BootP and DHCP

Flexible and Scalable Host Configuration

Shortcomings of RARP

- *Reverse Address Resolution Protocol*
- Only IP Address distribution
- No subnet mask
- Using hardware address for identification
- New methods needed: BOOTP, DHCP

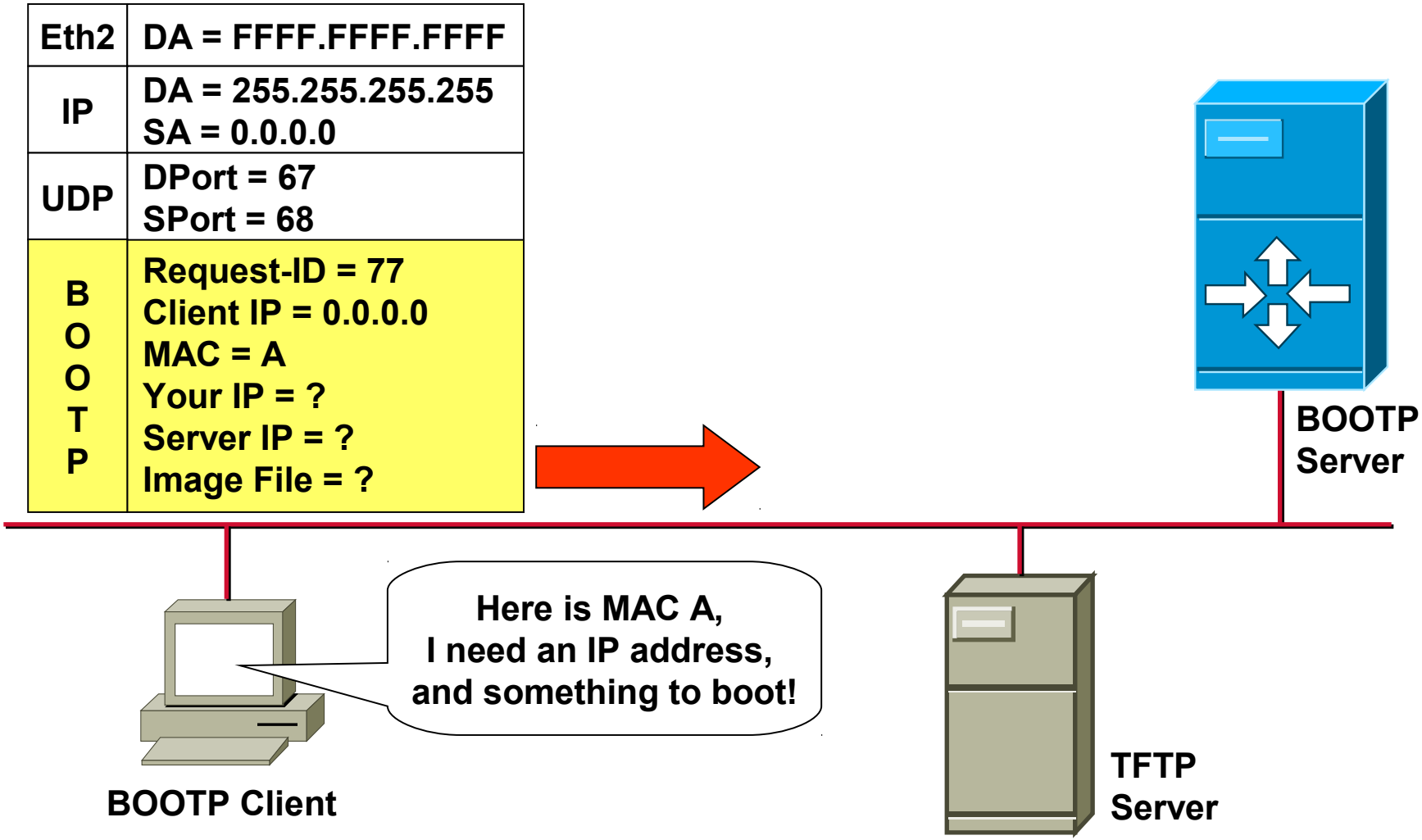
Bootstrap Protocol (BOOTP)

A static solution with many parameters

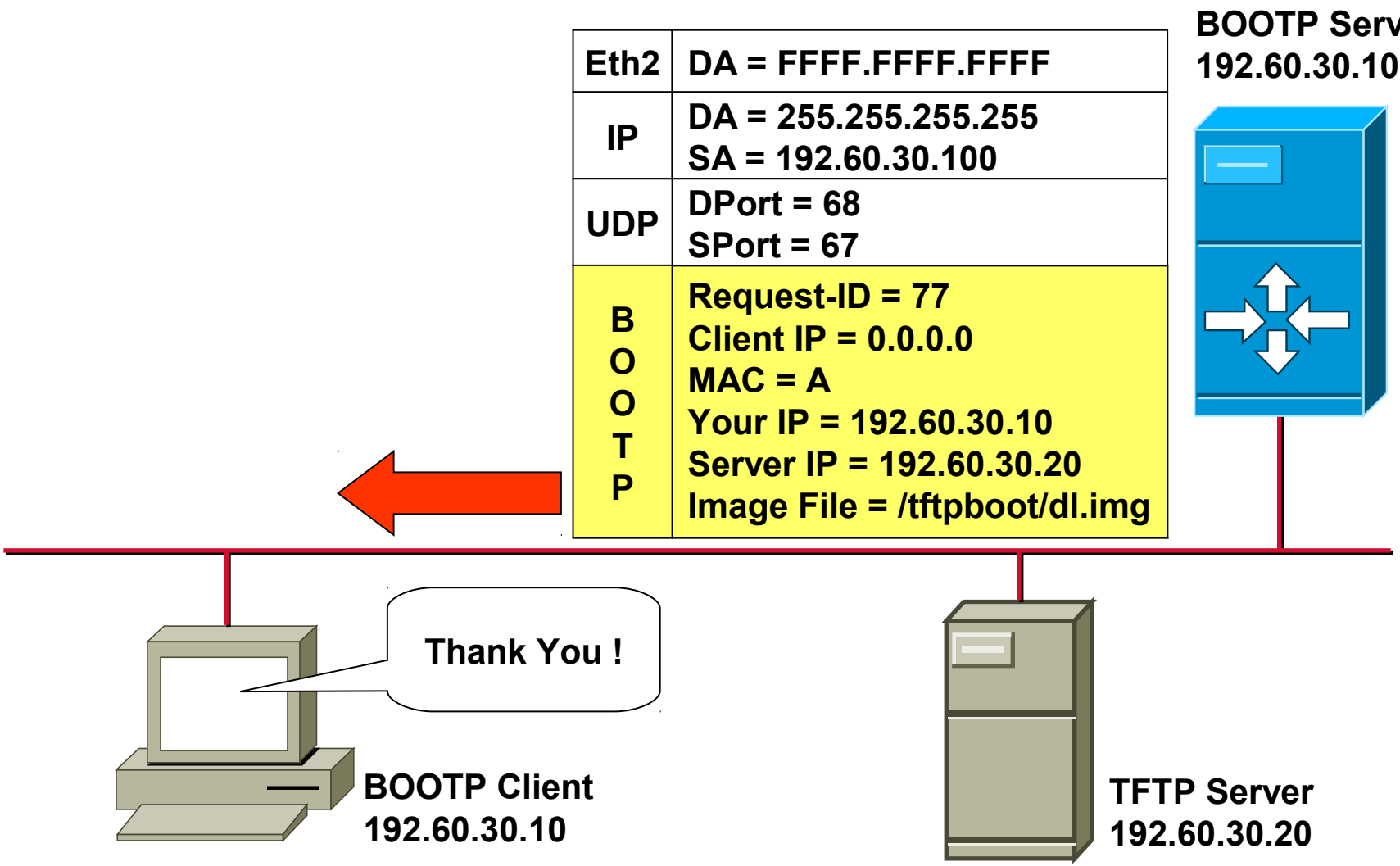
Goal

- Clients request IP address and other parameters from server
  - Subnet mask, configuration filename, ...
- IP addresses are predefined in a list
  - Fixed mapping MAC address ➔ IP address
- Defined in RFC 951 and RFC 1048

Bootstrap


Eth2
DA = FFFF.FFFF.FFFF
IP
DA = 255.255.255.255
SA = 0.0.0.0
UDP
DPort = 67
SPort = 68
BOOTP
Request-ID = 77
Client IP = 0.0.0.0
MAC = A
Your IP = ?
Server IP = ?
Image File = ?
BOOTP Server
Here is MAC A,
I need an IP address,
and something to boot!
BOOTP Client
TFTP Server

Bootstrap


BOOTP Server
192.60.30.100
Eth2
DA = FFFF.FFFF.FFFF
IP
DA = 255.255.255.255
SA = 192.60.30.100
UDP
DPort = 68
SPort = 67
BOOTP
Request-ID = 77
Client IP = 0.0.0.0
MAC = A
Your IP = 192.60.30.10
Server IP = 192.60.30.20
Image File = /tftpboot/dl.img
Thank You !
BOOTP Client
192.60.30.10
TFTP Server
192.60.30.20

Principles

- Separation of the boot task into a BOOTP-part and a TFTP-part
- BOOTP server only needs to maintain a small database !
- Image- and configuration-files can be stored on another machine
- BOOTP client is responsible for error detection

BOOTP - Message Format

OP	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECONDS		RESERVED	
CLIENT IP ADDRESS			
YOUR IP ADDRESS			
SERVER IP ADDRESS			
ROUTER IP ADDRESS			
CLIENT HARDWARE ADDRESS (16 Octets)			
SERVER HOST NAME (64 Octets)			
BOOTFILENAME (128 Octets)			
VENDOR SPECIFIC AREA (64 Octets)			

BootP - Message Fields

- Operation Code (OP)
  - Message Type
- Hardware Address Type (HTYPE)
- Hardware Address Length (HLEN)
- Hops
  - Broadcast loop/storm avoidance
  - Increased/checked by routers

BootP - Message Fields

- Transaction ID
  - Used for identification (random number)
- Seconds
  - Seconds elapsed since client started trying to boot
- Client IP-address
  - Filled in by client in boot request if known
- Your IP-address
  - Filled by server if client doesn't know its own address

BootP - Message Fields

- Server IP-address
  - Returned in boot reply by server
- Router IP-address
  - Server is part of another Subnet
  - IP-address of the BootP relay
- Client Hardware-address
  - MAC-address of client

BootP - Message Fields

- **Server Host Name**
  - Optional server host name
- **Bootfilename**
  - Contains directory path and filename of the bootfile
- **Vendor Specific Area**
  - Optionally contain vendor information of the BootP server
  - RFC 1048: also possible to mention the subnet mask, hostname, domain name, DNS, etc

Dynamic Host Configuration Protocol (DHCP)

A dynamic solution with even more parameters

Principles

- Nearly identical to BOOTP
  - Slightly extended messages only
  - More parameters
- Uses UDP communication
  - Client-Side: Port 67
  - Server-Side: Port 68
- Based on a leasing idea!
  - Dynamic configuration
- RFC 2131 and RFC 2132

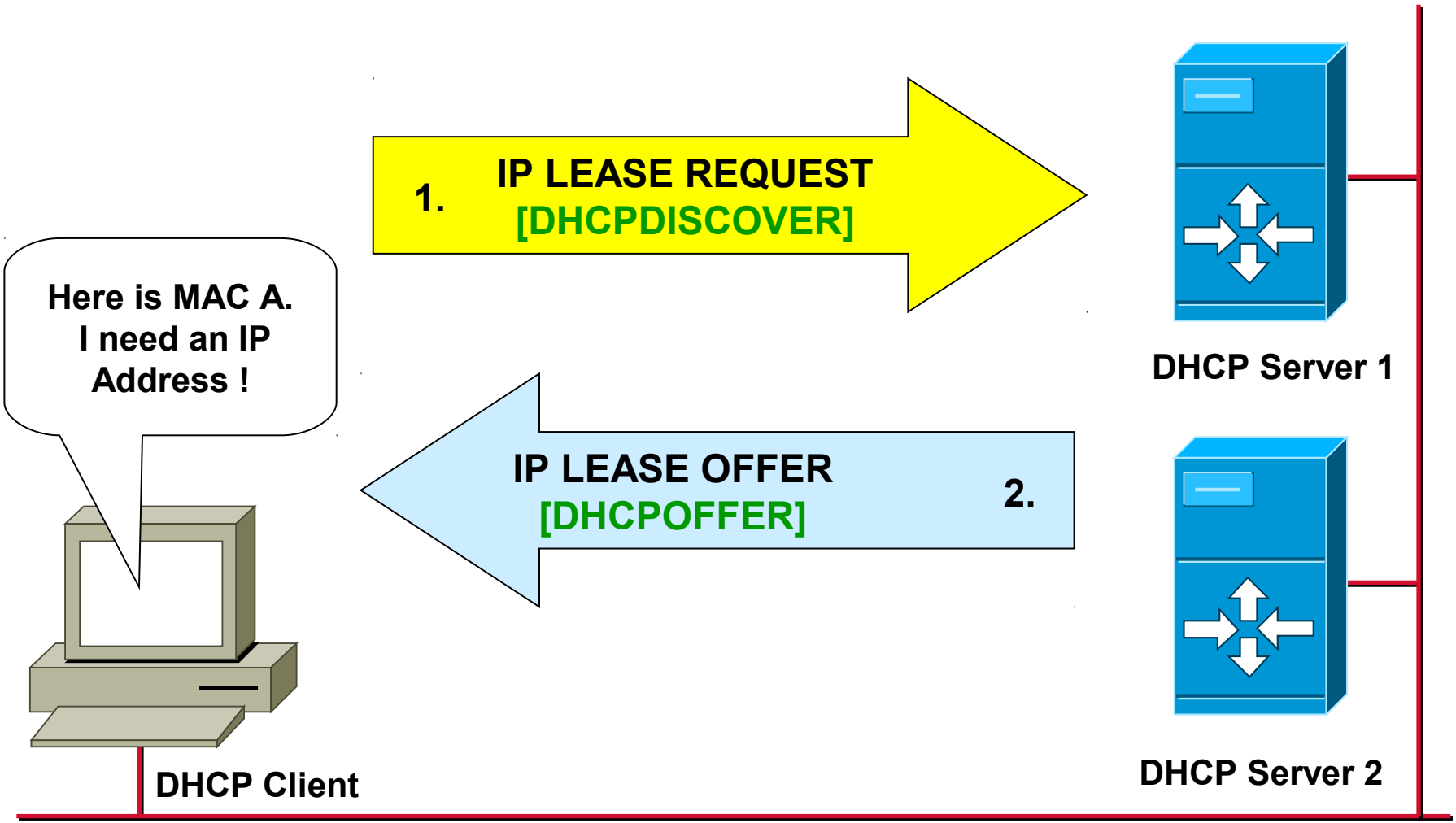
Flexible Configurations

- **Automatic:** Host gets permanent address
- **Dynamic:** Address has expiration date/time (leasing) !
- **Manual:** Fixed mapping MAC → IP

Parameters

- IP address
- Subnet mask
- DNS Server
- NetBIOS Name Server
- List of default gateways
- Ethernet Encapsulation
- Router Discovery (RFC 1256)
- Path MTU Discovery (RFC 1191)
- etc...

How Does It Work - 1

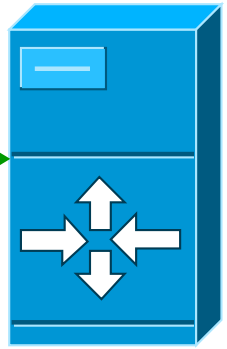


How Does It Work - 1

DETAILED

1. DHCPDISCOVER

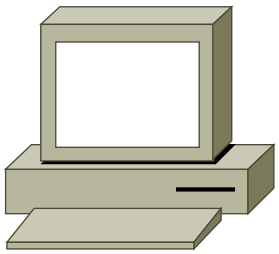
Source IP Address: 0.0.0.0
Dest. IP Address: 255.255.255.255
HW Address: MAC A



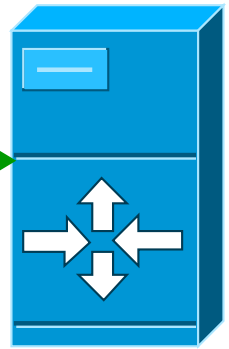
10.1.0.10

DHCPOFFER 2.

Source IP Address: 10.1.0.20
Dest. IP Address: 255.255.255.255
Offered IP Address: 10.1.0.99
Client HW Address: MAC A
Subnetmask: 255.255.255.0
Leaselength: 48h
Server ID: 10.1.0.20

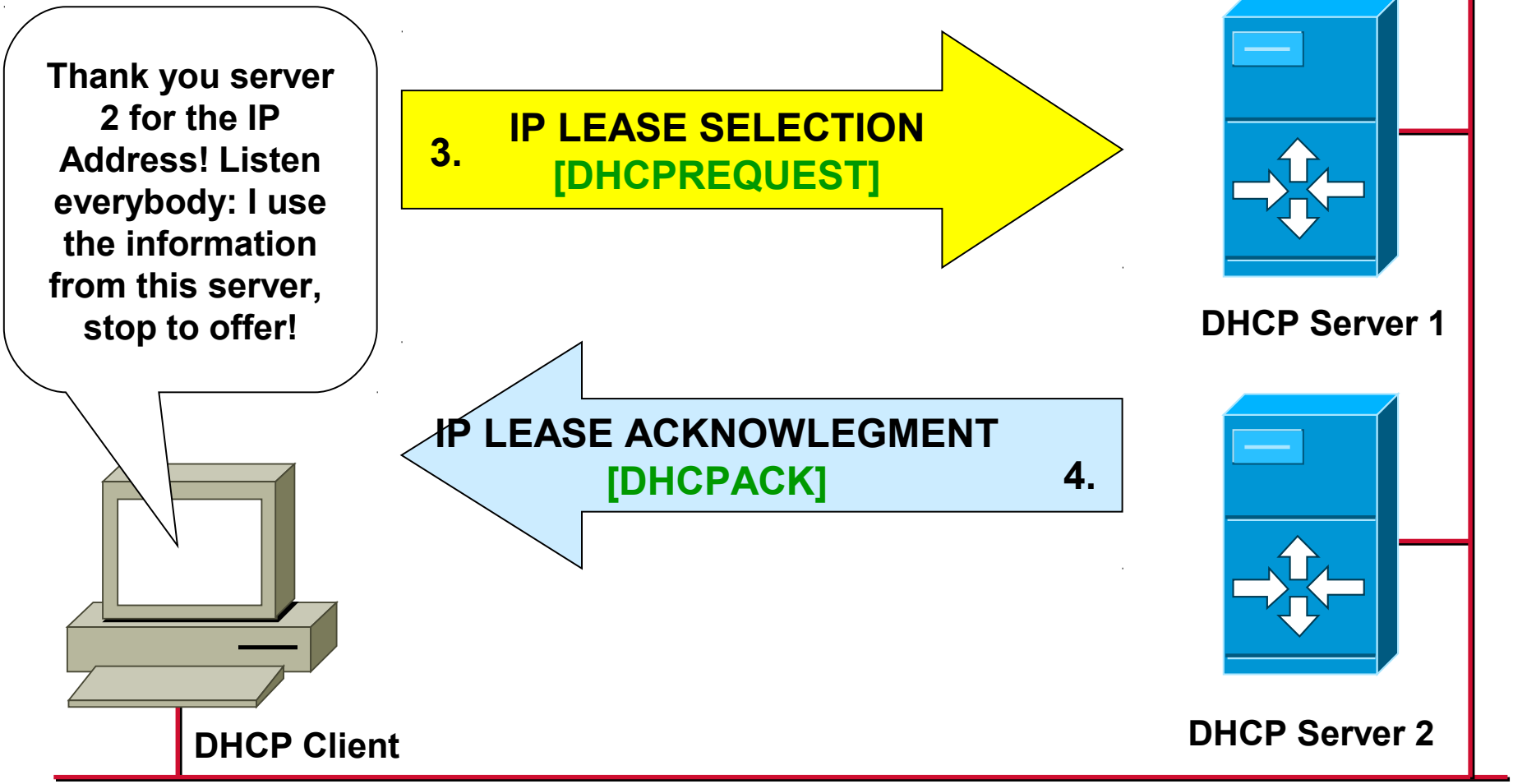


10.1.0.99



10.1.0.20

How Does It Work - 2

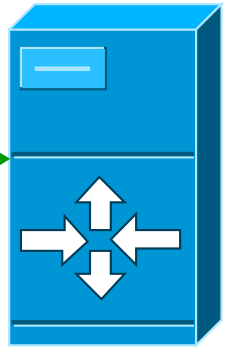


How Does It Work - 2

DETAILED

3. DHCPREQUEST

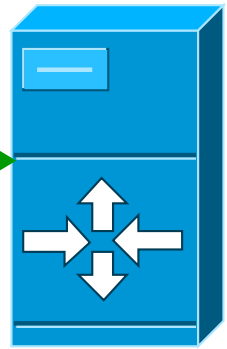
Source IP Address: 0.0.0.0
Dest. IP Address: 255.255.255.255
HW Address: MAC A
Req. IP Address: 10.1.0.99
Server ID: 10.1.0.20



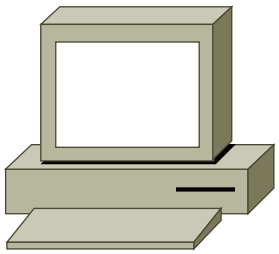
10.1.0.10

DHCPACK 4.

Source IP Address: 10.1.0.20
Dest. IP Address: 255.255.255.255
Offered IP Address: 10.1.0.99
Client HW Address: MAC A
Subnetmask: 255.255.255.0
Leaselength: 48h
Server ID: 10.1.0.20



10.1.0.20



10.1.0.99

Bound

- DHCPACK (success) is send by the server who's offer was accepted
- Client receives the DHCPACK
- Client enters the BOUND state
- TCP/IP is completely initialized

DHCPNACK

- DHCPNACK (no success) will be send if
  - Client tries to lease the previous IP address, but this address is no longer available
  - Client's IP address is invalid
  - Client may have been moved to an other subnet

DHCP - Message Format

OP	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECONDS		FLAGS FIELD	
CLIENT IP ADDRESS			
YOUR IP ADDRESS			
SERVER IP ADDRESS			
ROUTER IP ADDRESS			
CLIENT HARDWARE ADDRESS (64 Octets)			
SERVER HOST NAME (64 Octets)			
BOOTFILENAME (128 Octets)			
OPTIONS (312 Octets) DHCP MESSAGES !			

DHCP-specific Message Fields

- DHCPDICOVER
  - Client broadcast to find DHCP server
- DHCPOFFER
  - Response to a DHCPDISCOVER
  - Offering an IP address
- DHCPREQUEST
  - Request the parameters offered by one server
- DHCPINFORM
  - Client ask for more information

DHCP-specific Message Fields

- DHCPACK
  - Acknowledgement from server to client
- DHCPNACK
  - Negative ACK from server to client
- DHCPDECLINE
  - Message from server to client indicating an error
- DHCPRELEASE
  - Message from server to client canceling a lease and relinquishing network address

Timer

- After DHCPACK → beginning of the lease period is registered
- Located in the DHCPACK message
  - Lease Time
  - T1 (renewal attempt)
  - T2 (sub renewal attempt)
- T1 and T2 are configured at the DHCP server
  - T1 = 0,5 x lease time
  - T2 = 0,875 x lease time

Timer

- T1 and T2 start when client is bound
- Client RENEW the lease when T1 expired
  - Client enters RENEWING state and sends a DHCPREQUEST to the server
  - If server accept, a DHCPACK contains a new lease time

Timer

- If the lease could not be RENEWED after T1, the client makes another try after T2
  - Client try to connect other DHCP server
- DHCP server can answer with
  - DHCPACK and RENEWING the lease
  - DHCPNACK to force the client to reinitialize

Subnets

- DHCP is related to BootP
- DHCP messages are broadcast based
  - Not forwarded by routers
  - Or routers are configured as BOOTP Relay Agent