Abbreviations and Acronyms

2oo2: Two out of Two
2oo3: Two out of Three
3GPP: 3rd Generation Partnership Project
3oo3: Three out of Three
ACE: Axle Counter Evaluator
ACE: Access Control List
AP: Access Point
API: Application Program Interface
ASK: Amplitude Shift Keying
BFD: Bi-directional Forwarding Detection
BPSK: Binary Phase Shift Keying
B: Business (Used in X2X)
C: Consumer (Used in X2X)
CP: Control Plane
CBTC: Communications-Based Train Control
CBRS: Citizens Broadband Radio Service (150 MHz wideband of 3.5 GHz band)
Cisco FM: Cisco Fluidmesh
CLI: Command Line Interface
COTS: Commercial Off-The-Shelf
CPU: Central Processing Unit
CRC: Cyclic Redundancy Check
CSMA: Carrier Sense Multiple Access
CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
DDoS: Distributed Denial of Service
DF: Don't Fragment
FCAPS: Fault, Configuration, Accounting, Performance, Security
FDM: Frequency Division Multiplexing
FSK: Frequency Shift Keying
FTTH: Fiber-To-The-Home
G: Government (Used in X2X)
gNB: Next Generation Node B
MAC: Medium Access Control/Media Access Control
MF: More Fragments
OFDM: Orthogonal Frequency Division Multiplexing
OS: Operating System
OSI: Open Systems Interconnection
OSS: Operational Support Systems
P: Peer (Used in X2X)
POP: Point of Presence
PSK: Phase Shift Keying
QNS: Qualitative Numerical Data
QoS: Quality of Service
QUIC: Quick UDP Internet Connections
RRD: Round-Robin-Database
RFID: Radio Frequency Identification
RR: Resource Record
RTT: Round Trip Time
RW: Read & Write
SA: Standalone Deployment
SMB: Server Message Block
STP: Shield Twisted Pair
TDM: Time Division Multiplexing
TTL: Time To Live
UTP: Unshielded Twisted Pair

Corporations and Entities

ANSI: American National Standards Institute
AREMA: American Railway Engineering and Maintenance-of-Way Association
CENELEC: European Committee for Electromechanical Standardization
IEEE: Institute of Electrical and Electronics Engineers
ITU: International Telecommunications Union

Files

CSS: Cascading Style Sheets
HTML: Hyper Text Markup Language
JPEG/JPG: Joint Photographic Experts Group
JMX: Java Management Extensions (APIs)
MP3: MPEG Audio Layer 3

Internet and Websites

DNS: Domain Name System
ISP: Internet Service Provider
TLD: Top-Level Domain
URL: Uniform Resource Locator
W3C: World Wide Web Consortium (www)

Networks

5GC: 5G Core Network
AMF: Access and Mobility Management Function
G: Generation (Used in Cellular)
gNB: 5G NR Radio Base Station
LAN: Local Area Network (Building)
LTE: Long Term Evolution
MAN: Metropolitan Area Network (City)
MNO: Mobile Network Operator
NAT: Network Address Translation
NIC: Network Interface Card
NSP: Network Service Provider
PAN: Personal Area Network (Vicinity)
PDN: Packet Data Networks
UE: User Equipment
VLAN: Virtual Local Area Network
VPN: Virtual Private Network (WAN)
WAN: Wide Area Network (Country)
Wi-Fi: Wireless-Fidelity
WPA2: Wi-Fi Protected Access II
WLAN: Wireless Local Access Network
WWAN: Wireless Wide Area Network

Protocols

ARP: Address Resolution Protocol
ATS: Automatic Resolution Protocol
BGP: Border Gateway Protocol
BPDU: Bridge Protocol Data Units
DHCP: Dynamic Host Configuration Protocol
HTTP: Hypertext Transfer Protocol
HTTPS: Hypertext Transfer Protocol Secure
ICMP: Internet Control Message Protocol
IMAP: Internet Message Access Protocol
IP: Internet Protocol
IPsec: Internet Protocol Security
MRP: Media Redundancy Protocol
NTP: Network Time Protocol
POP3: Post Office Protocol version 3
RSTP: Rapid Spanning Tree Protocol
SCEP: Simple Certificate Enrollment Protocol
SFTP: Secure File Transfer Protocol
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
SNTP: Simple Network Time Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

TCP Flags

ACK: Acknowledge
CWR: Congestion Window Reduced
ECE: Explicit Congestion Notification Echo
FIN: Finish
PSH: Push
RST: Reset
SYN: Synchronize
URG: Urgent

General Definitions

Client: A device or software application that requests services or resources from a server.
Daemon: A background program or process that runs independently on a computer system to perform tasks or provide services. Named after Greek mythology's interpretation of a daemon as a mythical being working in the background.
Demultiplexing: The process of separating a combined stream or signal into individual parts. This is done at each layer, where the TCP/UDP port is used in level 4, IP for level 3, MAC address for level 2.
Flat Structure: Minimal or no middle management layers, with few hierarchical levels between employees and executives
Frequency Division Multiplexing: Where different channels are transmitted in different frequency bands.
Host: A device that can send or receive traffic.
Internet: A set of all connected networks (Planet).
Multiplexing: The process of sending multiple signals or streams in a single complex stream. A TCP/UDP port is assigned and added to the stream, along with other headers and the application data.
Network: A group of interconnected nodes/hosts that transports traffic between them
Network Linking Device: Any hardware that connects different network resources. This includes switches, routers, bridges, etc.
Process: A program that runs within the end host. The client starts the communication and the server waits for contact.
Protocol: Denotes how service implementation is carried out.
Server: A powerful computer or system that provides services and resources to other computers on a network, called clients.
Service: What a layer does (IP, TCP, etc.)
Service Interface: Denotes the means of access (e.g. Socket interface).
Standalone Deployment: A system or application that operates independently without relying on other systems or networks for its functionality.
Time Division Multiplexing: A round-robin multiplexing method where each user periodically gets the entire bandwidth for a little burst of time.

Units

bps: Bits per second
dBi: Decibel Isotropic
dBm: Decibel Milliwatts
Gbps: Gigabits per second
Mbps: Megabits per second
Msec: Millisecond

Models

OSI

7. **Application**
6. **Presentation**
5. **Session**
4. **Transport**
3. **Network**
2. **Data Link**
1. **Physical**

TCP/IP Model

4. **Application (OSI 5-7)**
3. **Transport(OSI 4)**
2. **Internet (OSI 2 & 3)**
1. **Network Access (OSI 1)**

To send data, go from layer 7-1 (multiplexing) & for receiving data, go from layer 1-7 (demultiplexing).

General Information

Computer Networks Usage

Business Applications

- Companies use networks for resource sharing with client-server model
- B2B, B2C, G2C, C2C, P2P

Home Applications

- Contains many networked devices (computers, home phones, etc.)
- No fixed client and servers P2P model

Mobile Users

- Smart devices like phones, smart lights, virtual assistants, etc.
- Wireless and mobile related but different

Social Issues

Anonymity: The ability to engage in online activities without revealing your real identity, such as your name, location, or other personally identifiable information.
Censorship: The legal control or suppression of what can be accessed, published, or viewed on the Internet.
Content Ownership: The legal and practical right to control how content is used, distributed, and modified.
Data Theft (Theft of Information): Refers to the unauthorized acquisition of data or information from an individual, organization, or system.
Piracy: The illegal copying, distribution, and use of copyrighted material online.
Network Neutrality: Principle that ISPs should treat all Internet traffic equally, without prioritizing or discriminating against certain content, applications, or services

IEEE802.11 (Wi-Fi)

- Clients communicate via an **AP** that is wired to the rest of the network
- Signals in the ISM band can vary in strength due to many effects such as multipath fading due to reflections
- Requires complex transmission schemes such as **OFDM**
- Radio broadcasts interfere with each other, so designs such as **CSMA** are used

Connection-Oriented & Connectionless

Connection-Oriented: A connection must be set up for ongoing use (and torn down after use). An example is phone calls.

- Reliable message stream (Sequence of pages)
- Reliable byte stream (Movie download)
- Unreliable connection (Voice over IP)

Connectionless: Messages are handled separately. An example is postal service.

- Unreliable datagram (Junk mail)
- Acknowledged datagram (Texting)
- Request-reply (Database query)

Service Primitives

- A service is provided to the layer above as primitives
- Primitives are normally system calls

ACCEPT	Accept an incoming connection from a peer.
CONNECT	Established a connection with a waiting peer.
DISCONNECT	Terminate a connection.
LISTEN	Block waiting for an incoming **connection**.
RECEIVE	Block waiting for an incoming **message**.
SEND	Send a message to a peer.

Network Security

DDoS	Attackers make resources (server, bandwidth) unavailable for legit traffic by overwhelming resource with bogus traffic.
IP Spoofing	Send packet with false source address. Allows for malicious actions without detection.
Packet Sniffing	A network monitoring technique where data packets transmitted across a network are capture and analyzed. A well known software is **Wireshark**
Spy Malware	Records keystrokes, websites visited, upload info to collection site, etc. Can be enrolled in botnet.
Virus	Self-replicating infection by **receiving/executing** object that gets itself executed.
Worm	Self-replicating infection by **passively receiving** object that gets itself executed.

Network Standardization

ITU	Telecommunications	G.992, ADSL, H.264, MPEG4
IEEE	Communications	802.3, Ethernet, 802.11, Wi-Fi
IETF	Internet	RFC (1034, 1035, 2616), HTTP/1.1, DNS
W3C	Web	HTML5 standard, CSS standard

Application Layer

Data

Mail Access Protocols

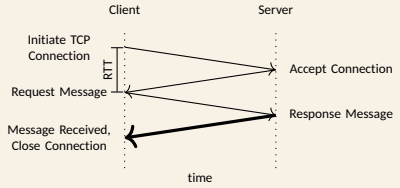
SMTP	• Handshake transfer of messages • Used to send emails from one mail server to another
POP3	• Downloads emails from the server to local device • Downloaded emails are generally unavailable on the server; only available on device
IMAP	• Allows user to access emails on a server and view on multiple devices • Emails remain on server and changes are synchronized

HTTP

- Webpage consists of objects
- Addressable by a single URL with a hostname (www.SOMETHING.idk) and an object pathname (/subdomain/object)
- Not specifically for email, but used for accessing web-based email services over the internet

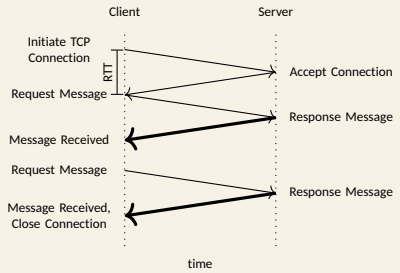
Non-Persistent

- At most one object sent at a time
- Requires multiple connections to download multiple objects
- Closes the connection after sending a response
- **2 RTTs** for sending each object (# of RTT = (2 RTT + time to transmit file) · # of files sent)



Persistent

- Multiple objects can be sent and received with one connection
- Leaves the connection open after sending a response
- **1 RTT** for file sending (# of RTT = 1 RTT for connection + (1 RTT + time to transmit file) · # of files sent)



Request

- ASCII
- Several methods such as GET, POST, etc.
- Uploading forms can be done via POST method or URL method

URL Method

- Used **GET** method
- Inputs are uploaded in the URL fields of the request line, separated with a '?' from the main URL and '&' between inputs

POST Method

CONNECT	Connect through a proxy
DELETE	Remove a web page
GET	Read a web page
HEAD	Read a web page's header
OPTIONS	Query options for a page
PUT	Store a web page
TRACE	Echo the incoming response

Response

1xx	Informational Response	• **100**: Continue • **101**: Switching Protocols
2xx	Successful	• **200**: OK • **201**: Created • **203**: Accepted
3xx	Redirection	• **301**: Moved Permanently
4xx	Client Errors	• **400**: Bad Request • **401**: Unauthorized • **402**: Payment Required • **403**: Forbidden • **404**: Not Found
5xx	Server Errors	• **502**: Bad Gateway • **505**: HTTP Version not supported

Web Cache

- A network entity that satisfies **HTTP** requests on behalf of the origin Web server
- Establishes **TCP** connection with proxy server
- Caches website information to reduce latency, traffic, and response time
- Installed by **ISP**

DNS

- Internet's "phone book"
- Maps **IP** to names and vice versa
- Host aliasing (IP address multiple names, where a complex name can have two simple aliases)
- Mail server aliasing, where it translates from a simple alias mail server to its canonical name and its IP address
- Load distribution between replicated Web servers (Many IP addresses correspond to one server name)

Classes

1. Root DNS Servers (Around 400 around the world managed by 13 different organizations)
2. TLD DNS Servers (org, com, edu, etc.)
3. Authoritative DNS servers (amazon.com, yahoo.com, etc.)

To find the IP address of a website:

1. Client queries one of the root servers to find .com DNS servers
2. Client queries one of the .com DNS servers to get authoritative DNS server
3. Client queries authoritative DNS server to get IP address

Types

- Recursive resolvers
- Root nameservers
- TLD nameservers
- Authoritative nameservers

Components

- Domain namespace
- Distributed database of name servers
- Resolver software that translates domain names into IP addresses

Insert Types

Also known as **DNS Record Types**, DNS Insert Types are the different kinds of information stored in the DNS that map domain names to IP addresses.
RR Format: (Name, Value, Type, TTL) **RR Fields**: (NAME, TYPE, CLASS)

Type	Type ID	Size	Description
A	1	32 bits	Web servers (IPv4)
AAAA	28	128 bits	Web servers (IPv6)
CNAME	5	Variable	Canonical Domain Name
HTTPS	65	4096 bits	HTTPS binding
MX	15	Variable	Mail Servers
NS	2	Variable, up to 255 chars	Authoritative Nameservers
TXT	16	Variable, up to 255 chars	Text record

Inserting Records

1. Register the name at **DNS** registrar
2. Provide the names, the IP addresses of authoritative DNS server (primary and secondary)
3. Inserts two **RRs** (type **NS** and **A**) into all .com TLD server for both authoritative servers (four records)

Note that a **type A** record for web servers and **MX** for mail servers need to be created. (https://www.internic.net)

e.g. elitelu.com
Assume that:

- **dns1.elitelu.com**: 212.221.111.1
- **dns2.elitelu.com**: 212.221.111.2

The final records:

- **elitelu.com, dns1.elitelu.com, NS**
- **elitelu.com, dns1.elitelu.com, A**
- **elitelu.com, dns2.elitelu.com, NS**
- **elitelu.com, dns2.elitelu.com, A**

Vulnerabilities

- DDoS Attacks
- Redirect Attacks (Man in the Middle, DNS poisoning, where bogus replies are sent to DNS server and caches them)

Presentation

Data

- Allows applications to interpret data meaning (how data is presented)
- Same data can mean different things in different formats
- e.g. JPEG, MP3, etc.

Session

Data

- Allows applications to maintain ongoing session
- Responsible for synchronization, check-pointing, OS, and scheduling

Cookies: The saved data from a session, which can be used for authorization, shopping carts, recommendations, and user session state. Four components, which are:

1. Header line for request
2. Header line for response
3. Cookie file on user's device
4. Back-end database

Transport Layer

Segments (TCP)/Datagrams (UDP) | Service-to-Service Delivery

Definitions

Secure Sockets Layer (SSL): A security protocol that provides encryption and authentication for internet communications.

General Information

- Distinguishes data streams-ports
- Provides logical communication between application processes running on different hosts
- Best effort delivery service (tries its best, but makes no guarantees)
- Does not guarantee segment delivery

Implementation

NOT in the network routers, but in end systems

Sender	• Converts application layer messages from a sending application process into segments • The segments break application messages into smaller chunks and add transport layer header to create layer segments • Passes the segment in the network layer, where it is encapsulated within a layer packet and sent to destination • Data sent will have a L4 header to denote where data goes and the type of port it goes to (TCP 1025 → 80)
Receiver	• Network layer extracts the transport layer segment from datagram and passes the segment up to the transport layer

Protocols

- Application developer must specify one of these two transport protocols
- Provides integrity/error checking for the headers
- Both **TCP** and **IP** provide integrity checking by including error-detection fields in their segments' headers
- Port number ranges from 0 to 65536($2^{16} - 1$)
- Port numbers 0 to 1023 are considered well-defined

TCP

(source IP, source TCP Port, destination IP, destination TCP Port)

Source Port	16 bits
Destination Port	16 bits
Sequence Number	32 bits
Acknowledgement Number	32 bits
Data Offset (DOffset)	4 bits
Reserved (Rsrvd)	4 bits
Flags	8 bits
Window	16 bits
Checksum	16 bits
Urgent Pointer	16 bits
Options	Variable (0-320 bits)
Data	Variable

- 20 byte header usually (Can be 21 bytes if from Telnet)
- Provides a "**full-duplex**" service
- Reliable transport, flow control, congestion control (prevents one TCP connection from swamping the links and routers with excess traffic)
- Strives to give each connection traversing a congested link an equal share of the link bandwidth
- Regulates the rate of traffic entering the network
- Does not provide timing, minimum throughput guarantee
- Not secure, but can use **SSL** for encryption
- Used for webpages or anything that requires a specific order
- **RST**, **SYN**, and **FIN** are used for connection setup and teardown
- **CWR** and **ECE** are used in explicit congestion Notification
- **PSH** indicates that the receiver should pas the data to the upper layer immediately
- **URG** bit is used to indicate that there is data in this segment that is marked urgent

Flags (Each 1 bit)

1: CWR	**2: ECE**
3: URG	**4: ACK**
5: PSH	**6: RST**
7: SYN	**8: FIN**

TCP Three-Way Handshake

Suppose **A** is the client and **B** is the server:

SYN	A → B	Used to initiate and establish signal by sending a SYN packet.
SYN-ACK	A ← B	The server responds with a SYN-ACK packet to the client if willing to accept the connection.
ACK	A → B	The client sends an ACK packet back to the server, acknowledging that they received the SYN-ACK packet and completes the handshake. They can send messages now
FIN	A | B	Terminates the connection.

- Ensures both sides are ready
- Synchronizes sequence numbers
- Reliable connection

UDP

(destination IP, destination UDP port)

Source Port	16 bits
Destination Port	16 bits
Length	16 bits
Checksum	16 bits
Data	Variable

- 8 byte header usually
- Unreliable and connectionless (fire and forget protocol)
- Does not provide reliability, flow control, congestion control, security, etc.
- Unregulated so UDP transport can send at any rate
- Used since it is a lot faster so for videos, online gaming, etc.
- **UDP DNS** responses limited to 512 bytes; responses exceeding this are truncated

SMB

- Network file sharing protocol that allows devices to share files and printers across a network

QUIC

- General purpose transport layer
- Supported by major search browsers such as Google Chrome, Microsoft Edge, Mozilla Firefox, Safari, etc.
- Improves the connection of connection-oriented web applications used TCP previously

Reserved Ports

TCP 20/21: FTP
TCP 22: SSH
TCP 23: Telnet
TCP 25: SMTP
TCP 43: NIC Name
TCP 80: HTTP
TCP 110: POP3
TCP 143: IMAP
TCP 443: HTTPS
TCP 8080: Alternate HTTP
UDP 53: DNS
UDP 67: DHCP

Network Layer

Packets | End-to-End Delivery

Definitions

ARP Table: A table that maps IP addresses to their corresponding MAC addresses within a local network.
Forwarding: When a packet arrives at router's input link/port and is directed to the appropriate output link. Takes place in a few nanoseconds, and is typically implemented in hardware.
Forwarding Table: A table that determines the correct output interface for a packet to be forwarded.
Host ID: Portion of the IP address used to locate the destination host in the destination network.
Line Card: A modular electronic circuit that transmits and receives ports for LAN and WAN. Found in every port of small and medium-sized routers.
Network ID: Portion of the IP address used to locate the destination network. All 0s if it is the host ID
Prefix: A network portion of an IP address denoted by a / followed by a number indication the number of bits used for the network. For example, IPv6 might indicate /64, which means the first 64 bits of the address are used for the network and the remaining bits identify the host.
Routing: The network-wide process of determining the route from one end user to another. Takes much longer timescales, usually seconds.
Routing Algorithm: Refers to the algorithms that calculate the route/path taken by packets from sender to receiver. Examples include Dijkstra's or A*.
Routing Protocol: Set of rules defining how routers exchange information to determine the best path for forwarding data packets.
Routing Table: A table that stores the destination addresses for networks, hosts, or subnets accessible through a router.
Tunneling: Connects two similar networks even when the middle network is different (IPv6 → IPv4 → IPv6). Packets are encapsulated over the middle network.
Unicast: A one-to-one communication method where a message is sent from a single sender to a specific, individual receiver.

Service

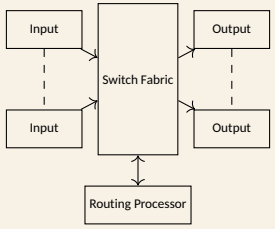
Guaranteed Delivery: Guarantees that a packet sent by a source host will eventually arrive at the destination host.
Guaranteed Delivery With Bounded Delay: No only guarantees delivery, but in a specified host-to-host delay bound (100 msec).
In-Order Packet Delivery: Guarantees packets arrive at destination in the order they were sent.
Guaranteed Minimal Bandwidth: This network-layer service emulates the behavior of a transmission link of a specified bit rate (e.g. 1 Mbps) between sending and receiving hosts. As long as the sending host transmits bits (as part of packets) at a rate below the specified bit rate, then all packets are eventually delivered to the destination host.
Security: The network layer could encrypt all datagrams at the source and decrypt them at the destination, thereby providing confidentiality to all transport-layer segments.

Devices

Gateways	• Connects two dissimilar networks • Connects coax to twisted pair • Most gateways contained in other devices

Router

- Facilitates communication between networks and routing
- Four parts: Input Ports, Output Ports, Routing Processor, Switch Fabric (Present on switches too)
- Packets might also be blocked from exiting a router (malicious sending host or forbidden destination host)



Routing Processor

- Performs control-plane functions
- Executes routing protocols, maintaining routing tables, and computes forwarding table for the router

Switch Fabric

- Responsible for transferring packets between various modules such as NICs, memory blocks, etc.
- Forwards packets from input port to output port

Router Steps

1. Packet comes in through input port
2. Router uses forwarding table to look up output port for the incoming packet
3. Arriving packet gets forwarded via the switch fabric
4. Forwarding table is computed/updated by routing processor
5. Forwarding table is copied by routing processor to the line cards over a separate bus

IP

- Identity of the host
- Connectionless protocol
- Provides internetworking, where routers are used to interconnect heterogeneous networks
- Hierarchical addressing, where all hosts in the same network has the same network ID
- Used to forward datagrams from one network to another network
- Assigned by **ICANN** to avoid conflicts
- Allocated in **prefixes** which is determined by the network portion
- Written by giving the lowest IP address in the block and size of the block
- Unreliable service/protocol since it does not guarantee delivery

Static: Permanent (Servers or other important equipment)
Dynamic: Occasionally changes (Consumers)
Local/Private: Automatically Generated
Public: Assigned by **ISP**

Fragmentation Parameters

Identification	Carries the packet sequence number
DF Bit	Do not fragment
MF Bit	More fragments follow this one
Fragment Offset	Start of the fragment (Multiple of 8)

IPv4

- 4 byte (32 bit) address and written as four octets/each byte (Each byte can go from 0-255)
- Faces address exhaustion, which means that there are not enough address in IPv4
- Requires a subnet mask as a result, which is a 32 bit sequence with a sequence of 1s followed by a block of 0s
- Resulted in the development of **NAT** and **IPv6** due to limited storage

NAT: A process that translates **private IP** addresses in a local network to a **public IP**, which enables multiple devices within a private network to share the same public IP address.
Subnet Mask: A logical subdivision of an IP network that is 32 bits (4 bytes). Dependent on the first byte of the IPv4 address. 255 is for the network and 0 is for the host.

Class A	1-126	255.0.0.0
Class B	128-191	255.255.0.0
Class C	192-223	255.255.255.0

e.g. IPv4 address: 128.112.123.80

- Subnet Mask Class: B
- Network: 128.112
- Host: 123.80

Note: 127 is a loopback. It is reserved for localhost

IPv6

Unicast: Identifies a single interface.
Anycast: Identifies a set of interfaces in such a way that a pack sent to an anycast address is delivered to the closest member of the set.
Multicast: Identifies a group of interfaces in such a way that a packet sent to a multicast address is delivered to all the interfaces in the group

- 16 byte address (128 bits) and written as eight groups of four hexadecimal digits with colons between groups
- e.g. 8000:0000:0000:0000:0134:AF12:1112:EF12
- Can be optimized, where leading 0s can be omitted (0134 → 134) and one or more groups of 0s can be removed with ::
- 8000:0000:0000:0000:0134:AF12:1112:EF12 → 8000::134:AF12:1112:EF12
- IPv4 → IPv6 by just adding :: (192.33.21.46 → ::192.33.21.46)
- No fragmentation fields and no header checksum
- There are no broadcast address since multicast addresses took over

Extension Header (In Order)	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

Internet Control Protocols

ICMP (Internet Control Message Protocol)

- Companion to IP that returns error info
- Required and used in many ways
- If something unexpected occurred, the main even is reported to the **sender** by the ICMP

Message Type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and Echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with a timestamp
Router advertisement/solicitation	Find a nearby router

ARP (Address Resolution Protocol)

- Finds Ethernet address of a local IP address
- Provides a mechanism to translate IP address to link-layer addresses
- Host queries an address and the owner replies
- Resolves the hardware address, where the request ARP broadcasts the request message and the target ARP responds with the target hardware address

Suppose that **A** wants to send a datagram to **B**, where **B's MAC address** is not in **A's ARP table**.

Same LAN	Different LAN
1. **A** broadcasts its ARP query packet, containing **B**'s IP address with a destination MAC address = FF-FF-FF-FF-FF-FF 2. **B** receives the ARP packet, replies to **A** with its MAC address and the frame is sent to **A**'s MAC address (unicast) 3. **A** caches IP-to-MAC address pair in its ARP table until information times out unless refreshed (plug-and-play)	• Data sent must use an intermediate **R** 1. Focus on addressing at IP (datagram) and MAC layer (frame) 2. Assume **A** knows **B**'s IP address 3. Assume **A** knows IP address of the first hop router, which is configured with the gateway 4. Assume **A** knows **R**'s MAC address by using the ARP

DHCP (Dynamic Host Configuration Protocol)

- Assigns a local IP address to host (either get it through hard coded by the system admin in a file or dynamically get the address from a server)
- Gets host started by automatically configuring it
- Host sends request to server, which grants a lease
- Can return the allocated IP address on a subnet along with the address of the first-hop router for the client (default gateway), name and IP address of the DNS server, and a network mask, which indicates network and host portion of the address
- Technically also part of level 7 since it manipulates layer 2 based on responses arrive through level 7
- Four step process

DHCPDISCOVER	Host broadcasts the message (OPTIONAL).
DHCPOFFER	DHCP server responds with message (OPTIONAL).
DHCPREQUEST	Host requests IP address and receives a message.
DHCPACK	Sent by servers to acknowledge the DHCPREQUEST and to finalize the lease of an IP address to a client.

Network Topologies

Bus	• All nodes are connected to single bidirectional communication line/cable called the trunk (backbone or segment) • Simple and low cost • One computer can send messages at a times • Passive topology - computers only listen for, not regenerate data
Star	• Centers on one node where all the others are connected and through which messages are sent • More cabling, thus higher costs • If the hub (switch) is down, no communication • Depending on hub, multiple devices can send messages at the same time
Ring	• All nodes connected in a loop/ring and unidirectional • Each computer serves as a repeater • Typical way to send data by token passing • Expensive and difficult to add computers • If one computer fails, whole network fails

Design Issues

- Store-and-Forward Packet Switching (Each router needs to store the entire packet before it can forward it to the next hop)
- Services to Transport Layer (Provides service its immediate upper layer, namely transport layer, through the network transport layer interface)
- Providing Connection Oriented Service
- Providing Connectionless Service

Internetworking

- Joins multiple, different networks into a single larger network
- Networks differ by services, packet size, reliability, security, addressing. etc.
- Connect by providing a common layer to hide differences (common IP layer since IP provides a universal packet format that all routers recognize)

Data Link Layer

Frames | Hop-to-Hop Delivery

Definitions

Carrier Sense Multiple Access / Collision Detection (CSMA/CD): A network access method primarily used in wired Ethernet networks, where multiple devices share a single transmission medium.
Cyclic Redundancy Check (CRC): An error detecting piece of code used to verify integrity by generating a checksum.
Link Layer Address: Name that can also be called a **LAN** address, a physical address, or a **MAC** address
Switch Table: A table that has the information on what interface to use to reach a specific device.

Services

Framing

- All layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link
- Frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields
- Structure specified by link layer protocol

Link Access

- A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link
- e.g. point-to-point links that have a single sender at one end of the link and a single receiver at the other end of the link, the MAC protocol is simple, the sender can send a frame whenever the link is idle

Reliable Delivery

Note: The link-layer reliable delivery can be considered an unnecessary overhead for low bit-error links, including fiber coax, and many twisted-pair copper link

- When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error
- Similar to a transport-layer reliable delivery service, a link-layer reliable delivery service can be achieved with acknowledgements and retransmissions
- Similar to a transport-layer reliable delivery service, a link-layer reliable delivery service can be achieved with acknowledgements and retransmissions
- Many wired link-layer protocols do not provide a reliable delivery service

Error Detection and Correction

Error correction is similar to error detection, except that a receiver not only detects when bit errors have occurred in the frame but also determines exactly where in the frame the errors have occurred (also corrects these errors)

- Link-layer hardware in a receiving node can incorrectly decide that a bit in a frame is zero when it was transmitted as a one, and vice versa
- No need to forward a datagram that has an error, many link-layer protocols provide a mechanism to detect such bit errors
- Done by having the transmitting node include error-detection bits in the frame, and having the receiving node perform an error check
- Usually more sophisticated and is implemented in hardware

Devices

Switches	• Full-duplex (Switching can be done without collisions) • Replaces hubs • Connects different devices on the same network and only intended nodes receives transmissions • Uses a switch table and updates it with incoming frames (learns location of sender and LAN segment) • Fast and secure • Stores and forwards Ethernet frames • Examine incoming frame's MAC address and selectively forward to one or more outgoing links when forwarded on segment • Uses CSMA/CD to access segment • Do not need to be configured (plug-and-play, self-learning) • Hosts unaware of the presence of switches • Hosts have dedicated, direct connection to switches • Buffer packets
Network Interface Cards (NICs)	• Level 1 (Physical item) & 2 (Deals with MAC addressing) • A network adaptor that connects node to the media • Unique MAC address

Sub-Layers

Media Access Control (MAC)	• Gives access to the NIC • Controls access to through media through CSMA/CD and token passing
Logical Link Control (LLC)	• Manages data link interface • Responsible for error detection and ensuring data integrity • Detects transmission errors using CRC and will request any resends

Implementation

- Combination of hardware and software, the place in the protocol stack where software meets hardware
- Implemented in a network adaptor, also sometimes known as a **NIC**
- Network adaptor is the link-layer controller (Usually a single, special-purpose chip that implements many of the link-layer services (framing, link access, error detection, and so on))
- Much of a link-layer controller's functionality is implemented in hardware

Source	The controller does the following: 1. Takes a datagram that has been created and stored in host memory by the higher layers of the protocol stack 2. Encapsulates the datagram in a link-layer frame (Filling in the frame's various fields) 3. Transmits the frame into the communication link, following the link-access protocol
Destination	The controller does the following: 1. Receives the entire frame 2. Extracts the network-layer datagram • If the link layer performs error detection, then it is the sending controller that sets the error-detection bits in the frame header, and it is the receiving controller that performs error detection

MAC Address

- 48-bit (6 bytes/6 paired hexadecimal values) unique identifier administered by IEEE
- 2^{48} possible addresses
- Used to identify a device on a network (no two adaptors have the same address)
- Flat structure (MAC address resembles a person's social security number)
- Were designed to be permanent, but now possible to change through software
- IEEE manages the MAC addresses
- Manufacturers buys portions of MAC address space consisting of 2^{24} addresses for a nominal fee
- IEEE allocates the chunk of 2^{24} addresses by fixing the first 24 bits of a MAC address and letting the company create unique combinations of the last 24 bits for each adaptor
- Used for level 2 addressing
- Burned onto NIC ROM and sometimes software settable
- e.g. 1A-2B-3C-4D-5E-6F
- Portable, unlike IP addresses

Ethernet

- Level 2 and 1 item
- Dominant wired LAN technology that is cheap and simple
- 10 Mbps - 400 Gbps
- Single chip, multiple speeds
- Used to use **bus** topology back in the mid 90s, now using **star** topology
- Connectionless (No handshaking between sending and receiving NICs)
- Unreliable (Receiving NICs doesn't send ACK or NAK to sending NIC)
- Ethernet's MAC protocol: Unslotted CSMA/CD with binary backoff

Parts of the Ethernet Packet and Frame (In order)

Part	Bytes	Information
Preamble	7	• Used to synchronize receiver • 7 bytes of 10101010 • Not part of the frame
Starting Frame Delimiter	1	• Indicates beginning of Ethernet frame • 10101011 • Not part of the frame
MAC Destination	6	• Address of device the packet is intended for • Adaptor passes data in frame to network layer if frame has matching destination address; otherwise thrown out
MAC Source	6	• Address of device the packet originated for
Payload (Data)	42-1500	• Data to be sent
EtherType (Type)	2	• Used to indicate which protocol is encapsulated in the payload of the frame and used for receiving • Mostly IP but others possible like AppleTalk or Novell IPX • Used to demultiplex at receiver
CRC	4	• Checks redundancy at receiver • Thrown out if error detected

Enterprise Access Networks

- Typically used in companies, universities, or any large organization
- Various transmission rates, ranging from 10Mbps to 10Gbps
- End systems typically connect to Ethernet switch

Physical Layer

Bits | Bit-to-Bit Delivery

Definitions

Bandwidth (Electrical Engineering): A measure of the width of a frequency range. Measured with **hz**.
Bandwidth (Computer Scientists): Rate of data transfer. Measured in **bps**
Digital Modulation: The process of converting data bits into signals.
Frequency (f): # of oscillations per second measured using **hz**
Harmonic: A sinusoidal wave with a frequency that is a positive integer multiple of a fundamental frequency of a periodic signal.
Modulation: Process of varying one or more properties of a periodic waveform (the carrier signal) to encode information onto it.
Period (T): Time between two consecutive max or min. $T = 1/f$
STP: Type of copper cable that consists of a pair of wires twisted together. Has an additional shield layer to reduce interference, but harder to install and more expensive.
UTP: Type of copper cable that consists of a pair of wires twisted together. Does not have an additional shield layer.
Wavelength (λ): Distance between two max or min. $\lambda = c/f$ in a vacuum.

Devices

Hub	• Center of star network • All nodes receive transmitted packets • Slow and insecure
Repeater	• Repeats signal since signals lose intensity due to energy loss

General Information

- Foundation where other layers are built on
- Determines **throughput**, **latency**, **error rate**
- Modulation needed to convert analog to digital

Fourier Analysis

$$g(t) = \frac{c}{2} + \sum_{n=1}^{\infty} a_n \sin(2\pi \text{nft}) + \sum_{n=1}^{\infty} b_n \cos(2\pi \text{nft})$$

- Time varying signal can be represented harmonics or infinite number of sines and cosines
- a_n and b_n are the sine and cosine amplitudes of the nth harmonic (terms) and c is a constant

Bandwidth-Limited Signals

- Having less bandwidth = losing some harmonics
- Degrades the received signal

Media Properties

- Bandwidth
- Delay
- Cost
- Ease of installation
- Maintenance

Guided Media

- Copper Wire (Twisted pairs, Coaxial Cable, Power lines)
- Fiber Optics (Single-mode, Multi-mode)

Unguided Media

- Terrestrial wireless
- Satellite
- Lasers through the air

Wires

Link Terminology

Full-duplex	• Bidirectional simultaneous transmission • e.g. Use different twisted pairs for each direction
Half-duplex	• Bidirectional but not simultaneous transmission • e.g. Senders taking turns
Simplex	• Only one fixed direction at all times • Not common

Twisted Pair

- Two insulated copper wires
- Used in LANs and telephone lines
- Twists reduce radiated signal (interference)
- Signal carried as the difference in voltage between two wires

Category 5 (CAT5)	• Half-duplex and **UTP** • Has 4 twisted wire pairs • 100Mbps Fast Ethernet uses two pairs, one for each direction • 1 Gbps Ethernet uses all four pairs in both directions simultaneously
Category 5e (CAT5e)	• Enhanced version of CAT5 • Significantly improved performance and network capabilities (1000Mbps Gigabit Ethernet and Full-duplex)
Category 6 (CAT6)	• Full-duplex and **UTP** • Compatible with CAT5 • 10 Gbps, thus faster • More stringent (strict) specifications for crosstalk and system noise, up to 100 m.
Category 7 (CAT7)	• Full-duplex and **STP** • Backwards compatible • Not recognized by TIA/EIA (Not as used)

Coaxial

- **Half-duplex**, but can enable full-duplex like behavior
- Two concentric copper conductors
- Common but more expensive than twisted pair
- Better shielding, more bandwidth for longer distances, and higher rates than twisted pair
- Used for video and TV since it needs larger bandwidth
- Replaced by fiber optic

50-ohm: Used for digital transmission.
75-ohm: Used for analog transmission, but now used for both digital and analog.

Internet Over Cable

- Reuses cable television plant
- Data sent on the shared cable tree from the head-end, not on a dedicated line per subscriber, unlike **DSL**
- Uses **FDM**

Power Lines

- Household electrical wiring
- 50-60Hz, too low for data

Fiber Optics

- Glass fiber carrying light pulses
- Pulse of light is 1 bit whereas no light pulse indicates 0
- Low error rate, thus more sparsely placed repeaters (light is immune to electromagnetic noises)
- Common for high data rates and long distances
- Three components: Light source, transmission media, and detector (generates pulse when light falls on it)

Single-Mode	Multi-Mode
• Narrow core (10 µm) • Light can not bounce • Used for lasers of long distances	• 50 µm core diameter • Light can bounce • Used for LEDs for cheaper, shorter distance links

FTTH

- Relies on the deployment of fiber optic cables to provide higher data rates to customers
- One wavelength for many houses
- Fiber is passive, so no amplifiers are needed
- Up to 100Mbps

Wireless Transmission

Pros	Cons
• Easy and inexpensive to deploy • Naturally supports mobility and broadcast	• Transmissions interfere and must be managed • Signal strengths vary, resulting in varied data rates

Electromagnetic Spectrum

- Signal carried in electromagnetic spectrum
- Travels at a speed of $c = 3 \times 10^8$ m/ sec
- Different bands like radio, microwave, infrared, UV, X-Ray, Gamma Ray

WAN

- Shared wireless access network connects end system to router via base station (access point **AP**)

WLAN

- Within building, around 100 ft
- IEEE 802.11 g/n/ac (Wi-Fi): 54/300/1000 Mbps transmission rate

WWAN

- Cellular data (2G, 3G, 4G, LTE, 5G)
- Between 1 and 100 Mbps and more

Baseband Transmission

- 4B/5B coding scheme
- Signal occupies frequencies from zero to a maximum
- Common for wires
- Introduced to limit the number of consecutive 0s or 1s
- Every 4 bits is mapped into 5 bit pattern with a **fixed** translation table (e.g. 0000 → 11110)

Non-Return-to-Zero (NRZ)

- Use a positive voltage to represent 1, negative voltage to represent 0
- More levels of voltages means that the symbol carries more bits

Non-Return-to-Zero Inverted (NRZI)

- Same as NRZ, but code the one as transition and zero as no transition (or opposite way)

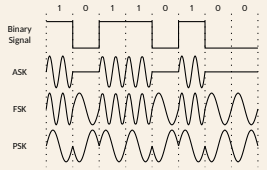
Manchester Encoding

- Mixes clock signal with data signal by using XOR
- When the clock is XORed with 0, it makes a low-to-high transition (logical 0)
- When the clock is XORed with 1, it makes a high-to-low transition (logical 1)

Passband Transmission

- Schemes that regulate the amplitude, phase, or frequency of the carrier signal to convey bits
- Occupies a band of frequencies around the frequency of the carrier signal that does **not** start at 0
- Not practical for wireless channels to send very low frequencies since size of the antenna ($\lambda/4$) would be large ($\lambda = c/f$)
- Common for wireless and optical channels
- Governed by regulated body
- Digital modulation is accomplished by modulating the carrier signal that sits in the passband

Modulation Methods



ASK	Use two different amplitudes to represent 0 and 1.
FSK	Two or more frequencies are used.
PSK	Carrier wave is shifted θ degrees at each symbol period. If there are two phases, this is called **BPSK**.

Calculations

One's Complement

Invert all bits (1 → 0 and 0 → 1) ($11010101 \rightarrow 00101010$)

TCP Acknowledgement Number

Acknowledgement Number = Sequence Number + Size of Segment
e.g. 356-byte segment has a sequence number field of 2512.
($356 + 2512 = 2868$ is the Acknowledgement)
Next sequence number would be the acknowledgement number!

UDP Packet Checksum

1. Calculate the one's complement sum.
2. Move the leading bit (most significant value) and add to the end if more than 4 hexadecimal values.
3. Find the one's complement of the sum.
4. Convert back to hexadecimal.

e.g. 4510, 003C, 1C46, 4501, 4006, B1E6, AC10, 1A63

$$\text{SUM} = 0x25EF2$$
$$0x25EF2 \rightarrow 0x5EF4 (0x5EF2 + 0x0002)$$
$$0x5EF4 \rightarrow 0101111011110100$$
$$0101111011110100 \rightarrow 1010000100001011$$
$$1010000100001011 \rightarrow 0xA10B$$

Packet Tracer

- Copper Stright-Through wires for different level (computer to switch)
- Copper Cross-Over wires for same level (switch to switch)
- Use the Home Router since none of the other routers work
- For laptop, add Linksys-WPC300N connector to make wireless (must power off first)
- "ping IPv4-ADDRESS-HERE" to check if current device is connected to another device

Sockets

Definitions

Sockets (kernel): Endpoint of communication.
Sockets (application): File descriptor that lets application **RO** from/to network

General

- Consists of a pair of programs: **client** and **server**
- When programs are executed, a client and a server process are created, and these processes communicate with each other by reading from and writing to sockets
- e.g. A client reads a string from its keyboard and sends it to the server, where the server gets the data and converts it to uppercase, sending it back to the client where the client displays it

General Socket Information

Address Family

AF_INET	IPv4
AF_INET6	IPv6
AF_UNIX	Unix

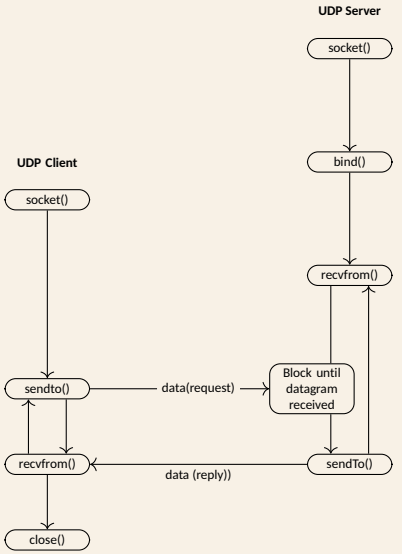
Socket Type

SOCK_STREAM	TCP
SOCK_DGRAM	UDP
SOCK_RAW	Raw

Functions

accept()	Accepts an incoming connection request, returning a new socket for the connection.
bind()	Assigns a local socket address to a socket, allowing the server to listen for connections.
connect()	Connects a client socket to a server socket address, establishing a connection.
sendto(), recvfrom()	Used for sending and receiving data with **UDP** sockets, where destination and source addresses are specified using socket address structures

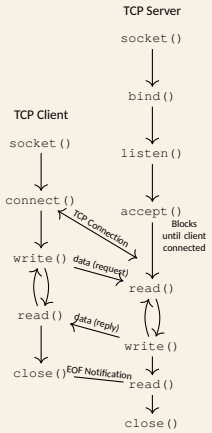
UDP Socket Programming



Use for speed and when some data loss is acceptable.

- Provides unreliable transfer of datagrams between client and server
- No "connection" between client and server since no handshaking
- Sender program explicitly attaches IP destination address and port # to each packet.
- Transmitted data may be lost or out of order when received

TCP Socket Programming



Use for reliable, ordered data transfer when accuracy is crucial.

- Client must connect to the server first
- Server process must first be running and have created a socket that welcomes the client's contact
- Client connects to the server by creating a TCP socket, specifying the IP address and port # of a server process
- Server TCP creates a new socket for the server process, which allows the server to talk to multiple clients (use port # to distinguish)

Configurations

2oo2	Requires both signals to agree to trigger a shutdown.
2oo3	Requires two out of three signals to trigger a shutdown.
3oo3	Requires all three signals to trigger a shutdown.

Interfaces for 5G

- Point-to-point interfaces that connect to different network elements
- Important for enabling communication and data flow between the **UE**

N1	**UE** & **AMF**	Handles registration, authentication, and mobility management procedures.
N2	**RAN** & **AMF**	Carries signaling and data between the **RAN** and the core network.
N3	**RAN** & **UPF**	Facilitates transfer of user data between **RAN** and core network.
N4	**SMF** & **UPF**	

Applications & Tech

Tools and Terms

3GPP: A cooperative effort of international standard bodies that develop and maintain mobile telecommunications. The project aims to create and maintain global mobile broadband standards, focusing on technologies like 2G, 3G, 4G, LTE-Advanced, and 5G mobile networks.
collectd: A Unix daemon that collects, transfers, and stores performance data of computers and network equipment.
DTrace: A command-line utility that enables uses to monitor and troubleshoot their system's performance in real time.
Elasticsearch: A free and open-source search engine based on Apache Lucene.
kubernetes: Open-source system that automates the deployment, scaling, and management of containerized applications.
Whisper (Database): A fixed size database that is used for Graphite. Data stored in big-endian.

AirSpan Control Platform

- Element Management System for the **5G gNBs**
- A unified management solution offering unparalleled control and efficiency for Public and Private Networks

Public Networks

- Seamless integration with **MNO OSS** through standard APIs
- **Plug and Play Configuration** - Automatically imports configurations to enable zero-touch setup.
- **Comprehensive Management** - Provides fault management, configuration details, performance metrics, and real-time status to **NMS/OSS**, simplifying RF data analysis, troubleshooting, and optimization.

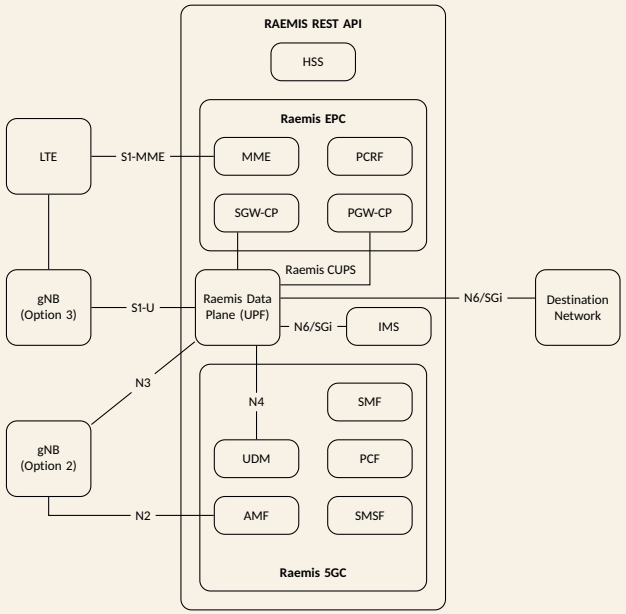
Private Networks

- **Unified Management Interface** - A single pane of glass for all network management needs.
- **Advanced Automation** - Service orchestration and automation for streamlined operations.
- **Rich Features** - Includes dashboards, analytics, optimization tools, and API integration for customer portals.
- **Deployment Flexibility** - Choose from cloud based solutions, private/public clouds, or on-premises deployment, all while ensuring full CBRS compliance

Druid Raemis

- A mature 3GPP-compliant 4G/5G core network platform that harnesses 5G, 4G, 3G, 2G, and Wi-Fi radios from any vendor to streamline the implementation of standalone networks
- The Raemis administrator can create multiple **PDNs**
- Layer 2 (TCP/IP model) network capabilities

Raemis EPC	Supports **4G** and **5G** non-standalone deployments.
Raemis 5GC	Designed specifically for **5G SA** deployments.



- Raemis UPF implements the standard N3

PDN Functions

- Security and Traffic Segregation
- Item Balancing
- QoS Allocation

Raemis API

- Exposes a powerful RESTful API that enables application developers to build on top of Raemis or integrate external applications

Raemis GUI

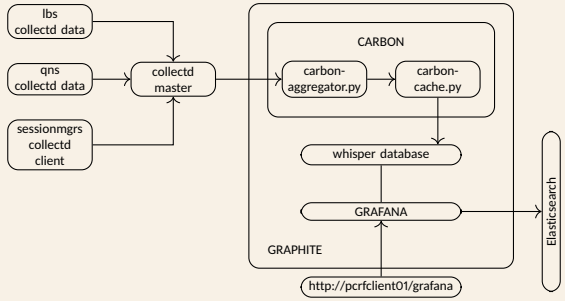
- Uses the Raemis API to access the core software and **3GPP** components of the network
- Hides the complexity of the network

Grafana

- Open-source Graphite web application (Where Graphite consists of three components: Carbon, Whisper, and Graphite Webapp)
- Monitoring tool used for storing and viewing time series data
- Multi-platform open source analytics and interactive visualization web application
- Produces charts, graphs, alerts, for the web when connected to supported data sources

Data Collection

1. Application writes data to **JMX beans**
2. Collectd clients run on all CPS virtual machines such as policy servers and data from **JMX beans** are collected in case of **sessionmgr**
3. Collectd clients push data to collected master node on **pcrfclient01**
4. Collectd master node forwards collected data to graphite database on **pcrfclient01**
5. The graphite database stores system-related statistics (CPU usage, memory usage, and ethernet interface statistics)
6. Carbon cache writes this data to Whisper database
7. Grafana pulls this data from Whisper database configuration and the query is executed in the GUI



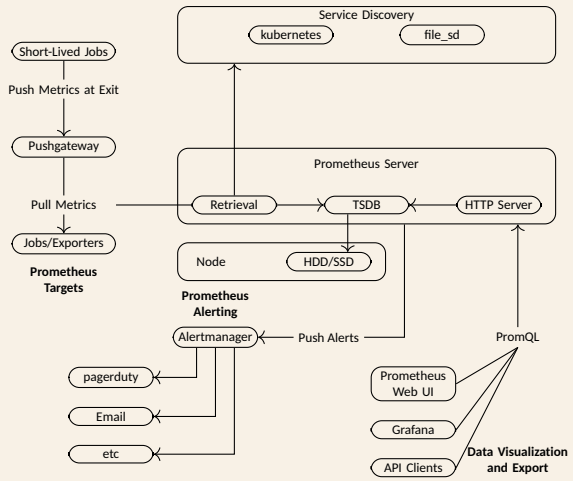
OpenNMS Horizon

- Open-source solution that helps visualize and monitor local and remote networks
- Offers comprehensive fault, performance, traffic monitoring, and alarm generation
- Supports any type of provisioning (auto, directed, topology, etc.)

Prometheus

- Used for event monitoring and alerting (CPU, RAM, etc.)
- Built using an **HTTP Pull Model** with flexible queries and real-time alerting
- Developed at SoundCloud starting 2012
- Multi-dimensional data model with time series data identified by metric name and key/value pairs
- No reliance on distributed storage
- Collected Data can be displayed with **Grafana**

Architecture



Windows 11

- Current latest major Microsoft's Windows NT OS
- Major changes to the Windows shell, which was influenced by Windows 10X, a canceled deluxe edition to Windows 10
- Redesigned Start menu, replacement of "live tiles" with a separate "Widgets" panel in the taskbar, etc.

Windows Server 2025

- Server-oriented releases of Windows NT OS
- Uses **SMB** instead of **QUIC**
- Compared to Windows, this is used for network servers, whereas base Windows 11 is used for desktop computers and personal use
- New features such as Bluetooth connection, DTrace, and additional emails and accounts