

April Coffee Chat

Home Networking

8:30 – 10:00 am

Thursday April 14, 2011

Hopi Room, Chaparral Center



Arnie Gelb
Joe Parla



Topics

- **Home networking overview**
- **Description, design & equipment**
- **Installation**
- **Configuration & testing**
- **Coming soon**
- **Other software tools and programs**
- **Other hardware**
- **Open discussion & questions**

Home Networking Overview

Reasons to home network

- Internet access, access to local and remote computers and servers
- Share devices such as printers, hard drives, NAS, SAN, optical drives, fax, etc.
- Share libraries, folders and files such as music, video, documents
- Project collaboration

Home Networking Overview

Terminology

AES – Advanced Encryption Standard

MAC – Media access control

SSID – Service set identification

TKIP – Temporal Key Integrity Protocol

WEP – Wireless Equivalent Privacy

WPA – Wi-Fi Protected Access

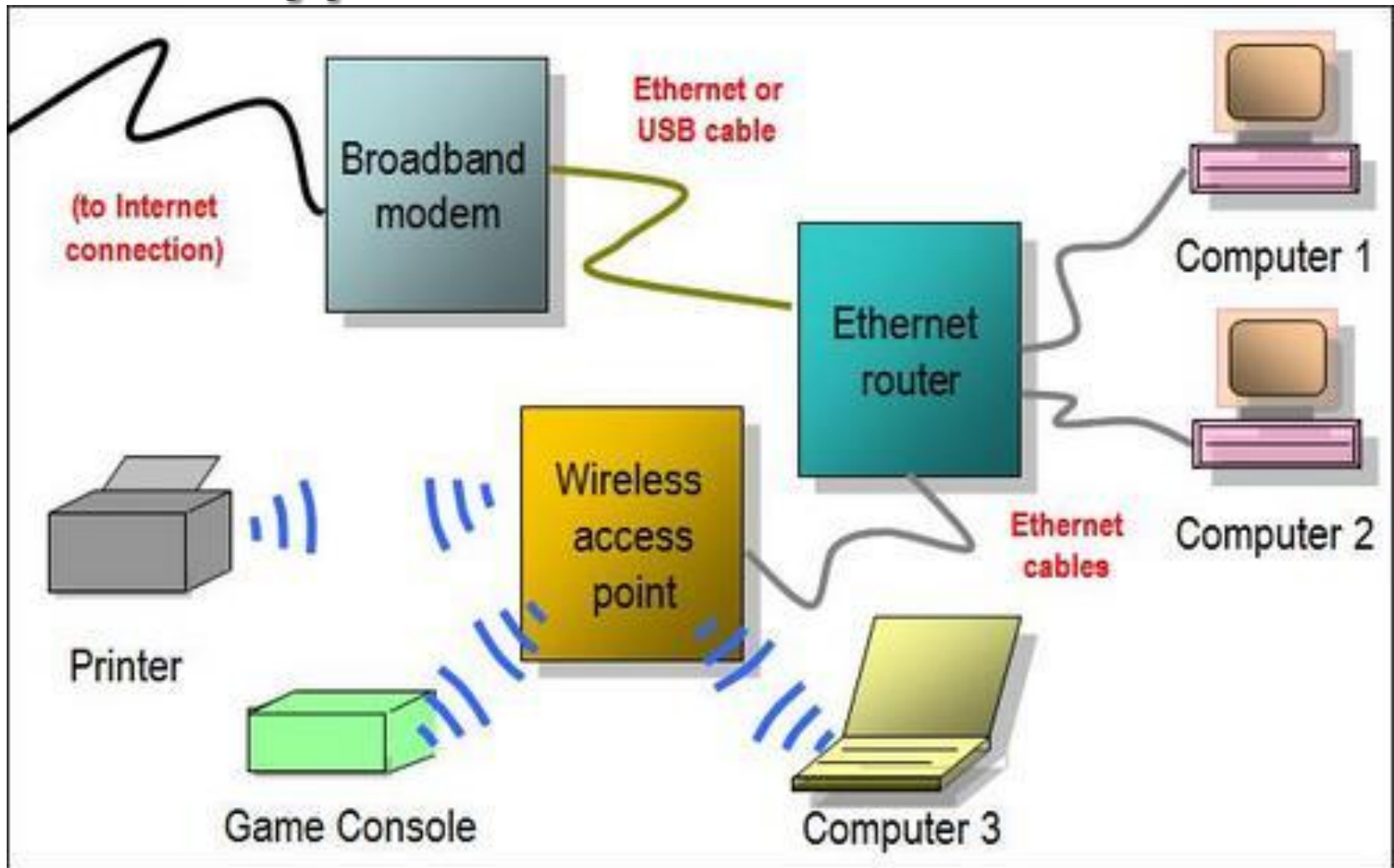
WPA2 – Wi-Fi Protected Access 2

Description, Design & Equipment

Types of home networks

- **Wired**
 - Ethernet/USB (most common)
 - USB
 - Home power lines
- **Wireless**
 - Wi-Fi (802.11a, b, g & n)
 - Cellular (3G, 4G & tethering)
 - Ad-hoc

Typical Home Network

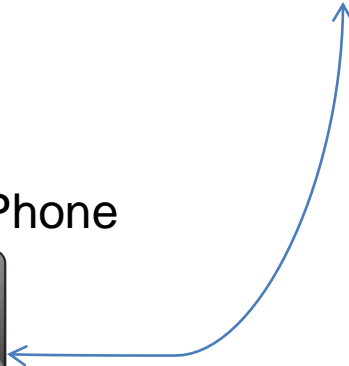


Tethering what is it?

Droid X
Android Phone



Verizon Network



Bluetooth
USB Connection
Wireless

PC or Tablet

With a smart phone you can use the unlimited data connection without incurring extra charges on your cell phone bill when you have the appropriate APP to get you to the INTERNET

Description, Design & Equipment

Wired networks

- Peer-to-peer with cross-over cable
- Dial modem & phone line
- DSL/Cable modem to computer
- DSL/Cable modem to router to computers

Wireless Components

From Computer Desktop Encyclopedia
Reproduced with permission.
© 2004 Cisco Systems, Inc.



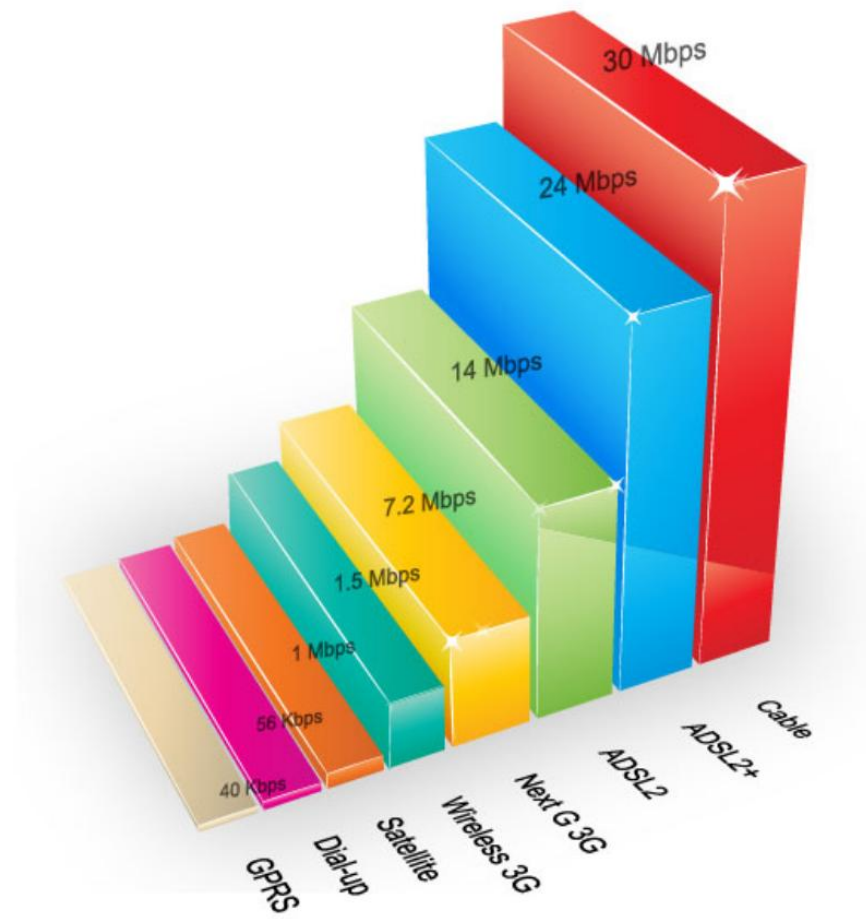
Access Point

Desktop Adapter
(PCI)

Laptop Adapter
(PC Card)

Wireless Components

Internet Speed Comparison



Router Speed Comparison

Wireless speeds

- **802.11b 11 Mbps**
- **802.11a 54 Mbps**
- **802.11g 11-54 Mbps**
- **802.11n 150 – 300 Mbps**

Wired Ethernet

- **10 – 100 Mbps**
- **1000+ Mbps**

Description, Design & Equipment

Wireless security access modes

- **WEP (with passphrase; RC4)**
- **WPA (with TKIP/AES)**
- **WPA2 (with TKIP/AES)**

Configuration

Default settings may:

- **Allow router access by others**
- **Allow Internet access by others**
- **Allow device access by others**
- **Allow file access by others**

Configuration

Determine access & sharing requirements

- Internet access, access to local and remote computers and servers
- Share devices such as printers, hard drives, NAS, SAN, optical drives, fax, etc.
- Share libraries, folders and files such as music, video, documents
- Project collaboration

Configuration

Review and secure the following:

- **Prevent router access by others**
 - Change admin logon and password
 - Restrict access by MAC address
- **Prevent Internet access by others**
 - Stop broadcast of SSID
 - Require encrypted key
- **Restrict device & file access by others**
 - Change workgroup name
 - Limit file and device sharing

Configuration

Configuration steps for typical router

Use disk or web-site if available; or:

- **Type IP address in browser (192.168.1.1)**
- **Enter “User Name” and “Password”**
- **Click “Wireless” Tab**
 - **Pick a “Wireless Network Mode” (B,G,mixed)**
 - **Click “Save Settings”**

Configuration

- **Click “Wireless Security” Tab**
 - **Pick “Security Mode” (WPA2 Personal)**
 - **Pick WPA Algorithm (AES)**
 - **Enter WPA Shared Key**
 - **Click “Save Settings”**

Configuration

Connection steps to wireless network

- **Click wireless icon/Open Network & Sharing**
- **Click connect to a network**
 - Refresh network list (double arrows; top right)
 - Select YOUR network
 - Note Security-enabled wireless network
- **Choose network then click “Connect”**
- **Enter “Network Key”**
- **Note “currently connected to network”**

Configuration

Wireless tips to increase security

- 1. Change Default Administrator Password**
- 2. Turn on WPA / WEP Encryption (WPA2)**
- 3. Change default SSID (Wi-Fi network name)**
- 4. Disable SSID broadcasting**
- 5. Enable MAC address filtering (advanced)**

Configuration

Wireless tips to increase security

- 6. Do not auto-connect to open Wi-Fi networks**
- 7. Assign static IP addresses to devices**
- 8. Enable firewalls on each computer and the router**
- 9. Position the router or access point safely**
- 10. Turn off the network during extended periods of non-use**

Coming Soon

Wi-Fi Direct

- **Direct device to device connections**
- **No router required**
- **Device has own name and security (WPA2)**
- **Make, accept or refuse requests**
- **Create Wi-Fi Direct groups**
- **Many devices will support multiple connection protocols**

Other Software Tools & Programs

Anti-virus

Anti-spyware

Anti-malware

Scheduled scanning

Open-source router firmware (advanced)

Backup procedure

Restore points

[ShieldsUP!](#)

Other Hardware

Firewalls

Switches

Hubs

Encryptors

Home Servers

Network Attached Storage (NAS)

Storage Area Network (SAN)

Home Network Summary

Attached multiple computers

Share hardware (printers, scanners, optical drives)

Share folders, files, data

Project collaboration

Control access

Practice safe computing

Test conditions regularly (scan, review logs, etc)

Next Coffee Chat

Thursday October 13, 2011

8:30 – 10:00 am

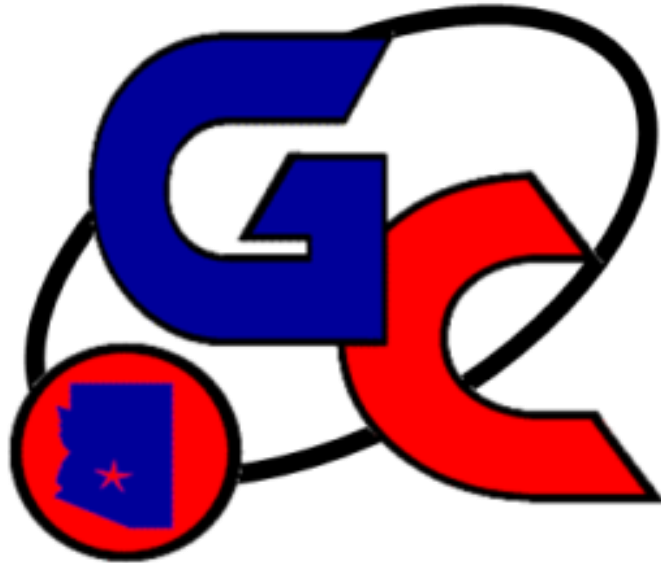
Hopi Room, Chaparral Center

Watch for Schedule in Grand Times

October through April

2nd Thursday of the Month

Thank you!



Grand Computers Club

www.grandcomputers.org