Residential Router

And what to try if you loose your Internet Connection
June 2011

Paul Lewis
paul@ComputerHomeHelp.com

Author's note:

This series of slides is intended to be presented in conjunction with other material:

- Flip-chart and white-board images created in real-time and
- A series of slides titled Introduction to Home Networks version 2

Route-Plan

A little revision and then the new stuff

1. A little about home networks and where the router fits in
2. A little about packets - why a packet network?
3. The telegram analogy - Layers and floors... eh?
4. What's an IP address and a Port
5. The postal analogy - data packets get around just like letters in the postal system - but faster and cheaper
6. How does the router do it's magic?
7. Let's look "inside" a router....with a browser
8. Things to check if you loose your Internet connection (before calling tech-support)
9. Q & A and answers to last week's questions

A Home Network

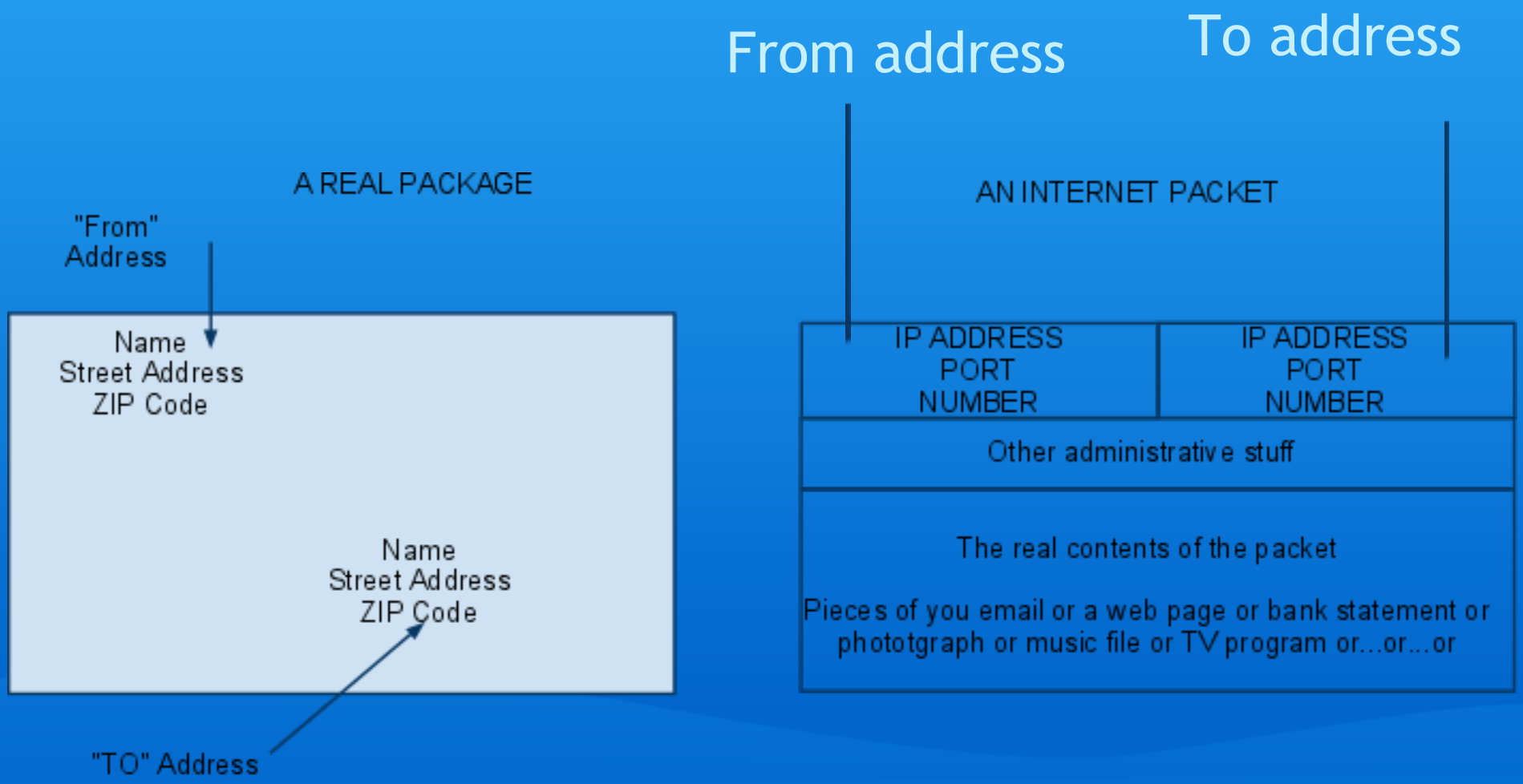
The router in your home network. (Who has one?)

Reasons to have a home network

- if you have more than one computer (shared Internet)
- if you have more than one computer (share files and pix)
- if you want to roam with your laptop computer
- if you want to locate your printer somewhere other than where you have your computer setup
- if you have visitors with a laptop - who want to connect

GoTo Home Networks presentation

Compare Real Package and Internet Packet (Significantly Simplified)



Name <=> Port number
Street Address <=> IP Address

The Telegram Analogy

See Introduction to Home Networks version 2

To the flip-chart or White-board

The regular postal system

- Real package into a single-family home
- Real package into a multi-family building

The Internet packet transport system

- Internet packet arriving at a single computer
- Internet packet arriving at a router + multiple computers

Street Address = IP (Internet Protocol) Address (Unique)
Persons Name = IP Port Number (Not unique)

Person -> Who deals with the incoming package
Port Number -> Which program receives the packet

Router - Main Functions - 1

1. Allocate an IP address from a pool of special IP addresses that are excluded from use on the Internet (non-routable addresses)
These addresses typically start with 192.168.xxx.xxx

2. Perform network address translation on each out-going packet. That is:
- changes the return IP address of the local computer (192.168...) to the IP address of the router so that returning packets are sent to the router
- changes the return port number so that it identifies the source computer when the packet returns to the router

Router - Main Functions - 2

When packets return to the router, the reverse process occurs.
The IP address is translated from the routable address (the address of the router) to the local IP address of the originating computer (192.168.....).
The router is able to perform this translation because it kept a record of the port number it attached to the out-going packets

Summary - Network Address Translation (NAT)

The router translates the incoming:
Routable IP address + Port number

to

A non-routable local IP address and local port number

To do this, it maintains a table of those translations.

Note: This system was created by Cisco to extend the number of effective IP addresses beyond the number 255 X 255 X 255 X 255

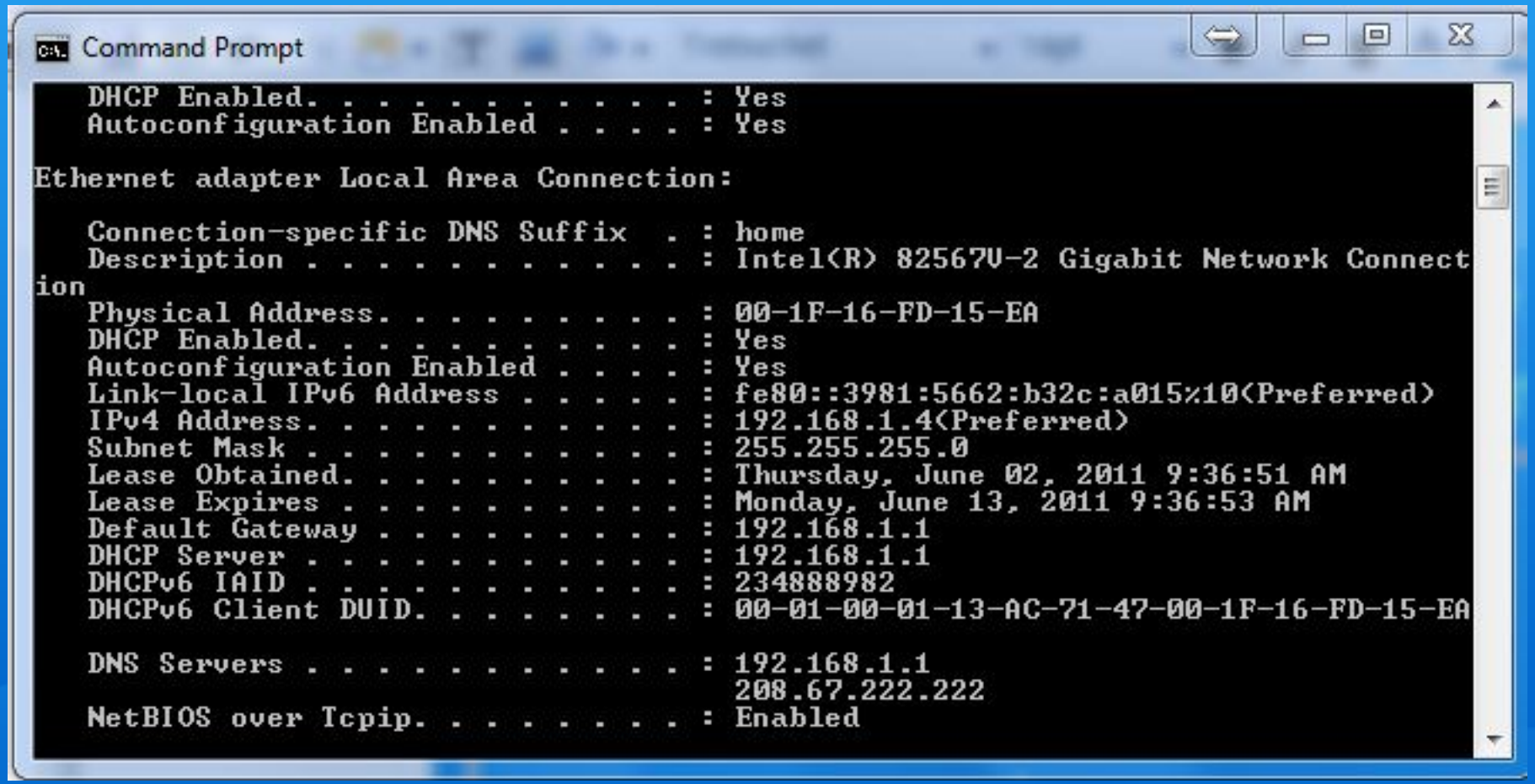
Some Simple Steps to Take

(if you loose your Internet connection)

- Turn off:
  - your computer
  - your router
  - your modem
- Restart in this order, your
  - modem
  - router
  - computer

Check if you have a real IP address (not 169.xxx.xxx.xxx) by using the ipconfig command. Open a command windows (the black background) like this:
Start -> Run -> type cmd hit Enter
Then at the priompt, type in the command: ipconfig /all and hit Enter

Example of ipconfig output



Some Networking Commands to Play with

net
ipconfig
hostname
ping
netsh
netstat
nbstat

Useful Links

Port Numbers:
http://en.wikipedia.org/wiki/Port_number

In computer networking, a **port** is an application-specific or process-specific software construct serving as a communications endpoint. It is used by transport protocols of the Internet Protocol Suite, such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). A specific port is identified by its number, commonly known as the **port number**, the IP address with which it is associated, and the type of transport protocol used for communication.
Transport Layer protocols, such as TCP and UDP, specify a source and destination port number in their packet headers. A port number is a 16-bit unsigned integer, thus ranging from 0 to 65535. A process associates its input or output channel file descriptors (sockets) with a port number and an IP address, a process known as *binding*, to send and receive data via the network.

How NAT works - Cisco

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

Open DNS

http://www.opendns.com/start/

http://www.opendns.com/support/kb/

Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,
image/png,*/*;q=0.5 Accept-Language: en-US,en;q=0.8 Connection: keep-alive Host:
www.grc.com Referer: http://www.grc.com/x/ne.dll?rh1dkyd2 User-Agent: Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.
0.696.77 Safari/534.24 Cookie: tpag=l2wwe2i51ndk2; ppag=l2wwe2i51ndk2;
tcss=l2wwe2i51ndk2; pcss=l2wwe2i51ndk2; tico=dxhaj1sjdjqot; pico=dxhaj1sjdjqot
Content-Length: 32 Content-Type: application/x-www-form-urlencoded Cache-Control:
max-age=0 Origin: http://www.grc.com Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
FirstParty: https://www.grc.com ThirdParty: https://www.grctech.com Secure: https:
//www.grc.com Nonsecure: http://www.grc.com Session: vvztzcbwst0ce

Packets - UDP and TCP

User Datagram Protocol (UDP)

The Transport Layer of your network (OSI Layer 4) will typically utilize two major protocols to move information:

- **UDP** (User Datagram Protocol), which is documented in RFC 768
- **TCP** (Transmission Control Protocol), which is documented in RFC 793
- With network protocols such as UDP and TCP/IP, the packets range from 64 to 1,500 characters, or *bytes*.

UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS—UDP ports 1021/1022), Simple Network Management Protocol (SNMP—UDPports 161/162), Domain Name System (DNS—UDP port 53), and Trivial File Transfer Protocol (TFTP—UDP port 69)

End