

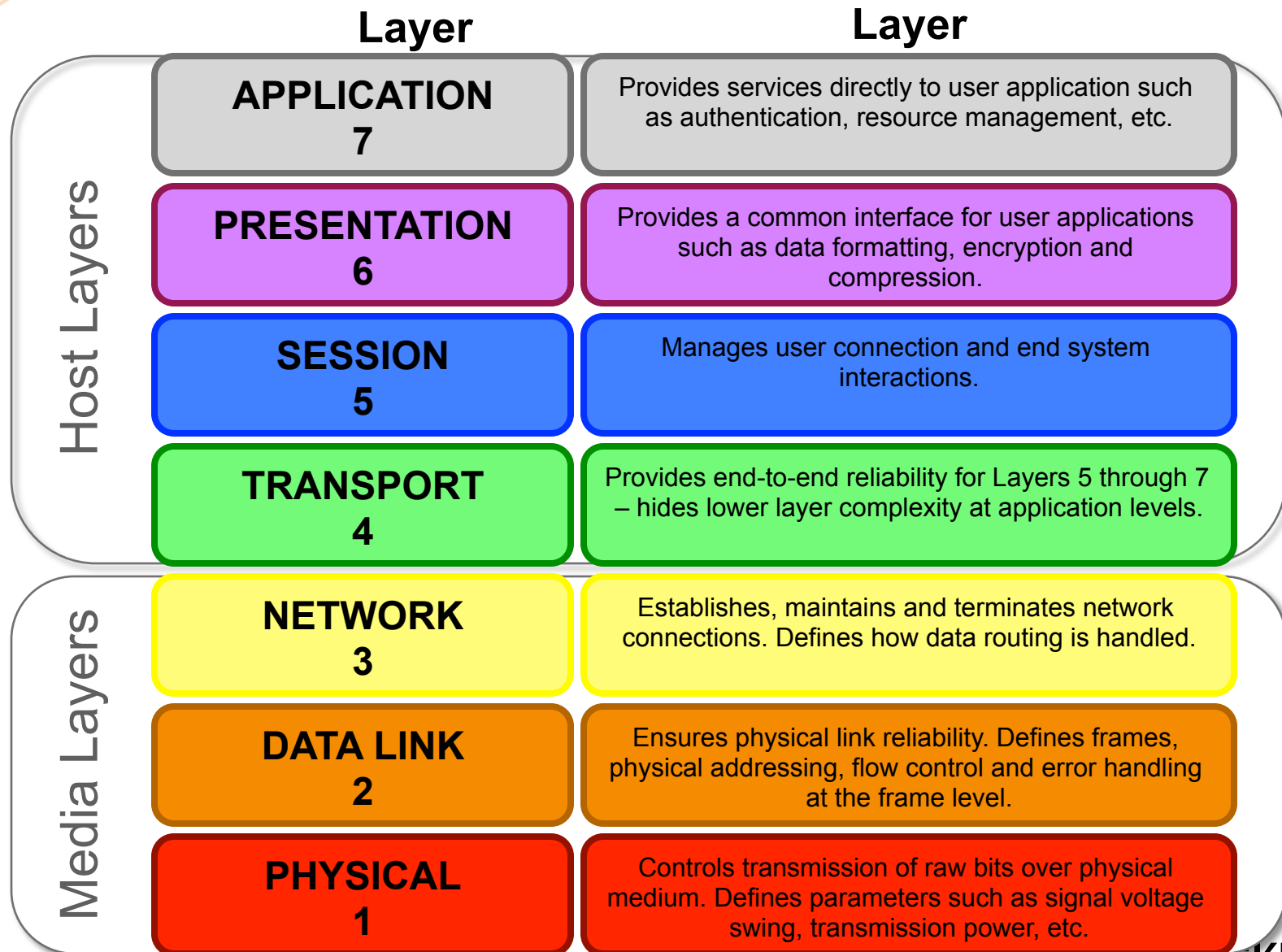
Networks & Routing

Jeanette Lee

Ruckus Wireless, Inc.

jlee@ruckuswireless.com

What's in a Network? OSI Model





Internet Protocol (IP)

- Suite of protocols works at Layer 2/3/4
- IP = L2/3
- User Datagram Protocol (UDP)/IP – L4
 - Stateless
 - Best effort with minimum of error check and no retries
- Transmission Control Protocol (TCP)/IP - L4
 - Reliable, ordered transmission with error checking and retries
- Ports are numbered and associated with a service, e.g. DNS, HTTP, etc.
 - Can be UDP or TCP (often support both)
 - Check /etc/services file on your Mac!

Common Network Addressing (L2)

- Media Access Control (MAC) address
- Unique 6 octet physical address of the network interface
- First three identify the Organizationally Unique Identifier (OUI) assigned by IEEE
 - <http://standards.ieee.org/develop/regauth/oui/public.html>
 - E.g. C4:10:8A:01:02:03 = Ruckus Wireless
- All FFs equals broadcast (all hosts) –
FF:FF:FF:FF:FF:FF

Common Network Addressing (L3 IPv4)

- Internet Protocol version 4 (IPv4)
- 32-bit address (4 dot decimal notation, 0-255)
 - Public IP networks (unique)
 - Private IP networks (not unique, require NAT for Internet access)
- Consists of a network portion and a host portion
 - Network – identifies one or more subnets within the range
 - Host – identifies individual host addresses
- Private networks defined by RFC 1918
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255
- All others are public

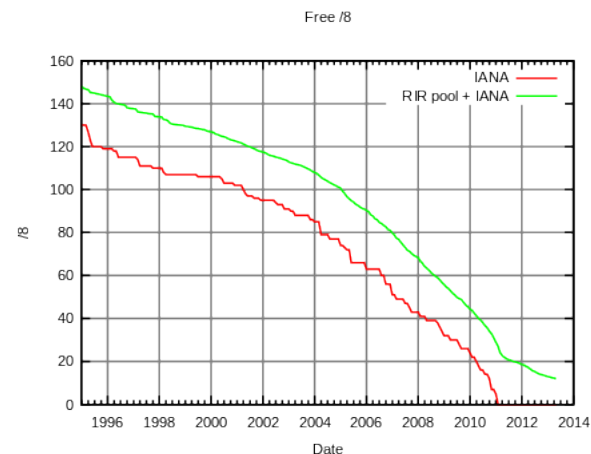
IPv4 Network Classes

Class	Leading bits	Network bits	Host bits	# of networks	Addresses per network	Address range
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0 – 127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0 – 191.255.255.255
C	110	24	8	2,097, 152 (2^{22})	256 (2^8)	192.0.0.0 – 233.255.255.255
D	1110	--	--	--	--	224.0.0.0 – 239.255.255.255
E	1111	--	--	--	--	240.0.0.0 – 255.255.255.255

- **Unicast** – denotes a unique host
- **Broadcast** – denotes all hosts on L2 network
 - 255.255.255.255
- **Multicast** – group of 1 or more hosts (Class D)
- On January 31 2011, the last two unallocated class A networks were assigned

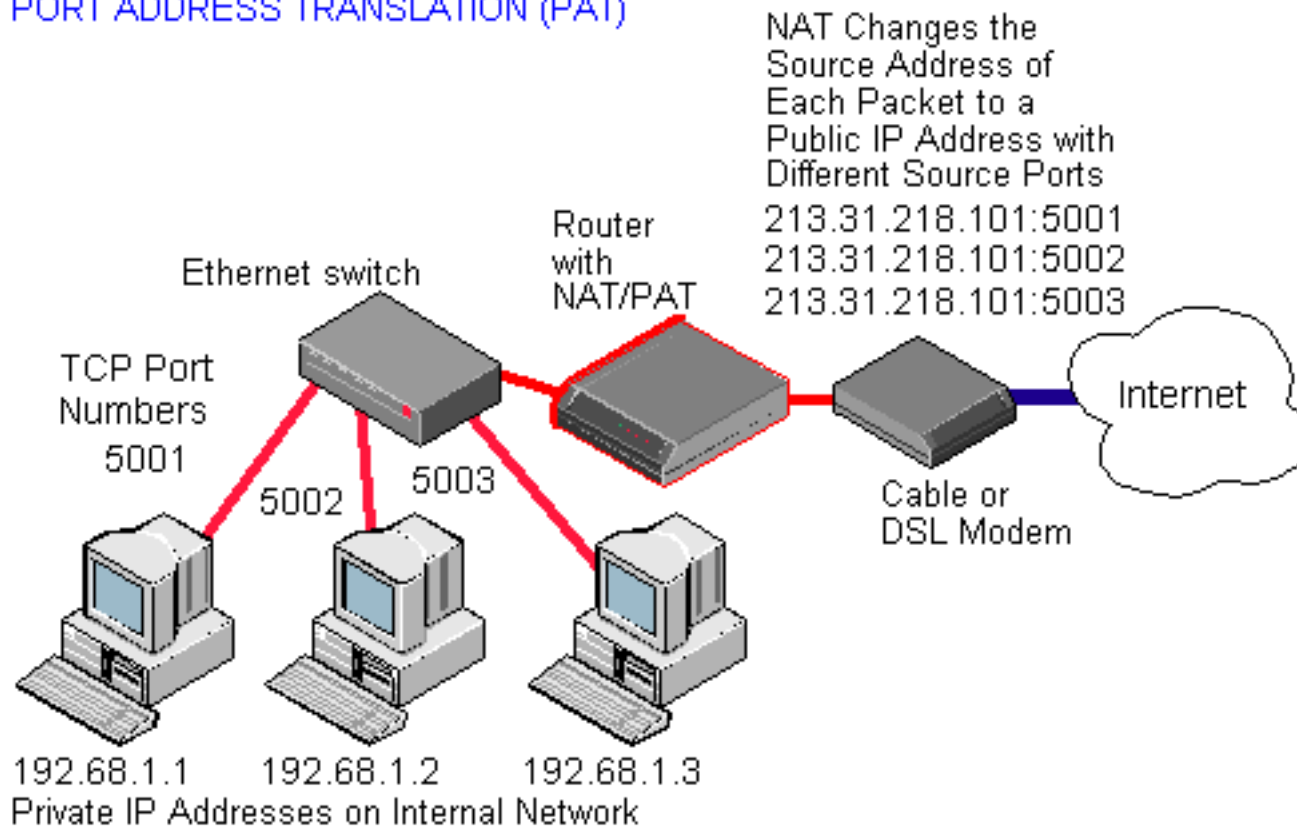
Network Address Translation (NAT)

- Allows a layer 3 device to “hide” a private network behind a single public IP address
- NAT device keeps a mapping of connections with internal hosts
- Outgoing connections only
- Many types of NAT, but Port Address Translation (PAT) is most common



Port Address Translation (PAT)

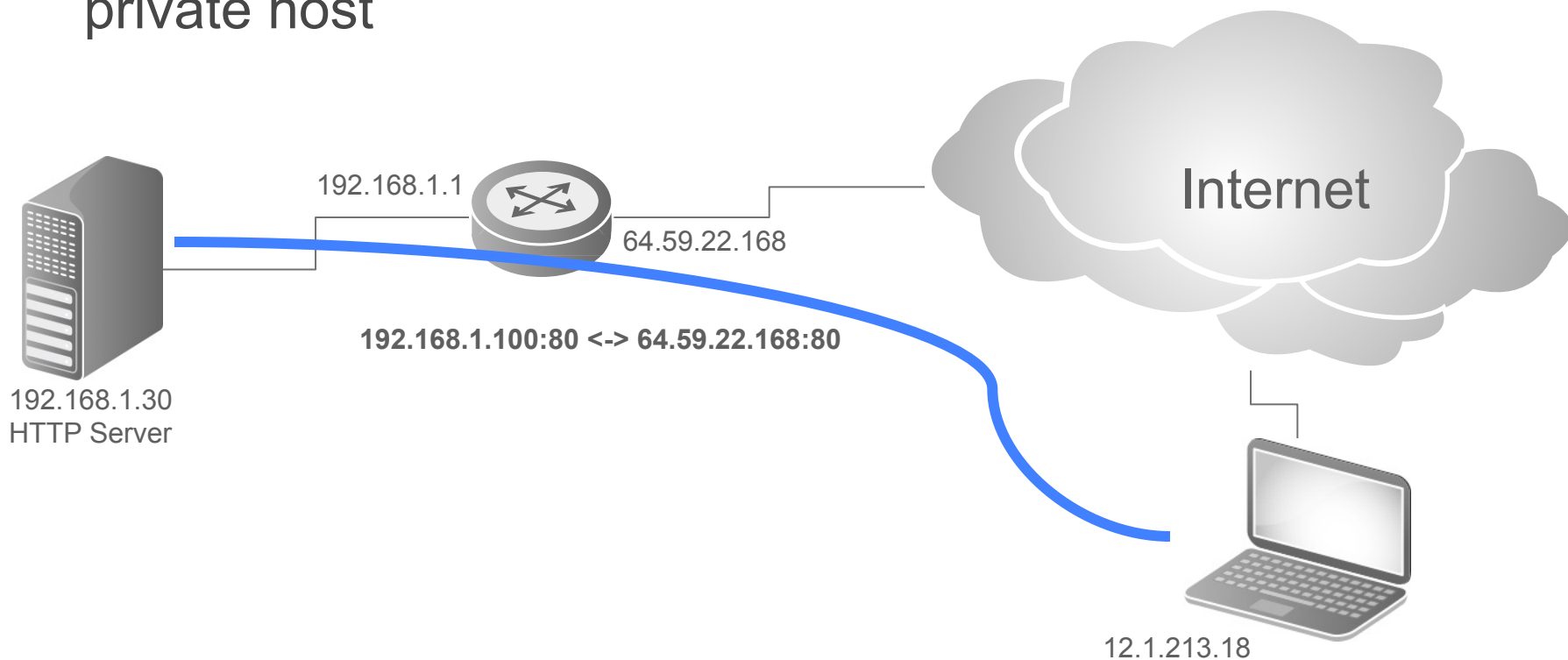
PORT ADDRESS TRANSLATION (PAT)



Avoid “double-NAT” at all costs!!! Breaks many apps!

Port Forwarding

- Simple way to allow incoming connections to a private-address host
- Ports on a public address are mapped to a service on a private host



Port Forwarding Example

The screenshot shows the 'Network' tab in the Ruckus Airport Extreme web interface. The 'Firewall Entry Type' is set to 'IPv4 Port Mapping'. The 'Description' is 'Personal Web Sharing'. The 'Public UDP Ports' and 'Public TCP Ports' are both set to '8080'. The 'Private IP Address' is set to '10.0.1.201'. The 'Private UDP Ports' and 'Private TCP Ports' are both set to '80'. A blue callout box points to the 'Private IP Address' field with the text: 'Your server's IP address – make sure it is statically assigned (no DHCP)'. At the bottom of the form are 'Cancel' and 'Save' buttons.

Base Station | Internet | Wireless | **Network** | Disks

Firewall Entry Type: IPv4 Port Mapping

Description: Personal Web Sharing

Public UDP Ports: 8080

Public TCP Ports: 8080

Private IP Address: 10.0.1.201

Private UDP Ports: 80

Private TCP Ports: 80

Cancel Save

Airport Extreme

1. Launch Airport Utility
2. Open Internet settings
3. Note your WAN IP address
4. Click Network
5. Make sure Router Mode is DHCP and NAT
6. Click the plus sign for Port Settings
7. Enter the ports for the service used outside your network
8. Enter the internal server IP
9. Enter the internal service ports
10. Save and restart

Your server's IP address – make sure it is statically assigned (no DHCP)

Cancel

Update



Routing vs. Layer 3 Switches

- Routers

- Typically dedicated box with WAN uplinks and a few LAN ports
- Support Internet routing protocols such as OSPF, IS-IS, etc.

- Layer 3 Switches

- No WAN ports
- Simple forwarding between local networks
- May support some basic routing protocols



Router/NAT Recommendations

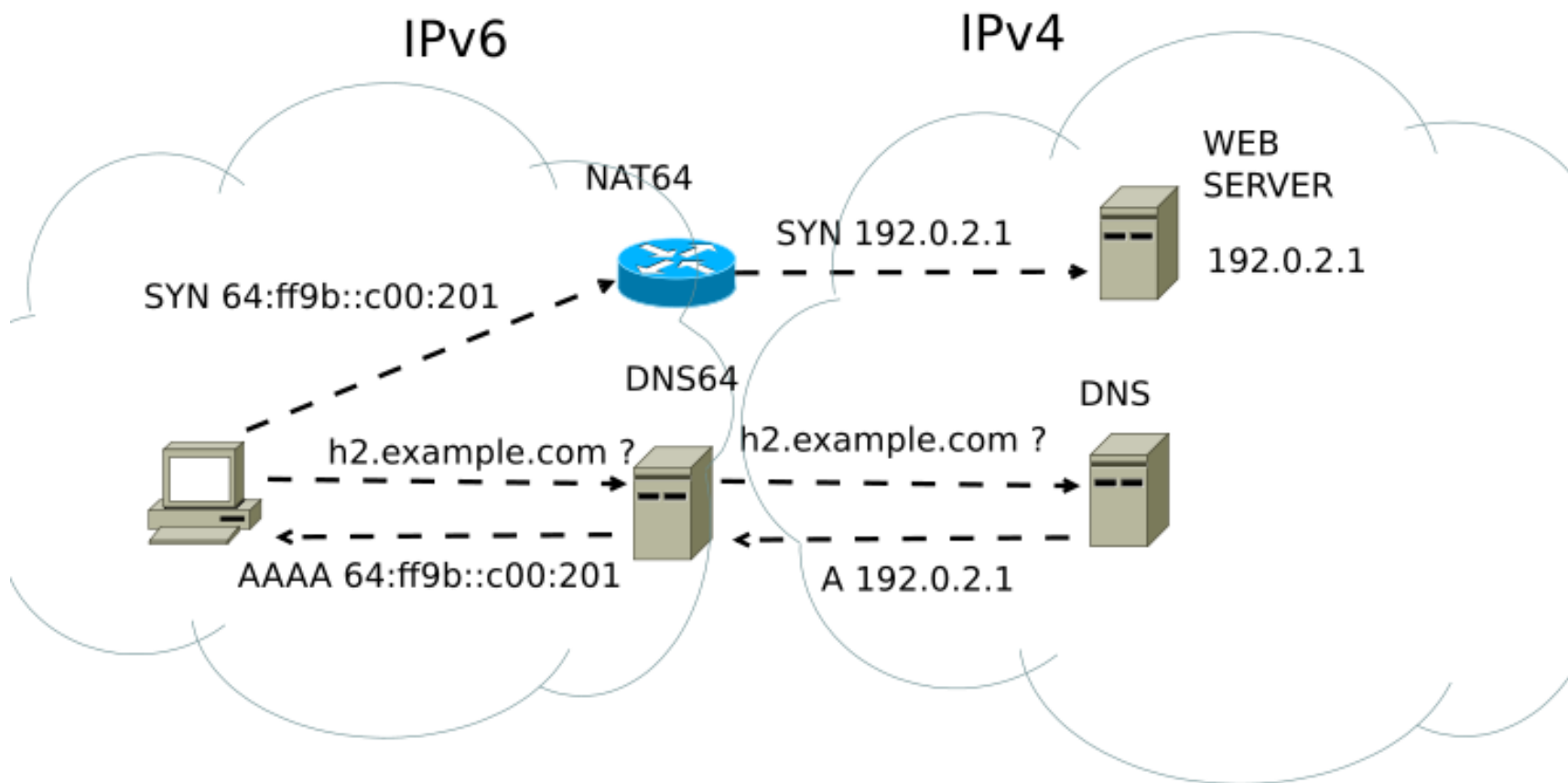
- There's a device for every budget
- Most home routers are adequate for home networking
- If you want to do more, features worth paying more for:
 - VLAN tagging – multiple networks w/routing or L3 forwarding
 - IPv6 support (6to4 and NAT64)
 - VPN server
 - QoS support
 - IDS/IPS
 - Gigabit Ethernet
 - Content filtering
- Airport Extreme – home/simple use only
- Cisco Small Business routers – the company that invented commercial routers, always a good choice

Next Generation IP (L3 IPv6)

- Fix IP address exhaustion of IPv4
- 128-bit address (8 groups of 4 hex)
 - 2001:0d8b:aa00:0042:aedf:01ee:cbdc:000a
 - All subnets are fixed 2^{64} addresses
- 2^{128} addresses or 3.4×10^{28} addresses per person for 10 billion people
- Dynamic address assignment
 - Stateful – DHCPv6 assigns address to client
 - Stateless – client chooses address based on advertisements
 - Stateless Autoconfiguration (SLAAC)
 - Built from Layer 3 64-bit subnet + MAC
- Not backwards compatible with IPv4

IPv6 and NAT64

- IPv4<->IPv6 translation
- Will require NAT64-capable device and DNSv6





IPv6 Readiness

- Impacts everything!!!

- Network

- Switches & routers
 - Clients

- Applications

- Everything

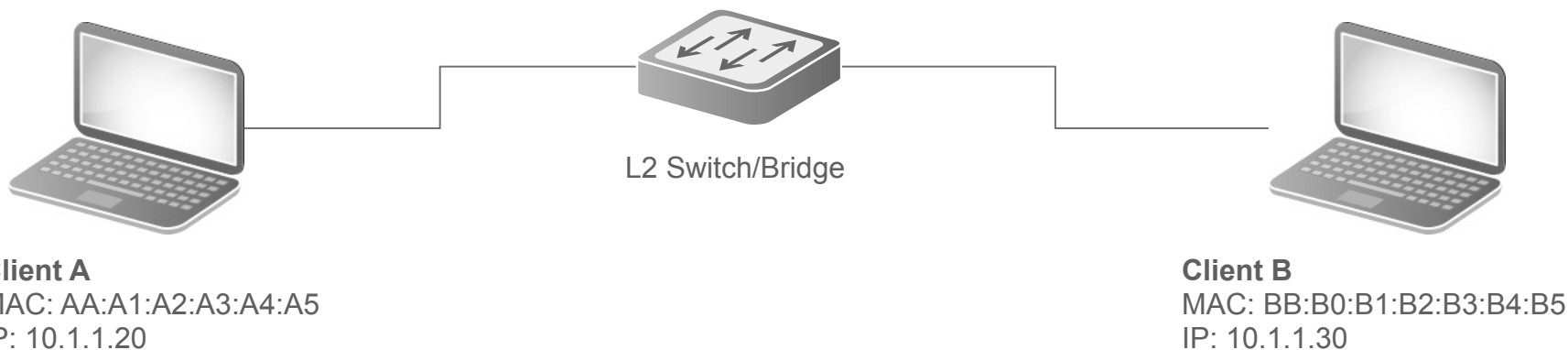
- Services

- DHCP
 - DNS
 - ...etc.

- Resources

- IPv6 ready list - <https://www.ipv6ready.org/db/index.php/public/>
 - Test your IPv6 connectivity - <http://test-ipv6.com/>
 - General info – <http://www.ipv6.com>
 - IPv6-ready routers - <http://www.sixxs.net/wiki/Routers>

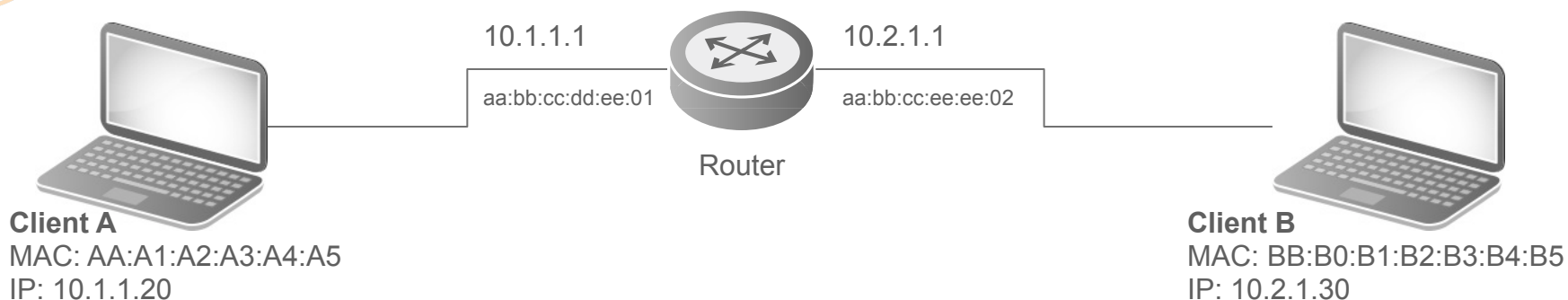
Follow a Conversation (Layer 2 IPv4)



1. ARP Broadcast:
I need to talk to 10.1.1.30 – who has this IP? →
2. I have the IP address 10.1.1.30!
My MAC is BB:B0:B1:B2:B3:B4:B5 ←
3. Unicast: Great! Here's some data! →

Source IP	Dest IP	Source MAC	Dest MAC	DATA
10.1.1.20	10.1.1.30	AA:A1:A2:A3:A4:A5	BB:B1:B2:B3:B4:B5	

Follow a Conversation (Layer 3 IPv4)



1. I need to send to 10.2.1.30
It's a different subnet, so
send to GW
ARP: Who has IP 10.1.1.1?
2. I have the IP address 10.1.1.1!
My MAC is aa:bb:cc:dd:ee:01
3. **ARP: Who has 10.2.1.30?**
4. I have the IP address 10.2.1.30!
My MAC is BB:B1:B2:B3:B4:B5
5. Great! Here's some data for 10.2.1.30!

Source IP	Dest IP	Source MAC	Source IP	Dest IP	Source MAC	Dest MAC	DATA
10.1.1.20	10.2.1.30	AA:A1:A2:A3:A4:A5	10.2.1.1	10.2.1.30	AA:BB:CC:DD:EE:02	BB:B1:B2:B3:B4:B5	

Red = broadcast
Blue = unicast



A Word About Subnets

- Excellent way to isolate traffic and devices
- A must have to separate Wi-Fi traffic from wired!
 - Reduce unnecessary traffic such as broadcasts
- Switch/router ports can be configured such that each port is a specific subnet
- OR, use VLANs to logically separate networks on the same physical LAN
- If you want hosts on different subnets to communicate, must have a router or L3 switch with ports on both subnets

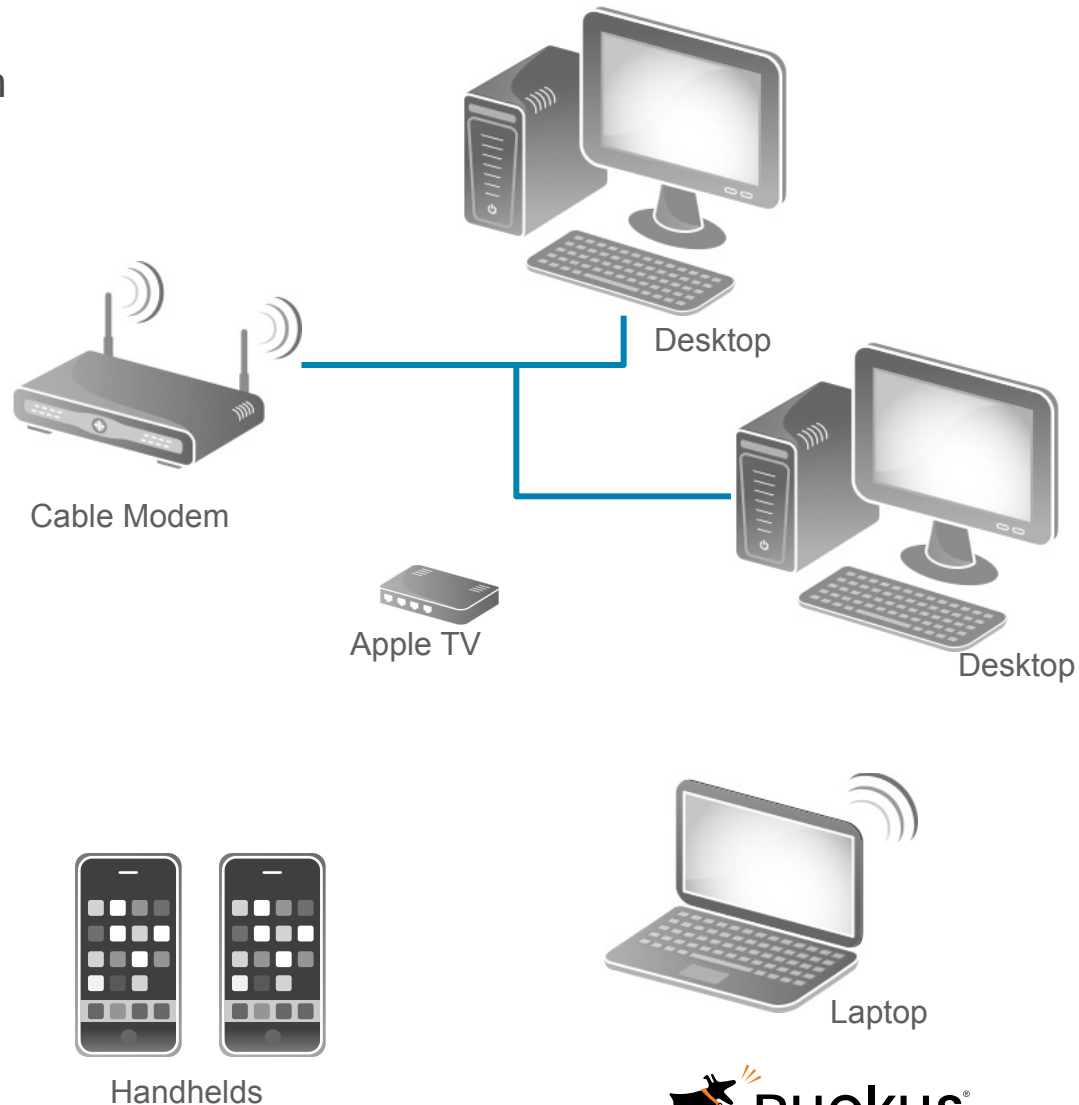


Cabling

- Most common:
 - Copper – CAT5, CAT5e, CAT6
 - Unshielded Twisted Pair, (UTP), Screened Twisted Pair (STP)
 - Differences mainly on shielding and amount of cross-talk
 - Fiber - multimode, single mode
- CAT5 – rated for up to 100 Mbps
- CAT5e – rated for up to 1 Gbps
- CAT6 – rated for up to 10 Gbps
- Fiber – speed of light (almost)
 - Terabits if you want it
- Fluke is the gold standard for cable testing equipment

Home Office Network

- Cable/DSL modem (possibly with integrated Wi-Fi)
- A few wired devices
- Some Wi-Fi devices
- No Ethernet switches
- Limited port forwarding



Small Office Network

- Cable/DSL modem or other CPE
- CPE may include router
- Ethernet switch(es)
- Wired servers
- Many Wi-Fi devices
- DMZ use
- VPN
- Multiple VLANs
- Guest access
- Advanced security

