An Introduction To Arp Spoofing

April, 2001

Sean Whalen • Sophie Engle • Dominic Romeo

GENERAL INFORMATION

“Introduction to ARP Spoofing” (April 2001)

Current Revision: 1.8

Available:

- http://chocobospore.org
- http://packetstorm.securify.com
- http://securityportal.com

PURPOSE

Audience

- Basic networking experience
- TCP/IP Reference Model
- Switched vs. non-switched networks

Topic: ARP Spoofing

- Introduction
- Operation
- Attacks
- Defenses
- Conclusion

INTRODUCTION

A computer connected to an IP/Ethernet LAN has two addresses:

- MAC/Ethernet Address
  - Address of the network card
  - In theory, unique & unchangeable
- IP Address
  - Virtual address
  - Assigned via software

INTRODUCTION

MAC/Ethernet Address

- Necessary for Ethernet to send data
- Independent of application protocols
- Divides data into 1500 byte frames
- Each frame has a header containing the MAC address of the source and destination computer

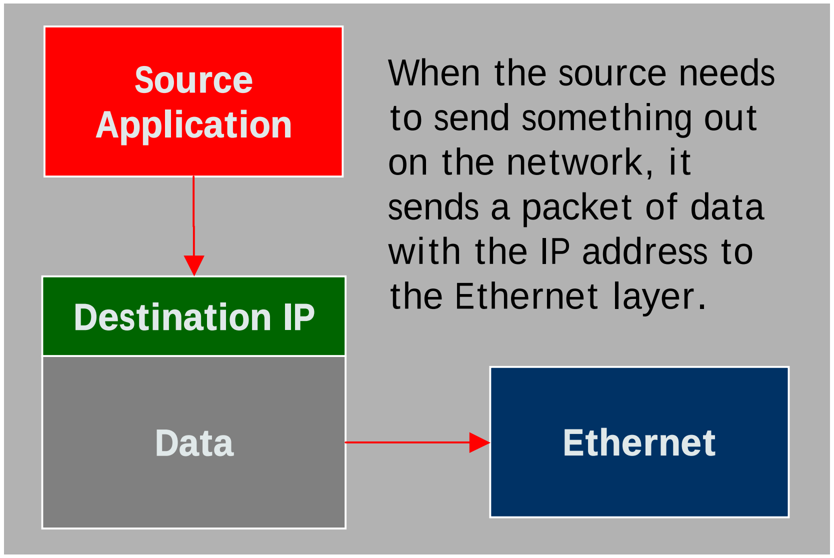
INTRODUCTION

IP Address

- Used by applications
- Independent of whatever network technology operates underneath it
- Each computer on a network must have an unique IP address to communicate

INTRODUCTION

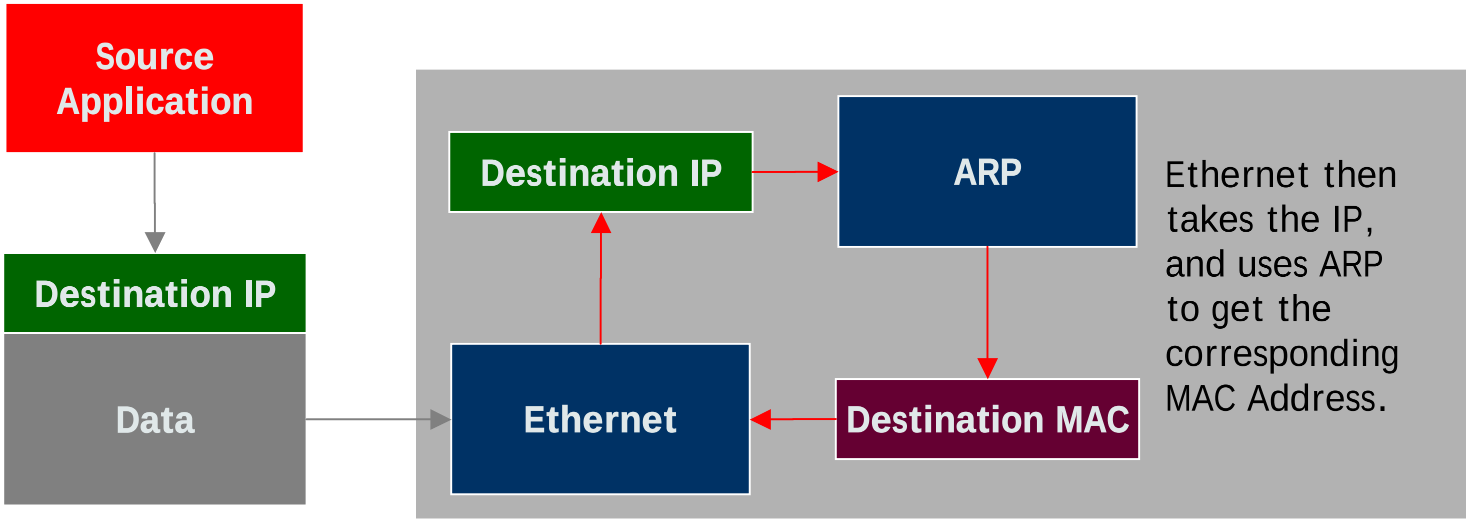
IP & Ethernet must work together!



When the source needs to send something out on the network, it sends a packet of data with the IP address to the Ethernet layer.

INTRODUCTION

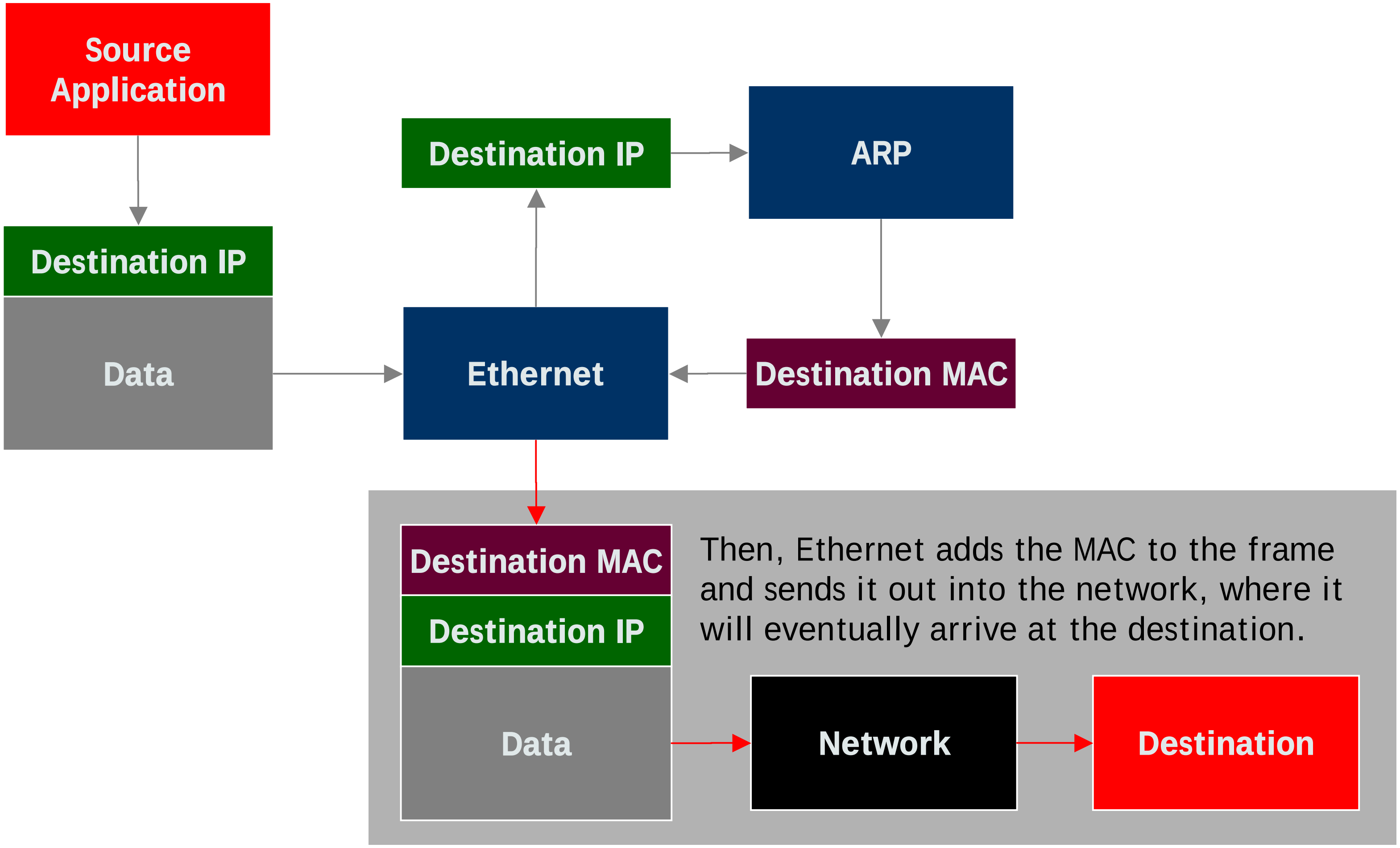
IP & Ethernet must work together!



Ethernet then takes the IP, and uses ARP to get the corresponding MAC Address.

INTRODUCTION

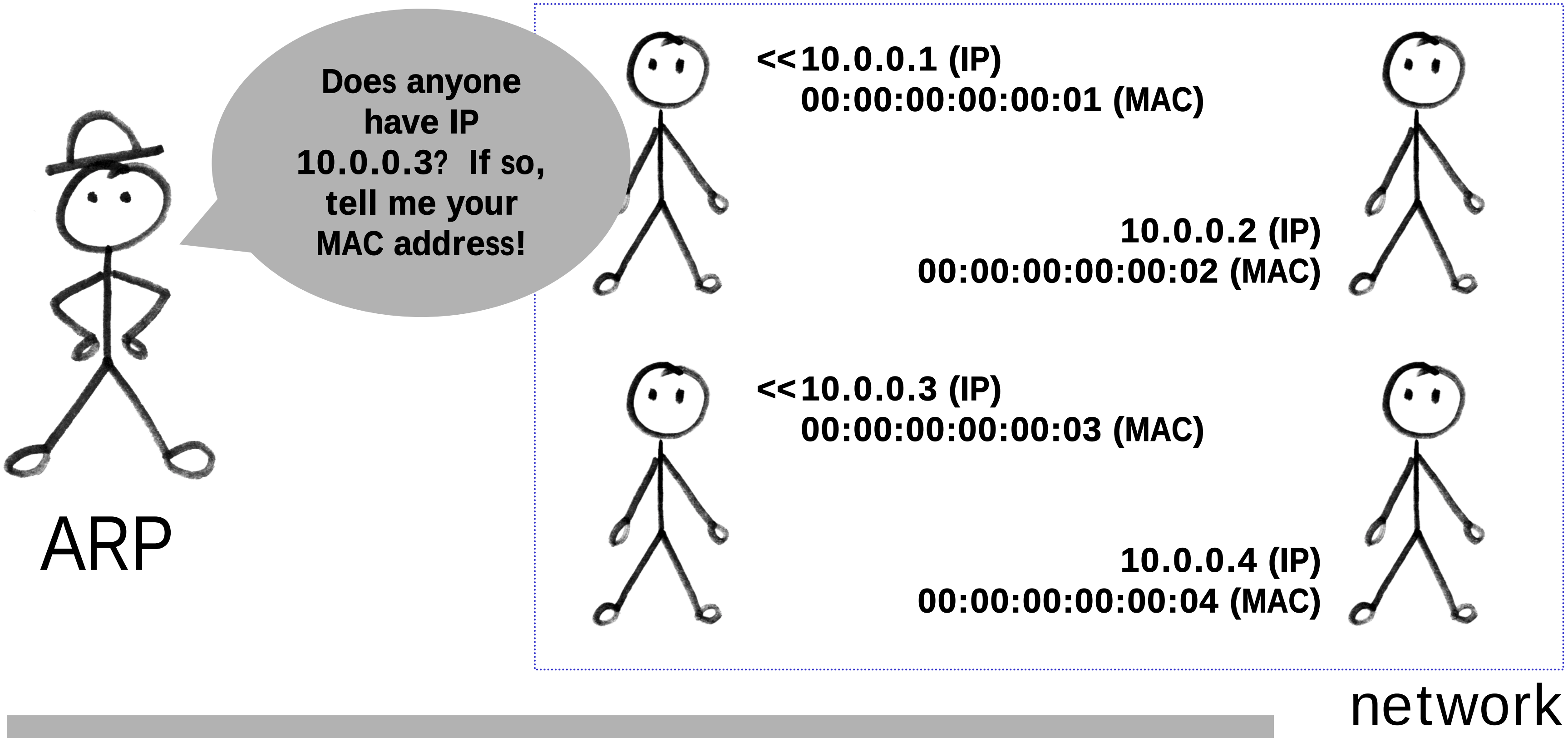
IP & Ethernet must work together!



Then, Ethernet adds the MAC to the frame and sends it out into the network, where it will eventually arrive at the destination.

OPERATION

ARP Request



Does anyone have IP 10.0.0.3? If so, tell me your MAC address!

ARP

<<10.0.0.1 (IP)
00:00:00:00:00:01 (MAC)

10.0.0.2 (IP)
00:00:00:00:00:02 (MAC)

<<10.0.0.3 (IP)
00:00:00:00:00:03 (MAC)

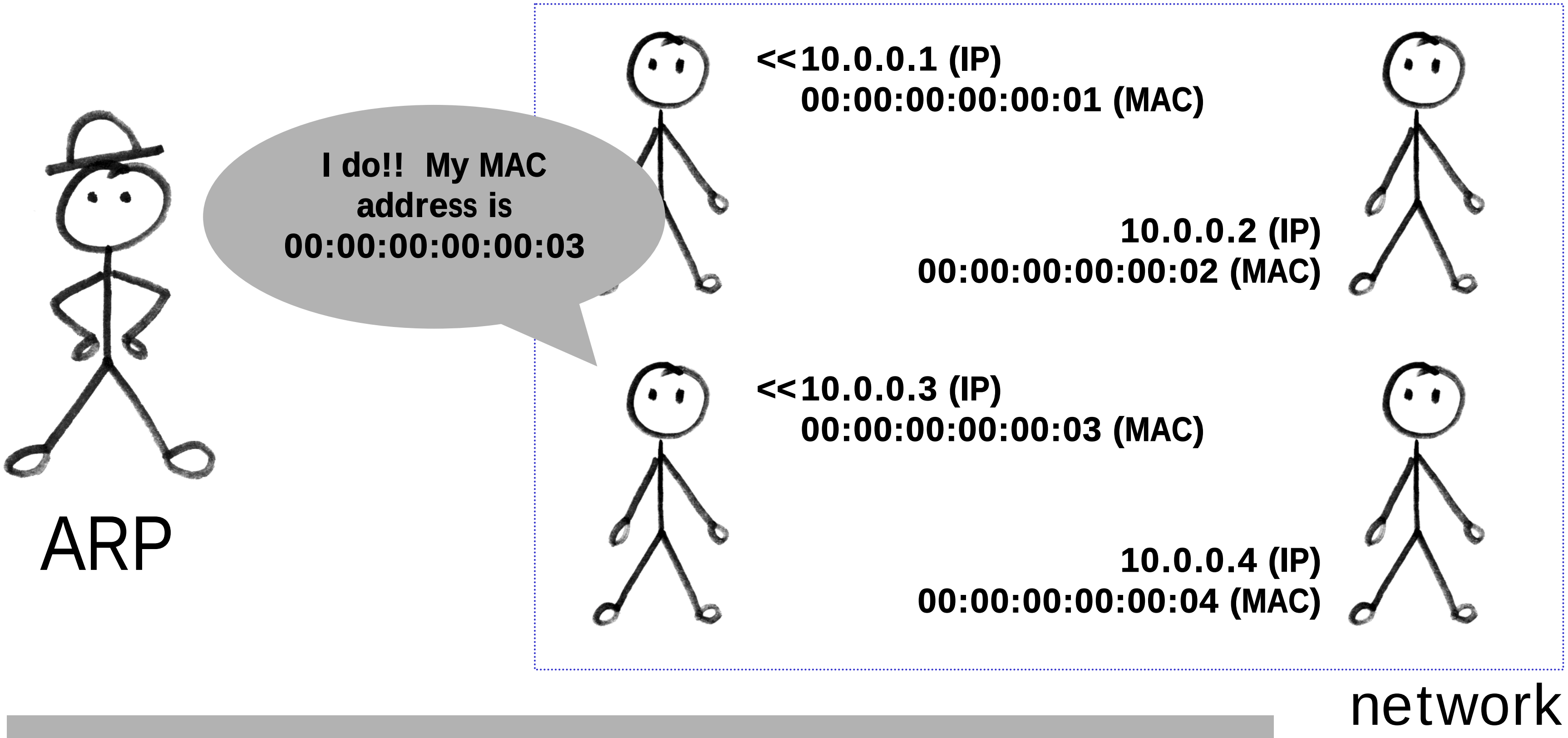
10.0.0.4 (IP)
00:00:00:00:00:04 (MAC)

network

First, ARP sends a request into the network asking for the MAC matching the given IP.

OPERATION

ARP Reply


I do!! My MAC address is 00:00:00:00:00:03
<<10.0.0.1 (IP) 00:00:00:00:00:01 (MAC)
10.0.0.2 (IP) 00:00:00:00:00:02 (MAC)
<<10.0.0.3 (IP) 00:00:00:00:00:03 (MAC)
10.0.0.4 (IP) 00:00:00:00:00:04 (MAC)
ARP
network

Everyone on the network listens for these requests,
and sends back it's MAC address if it's IP matches the request.

OPERATION

ARP Cache

- Kept locally to minimize the number of ARP requests being broadcast
- Updates the cache with the new IP/MAC associations for each reply
- Stateless protocol
  - Most operating systems will update the cache if a reply is received, regardless of whether they sent out an actual request

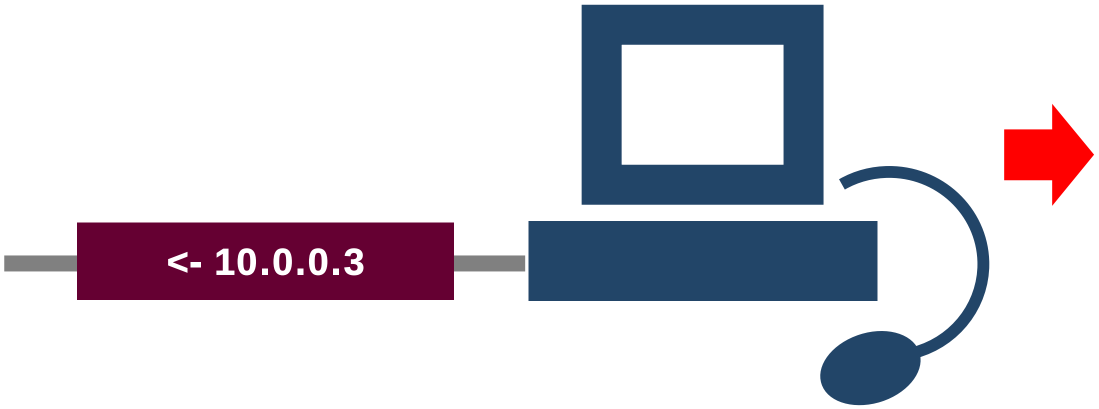
OPERATION

ARP Spoofing

- Involves constructing forged ARP replies
- Takes advantage of the ARP cache
- Process of corrupting cache is “Poisoning”

OPERATION

ARP Spoofing



ARP Cache

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01
10.0.0.2	00:00:00:00:00:02
10.0.0.3	

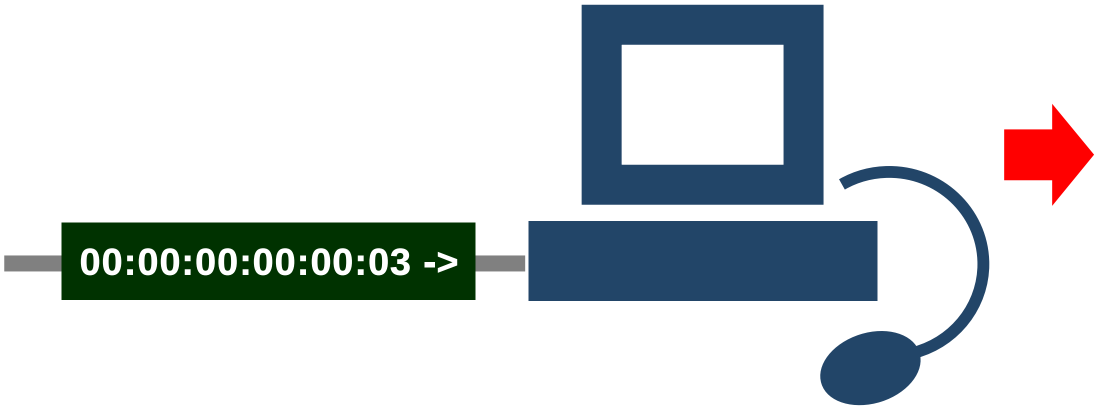
ARP Request

ARP Response

The computer needs to know what MAC address matches with 10.0.0.3, so it sends out an ARP request.

OPERATION

ARP Spoofing



ARP Cache

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01
10.0.0.2	00:00:00:00:00:02
10.0.0.3	00:00:00:00:00:03

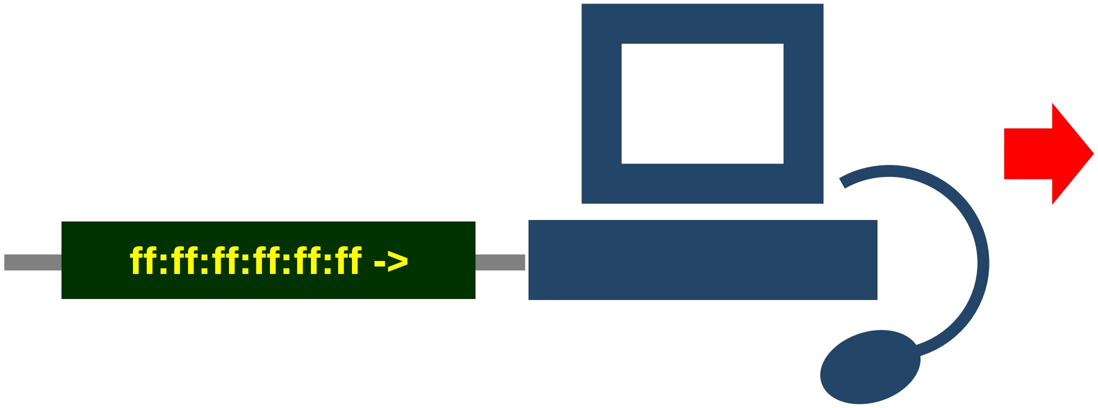
ARP Request

ARP Response

The computer gets back an ARP Response with the MAC address of 00:00:00:00:00:03. Then, the computer updates the ARP cache with the new IP/MAC Association.

OPERATION

ARP Spoofing



ARP Cache

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01
10.0.0.2	00:00:00:00:00:02
10.0.0.3	ff:ff:ff:ff:ff:ff

ARP Request

ARP Response

The computer need not send out an ARP Request to received an ARP Response.
Thus, if a spoofed response were to arrive, the computer would update the cache as usual.

OPERATION

ARP Spoofing

ARP Cache

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01
10.0.0.2	00:00:00:00:00:02
10.0.0.3	ff:ff:ff:ff:ff:ff

ARP Request

ARP Response

Now, when the computer sends data to 10.0.0.3, it will go to the computer with MAC address ff:ff:ff:ff:ff:ff instead of 00:00:00:00:00:03 like it should.

ATTACKS - SNIFFING

Promiscuous mode

- Allows network cards to examine frames that are destined for MAC addresses other than their own

Switches

- Routes frames to a single port, based on a table of MAC/port associations
- Prevents traditional sniffing

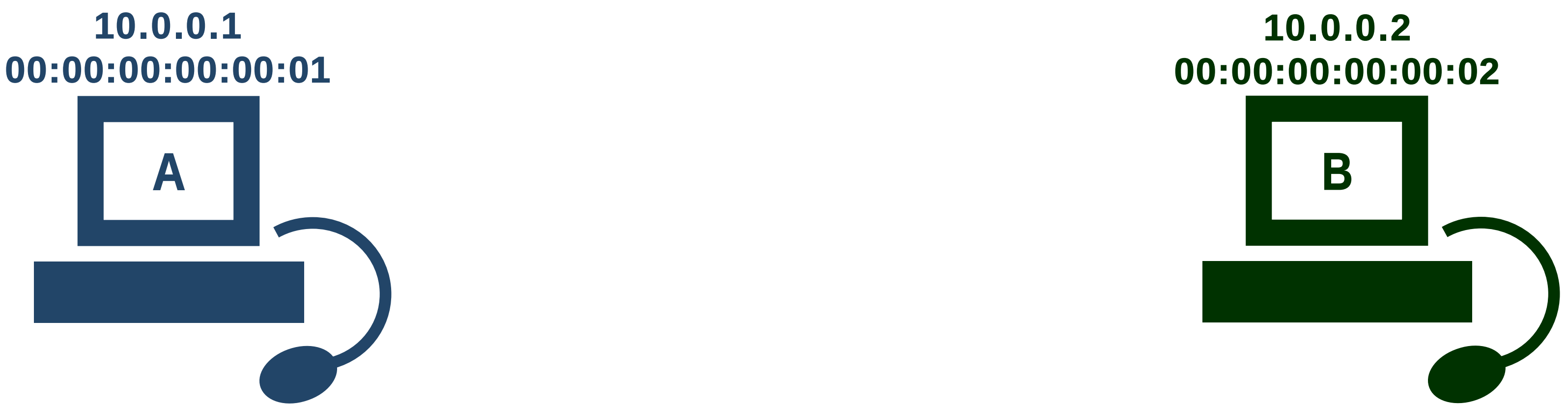
ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)

- A malicious user:
  - Inserts his computer between the communications path of two target computers
  - Forwards frames between the two target computers so communications are not interrupted
- All Internet traffic could be intercepted if this was performed between the target and router

ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)



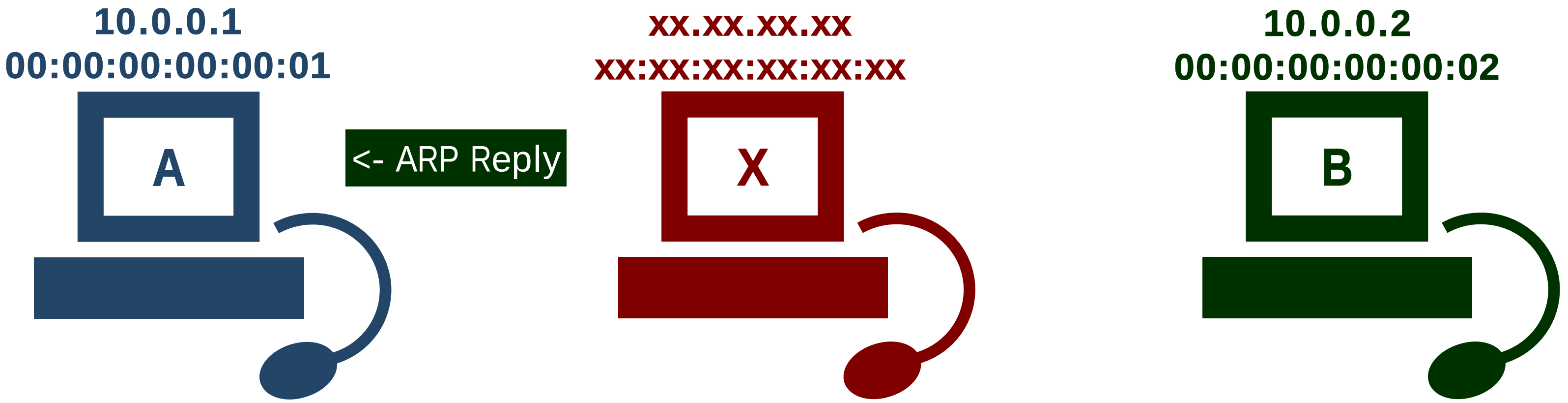
IP Address	MAC Address
10.0.0.2	00:00:00:00:00:02

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01

Computer A & B are communicating on a switched network.
(For illustration purposes, switch left out of picture.)

ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)



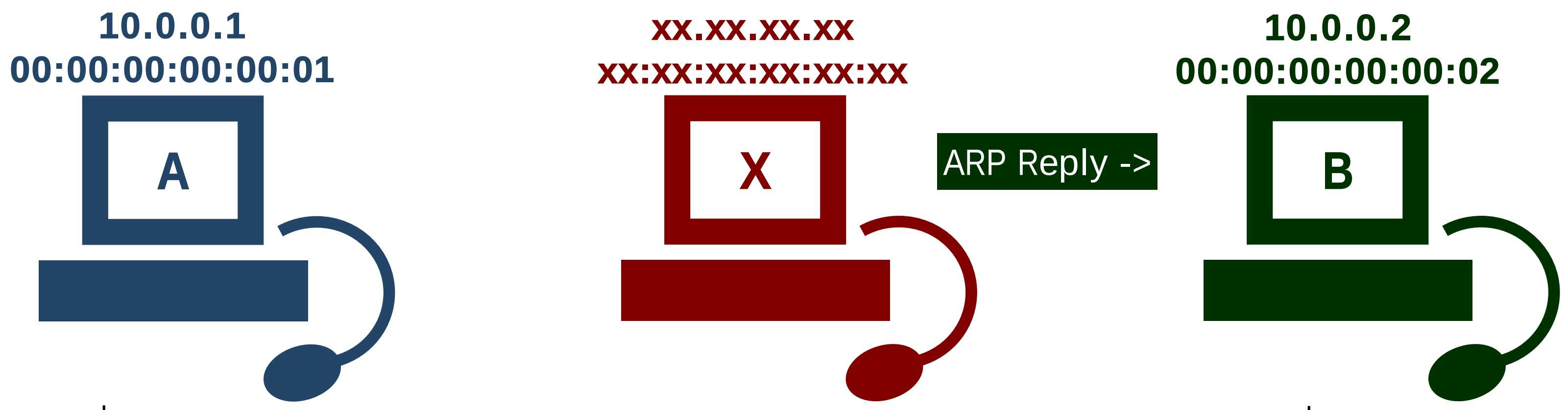
IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

IP Address	MAC Address
10.0.0.1	00:00:00:00:00:01

To intercept communications, computer X first sends a spoofed ARP reply to computer A. This reply replaces the IP address of B with the MAC of X.

ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)



10.0.0.1
00:00:00:00:00:01

A

xx.xx.xx.xx
xx:xx:xx:xx:xx:xx

X

ARP Reply ->

10.0.0.2
00:00:00:00:00:02

B

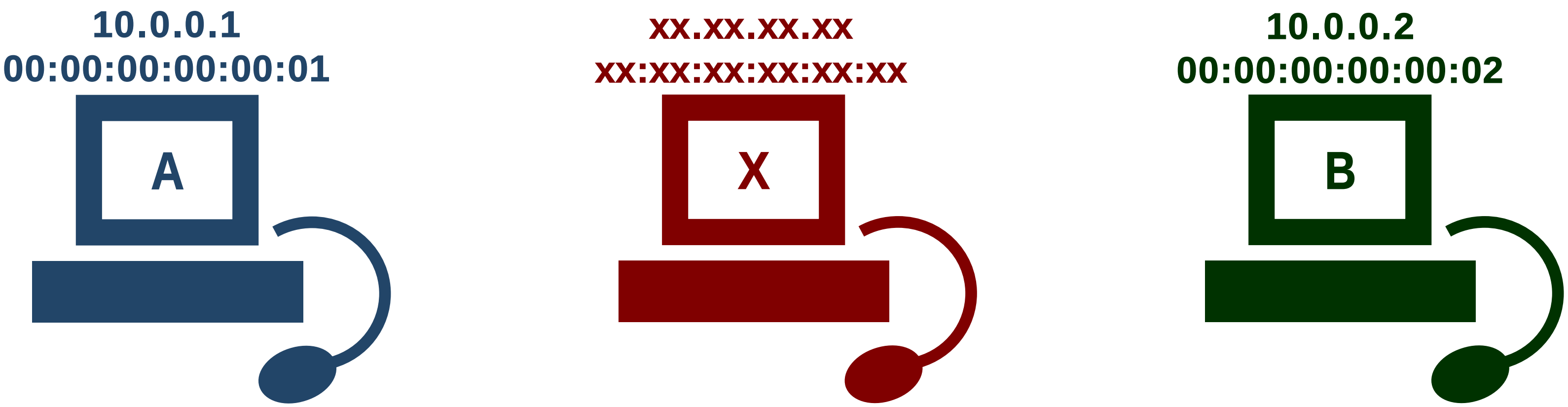
IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

IP Address	MAC Address
10.0.0.1	**xx:xx:xx:xx:xx:xx**

Computer X then sends a spoofed ARP reply to computer B.
This reply replaces the IP address of A with the MAC of X.

ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)



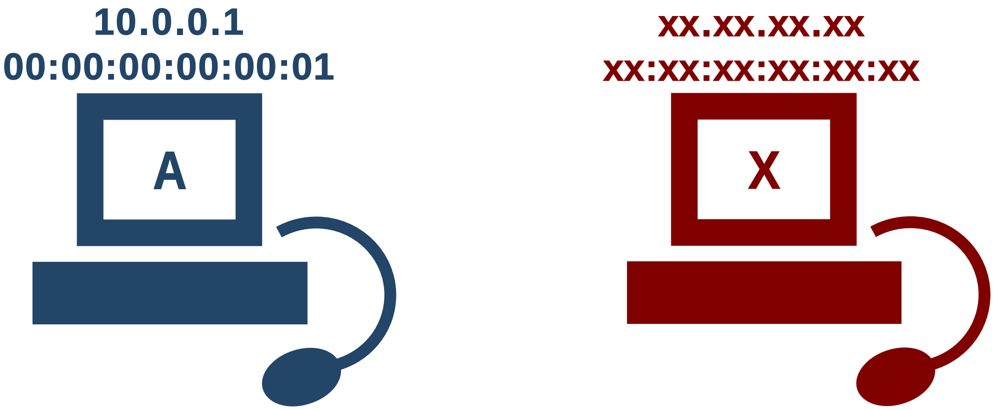
IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

IP Address	MAC Address
10.0.0.1	xx:xx:xx:xx:xx:xx

Now, when computer A wants to talk to B, it sends the data to X .
Likewise, computer B sends its data to X when it wants to talk to A.

ATTACKS - SNIFFING

Man-in-the-Middle Attack (MiM)



10.0.0.1
00:00:00:00:00:01

A

xx.xx.xx.xx
xx:xx:xx:xx:xx:xx

X

10.0.0.2
00:00:00:00:00:02

B

IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

IP Address	MAC Address
10.0.0.1	xx:xx:xx:xx:xx:xx

Computer X needs to do one more thing to prevent disrupting the communication Between A and B. It must forward the packets A sends to B on, and visa versa.

ATTACKS - SNIFFING

MAC Flooding

- Send spoofed ARP replies to a switch at an extremely rapid rate
- Switch's port/MAC table will overflow
- Results vary
  - Some switches will revert into broadcast mode, allowing sniffing to then be performed

ATTACKS - BROADCASTING

Sniffing

- Set the MAC address of the network gateway to the broadcast MAC
  - Enables sniffing of non-internal communications

Storms

- Poisoning caches with the broadcast address could cripple large networks

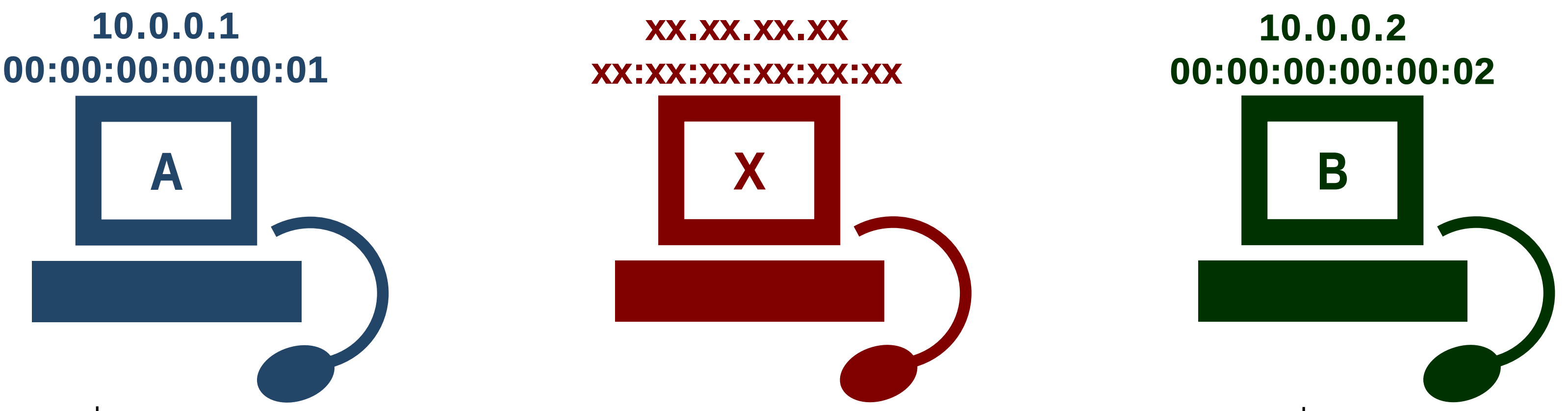
ATTACKS - DOS

Denial of Service

- Update ARP caches with non-existent MAC addresses
  - Causes frames to be dropped
  - Could be sent out in a sweeping fashion to DoS all clients on a network
- Possible side affect of post-MIM attacks

ATTACKS - DOS

DoS due to Post-MiM Attack



10.0.0.1
00:00:00:00:00:01

A

xx.xx.xx.xx
xx:xx:xx:xx:xx:xx

X

10.0.0.2
00:00:00:00:00:02

B

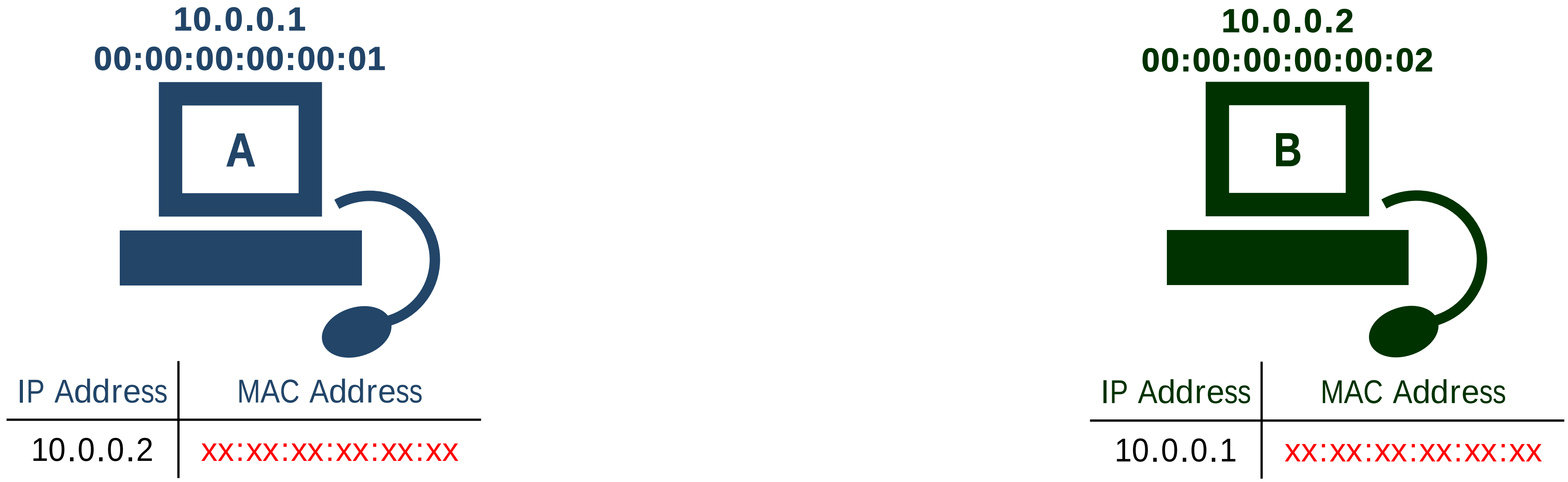
IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

IP Address	MAC Address
10.0.0.1	xx:xx:xx:xx:xx:xx

Computer X is currently using the MiM attack.

ATTACKS - DOS

DoS due to Post-MiM Attack



10.0.0.1
00:00:00:00:00:01

IP Address	MAC Address
10.0.0.2	xx:xx:xx:xx:xx:xx

10.0.0.2
00:00:00:00:00:02

IP Address	MAC Address
10.0.0.1	xx:xx:xx:xx:xx:xx

Even when X leaves the network, A & B still have each other's IP address assigned to the MAC of X. Since X is no longer on the network, the frames go nowhere.

ATTACKS - HIJACKING

Connection Hijacking

- Allows an attacker to take control of a connection between two computers
- Can result in any type of session being transferred

ATTACKS - CLONING

MAC Address Cloning

- MAC addresses intended to be globally-unique and unchangeable
- Today, MAC addresses can be easily changed
- An attacker could DoS a target computer, clone the target's MAC address, and receive all frames intended for the target

DEFENSES

Defenses

- No universal defense
- Static (non-changing) ARP entries
- Port security (or Port Binding, MAC Binding)
- Detection
  - ARPWatch
  - Reverse ARP (RARP)

DEFENSES - STATIC ROUTES

Static Routes

- ARP caches have static (non-changing) entries
- Spoofed ARP replies are ignored
- Creates lots of overhead
  - Each ARP cache must have a static entry for <u>every</u> computer on the network
  - Not practical for most LANs
- Results can also vary depending on operating system

DEFENSES - MAC BINDING

MAC Binding

- Feature found on high-quality switches
- Does not allow the MAC address associated with a port to change once it has been set
- Legitimate changes can be performed by the network administrator
- Does not prevent ARP spoofing, but does prevent MAC cloning & spoofing

DETECTION

Detection

- ARPWatch (Free UNIX Program)
  - Listens for ARP replies on a network and builds a table of IP/MAC associations
  - When IP/MAC associations change (flip-flop), an email is sent to an administrator
- Reverse ARP (RARP)
  - Requests the IP of a known MAC address
  - Can be used to detect MAC cloning
- Promiscuous Mode Sniffing
  - Many methods exist for detecting machines in promiscuous mode, and can be found in the Sniffing FAQ at http://www.robertgraham.com/pubs/sniffing-faq.html

DETECTION

The exact behavior of ARP varies with:

- Different operating systems
- Different operating system versions
- Different network hardware

CONCLUSION

ARP Spoofing is one of several vulnerabilities which exist in modern networking protocols.

- IP Spoofing
- TCP sequence prediction
- ICMP-based attacks

It is unlikely that these problems will be addressed until abused on a wide enough scale to force a change in the status quo.