NA

1. Flamestrike

   (a).

   https://en.wikipedia.org/wiki/Broadcast_radiation

   Broadcast storm is when a network system be overwhelmed by continuous broadcast traffic, network links fail and network communication fails. The switch will repeatedly rebroadcast the broadcast messages flooding the network, it will eventually result in a flood loop., causing network system to melt down.

   (b).

   https://en.wikipedia.org/wiki/Broadcast_radiation

   https://learningnetwork.cisco.com/thread/20298

   Broadcast storm sometimes is because ARP table is no longer reliable, MAC address flipping or seeing one MAC address on more than one port. We can reboot the machine to clear the recorded MAC address to solve the problem. In other cases, it may be caused by fatal network design or not properly configured Ethernet device. We can use wireshark to check packets, statistics, unusual conversations to check is there something wrong with devices, switches and ports. Attempting to find what happens and fix it.

   (c).

   https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

   https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

   STP prevents loops by blocking one or more of the links. If one of the links in use goes down, it would fail over to a previously blocked link. The loop-free tree of bridges will perform the spanning tree algorithm when they are first connected to the network or whenever topology changes. Then each bridge will determine the shortest path to the root bridge The designated bridge will forward packets from the LAN toward the root bridge. In this case, it can prevent loops.

2. Mac Pro

   (a).

   http://cc.cust.edu.tw/~ccchen/doc/F7713-ch09.pdf

   https://read01.com/zh-tw/M2n4oJ.html#.Wq29b-huZPY

   http://homepages.uc.edu/~thomam/Net1/ping_off_server_example.html

   https://www.youtube.com/watch?v=rYodcvhh7b8

   ARP, 10.0.0.1 -> 10.0.0.2, fa:ce:b0:00:00:0c -> FF:FF:FF:FF:FF:FF

   ARP, 10.0.0.2 -> 10.0.0.1, de:ad:be:ee:ee:ef -> fa:ce:b0:00:00:0c

   ICMP,10.0.0.1 -> 10.0.0.2, fa:ce:b0:00:00:0c -> de:ad:be:ee:ee:ef

ICMP, 10.0.0.2 -> 10.0.0.1, de:ad:be:ee:ee:ef -> fa:ce:b0:00:00:0c

(b).

Nothing on the gateway's mac address table. Because Mario and Zelda are on the same local net, the Gateway would not record their mac address.

(c).

ARP, 10.0.0.1 -> 10.0.0.254, fa:ce:b0:00:00:0c -> FF:FF:FF:FF:FF:FF

ICMP,10.0.0.1 -> 10.0.0.254, fa:ce:b0:00:00:0c -> ba:aa:aa:ad:c0:de

(d).

https://computer-networking.wonderhowto.com/how-to/hack-lan-passwords-with-ettercap-261954/

1. Sonic can install and open Ettercap, a ARP spoofing tool which can recognize several different packets that contain passwords including telnet.
2. Sonic can set the tool's IP address to match the IP subnet of Mario.
3. Sonic can use Ettercap to scan IP and MAC addresses of Mario's computer.
4. Sonic starts to send ARP packets across the LAN that contain Sonic's MAC address and Mario's IP address.
5. As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the Mario will go to the Sonic instead. Sonic can steal data including Mario's password.

3. Let's IPV6
    (a) ICMPv6 is used in layer 3
    (b) ff02::2
    (c) Why are you still using IPv4?