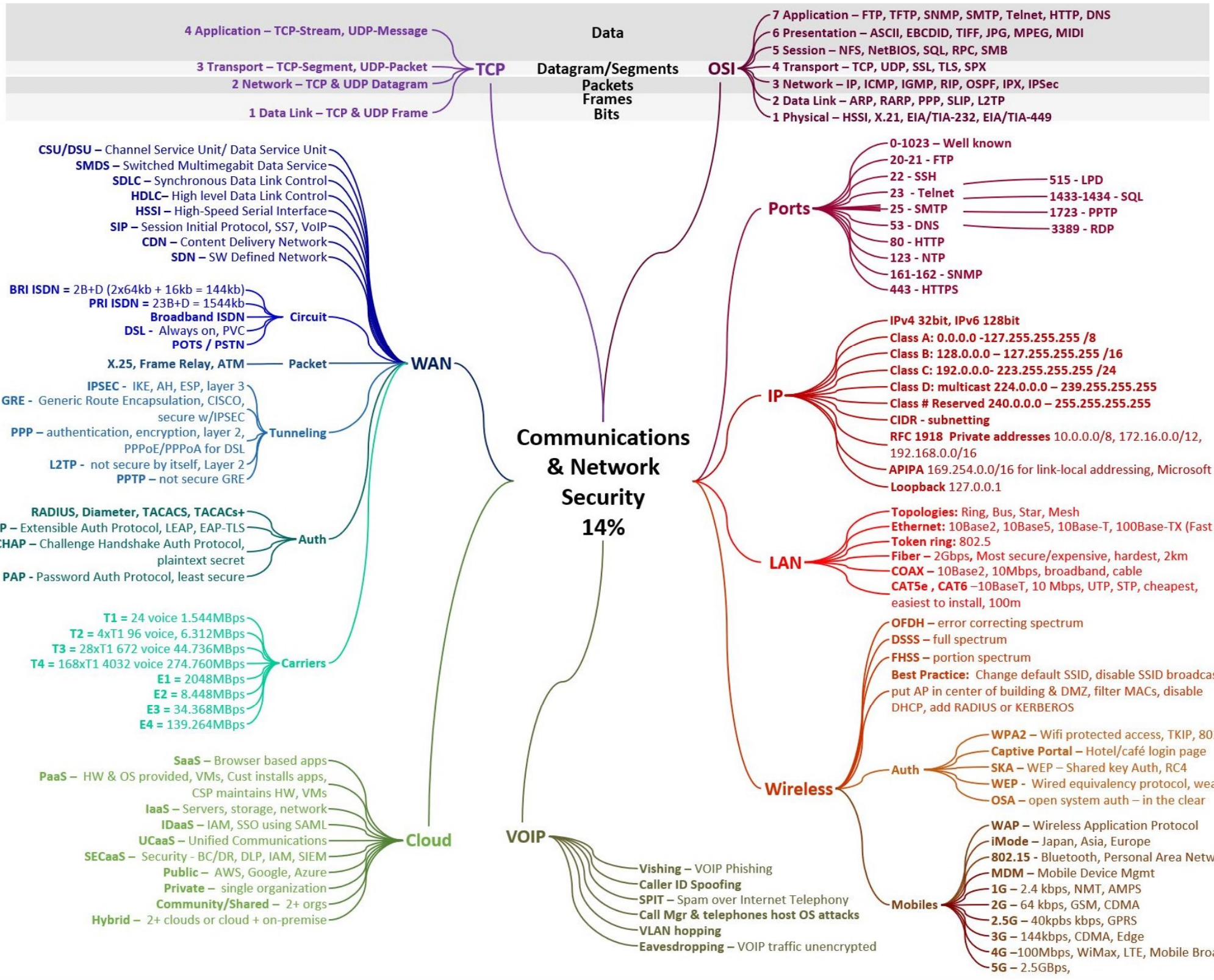
Communications & Network Security 14%
TCP
4 Application – TCP-Stream, UDP-Message
3 Transport – TCP-Segment, UDP-Packet
2 Network – TCP & UDP Datagram
1 Data Link – TCP & UDP Frame
Data
Datagram/Segments
Packets
Frames
Bits
OSI
7 Application – FTP, TFTP, SNMP, SMTP, Telnet, HTTP, DNS
6 Presentation – ASCII, EBCDID, TIFF, JPG, MPEG, MIDI
5 Session – NFS, NetBIOS, SQL, RPC, SMB
4 Transport – TCP, UDP, SSL, TLS, SPX
3 Network – IP, ICMP, IGMP, RIP, OSPF, IPX, IPSec
2 Data Link – ARP, RARP, PPP, SLIP, L2TP
1 Physical – HSSI, X.21, EIA/TIA-232, EIA/TIA-449
WAN
CSU/DSU – Channel Service Unit/ Data Service Unit
SMDS – Switched Multimegabit Data Service
SDLC – Synchronous Data Link Control
HDLC– High level Data Link Control
HSSI – High-Speed Serial Interface
SIP – Session Initial Protocol, SS7, VoIP
CDN – Content Delivery Network
SDN – SW Defined Network
Circuit
BRI ISDN = 2B+D (2x64kb + 16kb = 144kb)
PRI ISDN = 23B+D = 1544kb
Broadband ISDN
DSL - Always on, PVC
POTS / PSTN
Packet
X.25, Frame Relay, ATM
Tunneling
IPSEC - IKE, AH, ESP, layer 3
GRE - Generic Route Encapsulation, CISCO, secure w/IPSEC
PPP – authentication, encryption, layer 2, PPPoE/PPPoA for DSL
L2TP - not secure by itself, Layer 2
PPTP – not secure GRE
Auth
RADIUS, Diameter, TACACS, TACACs+
EAP – Extensible Auth Protocol, LEAP, EAP-TLS
CHAP – Challenge Handshake Auth Protocol, plaintext secret
PAP - Password Auth Protocol, least secure
Carriers
T1 = 24 voice 1.544MBps
T2 = 4xT1 96 voice, 6.312MBps
T3 = 28xT1 672 voice 44.736MBps
T4 = 168xT1 4032 voice 274.760MBps
E1 = 2048MBps
E2 = 8.448MBps
E3 = 34.368MBps
E4 = 139.264MBps
Cloud
SaaS – Browser based apps
PaaS – HW & OS provided, VMs, Cust installs apps, CSP maintains HW, VMs
IaaS – Servers, storage, network
IDaaS – IAM, SSO using SAML
UCaaS – Unified Communications
SECaaS – Security - BC/DR, DLP, IAM, SIEM
Public – AWS, Google, Azure
Private – single organization
Community/Shared – 2+ orgs
Hybrid – 2+ clouds or cloud + on-premise
VOIP
Vishing – VOIP Phishing
Caller ID Spoofing
SPIT – Spam over Internet Telephony
Call Mgr & telephones host OS attacks
VLAN hopping
Eavesdropping – VOIP traffic unencrypted
Ports
0-1023 – Well known
20-21 - FTP
22 - SSH
23 - Telnet
25 - SMTP
53 - DNS
80 - HTTP
123 - NTP
161-162 - SNMP
443 - HTTPS
515 - LPD
1433-1434 - SQL
1723 - PPTP
3389 - RDP
IP
IPv4 32bit, IPv6 128bit
Class A: 0.0.0.0 -127.255.255.255 /8
Class B: 128.0.0.0 – 127.255.255.255 /16
Class C: 192.0.0.0- 223.255.255.255 /24
Class D: multicast 224.0.0.0 – 239.255.255.255
Class # Reserved 240.0.0.0 – 255.255.255.255
CIDR - subnetting
RFC 1918 Private addresses 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
APIPA 169.254.0.0/16 for link-local addressing, Microsoft
Loopback 127.0.0.1
LAN
Topologies: Ring, Bus, Star, Mesh
Ethernet: 10Base2, 10Base5, 10Base-T, 100Base-TX (Fast Etherr
Token ring: 802.5
Fiber – 2Gbps, Most secure/expensive, hardest, 2km
COAX – 10Base2, 10Mbps, broadband, cable
CAT5e , CAT6 –10BaseT, 10 Mbps, UTP, STP, cheapest, easiest to install, 100m
Wireless
OFDH – error correcting spectrum
DSSS – full spectrum
FHSS – portion spectrum
Best Practice: Change default SSID, disable SSID broadcast, put AP in center of building & DMZ, filter MACs, disable DHCP, add RADIUS or KERBEROS
Auth
WPA2 – Wifi protected access, TKIP, 802.11i
Captive Portal – Hotel/café login page
SKA – WEP – Shared key Auth, RC4
WEP - Wired equivalency protocol, weak
OSA – open system auth – in the clear
Mobiles
WAP – Wireless Application Protocol
iMode – Japan, Asia, Europe
802.15 - Bluetooth, Personal Area Network, P
MDM – Mobile Device Mgmt
1G – 2.4 kbps, NMT, AMPS
2G – 64 kbps, GSM, CDMA
2.5G – 40kpbs kbps, GPRS
3G – 144kbps, CDMA, Edge
4G –100Mbps, WiMax, LTE, Mobile Broadbanc
5G – 2.5GBps,