



# Home Networking

Alan Baker  
June 13, 2006



# Overview

- Why have a home network?
- The three components of a network
- IP addresses and subnets
- Ethernet, wireless, and powerline networks
- Best Practices
- Q & A



Generic 10 / 100 Mbps  
ethernet card

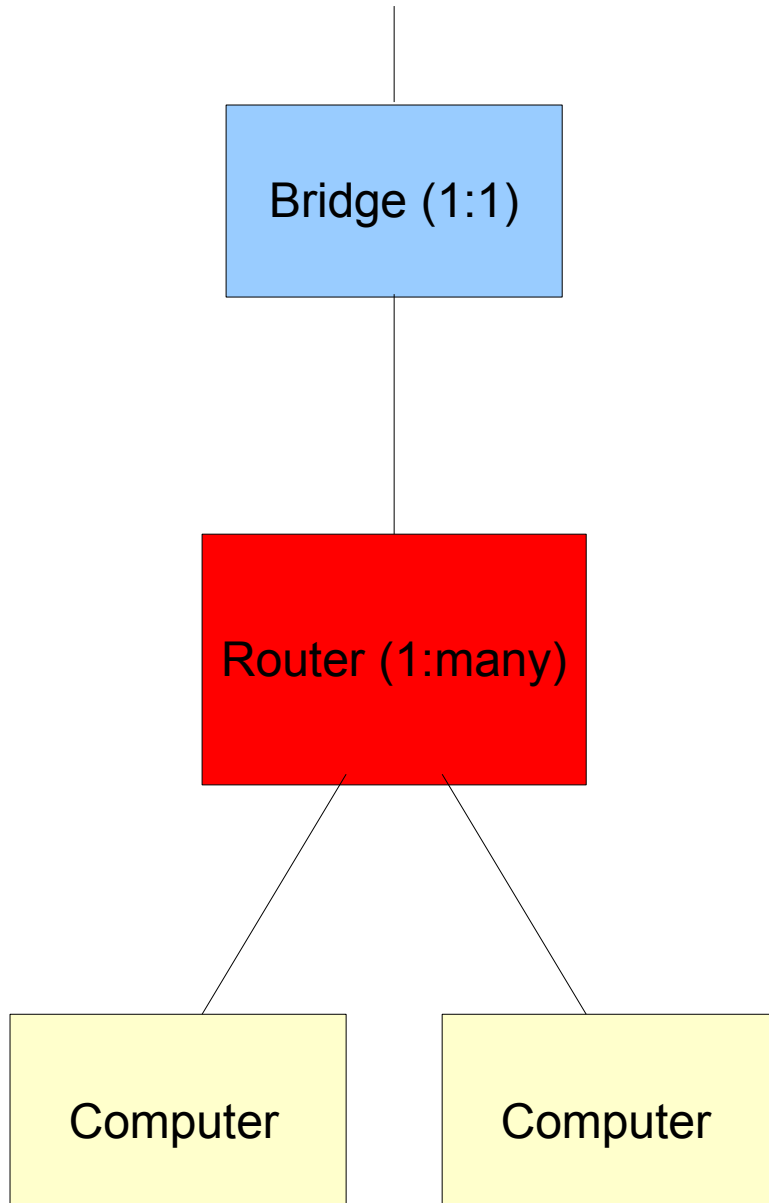
# Why have a home network?

- Internet access sharing
- Printer sharing
- Program and file sharing
- Wireless and wired computers
- Multi-player games
- Multi-room Voice Over Internet Protocol (VOIP)
- Get the weather forecast from your toaster



[http://www.theregister.co.uk/2001/06/04/bread\\_as\\_a\\_display\\_device](http://www.theregister.co.uk/2001/06/04/bread_as_a_display_device)

# Network Components



1. A **bridge** connects one network to another network (examples: wireless bridge, DSL modem, VOIP adapter)

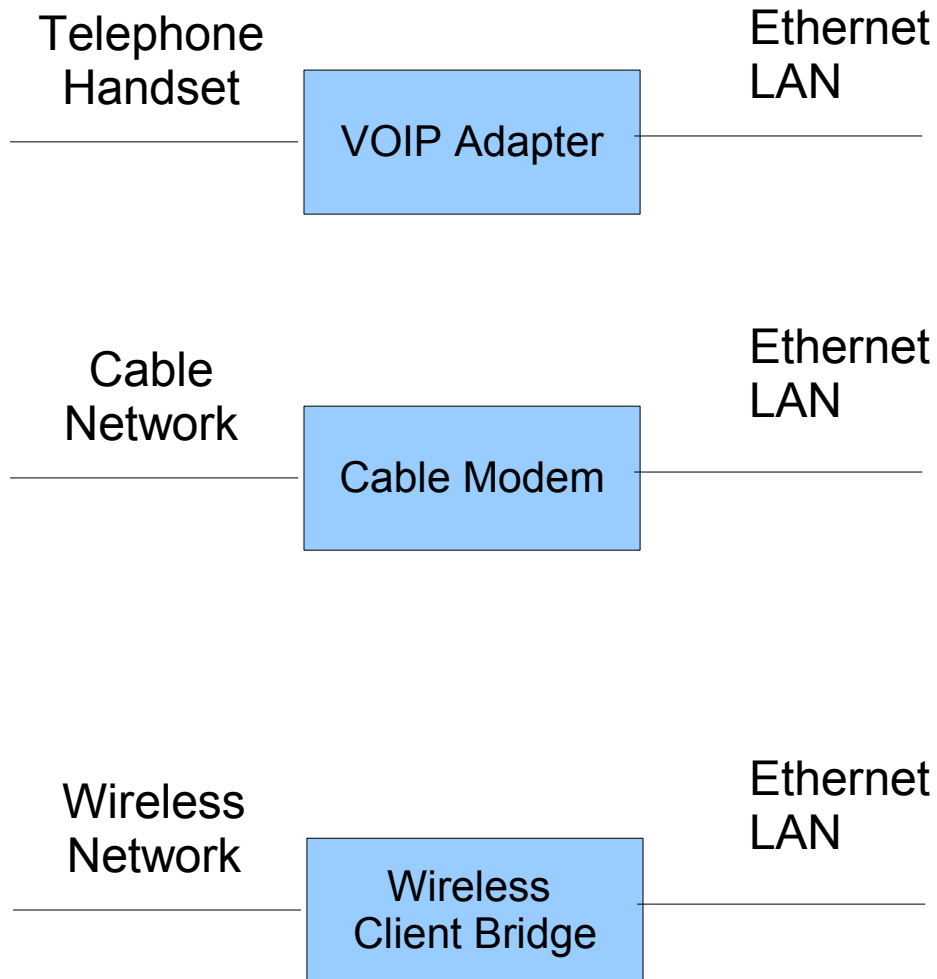


2. A **router** directs packets to multiple destinations (examples: router, hub, switch, wireless access point)



3. A **computer** may be a desktop, laptop, game console, Tivo, print server, toaster, etc.

# Bridge



## Function

- Connects two networks



D-Link DWL-G730AP travel wireless client bridge / wireless access point / router

# Router

## Functions

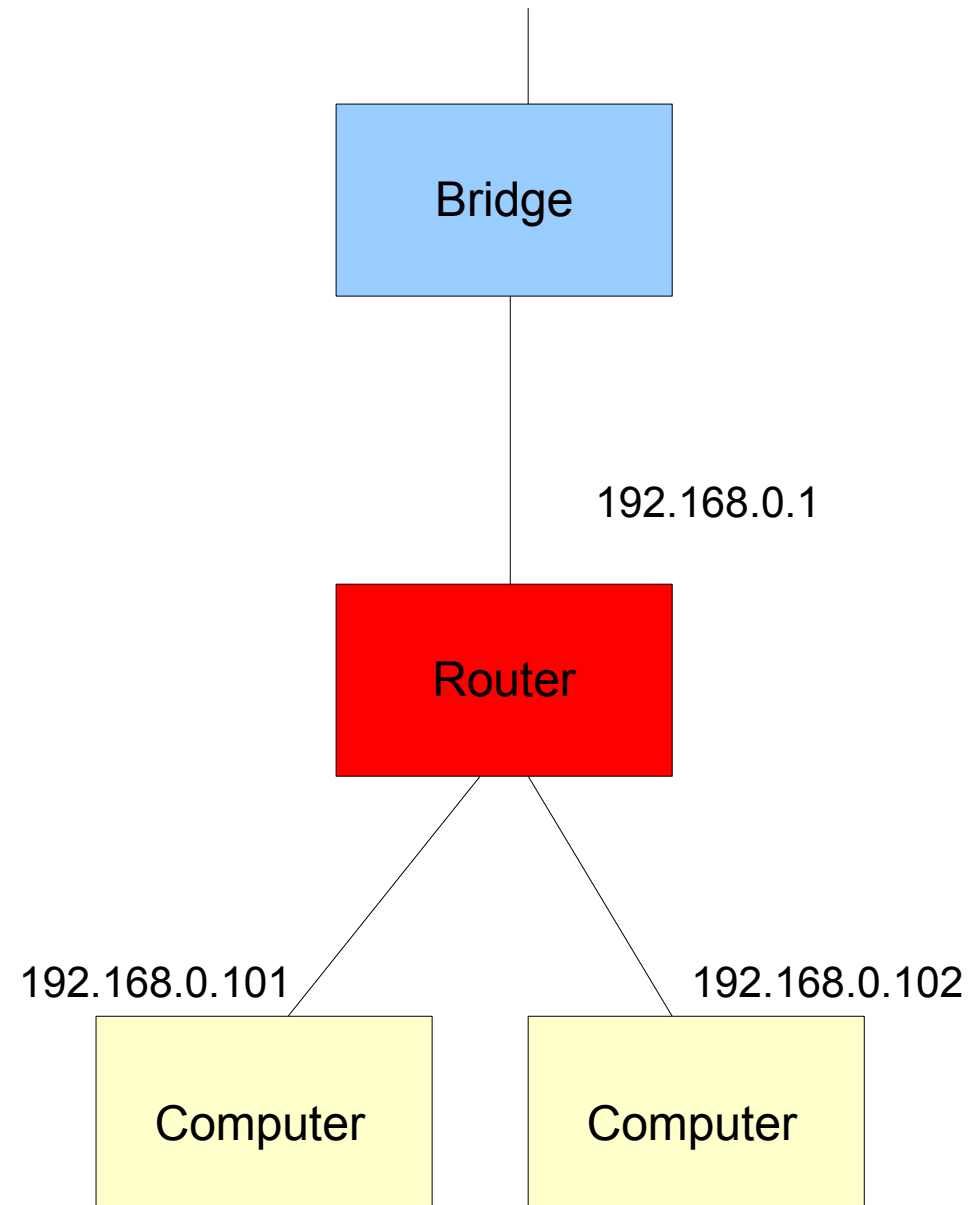
- Route each IP packet to the right address
- Manage and assign IP addresses
- Firewall



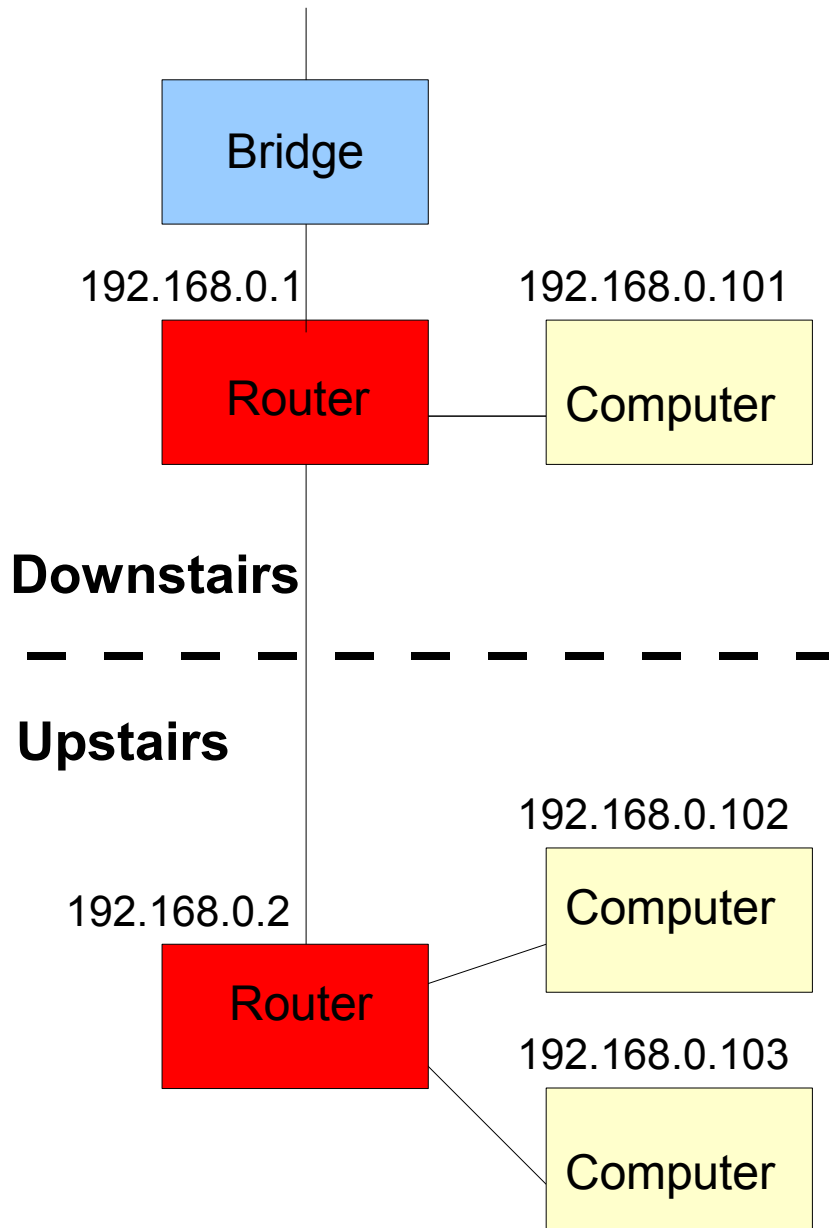
D-Link DI-604  
4-Port Ethernet Router

## 192.168.0 subnet:

- 192.168.0.1 – Router and DHCP server
- 192.168.0.101 – Computer
- 192.168.0.102 – Computer



# A Subnet with Two Routers



## 192.168.0 subnet:

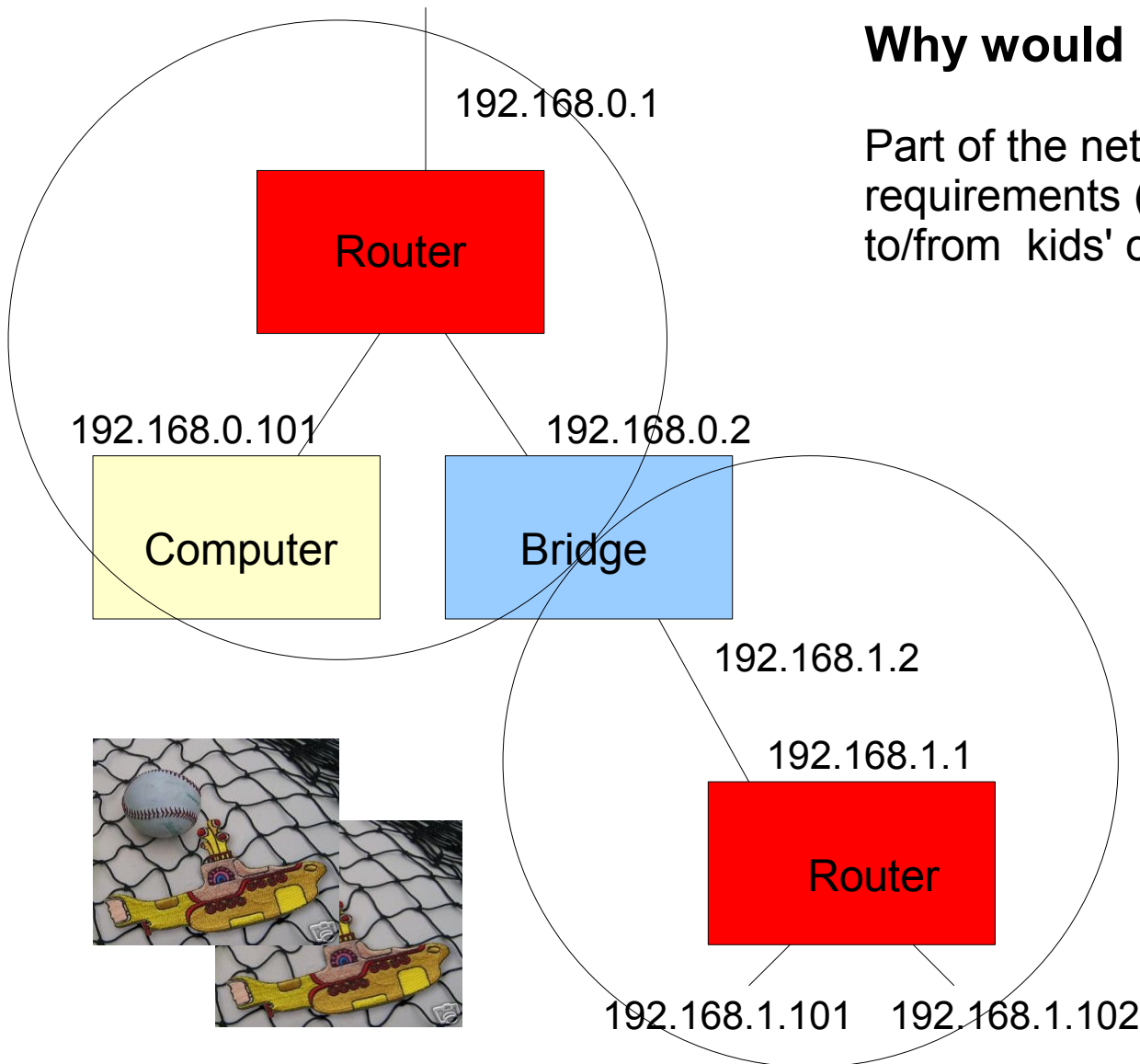
192.168.0.1 – Downstairs router and DHCP server  
192.168.0.101 – Downstairs computer

192.168.0.2 – Upstairs router used as a switch  
192.168.0.102 – Upstairs computer  
192.168.0.103 – Upstairs computer

# Advanced Topic: Two Subnets

## Why would I want two different subnets?

Part of the network has different security requirements (for example, restricting traffic to/from kids' computers)



### 192.168.0 subnet

192.168.0.1 – Router  
192.168.0.101 – Computer  
192.168.0.2 – Router used as a bridge

### 192.168.1 subnet

192.168.1.1 – Router  
192.168.1.2 – Router used as a bridge  
192.168.1.101 – Computer  
192.168.1.102 – Computer

# *Advanced Topic:*

## IP Addresses for Private Networks



- Class C: **192.168.0.0 through 192.168.255.255** (65,535 IP addresses)
- Class B: 172.16.0.0 through 172.31.255.255 (1,048,576 IP addresses)
- Class A: 10.0.0.0 through 10.255.255.255 (16,777,215 IP addresses)

Most home networks use class C addresses, but you can use class A and B addresses too.



# Network Comparison



Transmission Medium	Standard	Max Speed	Range	Cost	Notes
Wired	Ethernet	100 Mbps	328 ft	Low	Fast, simple, secure
Wireless	802.11G	54 Mbps	Beyond your house	Medium	Flexible, requires configuration
Power line	Homeplug	85 Mbps	Your house	Medium	Don't use powerstrip
Phone line	HPNA	10 Mbps	Your house	Medium	
Firewire	IEEE 1394	400 Mbps	15 ft		

# Examples of when to use

## Ethernet

- One or two computers near modem
- Tivo



## Wireless

- Laptop computer

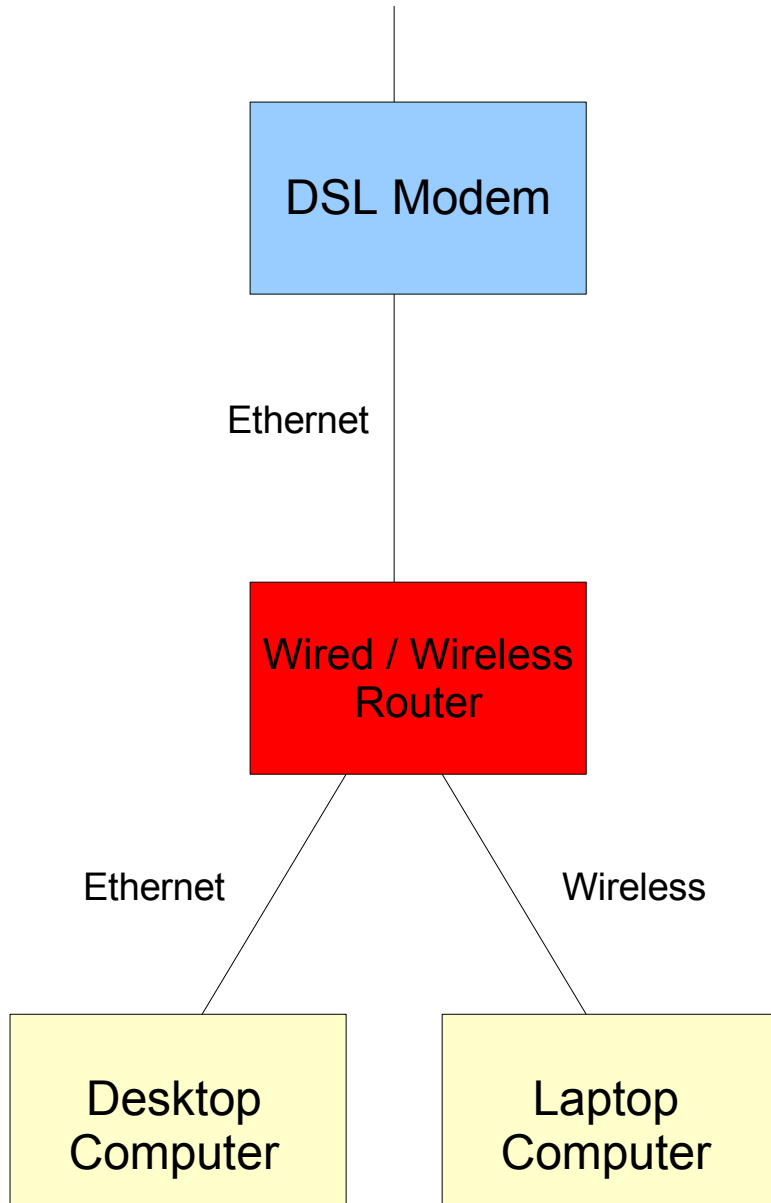


## Powerline

- Enough wall outlets

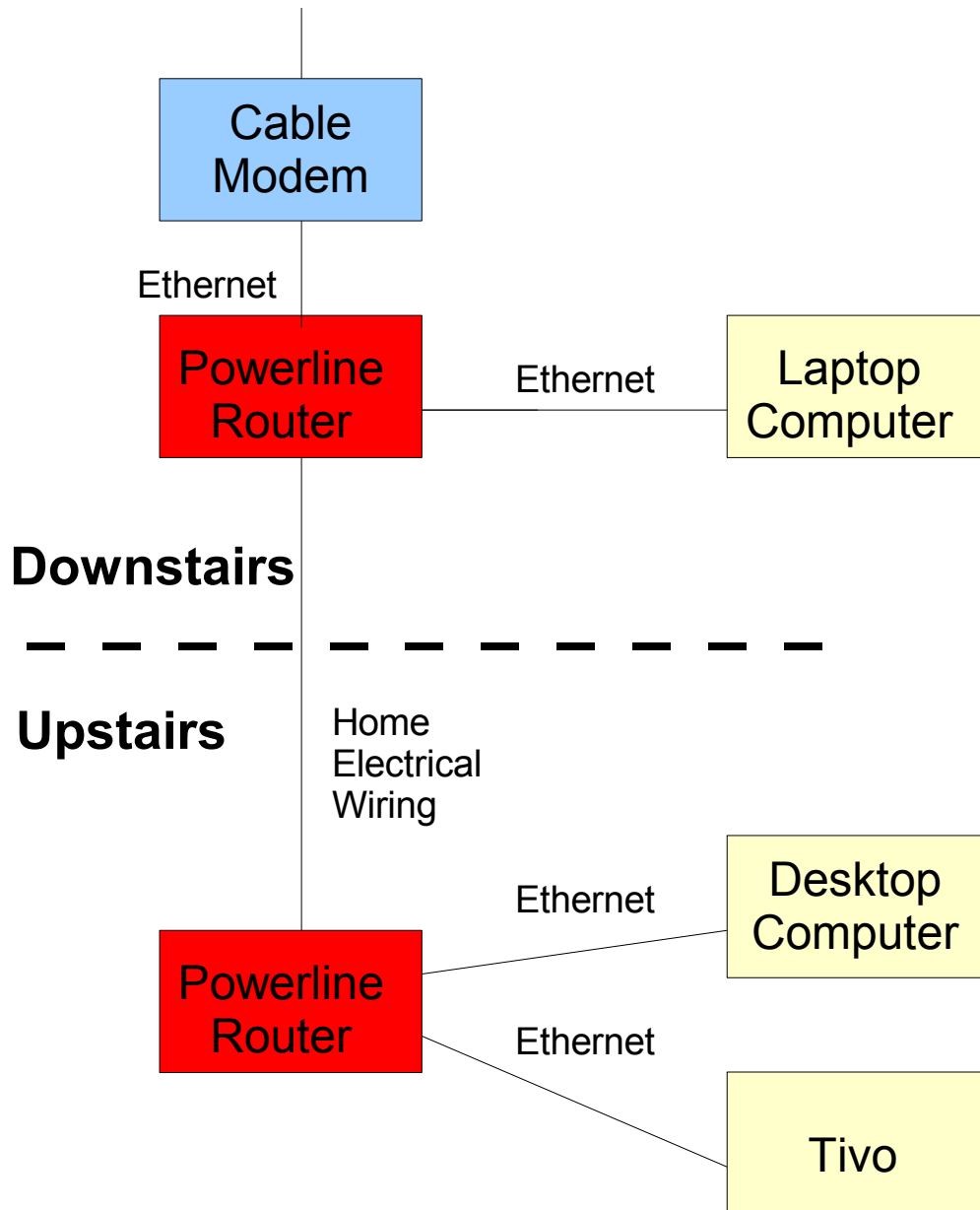


# Simple Home Network



Linksys WRT54G wireless access point / 4-port router

# Two-Story Home Network



Netgear XE104  
85 Mbps Wall-Plugged  
Ethernet Switch / Router

# Router owners' famous last words

- “It's just too much bother to <fill in the blank>”
  - **change the default password.** And if I forget it I can look it up in the manual. *(So can everyone else.)*
  - **filter ports.** My computer's firewall software does that. *(Unless a trojan horse program changes its settings. Does your DSL / cable modem blink even when your computer is off?)*
  - **filter MAC addresses.** I don't care which computers use my wireless network. *(You should care.)*
  - **use encryption.** I have nothing to hide. *(Ever use FTP or telnet?)*
  - **turn off broadcasting my wireless SSID.** Besides, I like telling everyone I have a Linksys router *(which has known security vulnerability xyz).*
  - **change the default wireless channel - everybody uses 6.** *(Use 1 or 11.)*



# More famous last words

- “I'll change this router setting because someday I might want to <fill in the blank>”
  - **change my router settings while I'm out of town.** (*What would be the consequences of enabling remote administration via the internet and not changing the default password?*)
  - **run a server.** (*Port forwarding and DMZ expose your computer to the internet.*)



# Questions and Answers

- **How do I connect a Tivo to my network?**
  - USB-to-ethernet converter: Use a model that Tivo recommends.
- **How do I set up a <fill in the blank> device?**
  - If the device has both a CD and a browser interface, use the browser interface.
- **Should I buy a device that combines the function of <device A> and <device B>?**
  - Combination devices are simpler and cost less
  - Individual devices have more security features



# References



- **Home networking**
  - <http://computer.howstuffworks.com/home-network.htm>
- **Ubiquitous networking**
  - <http://computer.howstuffworks.com/ubiquitous-network.htm>
- **Private IP address ranges**
  - [http://en.wikipedia.org/wiki/Private\\_IP\\_address](http://en.wikipedia.org/wiki/Private_IP_address)
- **IBM internal link**
  - [http://w3-03.ibm.com/tools/it/ittools.nsf/main/hncoc\\_home\\_lan\\_guide](http://w3-03.ibm.com/tools/it/ittools.nsf/main/hncoc_home_lan_guide)
- **Configure your router**
  - <http://www.smartcomputing.com/Editorial/article.asp?article=articles/2006/s1707/12s07/12s07.asp&emid=140867>

# Home Networking



# Things to Bring

- Dead routers
- Dead bridge (get from Eric?)
- Portable wireless bridge with USB adapter
- Webramp
- Soekris board
- Curta

# Kinds of Network Components



There are **exactly two** kinds of people in the world.

1. Those who believe there are two kinds of people in the world
2. Those who do not



Similarly, there are **exactly three** kinds of network components...

# Router Best Practices



- Change the default password
- Use IP address filtering
- Use port filtering
- Do not enable port forwarding
- Do not enable remote administration
- Do not enable DMZ

# Wireless Best Practices

All the above router best practices **plus...**

- Use MAC address filtering
- Use at least 128-bit encryption
- Use WPA pre-shared key or WEP encryption key
- Change your wireless SSID and don't broadcast it
- Use a less-busy wireless channel (1 or 11)
- Use Wi-Fi Speed Spray: <http://j-walk.com/other/wifispray>

