

Panel 1

Last time:

IP v6 header format

IP v6 addressing

8 groups of 4 hex # (with shortcuts)

IP v4 versus IP v6

- bigger address space
- no checksums for IP header
- QoS
- no fragmentation

⇒ Transport layer

- reliable source to dest. delivery!

Panel 2

⑤ Group 1: Firewall

Jeff Johnson + Steve Marinelli

④ Group 2: DNS

Frank Gonnello + Thomas Ockenhaus

③ Group 3: DHCP

Anthony Ambrose + Stefano Polo ✓

① Group 4: ICMP

Yuri Aleshkin + Ed Mikuszewski ✓

② Group 5: ARP + RARP

Chris Dubra + Michael Malinkov ✓

Panel 3

ICMP
Internet Control Message Protocol

Layer - Network layer

Version IP v4 & IP v6

Purpose Using networked computers - this protocol send error messages -

Messages - constructed @ the IP layer using datagram packets
- come from host and then are transmitted by use of datagram packets

Panel 4

IP datagram

Example router \Rightarrow TTL \Rightarrow sent to source datagram results in either error message or not

Utilites
tracert command - takes UDP datagram with IP TTL header field then is transmitted - with message

ping command - simply implemented by using echo messages \rightarrow reply \rightarrow request

Panel 5

The diagram illustrates the structure of an ICMP packet within an IP packet. It is shown as a sequence of four fields: MAC, IP head, ICMP head, and Data. The ICMP head is further detailed as a table with three columns: type (8 bits), code (8 bits), and ICMP checksum (16 bits). Below the diagram, it notes that there are 41 different types of ICMP and provides two examples: type 0 for echo reply and type 30 for trace.

MAC	IP head	ICMP head	Data
-----	---------	-----------	------

ICMP header		
8	8	16
type	code	ICMP checksum
	data	

41 different types of ICMP
example: type 0 = echo reply
type 30 = trace

Panel 6

The slide features a large orange horizontal bar at the top with the title "ARP AND NARP" in white text. Below this bar, the names of the presenters, Christopher J Dutra and Michael Malenkov, and their affiliation, Seton Hall University, are listed in a centered, black serif font.

ARP AND NARP

Christopher J Dutra
Michael Malenkov
Seton Hall University

Panel 7

Use Case of ARP

- Two hosts on **same** network-1 sends packet, 1 receives.
- Two hosts on **different** networks and want to communicate via 1 or more gateways or routers.
- **Router** needs to send packet to another router to reach its final destination.
- **Router** needs to send a packet from 1 host to another host on same network.

7

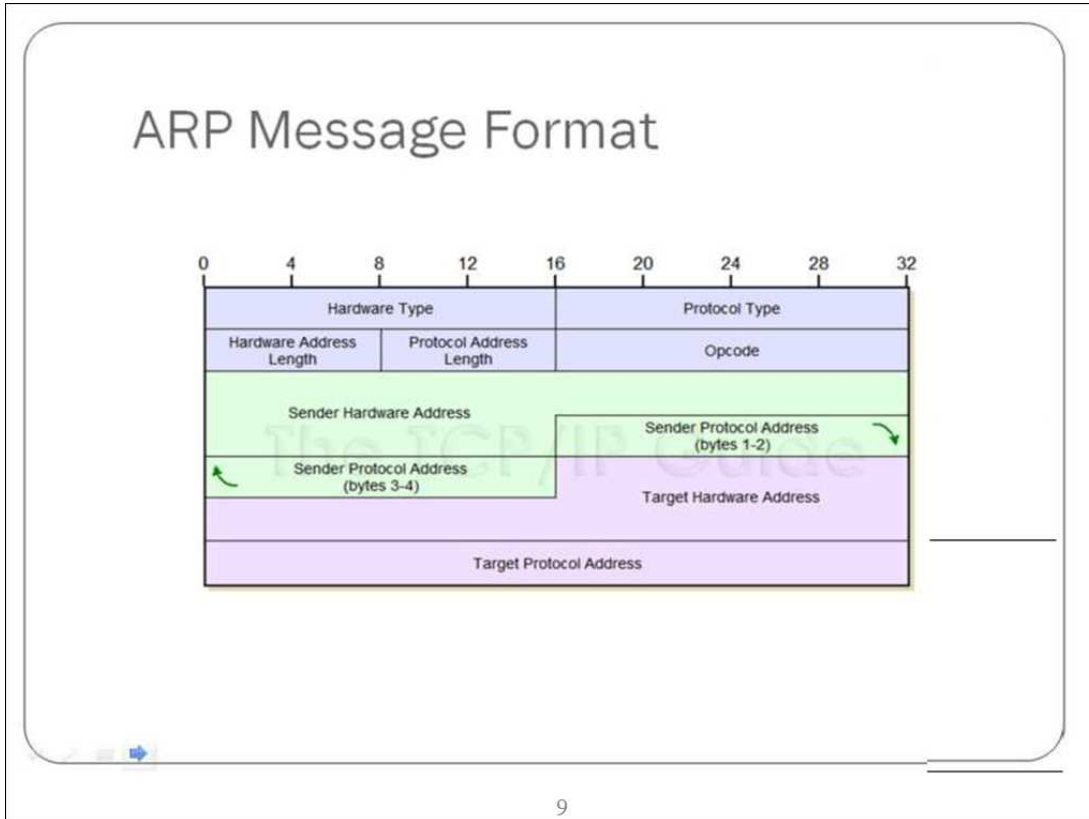
Panel 8

What is ARP?

- *Address Resolution Protocol*-Standard for locating the hardware address of a host only when the network address is available.
- Primarily used to convert IP addresses to Ethernet addresses.

8

Panel 9



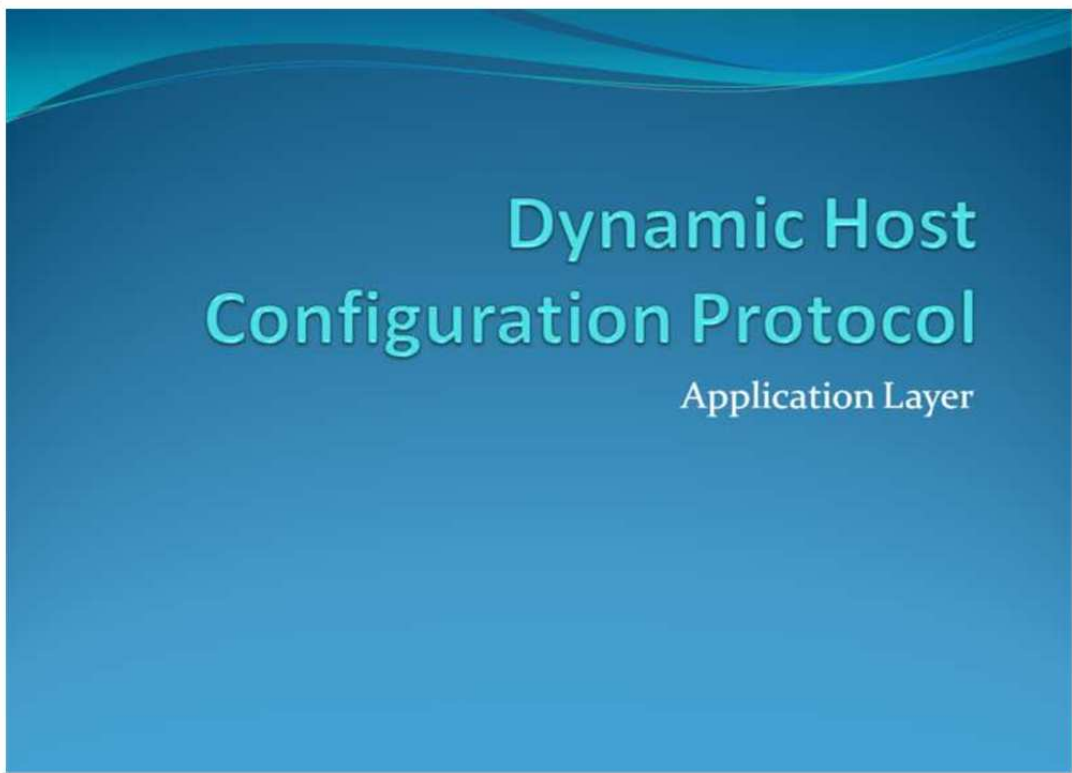
Panel 10

RARP

- Reverse Address Resolution Protocol- gives an IP address when only the hardware address can be found.
- For example, diskless workstations don't have any means of storing an IP address. When workstations are booted up, they only know the hardware address.
- RARP handles that by retrieving the IP.

10

Panel 11



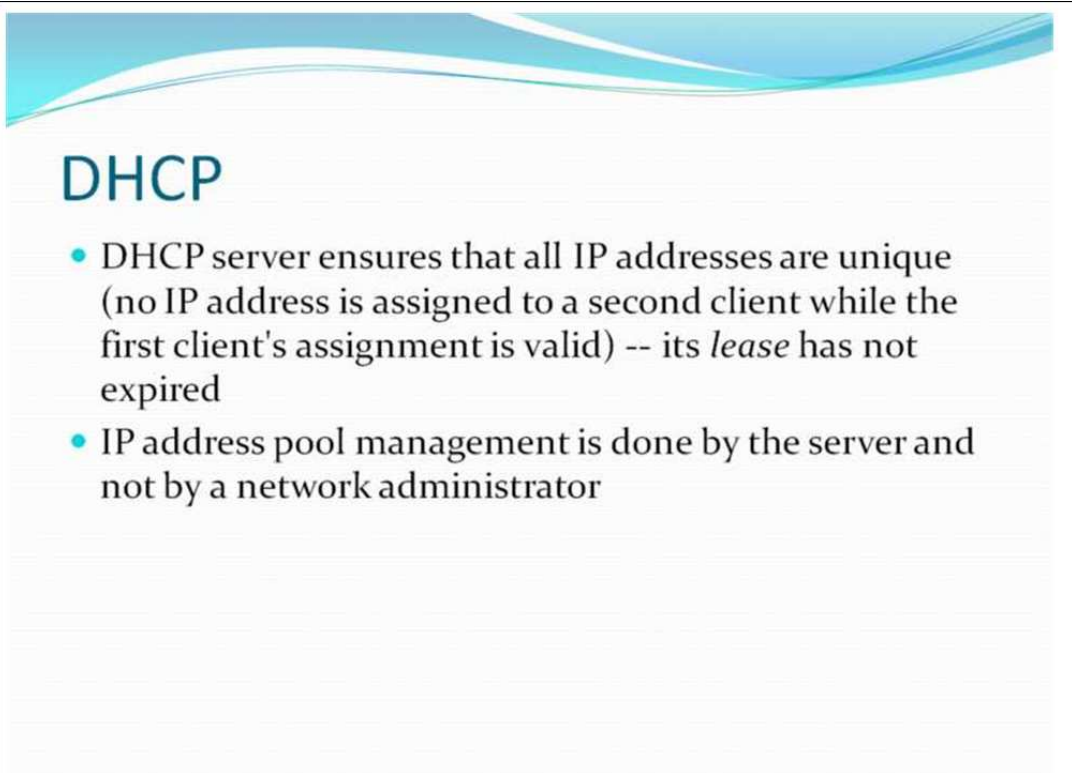
Dynamic Host
Configuration Protocol

Application Layer

11

This slide features a blue background with a wavy pattern at the top. The title 'Dynamic Host Configuration Protocol' is written in a large, light blue font, with 'Application Layer' in a smaller, white font below it. The slide number '11' is centered at the bottom.

Panel 12




DHCP

- DHCP server ensures that all IP addresses are unique (no IP address is assigned to a second client while the first client's assignment is valid) -- its *lease* has not expired
- IP address pool management is done by the server and not by a network administrator

12

This slide has a white background with a blue wavy pattern at the top. The title 'DHCP' is in a large, dark blue font. Below it are two bullet points in black text. The slide number '12' is centered at the bottom.

Panel 13




General Purpose

- Automates the assignment of IP addresses, subnet masks, default gateway, and other IP parameters
- Broadcast query requesting information from DHCP server
- DHCP server manages a pool of IP addresses and client configuration parameters
- Server assigns computer IP address, lease, subnet mask, default gateway

13

Panel 14




General Purpose

- Three modes
 - Dynamic
 - Automatic (DHCP Reservation):
 - Manual

14

Panel 15




Dynamic Mode

- Client is provided a lease on an IP address for a period of time
- Time: hours to months
- DHCP client can request renewal of the lease on the current IP address

15

Panel 16




Other Modes

- Automatic Mode (DHCP Reservation):
 - address is permanently assigned to a client
- Manual:
 - address is selected by the client and the DHCP protocol messages are used to inform the server that the address has been allocated
- Both used when tighter control over IP address is required
- Firewall allows access to the range of IP addresses that can be dynamically allocated by DHCP server

16

Panel 17




Security

- DHCP protocol does not include any security measures
 - Unauthorized DHCP Servers Attack
 - Unauthorized DHCP Clients
- To combat threats
 - authentication information into DHCP messages allowing clients and servers to reject information from invalid sources
- Widespread support
- Many clients and servers do not fully support authentication
- Other security measures are usually implemented around the DHCP server (such as IPSEC)

17

Panel 18



IP Address Allocation

- There are 3 main methods of allocating IP Address
 - **Dynamic** - There is a range of IP address assigned in the DHCP. The client requests an IP address. The request-and-grant process leases an IP Address to the client allowing the DHCP to reclaim the same IP when they are not renewed
 - **Automatic Allocation** - The DHCP server assigns a free IP address to a requesting client from a range defined by the Admin
 - **Manual Allocation** - The DHCP server assigns an IP address based on the table with the MAC Address. Only requesting clients with a MAC address listed in this table will be allocated an IP address.

18

Panel 19

DHCP and firewalls

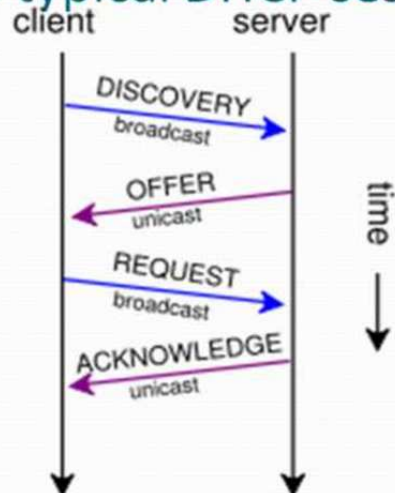
- Firewalls need to permit DHCP traffic explicitly. Packets must have a source address of 0x00000000 or the destination address of 0xffffffff.
- To allow DHCP, network administrators need to allow several types of packets through the server-side firewall. All DHCP packets travel as UDP datagrams; all client-sent packets have source port 68 and destination port 67; all server-sent packets have source port 67 and destination port 68.

HW
think about
it!

19

Panel 20

Schema of a typical DHCP session



20

Panel 21

DHCP discovery

- A client broadcasts through the subnet to find any DHCP servers. The client creates a UDP packet with a broadcast destination of 255.255.255.255.
- A client can also request its last-known IP address. If the client is still in a network where this IP is valid, the server will grant the request otherwise grant the next free IP Address.

21

Panel 22

DHCP offers

- A DHCP server receives an IP lease request. The server reserves an IP address for the client and sends the client an offer. The offer contains the client's Mac address, the IP address being offered, the duration and the DHCP server making the offer.
- The server determines the configuration, based on the client's hardware address

22

Panel 23

DHCP requests

- When the client receives an offer, it must tell the DHCP server that it has accepted the offer. When the client sends out this message, all other DHCP servers will withdraw any IP requests that it sends to the client. They will return any IP address they reserved for the client back to the pool. A client can only accept one offer per network interface.

23

Panel 24

DHCP acknowledgement

- When the DHCP receives the DHCPREQUEST message from a client, it sends an acknowledgment message, DHCPACK, back to the client. At this point, the TCP/IP configuration process is complete. The client has a valid IP address, the server and any other servers acknowledges this and no more requests are sent.

24

Panel 25

DHCP information

- A client can send a request to the DHCP server to request more information than the DHCPACK message had originally obtained. Such queries do not cause the DHCP server to refresh the IP expiry time in its database.

25

Panel 26

DHCP releasing

- The client sends a request to the DHCP server to release the DHCP and the client un-configures its IP address. Clients usually do not know when users may unplug them from the network, the protocol does not mandate the sending of *DHCP Release*.

26