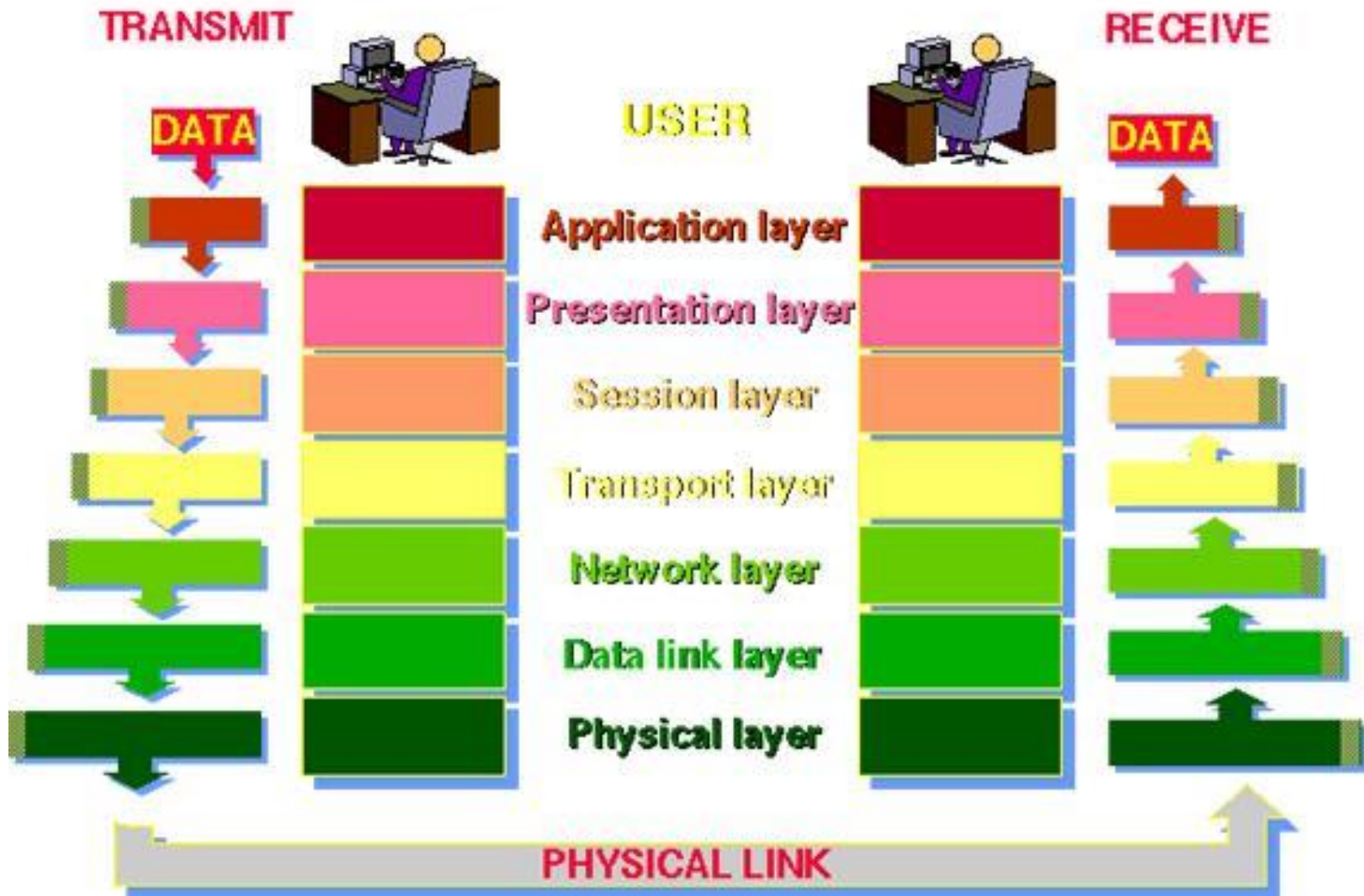# Basic Networking
For The Radio Amateur

Scott Honaker, N7SS

What is a Network?

- A **network** connects computers, mobile phones, peripherals and even IoT devices.

- Switches, routers, and wireless access points are the essential **networking components**.

- Through them, devices connected to your **network** can communicate with one another and with other **networks**, like the Internet.

THE 7 LAYERS OF OSI

TRANSMIT   USER   RECEIVE

DATA   DATA

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data link layer
Physical layer

PHYSICAL LINK

4

OSI Model
7. Application layer
NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet, DHCP, Netconf, etc.
6. Presentation layer
MIME, XDR
5. Session layer
Named pipes, NetBIOS, SAP, PPTP, RTP, SOCKS, SPDY, TLS/SSL
4. Transport layer
TCP, UDP, SCTP, DCCP, SPX
3. Network layer
IP, IPv4, IPv6, ICMP, IPsec, IGMP, IPX, AppleTalk, X.25
2. Data link layer
ATM, ARP, SDLC, HDLC, CSLIP, SLIP, GFP, PLIP, IEEE 802.2, LLC, L2TP, IEEE 802.3, Frame Relay, PPP, X.25
1. Physical layer
EIA/TIA-232, ITU-T V-Series, SONET/SDH, DSL, IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, USB, Bluetooth, RS-232, RS-449

Network Components

- Hubs/bridges
- Switches
- Routers
- Access points

Hubs and Bridges

- **Moves ALL traffic to ALL ports**
  - OSI Layer 1
- **Allows connecting machines together (provides crossover)**
  - Note Uplink Switch
  - Changes MDIX to MDI

Network Switches

- Moves packets between ports based on MAC address
  - OSI Layer 2
- Traffic only flows on necessary ports
- Lights indicate speed
- Auto-MDIX
- Managed or unmanaged
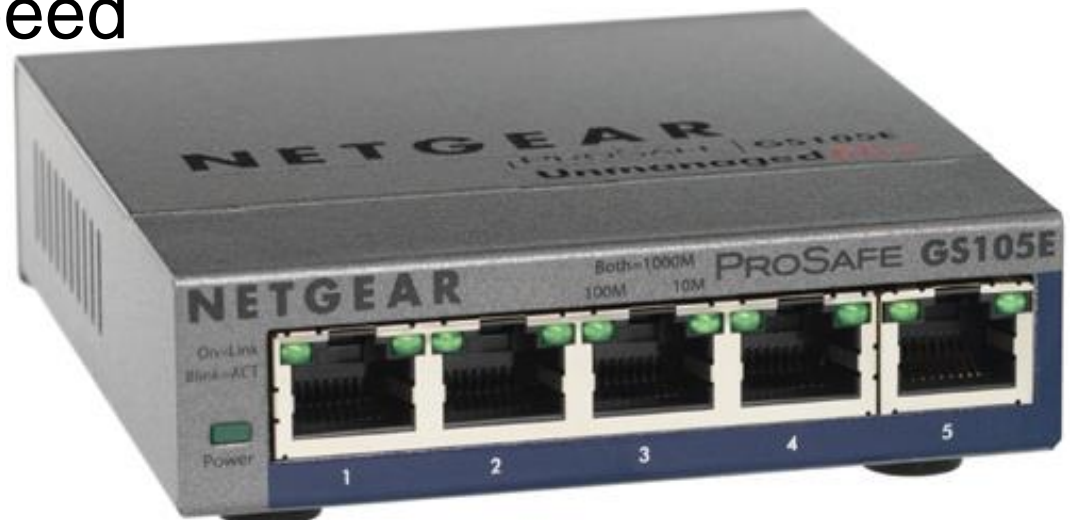
Router/Gateway

- Moves data packets between IP networks
  - OSI Layer 3
- Often have dedicated WAN ports
- Many include LAN switches
- Generally include firewall
- Often have DMZ port

Wireless Access Points

- **Moves data between wired and wireless networks**
  - OSI Layer 2
- **Multiple antennas offer diversity**
- **Modern units support simultaneous dual band and beam forming**

What is this?

- Antennas say wireless access point
- One yellow jack says router
- Four black jacks says network switch
- USB jacks means it includes a file server or NAS function

Network Technologies

- **Wired**
  - 10Base-T, 100Base-T, 1000Base-T
  - Power over Ethernet (PoE)
- **Wireless**
  - Wireless Standards
  - Wireless Channels
  - Wireless Encryption

Ethernet Physical Layer

- **10BASE-T (10MBit, Baseband, Twisted Pair)**
  - Category 3 or 5 network cable
  - 2 pairs required
  - 100 meter maximum length
- **100BASE-TX (Fast Ethernet)**
  - Category 5 network cable
  - 2 pairs required
- **1000BASE-T (Gigabit Ethernet)**
 - Category 5e or 6 network cable
  - 4 pairs required

Power over Ethernet (PoE)

- Used to power access points, cameras, IP phones, sensors, etc.
- Typically 25w at 44-48 volts available
- PoE capable switch or power injector required to supply power to cabling
  - May cause issues with some devices
- Equipment room and Command Vehicles have PoE switches

Wireless Standards

- 802.11a – 54Mbs at 5.8Ghz

- 802.11b – 11Mbs at 2.4Ghz

- 802.11g – 54Mbs at 2.4Ghz

- 802.11n – 54-600Mbs at 2.4 and 5.8Ghz

- 802.11ac – Up to 1Gbs at 5.8Ghz

2.4 GHz Wireless Channels
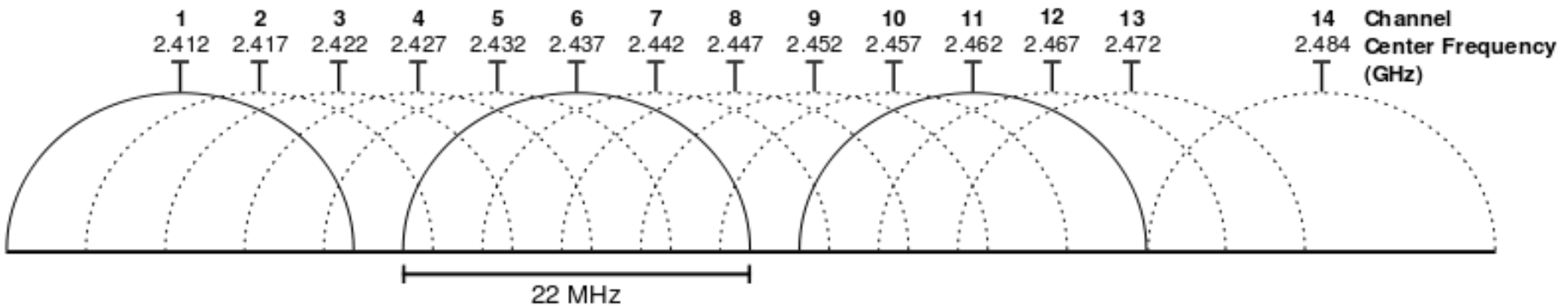
- 802.11b and g use overlapping 22MHz wide channels at 2.4GHz

- Full speed 802.11n needs 40MHz wide channel

- Channel 14 only available outside USA

- 5.8Ghz offers 21 non-overlapping channels

Wireless Encryption

- WEP, WPA and WPA2 encryption
  - WEP uses key of 10 or 26 hexadecimal digits
  - WPA key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters

Who Am I?

- ## MAC address
  - 3C-A9-F5-36-1F-0C

- ## LAN address
  - IP version 4 (IP V4) – 192.168.1.100
  - IP version 6 (IP V6) – 2601:601:9100:2d80:9cd0:8c87:513e:4bfa

- ## WAN address
  - IP V4/IP V6

IP version 4

- Four octets offer 4 billion addresses
  - Why would we need any more?
- Common "private" IP ranges
  A. 10.0.0.0 - 10.255.255.255 (16,777,216 addresses)
  B. 172.16.0.0 - 172.31.255.255 (1,048,576 addresses)
  C. 192.168.0.0 - 192.168.255.255 (65,536 addresses)
- "Loopback" address – 127.0.0.1

Subnets and Gateways

- Subnet mask determines number of addresses available on network
  - 10.0.0.1/255.0.0.0 – 16 million
  - 172.16.0.1/255.255.0.0 – 65 thousand
  - 192.168.1.1/255.255.255.0 – 254
- Even devices on the same wire can't communicate without compatible addresses
- Default Gateway is path to other networks (Internet)

Static vs. DHCP

- Assigning static addresses is tedious and inflexible
- Dynamic Host Configuration Protocol allows addresses to be assigned automatically
- "Reservations" can be made on DHCP server
- DHCP offers an address "lease" time

Domain Name System (DNS)

- DNS converts host name to IP address
- PING commacademy.org
  - Pinging commacademy.org [206.130.100.208] with 32 bytes of data:
 - Reply from 206.130.100.208: bytes=32 time=51ms TTL=55

Network Tools

- **Command line**
  - PING – Check device status
  - IPCONFIG /ALL – View network configuration
- WhatIsMyIP.com – Find WAN address
- FING, Advanced IP Scanner – Scan network
- NMAP – Network mapper
- Router web interface generally offers a useful status screen and tools

Network Status Example

- WAN IP (Internet) 50.158.76.27

- LAN IP (Intranet) 192.168.1.101

- Subnet Mask 255.255.255.0

- Router/Gateway 192.168.1.1

- DHCP Range 192.168.1.100-199

- Access Point 192.168.1.250 (Static/Reservation)

- Switches 192.192.1.240, 192.168.1.241 (Static)

Network Map Example
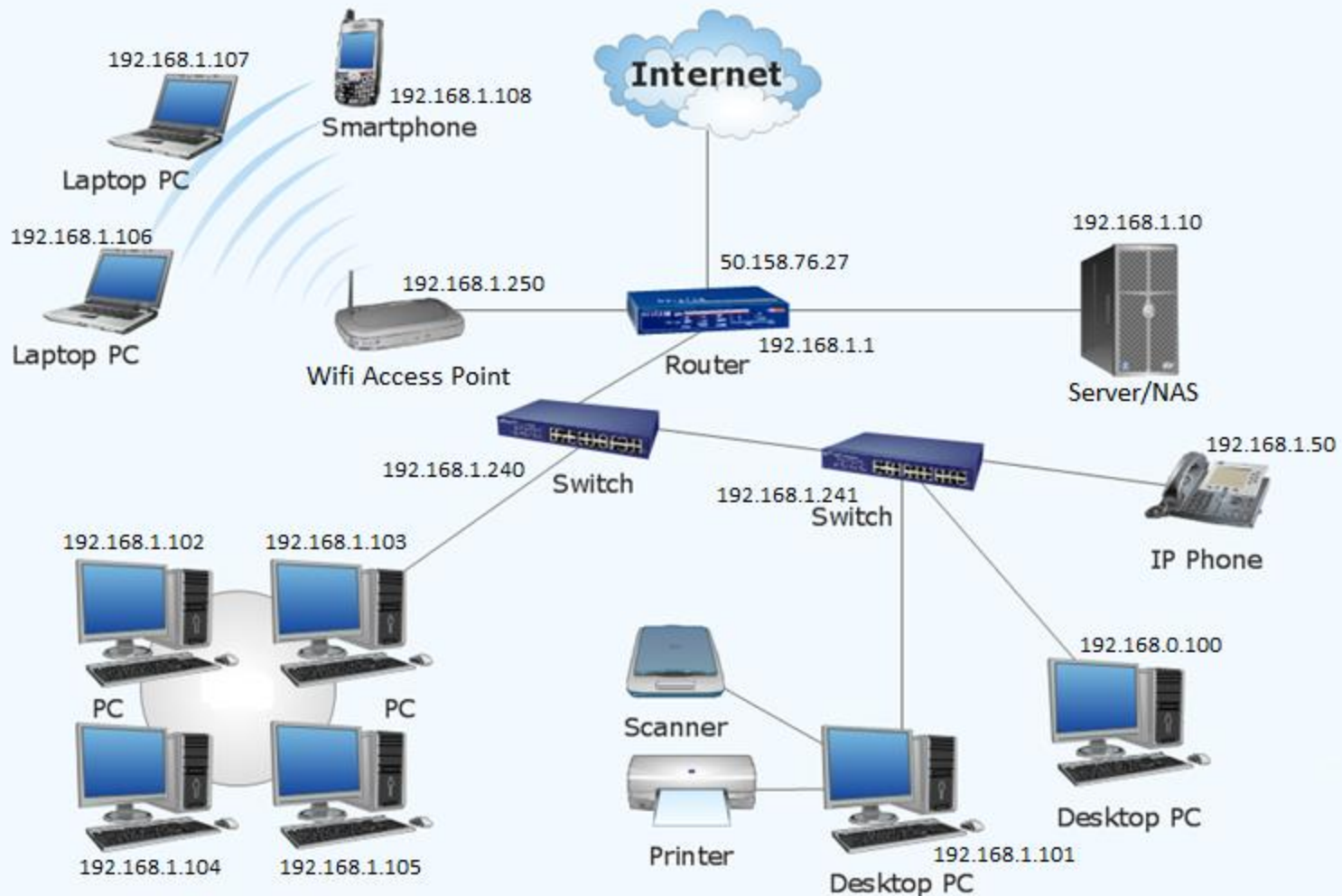
Ports

- A port is associated with an IP address of a host and the protocol type of the communication.

- Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the **port number**.

- Specific port numbers are commonly reserved to identify specific services.

- The lowest numbered 1024 port numbers are called the well-known port numbers, and identify the historically most commonly used services.

Common Ports

Port	Protocol
20	File Transfer Protocol (FTP) data transfer
21	File Transfer Protocol (FTP) control (command)
22	Secure Shell (SSH), secure logins
23	Telnet protocol—unencrypted text communications
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	Hypertext Transfer Protocol (HTTP)
123	Network Time Protocol (NTP
194	Internet Relay Chat (IRC)
443	Hypertext Transfer Protocol over TLS/SSL (HTTPS)
3389	Remote Desktop Protocol (RDP)

Opening Ports in Firewall

- Accessing web servers, remote desktop or other services remotely requires opening the port

- The router needs to know the port number and the LAN address to send the traffic

- The local (Windows) firewall needs to be opened to allow the traffic

- Other (virus) scanners may also need to be opened

Remote Desktop Protocol (RDP)

- Remote Desktop Server built into Windows
- Remote Desktop Client also included
- Effectively remotes the keyboard, video, mouse over encrypted channel
- When accessing via Internet, needs a fixed name/address
- Must open a port in the firewall (3389)

TeamViewer

- Teamviewer is a good alternative to RDP
- Basic service is free
- Uses a central server so no open firewall port
- Install on client and host machine
- Just supply ID and password to connect
- www.TeamViewer.us

Questions?