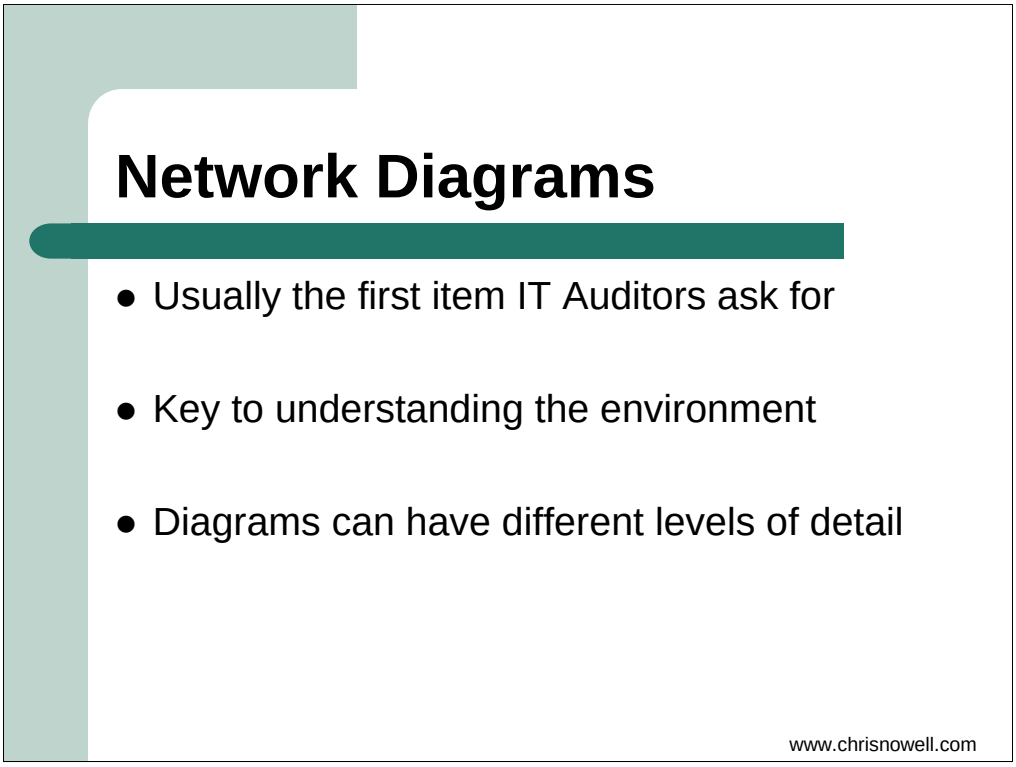
www.chrisnowell.com

A firewall *click* filters traffic into the gateway to keep unwanted traffic and risks out *click*

It does so based on rules. These rules work at different levels.

Programs communicate on different ports and protocols. Firewalls can limit traffic based on these ports and protocols or can allow only traffic to or from specific MAC or IP addresses, or can filter the contents of the data.

Firewalls can run on dedicated hardware called appliances, on generic servers with at least two NICs, or as software on your PC to provide a last line of defence.



Now that we've seen the main components of a network, a network diagram should be a breeze.

click

Network diagrams are typically the first thing that Information Systems Auditors asks for.

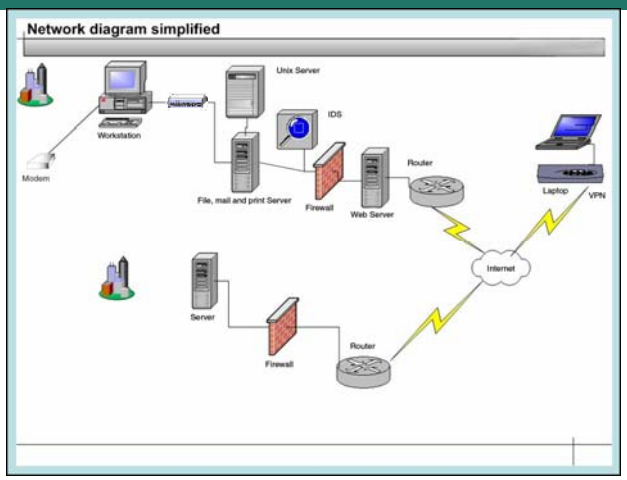
click

It is key to understanding the environment, since it indicates the critical components of the network, which give us a good idea where to look for problems.

click

These diagrams come in varying levels of detail, from large groups, to every server and router.

Simplified Network Diagram



www.chrisnowell.com

This network diagram is simplified because not all devices are actually shown and the precise connection details are not shown either.

For example, the single workstation would actually represent many workstations.

Can someone tell me what network device would be between the servers and the workstations?

click

(a switch).

What's the IDS? (Intrusion detection system checks either for signs of intrusion based on signatures or variations from normal activities)

Modems are typically no longer allowed to be connected directly to workstations, since attackers can dial into them and they may allow users to connect to insecure networks..

Why is the web server on the right side of the firewall?

Wireless Router

- Converter (WAP)
- Wireless like a Hub, sniffing
- Switch
- Firewall
- Router

www.chrisnowell.com

The most common non-work-related questions posed to IT staff relate to setting up a wireless network at home. Most of you who want to do so will start with a retail wireless router, which is intended for home use. Since most home users don't want to have to set up a complicated network infrastructure, a typical home wireless router includes most of the devices we have explored today.

click

The primary function of a wireless access point is to act as a converter. The wireless router includes a wireless access point that converts the wired network that uses ….

_____ what kind of cable again? (twisted pair) to the wireless medium, which uses

_____ what kind of radio waves again? (microwaves)

click

The wireless router repeats the signal sent in from the wired network through the wireless access point to all of the wireless network cards. Can someone tell me what the wired device that does this is called?

click

(a hub).

This is very easy to sniff, since you don't even have to be physically connected to the network, which is why security is such a strong concern in wireless networks.

click

Many retail wireless routers include several ports on their backs to connect to several workstations using twisted pair wires. They will repeat only the data destined to specific computers. Can someone tell me the name of the other device that does this?

click

(switch)

Since security is such a concern on the wireless network, wireless routers typically allow you to define rules to protect your home network from external threats and bad traffic. Can someone remind me what kind of device does this?

click

Firewall.

Finally, as the name implies, the goal of the wireless router is to act as a

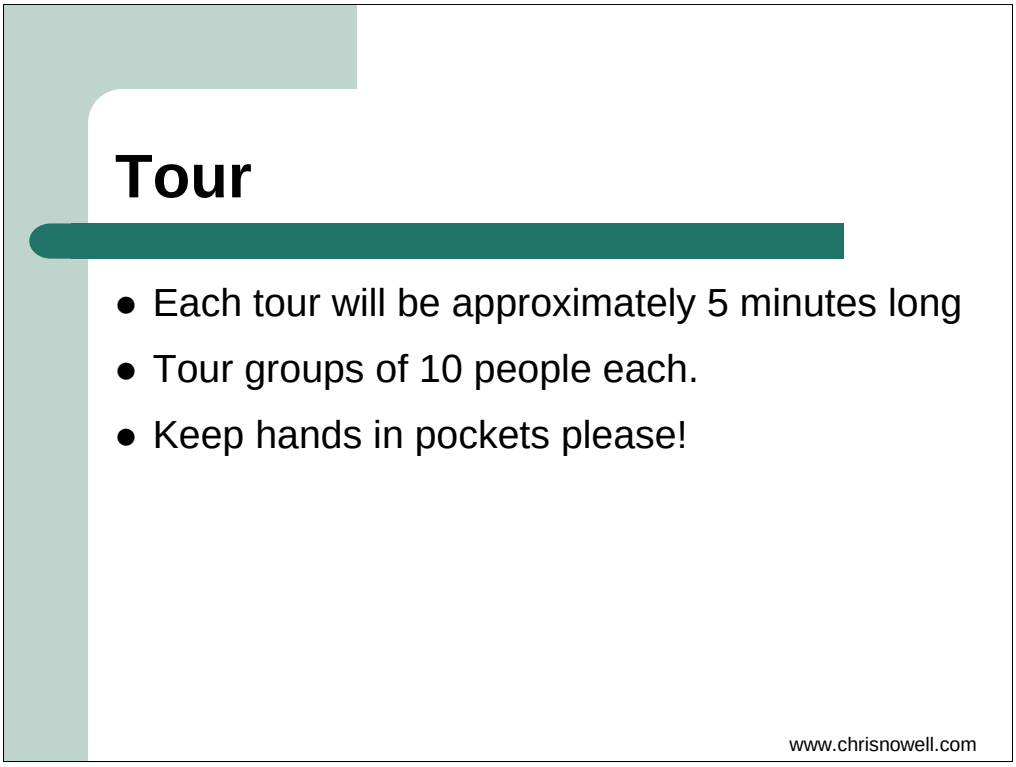
click

Router, and connect two networks together.

Of course, to learn to properly set up your wireless network and not be vulnerable to attacks, you should come to our wireless networking session

Questions ?

www.chrisnowell.com



The network device you accidentally unplug could be your own