

# Networks and Routing

Luis Giraldo



# IPv4 networking

- What makes up an IP packet
- Broadcast Domains
- Collision Domains



# IPv4 Packets



Header

Data

- Header
  - As small as 20 bytes
  - As large as 60 bytes including options (options rarely used)
- Data
  - As small as 0 bytes
  - Including header, as large as 65,535 bytes



# IPv4 Header

- Version (e.g. 4)
- Internet Header Length (IHL)
- Differentiated Services Code Point (DSCP)
- Explicit Congestion Notification (ECN)
- Total Length
- Identification
- Flags



# IPv4 Header (cont.)

- Fragment Offset
- Time to Live (TTL)
- Protocol
- Header Checksum
- Source Address
- Destination Address
- Options



# IPv4 Data

- Contents are interpreted based on the value of the Protocol header field
- List of Protocol Numbers
- Packet may be fragmented if MTU is exceeded
- If “more fragments” flag is set, or “fragment offset” is not zero, receiver knows packet is a fragment
- Receiver uses ID to find matching fragments



# Broadcast Domains

- A switched network uses MAC addresses on a LAN (broadcast domain), which allows devices to communicate with each other directly based on their MAC address, irrespective of whether a router is available or reachable.
- Switches keep info in MAC Address Table
- Computers keep info in ARP table
- ISPs and /30 nets



# Collision Domains

- Result from hub-based networks
- Is very inefficient (makes networks slow)
- Collisions resolved by CSMA/CD
- Switching with full-duplex eliminates collisions



# Routers

- How subnets and IP addresses define your LAN
- Function of a router in sending traffic to networks beyond the LAN



# Subnets

- Subnet = Sub-network
- Smallest Subnet = broadcast domain
- Subnet defines network/host bits
- Common subnet for small business or home networks: /24 (CIDR), or 255.255.255.0
- Consider smaller subnets when possible, to increase network performance.



# Smaller Subnets

- Example: Office of 25 users with 2-3 servers.
- Instead of a /24 (255.255.255.0) LAN, consider 2 x /25 (255.255.255.128) LANs.
- Network 1: 192.168.0.0/25
  - Hosts: 192.168.0.1 - 192.168.0.126
- Network 2: 192.168.0.128/25
  - Hosts: 192.168.0.129 - 192.168.0.254



# Subnet Mask Cheat Sheet

	Hosts	Netmask	Amount of a Class C
/30	4	255.255.255.252	1 / 64
/29	8	255.255.255.248	1 / 32
/28	16	255.255.255.240	1 / 16
/27	32	255.255.255.224	1 / 8
/26	64	255.255.255.192	1 / 4
/25	128	255.255.255.128	1 / 2
/24	256	255.255.255.0	1
/23	512	255.255.254.0	2
/22	1024	255.255.252.0	4
/21	2048	255.255.248.0	8
/20	4096	255.255.240.0	16
/19	8192	255.255.224.0	32
/18	16384	255.255.192.0	64
/17	32768	255.255.128.0	128
/16	65536	255.255.0.0	256



# Routing Beyond the LAN

- Do I know of this IP address?
  - If no, send packets to default route (0.0.0.0 0.0.0.0), which is typically the ISP's router.
  - Especially with RFC 1918 addresses, this is where NAT/PAT occurs - the internal network address is “translated” to the router's public IP address (as the source), which is “routable”.



# NAT

- Network Address Translation:
  - Internal “private” IP is translated to an external “public” IP, which can be routed.
- IPv4:
  - Assigns a public IPv4 address to a private (RFC1918) IPv4 address using one-to-many, one-to-one.
- IPv6 example
  - There is no NAT per se, since each device has a unique address. But uses a network prefix, provided by the ISP.



# IPv4 NAT

- Public IP Address of 1.1.1.1 assigned to my router, my router hands out private IPs on a local LAN (e.g. 192.168.0.0/24)
- Some routers support one-to-one NAT, where multiple public IPs being routed to my router can be “assigned” to multiple internal hosts.



# PAT

- Port Address Translation
- Is an extension of NAT, permits multiple devices to be translated to the same public IP address.
- PAT allows multiple connections to same external port (see Netstat output)



# IPv6 Networking

- Why IPv6 is necessary
- How an IPv6 address is constructed
- IPv6 via DHCP
- How to know if your public/private network is ready for IPv6



# Why is it necessary?

- IPv4 address exhaustion reached - IANA assigned last batch of /8 blocks.
- IPv4 was a “test”...(DARPA)
- Much larger address space
- Improved network management and routing efficiency



# IPv6 Address Construction

- 128-bit address consists of 8 groups of 4 hexadecimal digits separated by colons:
- 2001:0db8:0000:0000:0000:ff00:0042:8329
- Can be abbreviated by removing leading zeroes, and omitting consecutive sections of zeroes :
- 2001:db8::ff00:42:8329



# IPv6 Host Identifier

2001:0db8:0000:0000:0000:ff00:0042:8329



64-bit host identifier



# IPv6 Address Abbreviation

2001:0db8:0000:0000:0000:ff00:0042:8329

2001:db8::ff00:42:8329



# IPv6 via DHCP

- Hosts can auto-configure: Stateless Address Autoconfiguration (SLAAC) using NDP (Neighbor Discovery Protocol) - requires a /64 subnet, and leverages ICMPv6.
- Hosts can also obtain DHCPv6 address
- UDP Port 546 for clients, UDP 547 for servers
- Utilizes Prefix delegation at the gateway



# IPv6 via DHCP

- DHCP Unique Identifier (DUID) is used by client when requesting an address from a DHCPv6 server.
- IPv4: DORA (Discover, Offer, Request, Acknowledge)
- IPv6: SARR (Solicit, Advertise, Request, Reply)



# Is Your Network Ready?

- IPv6 is not interoperable with IPv4
- Runs in parallel to IPv4
- Can be tunneled inside of IPv4 for compatibility or using 6to4 (Teredo).
- Some free services can provide IPv6 tunneling, like Tunnel Broker.

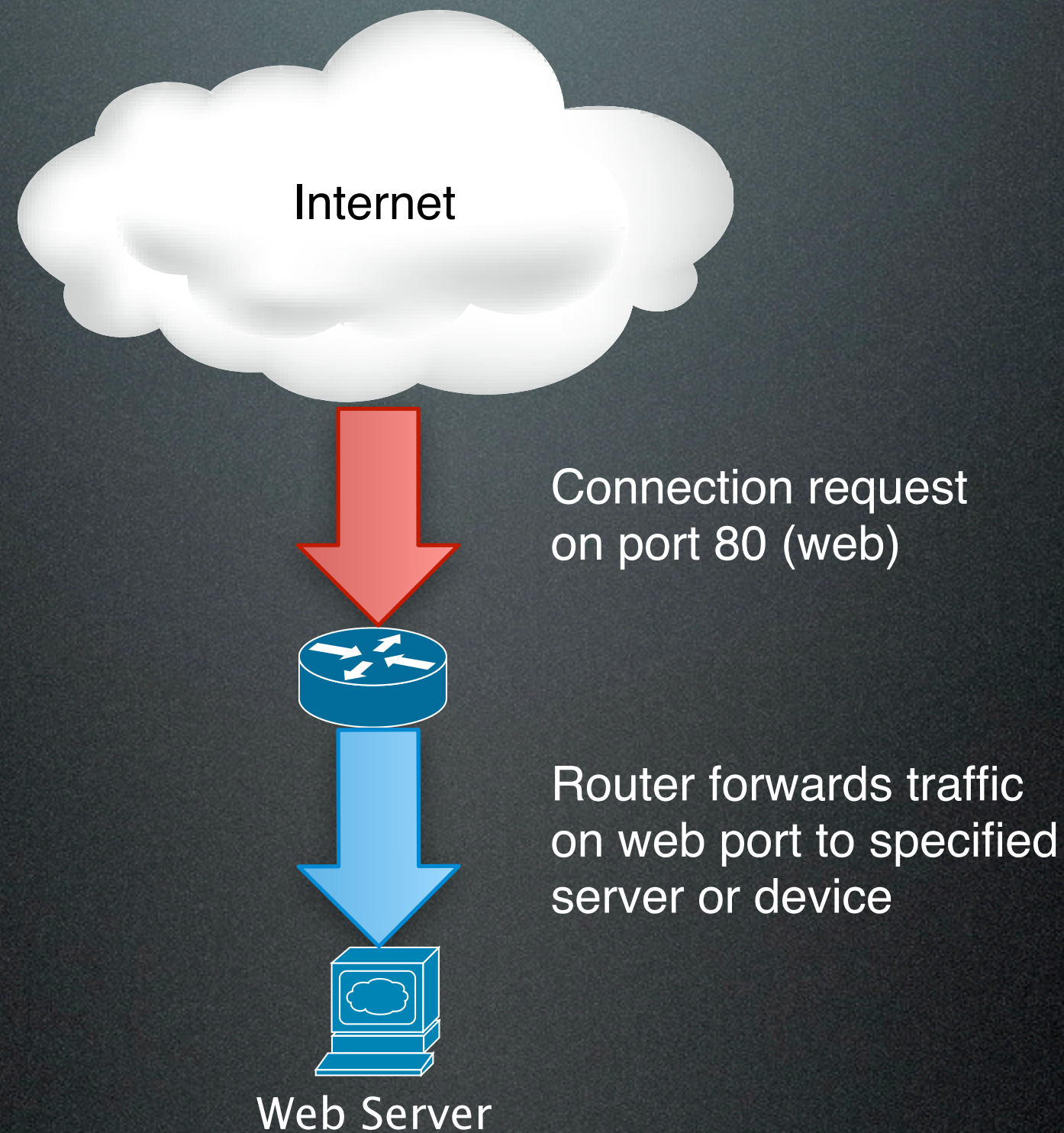


# Show a diagram of port forwarding

- Explain what port forwarding is while referencing your drawing or diagram
- Explain how to configure it on an Apple Airport Extreme Base Station, and another similarly priced or cheaper SOHO router of your choosing.
- Show the differences in the interfaces either with screen shots in your slides or by breaking out of your presentation and navigating to the interfaces live in real time (but be careful here, stuff breaks, and if it does while you are on stage you will need a back up plan), and also make note that the AEBS automatically handles several items for you, and is manageable from the ML Server App
- Also note that the AEBS port forwards and routes Mac OS X Server's VPN's perfectly, and many other vendors routers do not allow enough control to disable firewalls, enable GRE, or whatever else might be necessary to route your VPN or other custom traffic properly.



# Port Forwarding





# Port Forwarding (AEBS)

**Port Mapping Setup Assistant**

---

Choose a service from the pop-up menu or enter the public and the private IP address and ports that you want to map between.

Service:

Public UDP Port(s):

Public TCP Port(s):

Private IP Address:

Private UDP Port(s):

Private TCP Port(s):



# Port Forwarding (Linksys)

**LINKSYS®**  
A Division of Cisco Systems, Inc. Firmware Version: v1.42.2

**Wireless-G Broadband Router**

**Applications & Gaming** | **Setup** | **Wireless** | **Security** | **Access Restrictions** | **Applications & Gaming** | **Administration** | **Status**

Port Range Forward | DMZ

**Port Range Forward**

Port Range					
Application	Start	End	Protocol	IP Address	Enable
NPDS	8080	to 8080	TCP	172.16.3.25	<input checked="" type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>
	0	to 0	Both	172.16.3.0	<input type="checkbox"/>

[More...](#)

**Save Settings** **Cancel Changes**

**CISCO SYSTEMS**



# Port Forwarding (Meraki)

Description	Protocol	Public port	LAN IP	Local port	Allowed remote IPs	Actions
D-Link	TCP ▾	14972	10.12.35.29	80	any //	X
iBaby	TCP ▾	14971	10.12.35.35	14971	any //	X
Becker	TCP ▾	80	10.9.88.10	80	any //	X
SCEP	TCP ▾	1640	10.9.88.10	1640	any //	X
Becker443	TCP ▾	443	10.9.88.10	443	any //	X
Daylite1	TCP ▾	6180-6183	10.9.88.2	6180-6183	any //	X
Daylite2	TCP ▾	6185	10.9.88.2	6185	any //	X
Daylite3	TCP ▾	6188	10.9.88.2	6188	any //	X



# What I like...

- I've been using Cisco IOS-based, or Meraki appliances
- Meraki is dead-easy to work with for configuration
- Maximum stability, enterprise-grade feature sets
- Awesome technical support



# Cabling, patch panels and vendors

- Category 5, 5e and 6 defined and the practical differences explained.
- Talk about why you need to pay attention to the patch panels category rating.
- Talk about ways to test cables in the walls
- Talk about Fluke network testers, and why you should always use a dongle to test a cable, and not plug it directly into your \$700 tool. (A bad end that was poorly crimped can stretch out and ruin the connector in the tool)
- Consider whether making cables from scratch is a good use of your time, when it's possible to buy patch cables very inexpensively, or, for large installations, to outsource to a vendor who does cabling exclusively.
- Show a diagram of how to custom build a cable, bring your own crimp tool, cable and ends, and if possible use an iPad or some other camera on a mounted tripod to transmit what you are doing to the screen, so the audience can watch you make a cable.
- Make recommendations for your favorite cable tester, your favorite crimp tool, and talk about using sites like [monoprice.com](http://monoprice.com) to find great deals.



# Cat 5, 5e, 6

- Cat 5 is rated for 100 Mbit, Cat 5e is rated for 1 Gbit, Cat 6 is rated for 10 Gbit.
- Cat 5e has 100MHz of bandwidth, vs. 200MHz in Cat 6
- Cat 6 has better interference rejection
- Cat 6 will produce less errors and be less prone to noise
- Cat 6 is reverse-compatible with Cat 5/5e



# Patch Panel Ratings

- Same as with cabling, patch panel ports need to be rated for the type of bandwidth required.
- Since Cat 6 is backwards-compatible, my suggestion is to always install Cat 6-rated patch panels and cabling if possible, this way fixed cabling doesn't have to be replaced in the future when applications need the extra bandwidth.



# Network Testers

- Fluke testers are the best but are pricey
- Main features needed are:
  - Ability to find length at which there is a problem
  - Confirm that cable is wired properly
  - Certify the cable for the rating required (e.g. 10Mb/100Mb/1Gb/10Gb)



# To Make or Not to Make

- Not a good use of my time to make Ethernet cables, but sometimes needed if a replacement or custom length is required in a pinch
- Prefer to work with top-tier vendors for quality cabling (e.g. Belden, Tyco/Amp)
- Stay away from cheap cabling whenever budget allows



# To Make or Not to Make

- Orange-white first, brown last, and reverse blue splits the greens.

