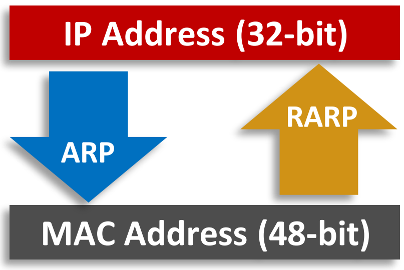
ARP (Address Resolution Protocol) – Cheat Sheet – Part-1 v1

Version 2

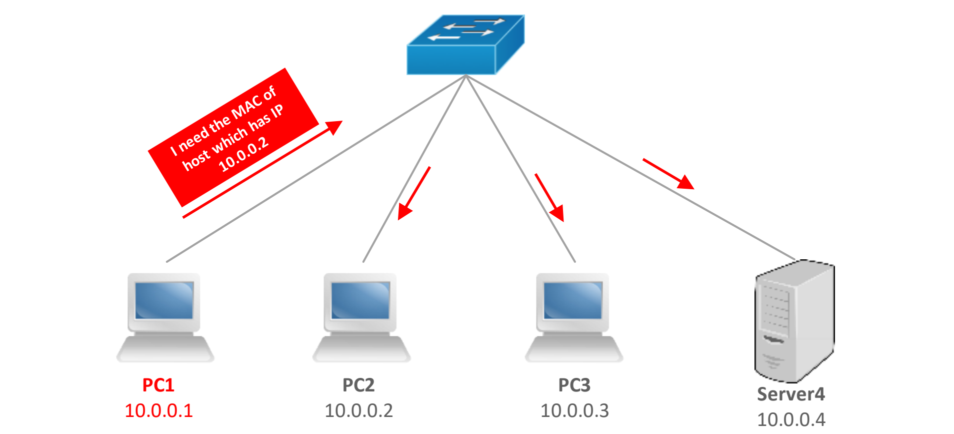
Key Attributes

Protocol Type:	Layer2 (Data Link Layer)
Purpose:	Physical to Logical Address mapping (IP to MAC)
Standard:	RFC826 (1982)
Founder:	David C. Plummer

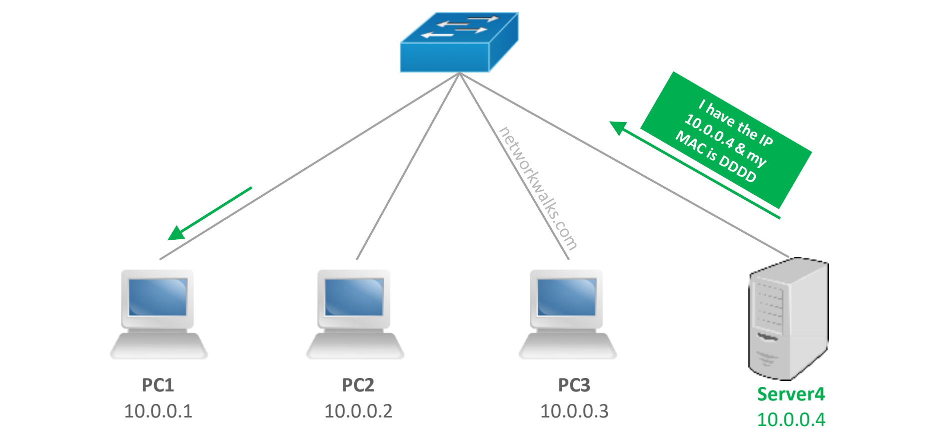
"ARP is a Layer-2 Protocol used for discovering MAC from IP Address"



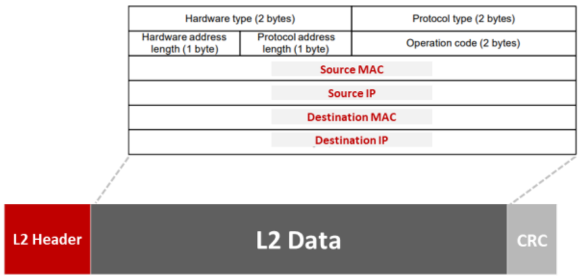
ARP Request



ARP Reply



ARP Frame Format



Hardware type (2 bytes)		Protocol type (2 bytes)
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes)
Source MAC		
Source IP		
Destination MAC		
Destination IP		

ARP Types

ARP	IP to MAC mapping
Inverse ARP	MAC to IP mapping
Proxy ARP	A security feature in which a proxy device on the network answers the ARP queries for an IP address that is not on that network
Gratuitous ARP	ARP request issued by an IP address and addressed to the same IP address to confirm duplicate IP on the subnet
Serial Line ARP (SLARP)	ARP request used for serial interfaces that use HDLC encapsulation
Reverse ARP	Mapping MAC to IP for someone else. RARP is obsolete now. It was replaced by BOOTP & later by DHCP.

ARP Security Threats

ARP does not provide methods for authenticating ARP replies on a network. Therefore, a forged ARP Request or Reply from a local attacker can be used to update the ARP cache of a remote system with a forged entry (ARP Poisoning) which is used to redirect IP traffic to other hosts. Some common types of Attacks include:

- **ARP Spoofing Attacks:** Attacker sends forged ARP frames & ARP replies & maps Victim's IP with Attacker's MAC (e.g. Ettercap Tool)
- **ARP Poisoning Attacks:** After ARP Spoofing, the attacker poisons the victim's ARP table & creates forged MAC-to-IP mappings
- **DoS Attacks:** After ARP Spoofing, attacker is able to perform DoS Attacks
- **MiTM (Sniffing) Attacks:** After ARP Spoofing, attacker is able to perform MiTM Attacks
- **Session Hijacking Attacks:** After ARP Spoofing, attacker is able to perform Session Hijacking Attacks

ARP Security Mitigations

- ✓ Use DAI (Dynamic ARP Inspection) to prevent ARP Poisoning Attacks
- ✓ Use the DHCP Snooping Database with other techniques to secure ARP
- ✓ Use Packet filters that do not allow Packets with conflicting info (e.g. packets that come from outside but have an inside source IP)
- ✓ Implement Strict Admission Control Policies
- ✓ Implement Port Security. Do not allow any device to connect without Authentication
- ✓ Use ARP spoofing detection software which inspect and certify data before it is transmitted and block the data that appears to be spoofed
- ✓ Use cryptographic network protocols like TLS, SSH, HTTPS and other secure communications protocols to prevent ARP spoofing attack by encrypting data prior to transmission and authenticating data when it is received

ARP Commands (Cisco)

ARP feature is enabled on all vendor equipment by default and is set to use Ethernet encapsulation usually but we can create static ARP entries as well as in below:

```
R1(config)# arp 10.0.0.0 aabb.cc03.8200 arpa
R1# clear arp-cache          R1# show ip arp
```

network Walks

/Network Walks

/NetworkWalks

/company/networkwalks

Your Feedback, Comments are always Welcomed: info@networkwalks.com