Networking Basics

The 10k-foot overview

Josh Turiel, JH Turiel & Associates, Inc.
jht@jhturiel.net

Areas to cover

- Standards – who makes them?
- What's a network?
- Pre-Wireless
- Devices – Router/firewall, switch/hub
- The OSI 7-layer burrito
- Routing 101

Standards Bodies

- IEEE (physical and electrical standards)
  - 10BaseT, Gigabit Ethernet, 802.11n/WiFi, etc.
  - (http://standards.ieee.org/)
- IETF (protocol standards)
  - IPv4
  - IPv6 (you'll hear more later)
  - SMTP
  - DNS
  - All defined by the RFC process (http://www.ietf.org/about/standards-process.html)

What is a network?

- I have a simple definition:
  - "Any time two or more independent devices are connected using a shareable media to exchange information"

This means one Mac and an Apple TV in a house equals a network.

So does a Fortune 500 company's gear. And everything in between.

Topology

- A network can take many forms
- Part of it can be wired, part wireless
- Can be extended over a distance
- Still uses a common *protocol* (almost always TCP/IP v4 nowadays)

Realistically…

- 99% of networks you will see are simple.
  - Single core switch
  - Runs to multiple drops throughout 1building
  - Some smaller switches at ends where presence needs multiplying (2 computers where 1 was wired for, computer + network printer, etc.)
  - Servers in central area
  - Single wireless AP (or more if needed for coverage)

About Wireless

- Wireless Access Points are typically used in larger networks or networks with an existing router (basically a bridge connecting wireless segment to LAN)
- I typically use Apple AirPort products as APs – easier to manage and very good performance
- Using a consumer wireless router in place of an AP is not usually a great idea (people will cover this later in detail)
- Be aware of coverage limitations

Wireless Alphabet Soup

- 802.11a=54Mb/s, 5GHz
- 802.11b=11Mb/s, 2.4GHz
- 802.11g=54Mb/s, 2.4GHz
- 802.11n=up to 600Mb/s, 2.4 & 5GHz
- Coming soon – 802.11ac (gigabit)

Device definitions (practical)

- A Router is the box that connects two different networks and translates between them. Best example is your network/Internet connection
- They usually have rudimentary security
- A firewall is easiest to imagine as a router with advanced security
  - Typically with the ability to set rules defining what to do with traffic and to manage multiple networks
- There is a lot of blurring of the lines at the SOHO level
- NAT is <u>not</u> a firewall!

Other devices

- Hubs are rarely used anymore. In a hub, every connection in the hub is physically part of the same network *segment*
  - As a result, they are much more congestion-prone
  - However, hubs are useful when you need to monitor traffic, since a station there can see all other traffic on the hub
- Switches divide each physical connection into a logical segment
  - Shunt traffic at high speeds between them

(continued)

- A switch can handle far more traffic than a hub, up to the limits it's *backplane* can process
  - More pricey switches generally have faster and/or expandable backplanes
  - Also, higher end switches can often be managed, allowing you to prioritize traffic by type or split into multiple VLANs (virtual LANs) where ports can be separated from one another.

mmm, Burritos…

- Back in the olden days when all protocols were proprietary (AppleTalk, NetBEUI, IPX, Vines, etc.), standards bodies lived in terror.
- The ISO (International Standards Organization) came up with a master protocol of their own, dubbed OSI (Open Systems Interconnection). They defined it using a *7-layer model*).
- What became of this? Well, OSI was a failure. TCP/IP became the global network standard with the rise of the Internet. All the others faded away, too. But the 7-layer model remains.

The OSI Model

- Layer 1: Physical
- Layer 2: Data Link
- Layer 3: Network
- Layer 4: Transport
- Layer 5: Session
- Layer 6: Presentation
- Layer 7: Application

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

I believe the model is too broad

- Almost anything can be defined using a 7-layer model. For instance, the Taco Bell 7-layer burrito:
- Layer 1: Refried beans
- Layer 2: Rice
- Layer 3: Lettuce
- Layer 4: Tomatoes
- Layer 5: Guacamole
- Layer 6: Cheese
- Layer 7: Sour Cream

(I'm not the first to tread this ground)

Or, if that doesn't work:

- Layer 1: 2 All Beef Patties
- Layer 2: Special Sauce
- Layer 3: Lettuce
- Layer 4: Cheese
- Layer 5: Pickles
- Layer 6: Onions
- Layer 7: Sesame Seed bun

There is a point to this…

More realistically:

OSI Model	TCP/IP Model (DoD Model)	TCP/IP – Internet Protocol Suite
Application	Application	Telnet, SMTP, POP3, FTP, NNTP, HTTP, SNMP, DNS, SSH, …
Presentation		
Session		
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, ARP, DHCP
Data Link	Network Access	Ethernet, PPP, ADSL
Physical		

IP Addressing

- Every device has an address. Along with that are:
  - *Subnet Mask* – the string that defines how large a subnet is
  - *Broadcast Address* – a special address that reaches all devices on the subnet
  - *Gateway Address* – the address of the router that will send traffic away from the subnet

This will be covered in-depth in the next session.

So in the end

- TCP/IP can be pretty much defined for practical matters with a 4-layer model
- The 7-layer model makes a useful computer science reference, but is too generic for my liking
- Wired/wireless, cable, DSL, cellular, all fall in Network Access layer
- Client/Server services run in the Application layer
- And all this will come in-depth as the day progresses!