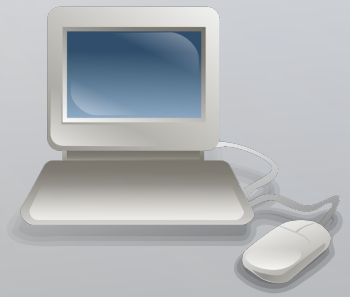
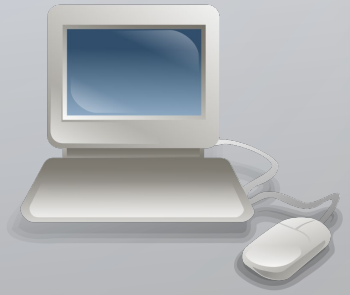
DHCP SECURITY

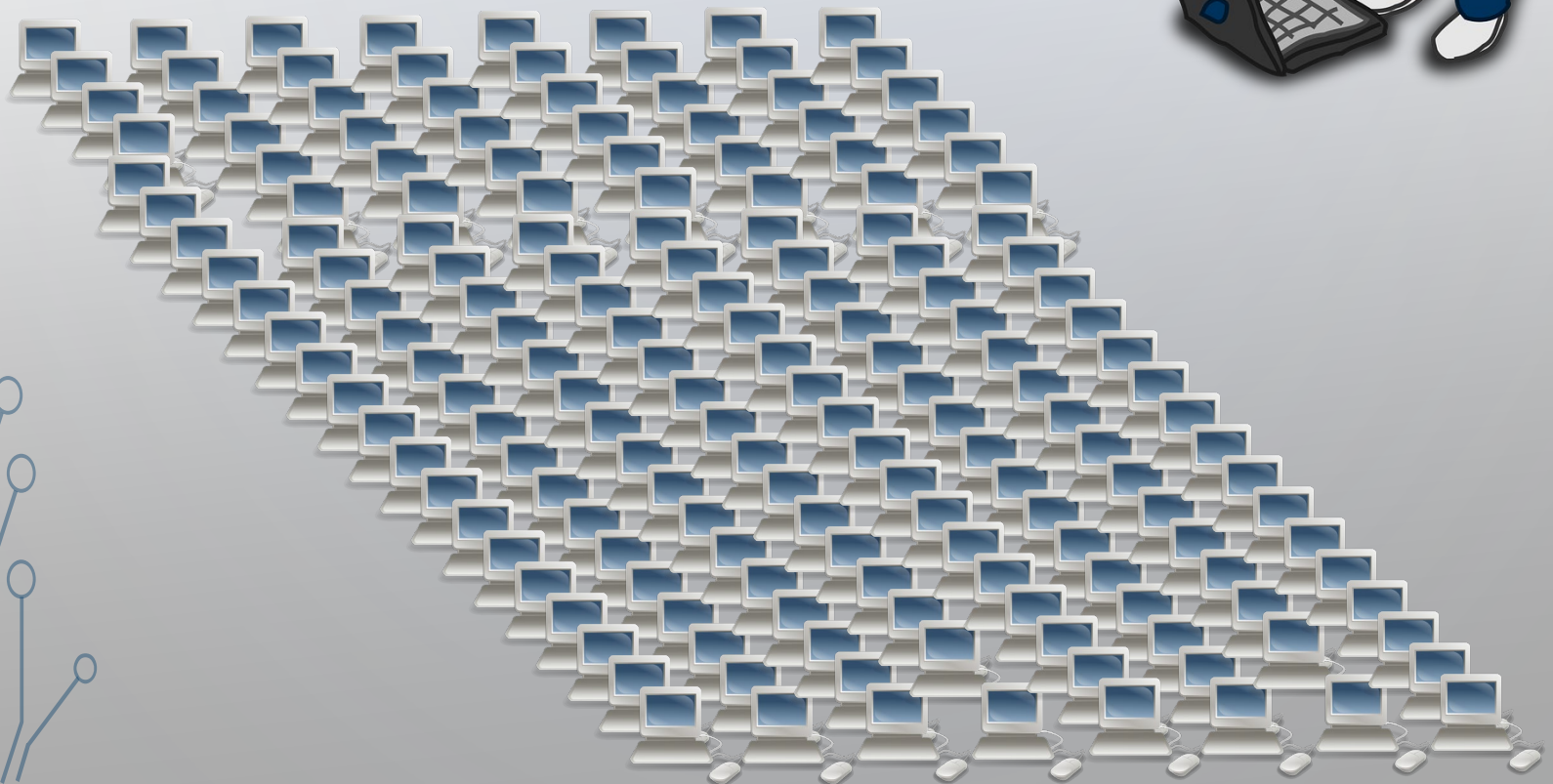
BY DAVID GELLER AND MATTHEW SARBINOWSKI

SCENARIO 1



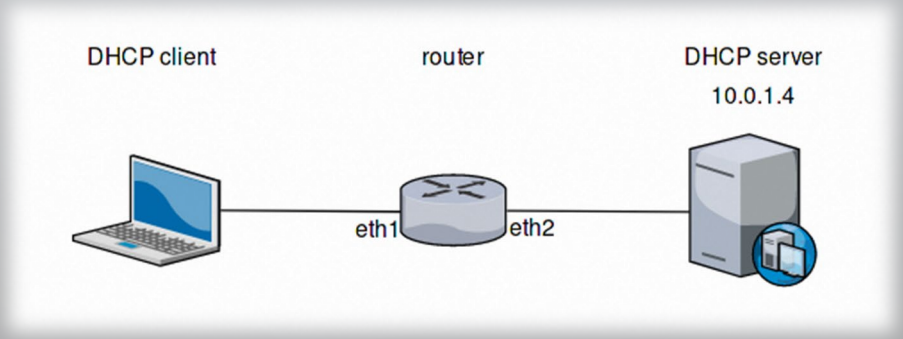


SCENARIO 2



WHAT IS DHCP?

- Stands for Dynamic Host Control Protocol
- Application layer protocol
- Involves UDP communications between server and client
- **JOB: assign IP addresses to clients including subnet mask info, default gateway IP addresses and DNS addresses**



DHCP PACKET

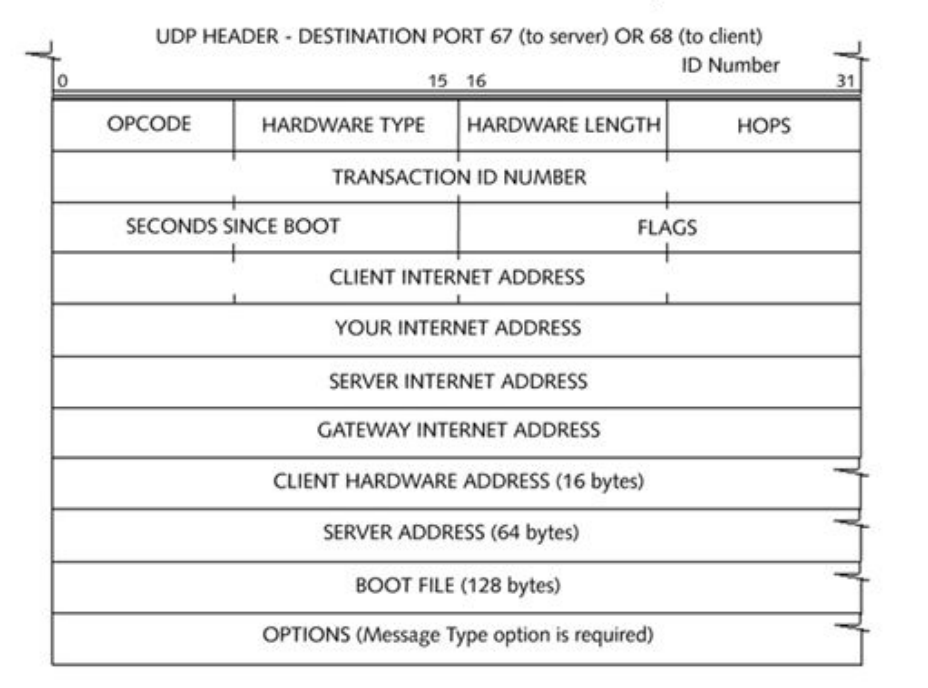
Client IP Address = client puts current IP address (if valid); otherwise it is set to 0

Your IP Address = address the server assigns to client

Server IP Address = address the client should use for next step (may or may not be the server)

Server Address = Name of server replying (if given)

Options = Holds DHCP options, as well as parameters required for basic operation



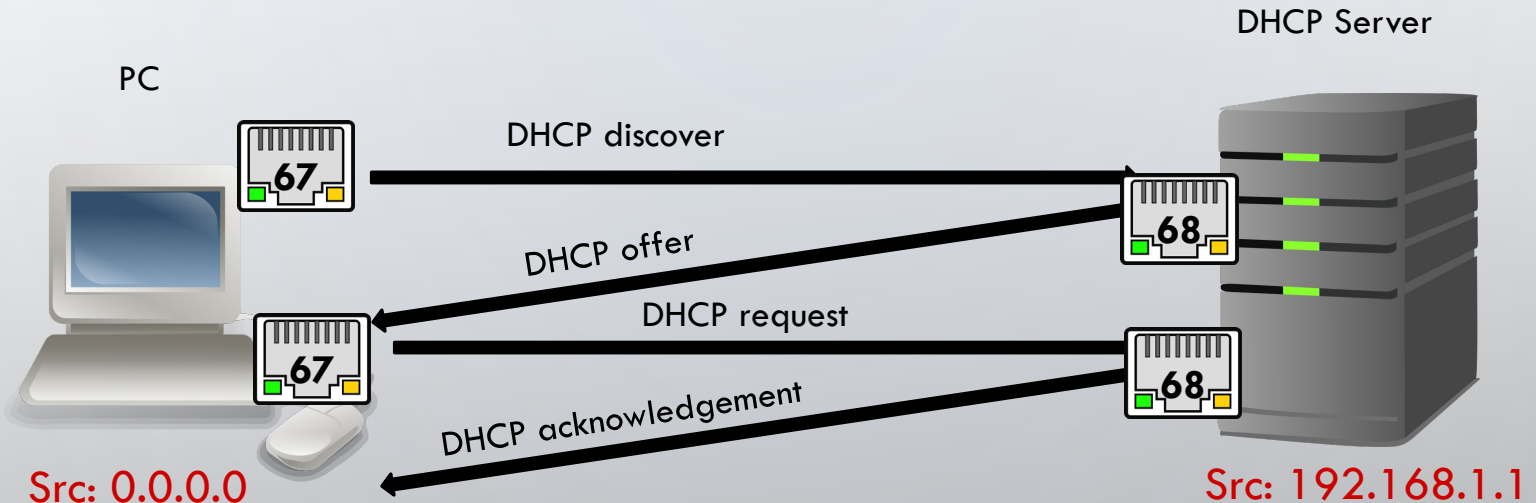
DHCP MESSAGE OPTIONS

Table 7-1: DHCP Message Types

Type Number	Message Type	Description
1	Discover	Used by the client to locate available DHCP servers
2	Offer	Sent by the server to the client in response to a discover packet
3	Request	Sent by the client to request the offered parameters from the server
4	Decline	Sent by the client to the server to indicate invalid parameters within a packet
5	ACK	Sent by the server to the client with the configuration parameters requested
6	NAK	Sent by the client to the server to refuse a request for configuration parameters
7	Release	Sent by the client to the server to cancel a lease by releasing its configuration parameters
8	Inform	Sent by the client to the server to ask for configuration parameters when the client already has an IP address

Other DHCP Server

HOW IT WORKS? (DHCP HANDSHAKE)



PC: Is anyone out there? I need an IP address!

DHCP Server: I'm over here! I'll offer you this IP address: 192.168.1.10

PC: Thank you! I'll take IP address: 192.168.1.10

DHCP Server: You're welcome! Here is your IP address, subnet mask info, default gateway and DNS address

WIRESHARK EXAMPLE

Step 1: Run wireshark capture

Step 2: Run windows CMD on windows 10

Step 3: type in ipconfig /release

Step 4: type in ipconfig /renew

Step 5: filter DHCP

No.	Time	Source	Source MAC	Destination	Dest MAC	Protocol	DHCP
176	10.968705	192.168.1.10	Micro-St_e3:08:c7	192.168.1.1	HitronTe_c3:a7:32	DHCP	Release
345	14.951192	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Discover
346	14.980474	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	Offer
347	14.980822	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Request
349	15.064161	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	ACK

WIRESHARK: DHCP DISCOVER

No.	Time	Source	Source MAC	Destination	Dest MAC	Protocol	DHCP
345	14.951192	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Discover
346	14.980474	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	Offer
347	14.980822	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Request
349	15.064161	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	ACK


```
> Frame 345: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
> Ethernet II, Src: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcd9f5786
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.10)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

WIRESHARK: DHCP OFFER

No.	Time	Source	Source MAC	Destination	Dest MAC	Protocol	DHCP
345	14.951192	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Discover
346	14.980474	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	Offer
347	14.980822	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Request
349	15.064161	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	ACK

```
> Frame 346: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
> Ethernet II, Src: HitronTe_c3:a7:32 (ac:20:2e:c3:a7:32), Dst: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcd9f5786
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000…
```

WIRESHARK: DHCP REQUEST

No.	Time	Source	Source MAC	Destination	Dest MAC	Protocol	DHCP
345	14.951192	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Discover
346	14.980474	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	Offer
347	14.980822	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Request
349	15.064161	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	ACK

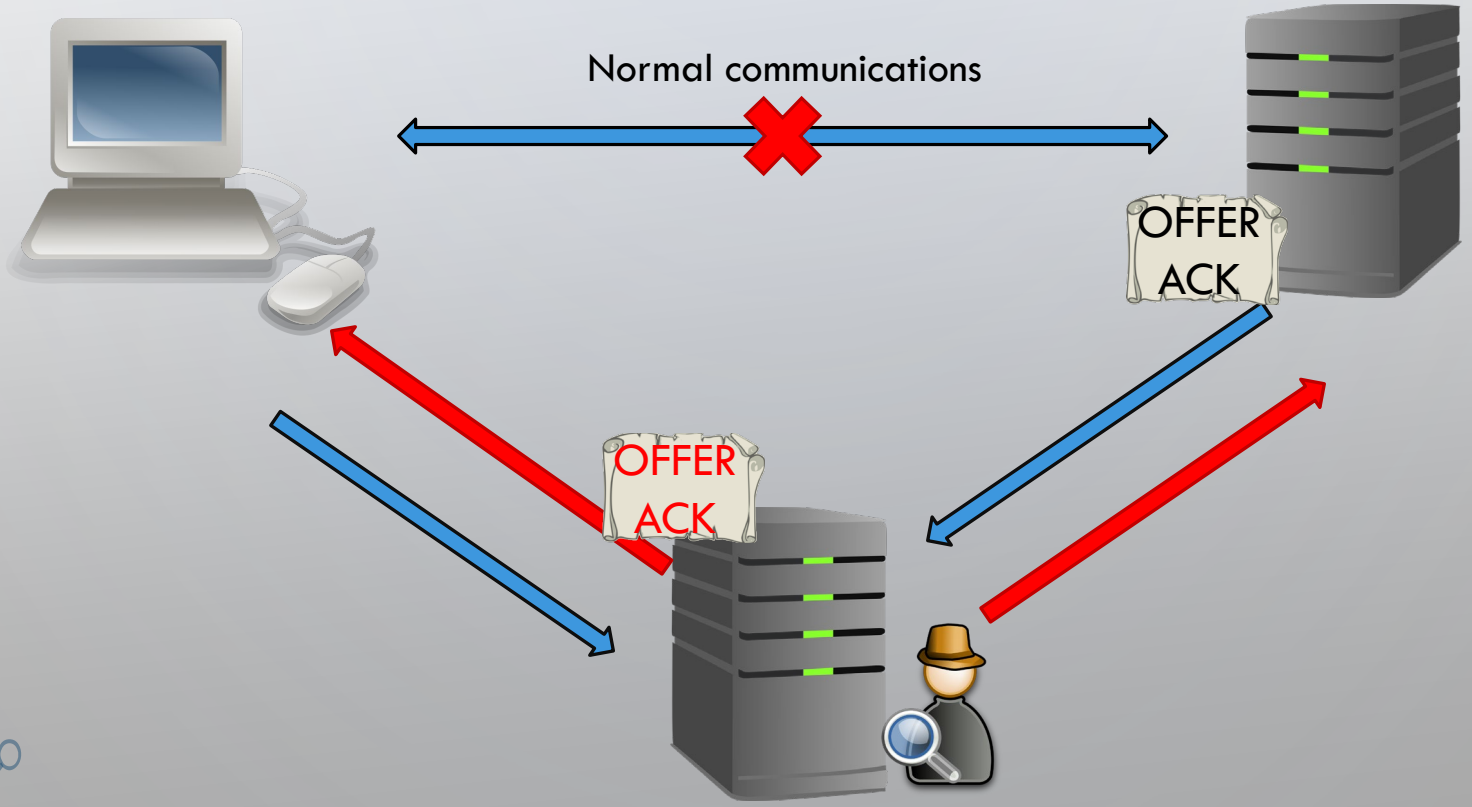
```
> Frame 347: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
> Ethernet II, Src: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcd9f5786
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.10)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

WIRESHARK: DHCP ACK

No.	Time	Source	Source MAC	Destination	Dest MAC	Protocol	DHCP
345	14.951192	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Discover
346	14.980474	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	Offer
347	14.980822	0.0.0.0	Micro-St_e3:08:c7	255.255.255.255	Broadcast	DHCP	Request
349	15.064161	192.168.1.1	HitronTe_c3:a7:32	192.168.1.10	Micro-St_e3:08:c7	DHCP	ACK

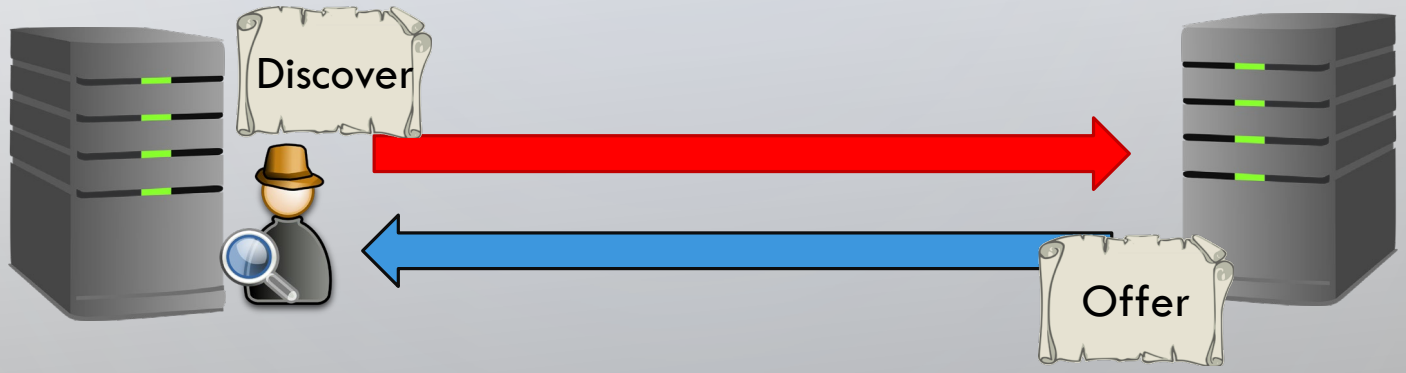
```
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xcd9f5786
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.10
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Micro-St_e3:08:c7 (d4:3d:7e:e3:08:c7)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (604800s) 7 days
  > Option: (12) Host Name
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  v Option: (255) End
      Option End: 255
    Padding: 000000000000000000000000000000000000000000000000…
```

DHCP SERVER SPOOFING (MITM ATTACK)



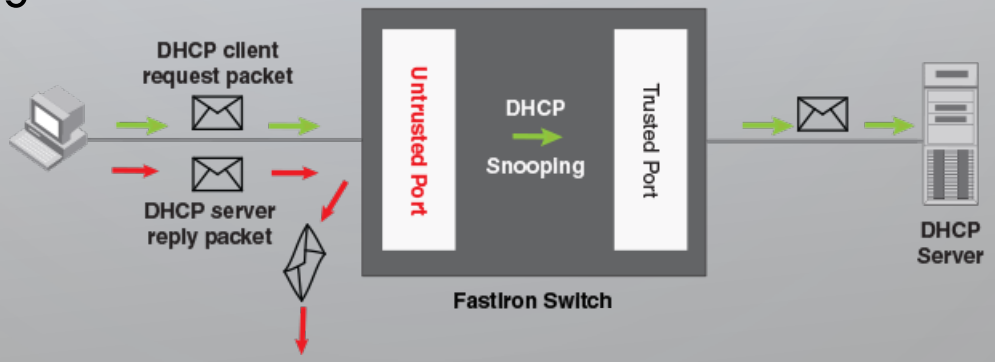
DHCP DISCOVER FLOOD (DOS ATTACKS)

DHCP STARVATION (DOS ATTACKS)



MITIGATION

- DHCP SNOOPING
  - Creates trusted and untrusted ports
  - Creates a DHCP Snooping Database
  - Messages are rate limited
- Option 82 Relay Agent
  - Allows switch/router to identify itself and the client that sends the messages



MITIGATION

```
switch#
switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
99,999
DHCP snooping is operational on following VLANs:
99
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
GigabitEthernet0/13        yes         unlimited
GigabitEthernet0/22        yes         unlimited
GigabitEthernet0/24        yes         unlimited
```

DHCP Snooping Database

EXAMPLES OF ATTACK IN NEWS

- Tbd…