Miscellaneous Network Topics

CSC 343·643

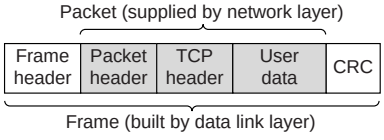
WAKE FOREST
UNIVERSITY
Department of Computer Science

Fall 2013

Network Device Review

- Variety of devices to transmit data from machine to machine
  - Consider the different types of devices using OSI model

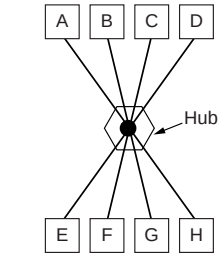
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub



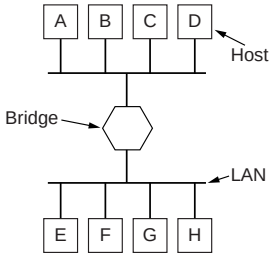
- Each device operates at a *certain level*
  - Level indicates the information used to switch/route

Hub, Switch, and Bridge

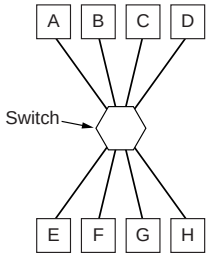
- Computers A-H are interconnected via a hub, bridge, or switch



Hub interconnecting machines



Bridge interconnecting machines



Switch interconnecting machines

- A hub is a **layer 1** device
  - Data sent by one machine is transmitted to all

    How does the hub utilize the physical layer header?

  - All the machines are on one *collision domain*

- A bridge is a **layer 2** device
  - A Bridge forwards frames from one LAN to another
  - Reads the frame destination address then forwards the frame

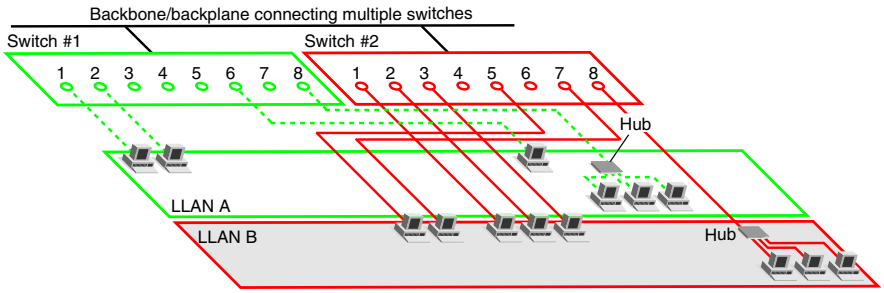
    What is the advantage compared to using a hub?

  - Each LAN is a collision domain
- A switch is a **layer 2** device
  - Forwards frames from one machine to another
  - Each port is a collision domain

    What is the advantage compared to using a bridge?

LAN Configurations

- Initially LANs were configured *geographically*
  - For example, a LAN was created per floor of a building
  - LANs were then interconnected via bridges
- An alternative is to configure LANs *logically*
  - Each computer network cable goes to a central site



  - Each LAN is a separate hub/switch located at the central site

- Allows LANs based on organizational (company) structure
  - All computers in a department on one LAN (Wake Forest)
  - Logical LAN allows this regardless of the physical location

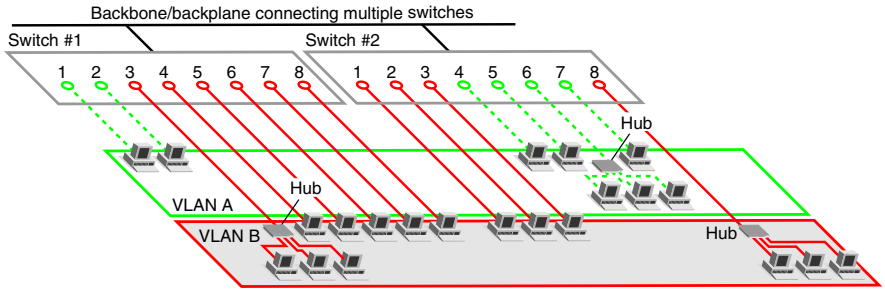
    Any other reason for using logical LANs?

    If the logical LANs are interconnected, is this any different than a single LAN? Are the advantages lost?

- The logical LAN provides flexibility and geographic independence
  - However to change the logical LAN a machine is connected to, requires *the system admin to walk to the closet, chase the correct cable, disconnect from the old hub/switch, find an open new port on the new switch, ...*

Virtual LAN

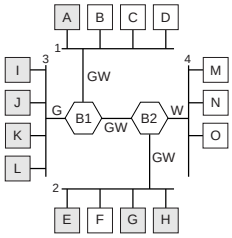
- Virtual LANs (VLANs) allow LAN changes in software
  - No physical connection changes
  - VLAN-aware switches configured to create VLANS



- Machines interconnected via VLAN-aware switches/bridges
  - System admin determines the number of VLANs desired
  - Frames forwarded to machines on the same VLAN

VLAN Bridge Example

- Assume 4 physical LANs interconnected via 2 VLAN bridges
  - 2 VLANs exist, White (W) and Gray (G)

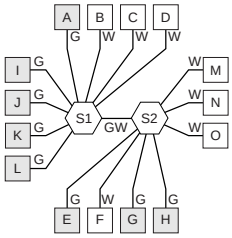


  - Each VLAN-bridge port has a color (possible more)
- Machine I broadcasts a frame (everyone on gray VLAN receives)
  - Bridge B1 forwards it to LAN 1 and bridge B2
  - Bridge B2 forwards it to LAN 2

    Will machines B, M, or F see the frame?

VLAN Switch Example

- Assume same 15 machines interconnected via 2 VLAN switches
  - 2 VLANs exist, White (W) and Gray (G)



  - Each VLAN-switch port has a **single** color
- Assume machine A broadcasts a frame
  - Switch S1 forwards it to machines I, J, K, and L, and switch S2
  - Switch S2 forwards it to machines E, F, and G

    What is the advantage over VLAN-aware bridges?

VLAN Switches and Bridges

How does the VLAN switch know the color of a frame?

1. Associate a color with every VLAN-switch/bridge port
   - When a frame arrives on the port, it is given that color

     Any problems?

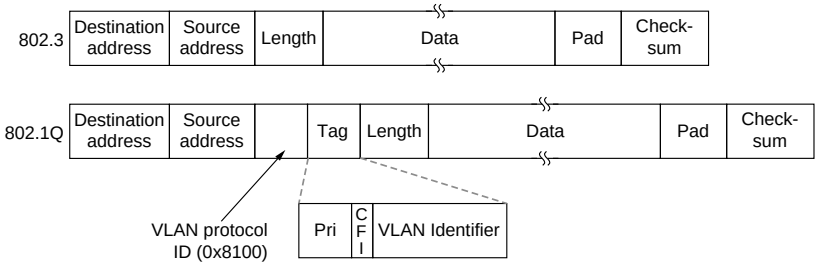
2. Every MAC address is assigned a VLAN color
   - Keep a table of MAC addresses and the associated color

     Can we mix VLANs on the same physical LAN?
3. Layer 3 address (IP) is assigned a VLAN color
   - Switch examines the payload of the frame, then assigns a color
   - **Violates** a fundamental rule of networking!

Regardless of the method, determining the color must be done quickly!

IEEE 802.1Q

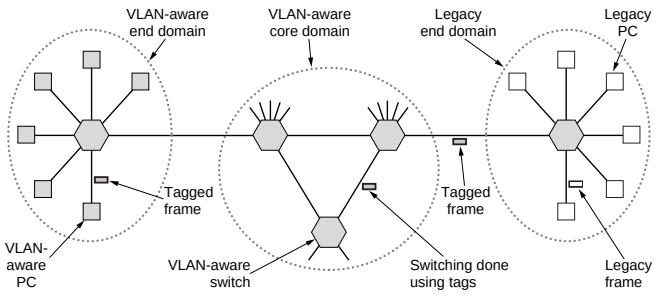
- To minimize delay, need to quickly determine the frame color
  - Previous two methods required a table look-up operation
  - Best solution is to have the source (generating the frame) assign the color and store the color in the frame
- IEEE 802.1Q defines the VLAN aware frame
  - A new frame format that stores the VLAN identifier (color)



A new frame format? Are existing Ethernet cards now obsolete?

Legacy and VLAN-Aware Ethernet

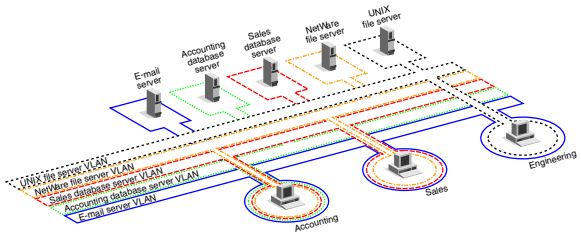
- Legacy Ethernet cards can exist in a 802.1Q VLAN network
  - The VLAN-aware switch is responsible for altering the frame
  - Does require a table look-up operation...



- The *hope* is that new Ethernet cards will incorporate 802.1Q
  - For example gigabit Ethernet cards are 802.1Q compliant

VLAN Objectives

- VLANs allow a network to be broken into smaller pieces
  - VLANs are smaller parts of an existing LAN



- Switches forward (*or should we say route...*) frames
  - Forwarding decisions are based on the VLAN color
  - Broadcast frames only seen by members of same VLAN

  Where have we seen this functionality before? Why use layer 2 instead of layer 3?

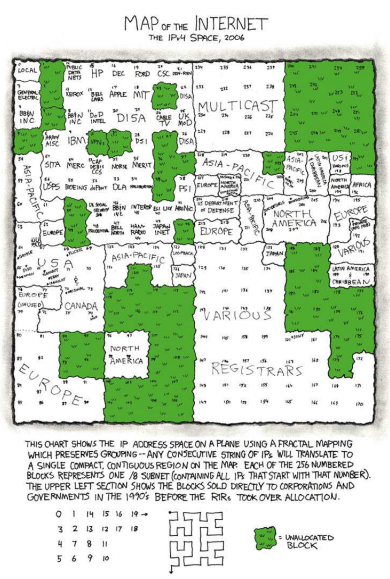
IP Address Management

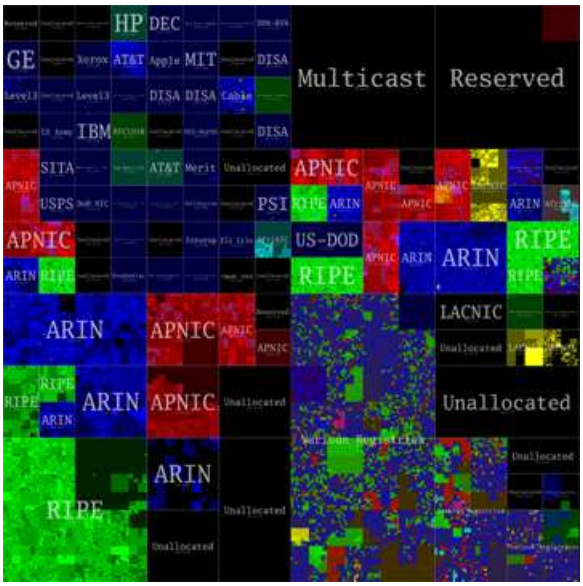
- A small LAN needs access to the Internet, *how can this be done?*
  - Every device that accesses the Internet needs a unique address
  - *Buy a class B or C address?*
  - *Contract with an ISP for an address block?*

  What are the issues with the previous two methods?

- It has been reported that IP addresses are scarce
  - *There are debates about the IPv4 address shortage*
  - IPv6 is supposed to resolve this issue, but...
- Need methods for *sharing* IPv4 addresses

IP Address Map





- Visualizing the Internet is challenging, but XKCD did a reasonable job

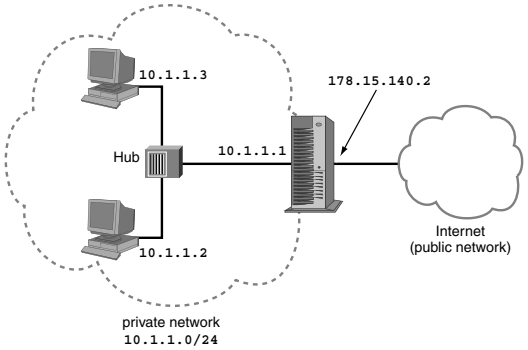
Network Address Translation

- Network Address Translation (NAT) [RFC 2663, 3022]
  - Originally proposed for the IPv4 address solution
  - Maps one network address to another (address sharing)
- **Private** and **public** networks
  - Private network devices do **not** access the Internet directly
  - As a result, they are considered **non-routable**
  - Three addresses are designated as private

Private Address	Number of Hosts
10.0.0.0 to 10.255.255.255/8	16,777,216
172.16.0.0 to 172.31.255.255/12	1,048,576
192.168.0.0 to 192.168.255.255/16	65,536

  - Everyone can use these addresses

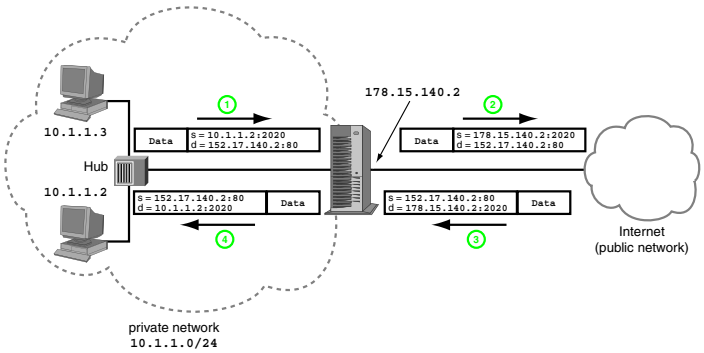
- For example, assume a small LAN consists of three devices



  - Every private device has a unique private address `10.1.1.0/24`
  - The router has a private and public address
- NAT will allow the private machines to access the Internet, using only **one** public address

General NAT Operation

- NAT is performed at the gateway (router) of the private network



- Suppose `10.1.1.2` sends to the web-server `152.17.140.2`
  - For departing packets, NAT router replaces the source address (private address) with its public address
  - For arriving packets, NAT router replaces the destination address (NAT public address) with the original private address

- Given multiple connections exist simultaneously, *how does the NAT router know who's packets belong to whom?*
- When a private machine access a public machine
  - Private machine selects random source port and creates packet
  - NAT takes the packet replaces the source address and the source port (used to identify the session)
  - As packets arrive from public network, use destination port number to determine the private machine
- A NAT table is created at the router

Private Address & Port	Public Address & Port
10.1.1.2, 2020	152.17.140.2, 2020
10.1.1.3, 1848	152.17.140.22, 7095
10.1.1.4, 2020	152.17.140.2, 5050

How many connections can NAT handle simultaneously?

SNAT and DNAT

- Previous described Source Network Address Translation (SNAT)
  - Connection **initiated** from a private machine
  - Private source address replaced with public address

  Can a public machine start a connection to a private machine?
- Destination Network Address Translation (DNAT)
  - Connection **initiated** from a public address
  - Packet from public network translated to a private address
  - Typically, based on destination port number
  - For example all public traffic destined for port 80 is forwarded to **one** private machine

  What can DNAT be used for?

Advantages and Disadvantages of NAT

- Advantages
  - Allows a network to share **one** public address
  - Provides some security

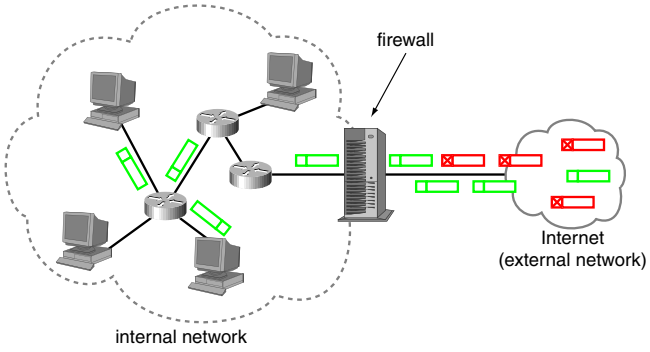
    How does NAT provide security?

- Disadvantages
  - Private machines are not truly routable
  - NAT router is a single point of failure
  - Table-look operation adds delay
  - Some applications may negotiate new port numbers
  - Only works for TCP and UDP protocols

    What? What other transport protocols are there?

Network Firewalls

- A firewall is located between the Internet and internal network
  - Inspecting traffic, the firewall drops or accepts packets



  - As a result, the firewall provide access control to the Internet
- The firewall applies a security policy to each arriving packet

Firewall Security Policy

- Security policy is an **ordered** list of rules
  - Rules are commonly represented as a 5-tuple: protocol type, IP source address, source port number, IP destination address, and destination port number
  - Fields can be fully specified or contain wildcards '*'

No.	Proto.	Source IP	Source Port	Destination IP	Destination Port	Action
1	TCP	140.*	*	*	80	accept
2	TCP	150.*	*	120.*	80	accept
3	TCP	140.*	*	130.*	20	accept
4	UDP	150.*	*	*	3030	accept
5	*	*	*	*	*	deny

  - Every rule has an action **accept** or **deny**
- Rules are applied to every packet, (starting with the first rule)
  - If a packet matches a rule, the associated action is performed

Other Types of Firewalls

- Previous firewall is called a **packet screen**
  - Rules applied to each packet
  - No **state** information is stored
- Stateful firewalls maintain connection information
  - Assume a connection is established from the internal network
  - Firewall keeps track of this connection
  - Packets that arrive from the external network must be part of an **existing** connection
- Application firewalls (gateways) inspect the payload of packets
  - Can accept or drop packets based on data in the packet

What is the disadvantage of these advanced firewalls?

Network Attacks

- Network attacks can be categorized based on their objectives
- Obtain, fabricate, or modify information/services
  - Sniffing packets for data
  - Spoofing addresses (make others believe you are someone else)
  - Promoting your traffic to a *better* service class
- Disrupt network services
  - Cause another machine to *crash*
  - Send packets to disrupt communication
  - Use network resources making them unavailable

  What is the difference between "class promotion" and "using network resources making them unavailable"?

Sniffing

- Easiest and most common way to gather information
- In a broadcast network, frames are sent to all *local* machines
  - The NIC will hear all the frames, but will normally only respond to frames with its MAC as the destination address (*only passes frames with its MAC address to layer 3*)
  - Setting the NIC to *promiscuous*, all frames transmitted will be obtained (*all are sent to layer 3*)
  - Often referred to as *passive sniffing*
- *What kind of information can be obtained?*
  - All the information, just need to interpret

How can we prevent this attack?

Defeating *Older* Ethernet Switches

- Switched Ethernet decreases, if not, eliminates sniffing
  - Typically each machine connects directly to the *switch*
  - Smarter than a hub, switch reads frames (destination MAC address) and forwards it to the correct machine **only**
  - Therefore, the switch must keep a table

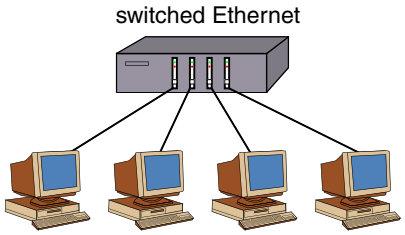
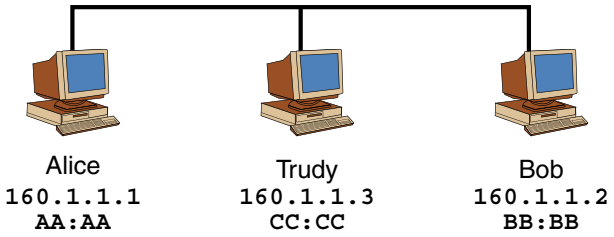


Table contents would be?

- How the switch creates the MAC table
  - When a machine first connects, it sends an ARP to the switch
  - ARP message states "my MAC address is x"
  - Switch stores the MAC and the line it is associated with
- The problem with *older* switches
  - Tables have a finite size
  - An attacker can send a *flood* of fake ARP messages, each with a unique random MAC address
  - Switch add entries until the table is full
  - Once the table is full, older switches will begin forwarding frames to **all** computers
  - Now attacker can sniff traffic, the switch is just a hub

Spoofing

- The idea behind spoofing it to masquerade as another computer
  - Allows a *(wo)man-in-the-middle* attack
- *Why not set the IP address as another machine?*



  - Trudy can reset her IP address and masquerade as Bob

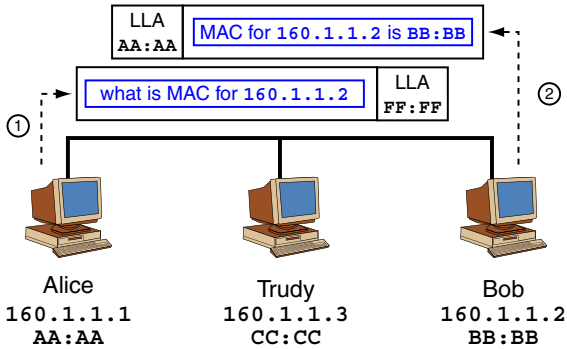
```
ifconfig eth0 160.1.1.2 up
```

  - *However, this will not work due to ARP*

ARP Review

ARP seeks to determine a MAC address given an IP address

- Computer would broadcast "*If your IP address is $w.x.y.z$, then please send me your MAC address*"
- Computers receive request and the *correct* computer **replies**

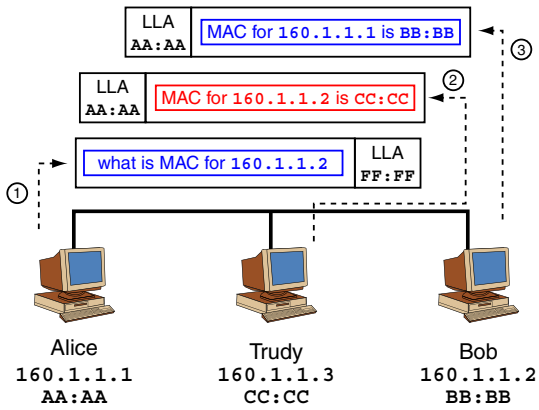


How do you know the request is broadcasted?

- Once an ARP reply is received it is added to table (cache)
  - Cache increases performance
  - Since it is a cache, entries expire
  - For this reason, ARP is considered a *stateless* protocol

    Why not keep all ARP entries forever?

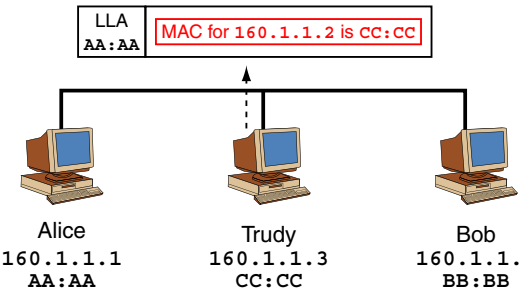
- If Trudy resets her IP address to Bob's, a race condition results
  - Trudy and Bob reply to ARP request



  - Last ARP reply is stored by Alice (never certain which)
  - *System admin should be looking for this behavior...*

ARP Spoofing

- A simple way of preventing the ARP *race* condition
  - Trudy could send an *unsolicited* ARP reply to Alice



  - Alice would store the entry in her ARP table (*ARP poison*)
  - Anytime Alice would send to Bob, she would send to Trudy

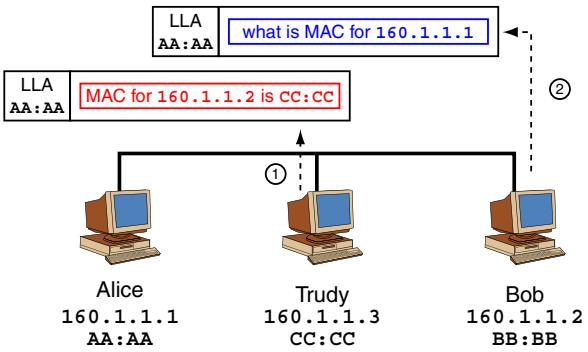
    Won't Bob see the ARP spoof from Trudy?

Hello, are you there? ARP

- Many systems (including Linux) try to update ARP tables
  - System will occasionally go through the ARP table and send ARP requests for each entry

    Why is this advantageous?

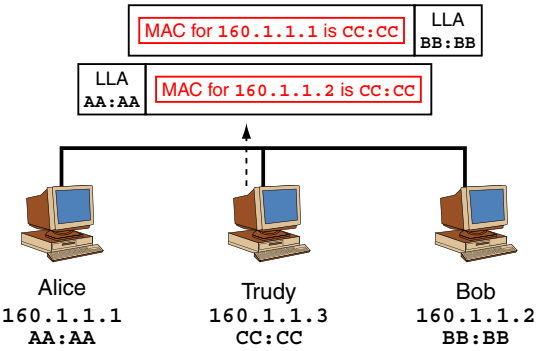
- So, Bob would send an ARP request to Alice for her MAC



- Once Alice receives the ARP request, she would reply
  - One of two scenarios could occur
    1. Bob would never receive a reply, thinking Alice (or he) is disconnected he calls the admin
       What happened to the reply?
    2. Alice receives the request and updates her table with Bob's real MAC (removing the poison)
  - In either case, the spoof is over...

Feeding Both Sides Poison

- To keep both sides quite, Trudy should *feed* both sides
  - Trudy tells Alice Bob's MAC is `CC:CC`
  - Trudy tells Bob Alice's MAC is also `CC:CC`



- Of course since these are caches, Trudy must constantly send
  - For example, send ARP poison every 40 seconds

More ARP Damage

- ARP spoofing is very dangerous
  - It is a layer 2/3 protocol
  - Independent of platform (everyone is susceptible)
- ARP can be used for more than Man-in-the-Middle (MiM) attacks
  - Constantly sending a victim a nonexistent MAC address
    "could have a quite a spectacular effect on one's [the victim's] mental health" - Yuri Volobuev
  - Broadcast the wrong address of an important computer
    What is the effect? Can you give an example?

Anyway to prevent these attacks?

Denial of Service

- Denial of Service (DoS) attacks
  - Attacker wants to prevent the legitimate use of the system
  - System can be the computer, network, services, etc...
- DoS categories

	Stopping Services	**Exhausting Resources**
locally	Process killing System reconfiguring Process crashing	`fork` until full Fill file system
remotely	Bad packet attack Changing network configuration	Packet flood