

# MRL

## Fundamentals of IP

May 5th, 2008

Presented by  
Clinton J. Campbell, CISSP

[ccampbell@mrleng.com](mailto:ccampbell@mrleng.com)

Monte R. Lee & Company  
Consulting Engineers  
Oklahoma City, OK 73116  
Phone: 405-842-2405

[www.mrleng.com](http://www.mrleng.com)

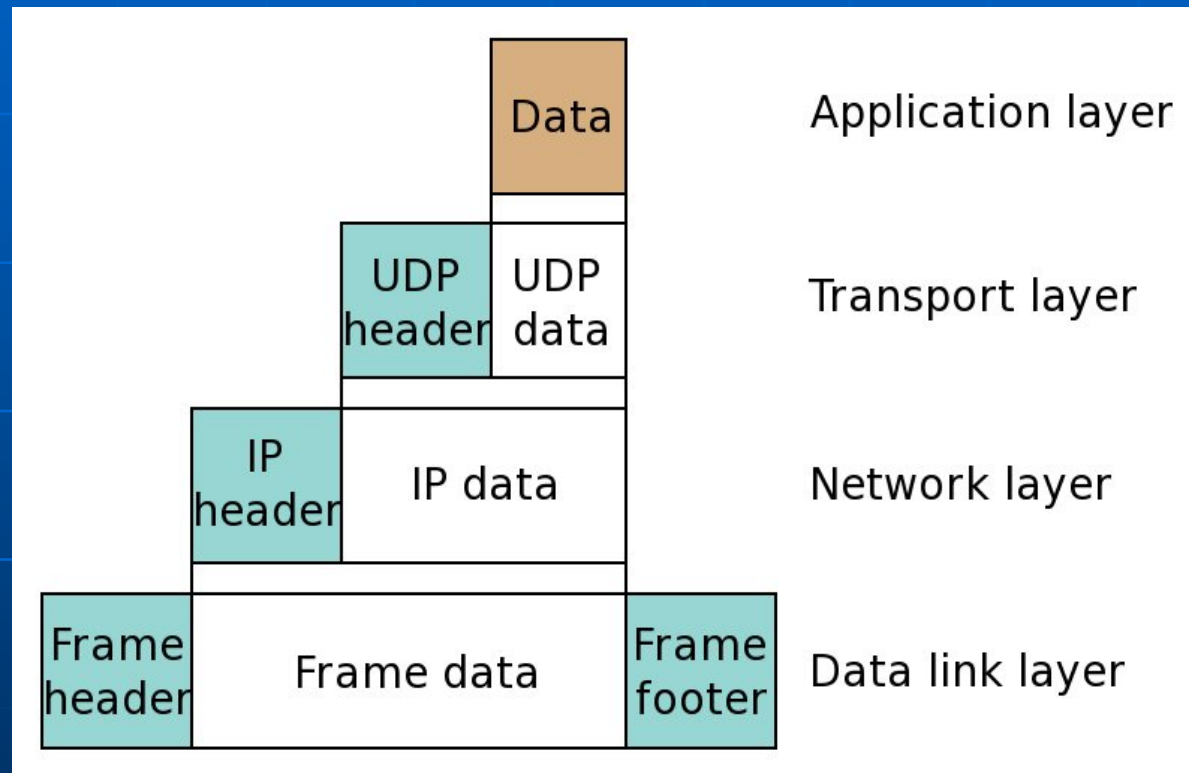
# Overview

- Introduction to IP
  - Protocol structure
  - Network architecture
  - Applications
- Issues relevant to IP Transition
- Security

# Protocol Layering

- Advantages
  - Design
  - Efficiency
- OSI
  - 7 layers: Presentation, Application, Session, Transport, Network, Link, Physical
- TCP/IP
  - 4/5 Layers: Application, Transport, Network, Data link/Physical
  - Not a fundamental design requirement

# Layering in Packets



# IP Layer

- Unique global addressing
  - 32 bit address space
- Functions over heterogeneous networks
- Connectionless
- Best effort delivery
- Error detection

# Packet Structure

- Link layer framing
- IP Header
  - Version, QoS, TTL, length fields, fragmentation, source and destination addresses
  - Options: Source routing, time stamp, record route, etc...
- Packet data
  - Upper layer protocol header
  - Application data

# Addressing

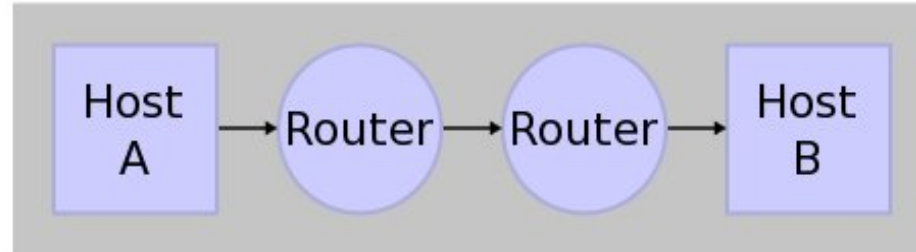
- Hierarchical address scheme
  - Network and host
  - Address classes vs. CIDR
  - Public vs. private address ranges
  - Special addresses
- Port and network address translation

# Transmitting Packets

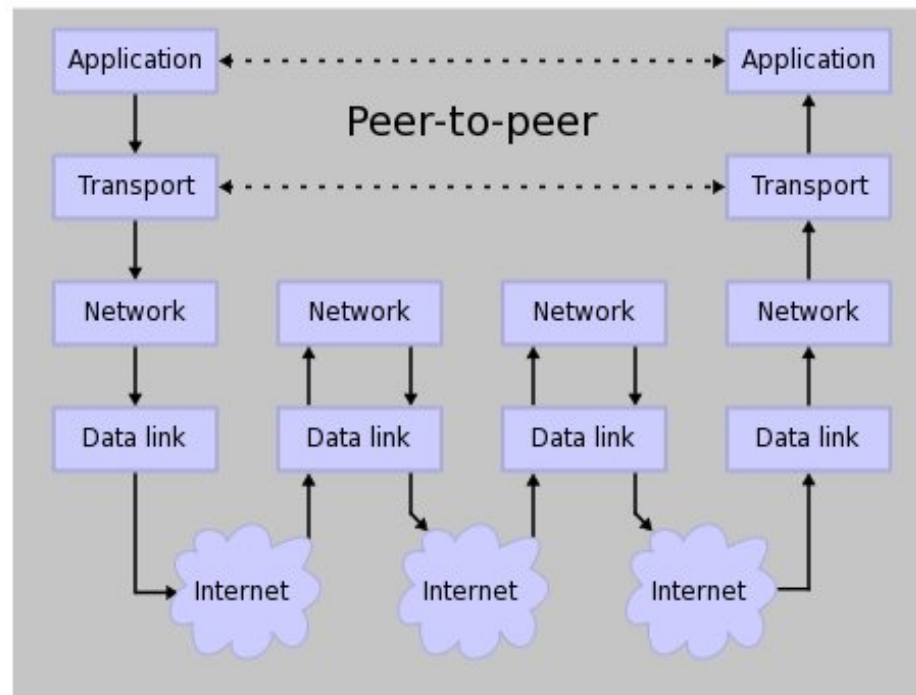
- Link layer
  - Address Resolution Protocol (ARP)
- Network Layer Routing
  - Internet is a “network of networks”
  - State complexity at edges
  - Routing complexity in gateways
    - Interior gateway protocols
    - External gateway protocols

# Transmitting Packets

## Network Connections



## Stack Connections



# Internet Control Message Protocol (ICMP)

- Network layer protocol
- Transported over IP
- Works “hand-in-hand” with IP
  - Network testing (Ping)
  - Error reporting
  - Congestion Reporting
  - Route Redirection

# Transport Layer

- End-to-end communication for applications
- Multiplex using source/destination ports
- User Datagram protocol (UDP)
  - Connectionless
  - Low overhead

# Transport Layer (part 2)

- Transmission Control Protocol (TCP)
  - Connection oriented
  - End-to-end reliability
  - Resequencing
  - Flow control
  - Extra overhead  
(handshake/acknowledgement)

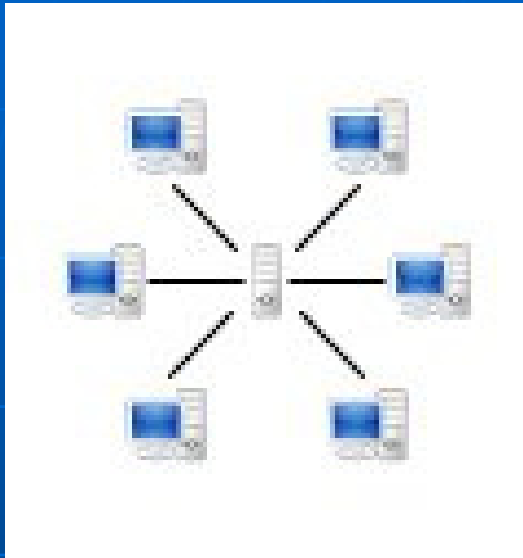
# IPv6

- Addressing (128 bit space)
  - Unicast/multicast/anycast
- ICMPv6
  - Neighbor discovery
  - Autoconfiguration
- Extension headers
- Integrated security and mobility
- Transition mechanisms

# Common Applications

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Hypertext Transfer Protocol (HTTP)
- Email
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (POP3)
  - Internet Message Access Protocol (IMAP)
- Secure Socket Layer (SSL)
- Telnet/Secure Shell (SSH)

# Communication Architectures



- Client-Server

- Web

- Online gaming

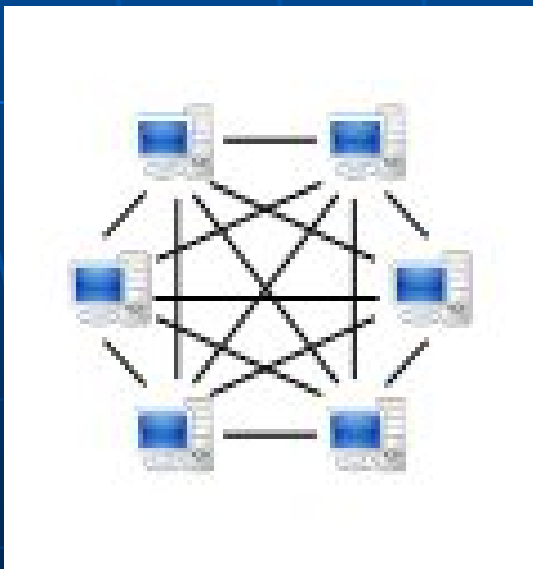
- Database

- Email

- Peer-to-Peer (P2P)

- File sharing networks

- Telephony



# Control/Transmission Protocols

- Session Initiation Protocol (SIP)
- Session Description Protocol (SDP)
- H.323
- Real-time Transport Protocol (RTP)
- Real-time Transport Control Protocol (RTCP)

# Quality of Service (QoS)

- Issues:
  - Dropped/error packets
  - Delay
  - Jitter
  - Out-of-order delivery
- Differentiated Services (DiffServ)
  - Priority markings in packet
  - Queuing strategies to tailor performance

# Security Objectives

- Confidentiality / Integrity / Availability
- Access control
  - Authentication
  - Authorization
- Non-repudiation
- Security vs. complexity (attack surface)
- Layered security & redundancy
- Audit & compliance

# Security Mechanisms

- Network and application security
  - Filtering/firewalls
  - Intrusion detection & prevention
  - Configuration/patch management
  - Identity & access management
- Cryptography
  - IPsec
  - SSL/TLS
  - Key management (PKI/SKM)
  - Standards vs. DIY
- P2P vs. client-server

