

the **most important points** from the lecture

L3: Network Layer

1) Network Layer Fundamentals

1. The **Network Layer (Layer 3)** enables end devices to exchange data across networks.
 2. The main protocol used at this layer is **IP (Internet Protocol)**.
 3. Two versions exist: **IPv4** and **IPv6**.
 4. The Network Layer performs four basic operations:
 - Addressing
 - Encapsulation
 - Routing
 - De-encapsulation
-

2) IP Encapsulation

5. IP encapsulates the **Transport layer segment** into a packet.
 6. IPv4 or IPv6 can carry Layer 4 data without affecting it.
 7. All Layer 3 devices (routers) examine the IP packet as it travels.
 8. The **Source and Destination IP addresses do not change** from end to end (except when NAT is used).
-

3) IP Characteristics

9. IP is **connectionless**.
 10. It does not establish a session before sending packets.
 11. It does not provide acknowledgments or synchronization.
 12. Reliable delivery is handled by **TCP** at the Transport Layer.
-

4) Important IPv4 Header Fields (Exam Focus)

13. IPv4 header is written in binary format.
 14. IPv4 address size = **32 bits**.
 15. Version field = 4 bits (0100).
 16. **Source IP Address** and **Destination IP Address** are critical fields.
 17. **TTL (Time To Live)** decreases by 1 at each router.
 18. When TTL reaches 0, the packet is discarded.
 19. **Protocol field** identifies next layer protocol (TCP, UDP, ICMP).
 20. **Header Checksum** detects errors in the header.
-

5) IPv4 Limitations

21. IPv4 address depletion (address exhaustion).
 22. NAT broke true end-to-end connectivity.
 23. NAT increases network complexity and troubleshooting difficulty.
-

6) IPv6 Key Points

24. Developed by **IETF**.
 25. Solves IPv4 limitations.
 26. Address size = **128 bits**.
 27. Eliminates the need for NAT (large address space).
 28. Simplified header improves performance.
 29. IPv6 header size = fixed **40 bytes**.
 30. Removed fields from IPv4:
 - Flag
 - Fragment Offset
 - Header Checksum
 31. TTL is replaced with **Hop Limit**.
 32. Includes **Flow Label** field for traffic handling.
-

7) Host Forwarding Decision

33. Packets are always created at the source device.

34. Each host builds its own routing table.

35. A host can send packets to:

- Itself (127.0.0.1 or ::1)
- Local hosts (same LAN)
- Remote hosts (different network)

36. Remote traffic is sent to the **Default Gateway**.

8) Default Gateway

37. Can be a Router or Layer 3 Switch.

38. Must have an IP address within the same LAN network.

39. Forwards traffic outside the local network.

40. Without a default gateway, traffic cannot leave the LAN.

41. In IPv4: configured manually or via DHCP.

42. In IPv6: learned through Router Solicitation or manual configuration.

9) Host Routing Table

43. In Windows, use:

- `route print`
- `netstat -r`

44. Routing table sections:

- Interface List
 - IPv4 Routing Table
 - IPv6 Routing Table
-

10) Router Packet Forwarding Process

45. Router receives a frame.
 46. Removes Layer 2 header.
 47. Examines Destination IP address.
 48. Searches routing table for best match.
 49. Re-encapsulates packet with new Layer 2 header.
 50. Forwards packet out appropriate interface.
-

11) Types of Routes in a Router

51. **Directly Connected (C, L)**
 52. **Remote Routes** (learned statically or dynamically)
 53. *Default Route (S)**
-

12) Static Routing

54. Configured manually.
 55. Requires manual updates when topology changes.
 56. Suitable for small, non-redundant networks.
-

13) Dynamic Routing

57. Automatically discovers remote networks.
58. Maintains up-to-date routing information.
59. Selects best path automatically.
60. Recalculates routes when topology changes.