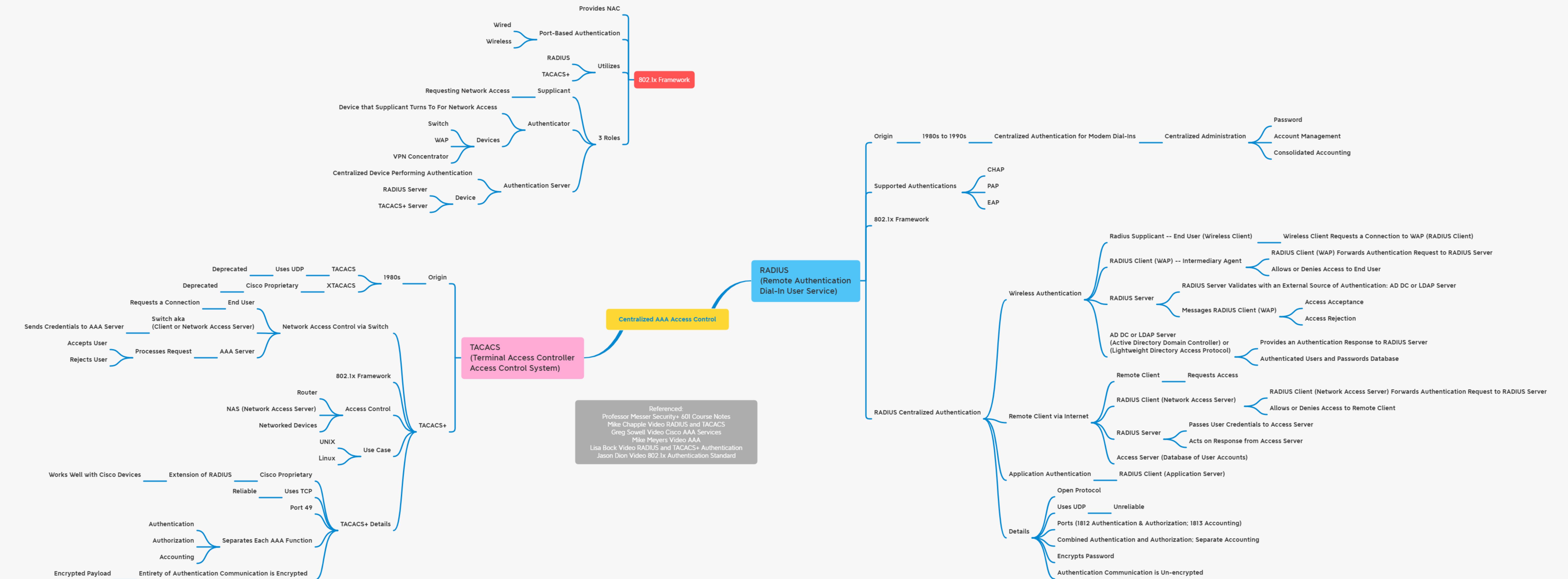
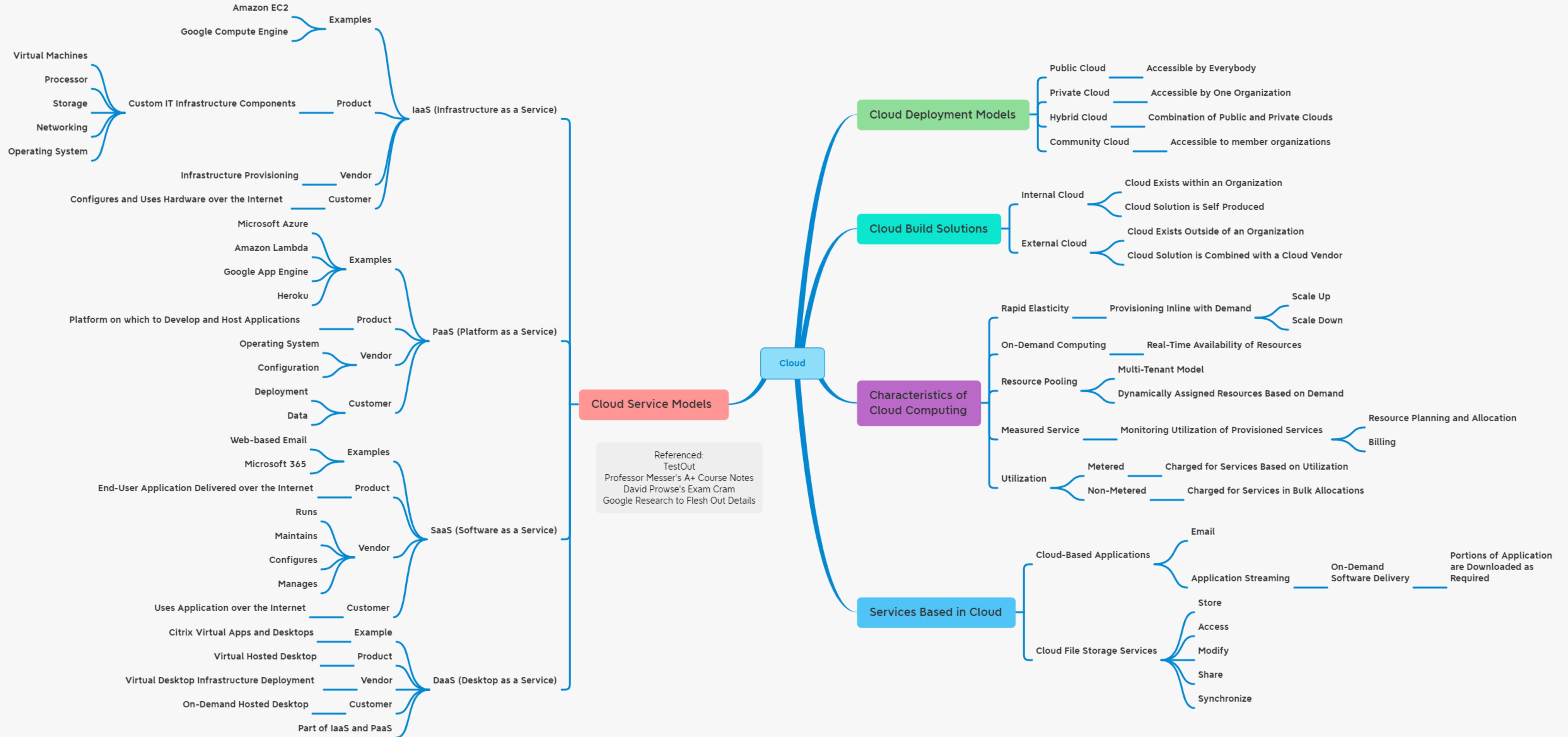
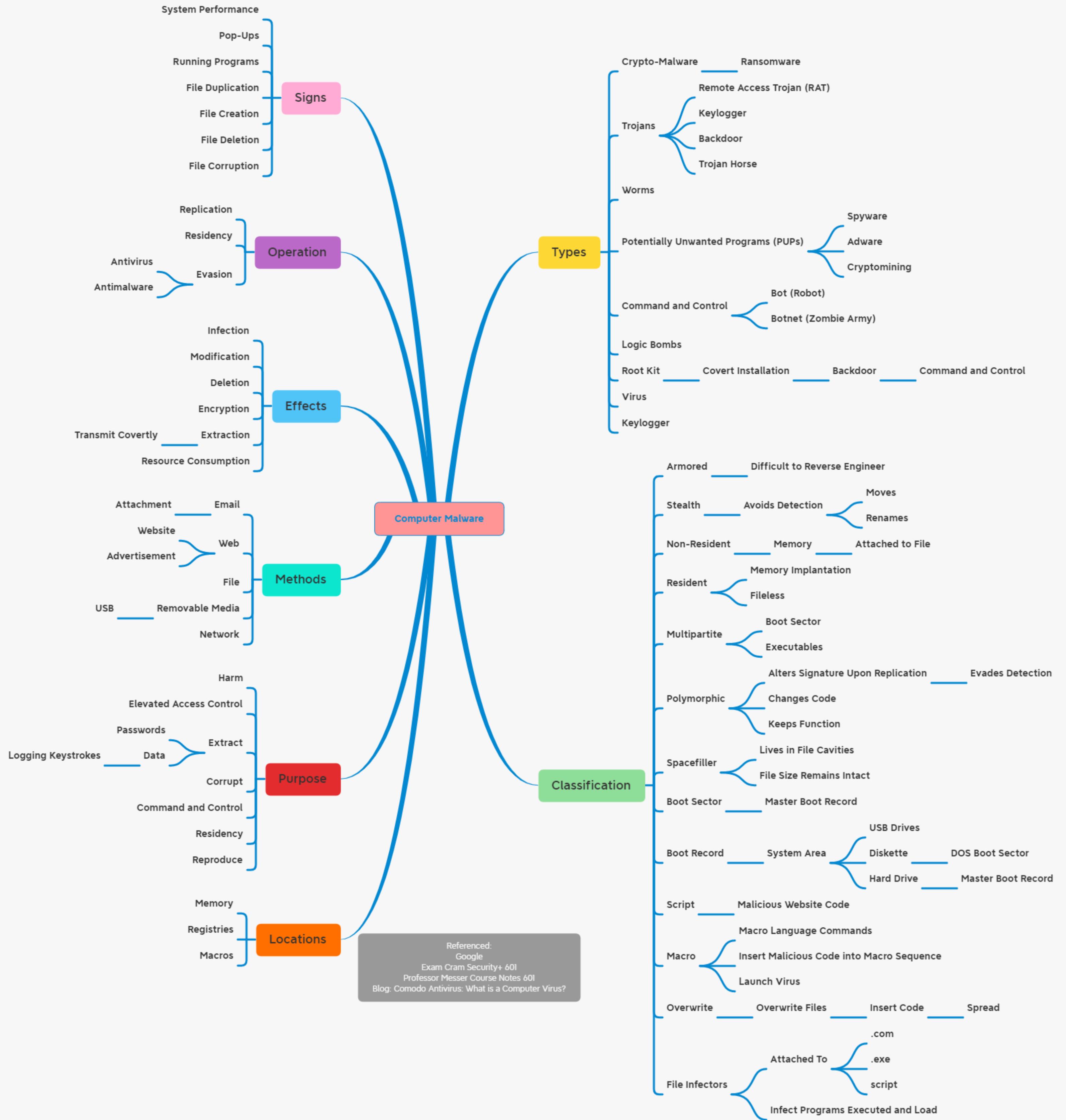


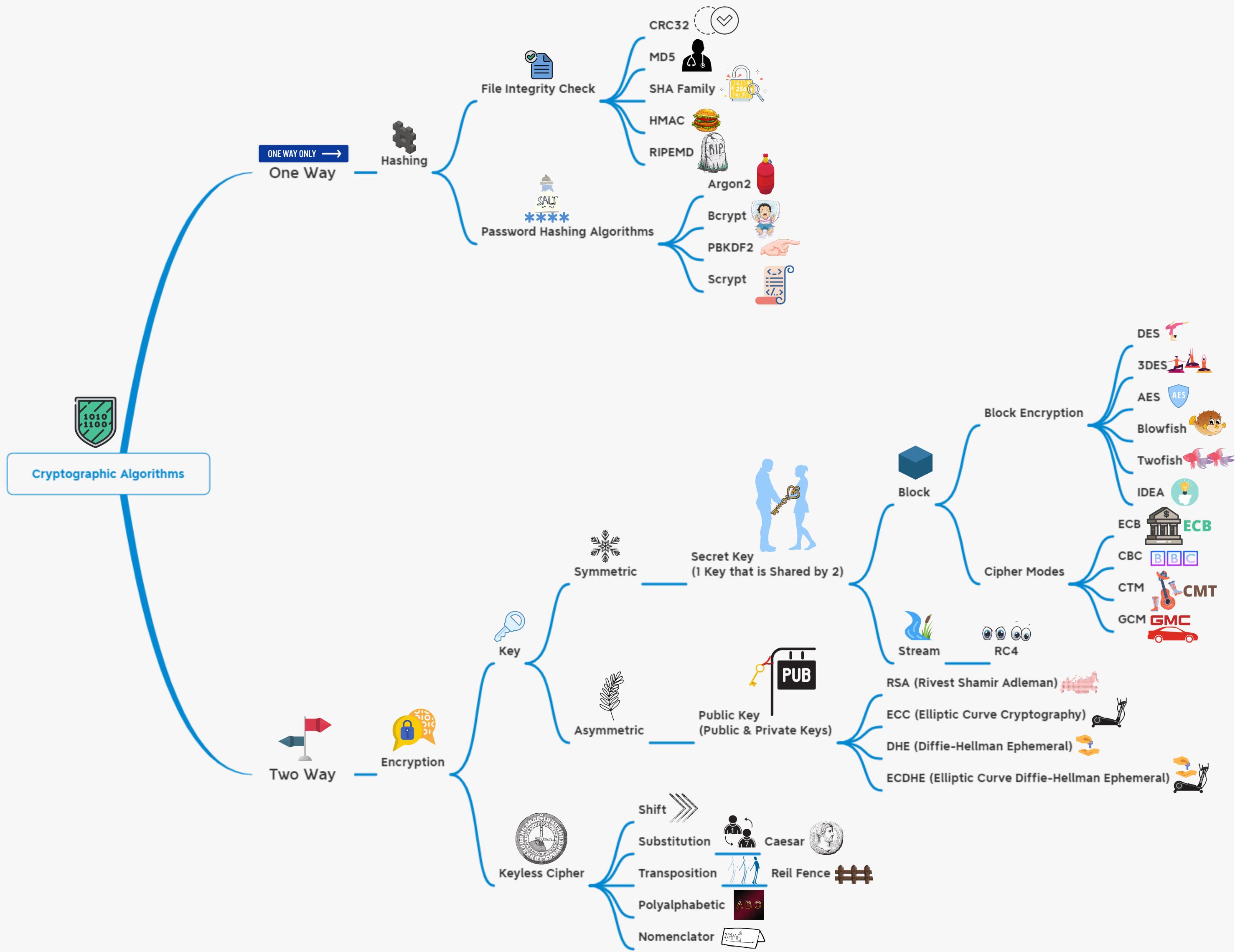
Referenced:

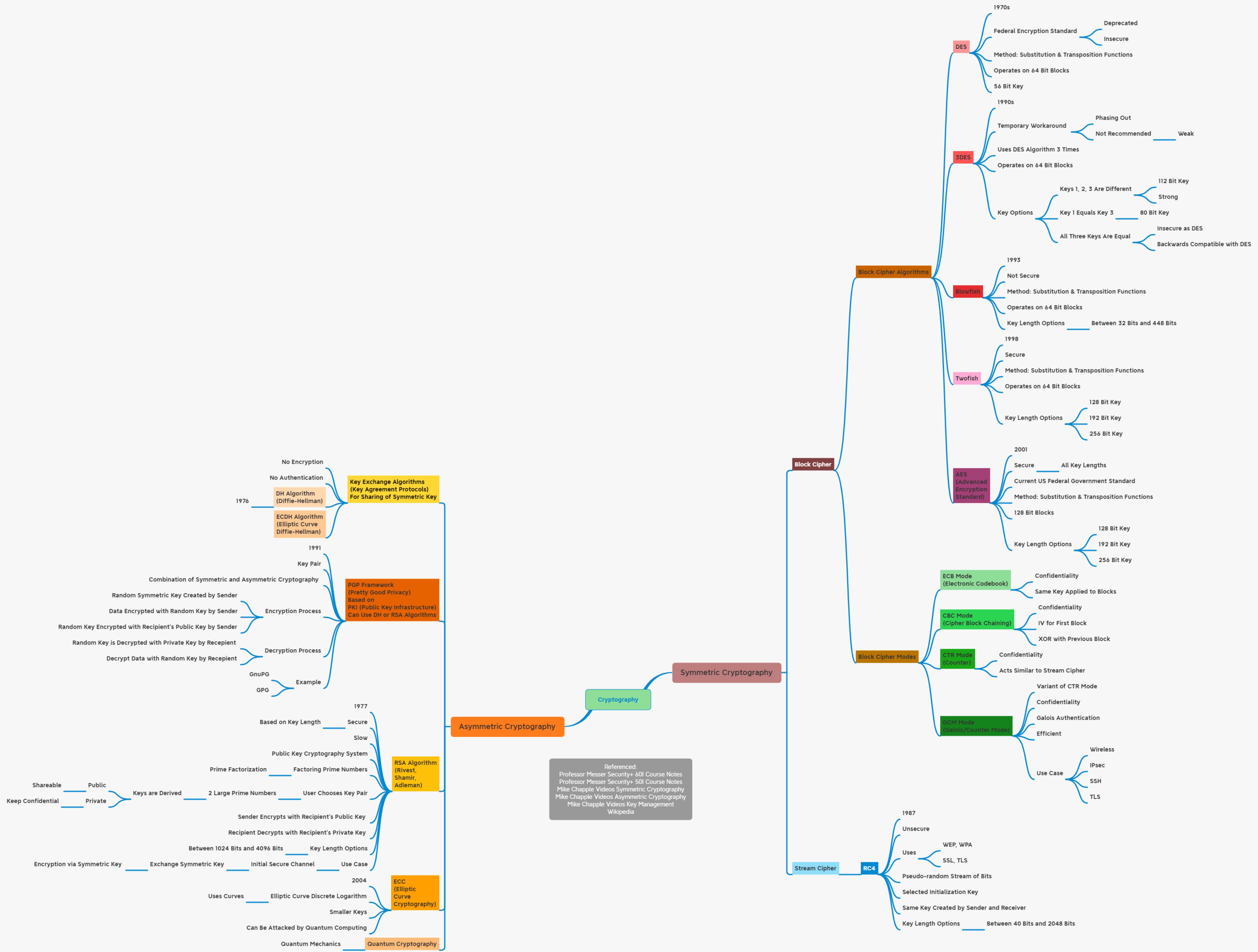
- Jonathan Reichental video Blockchain
- Morten Rand-Hendriksen video What is a Blockchain?
- Professor Messer Security+ 601 Course Notes

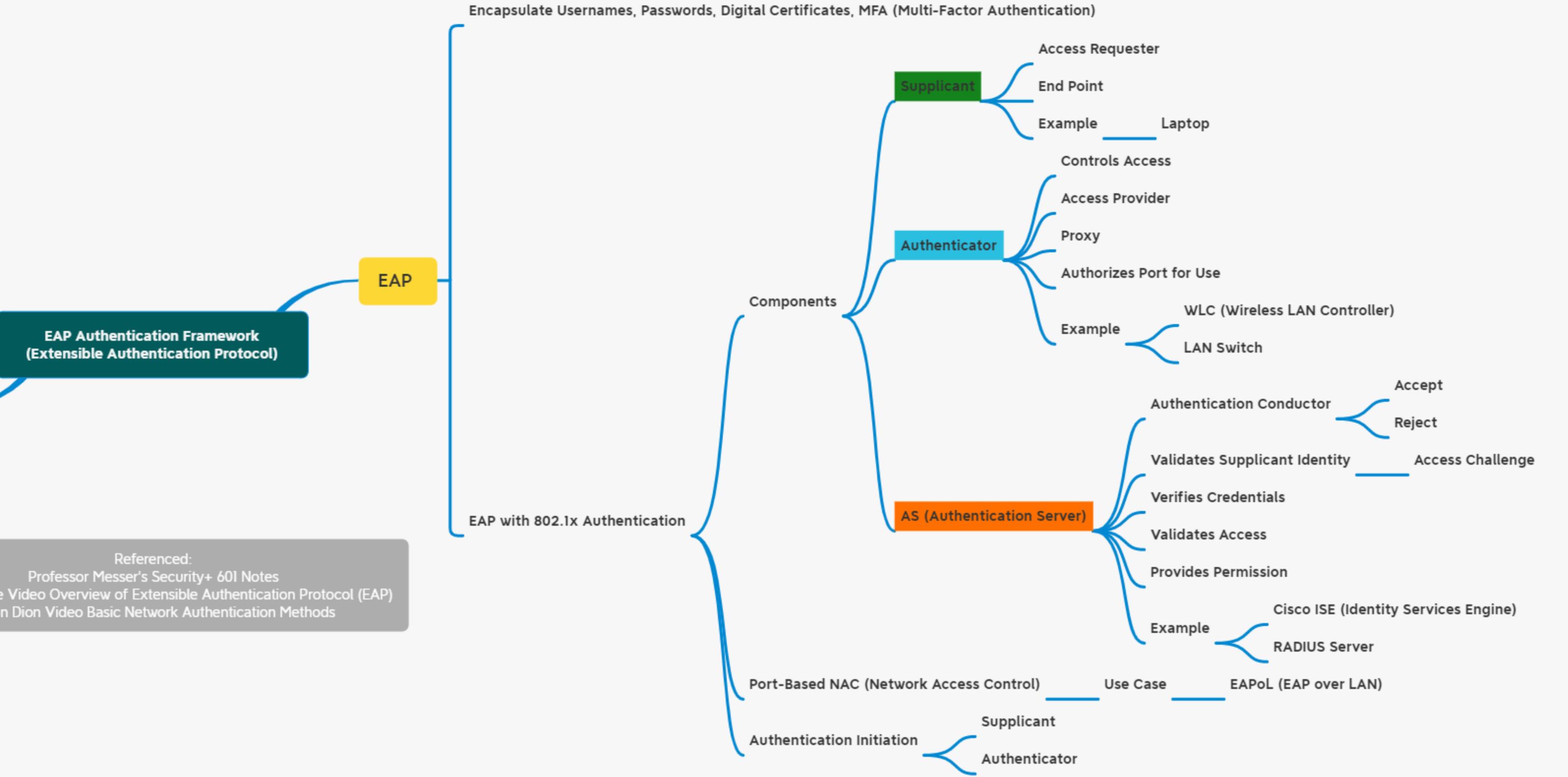
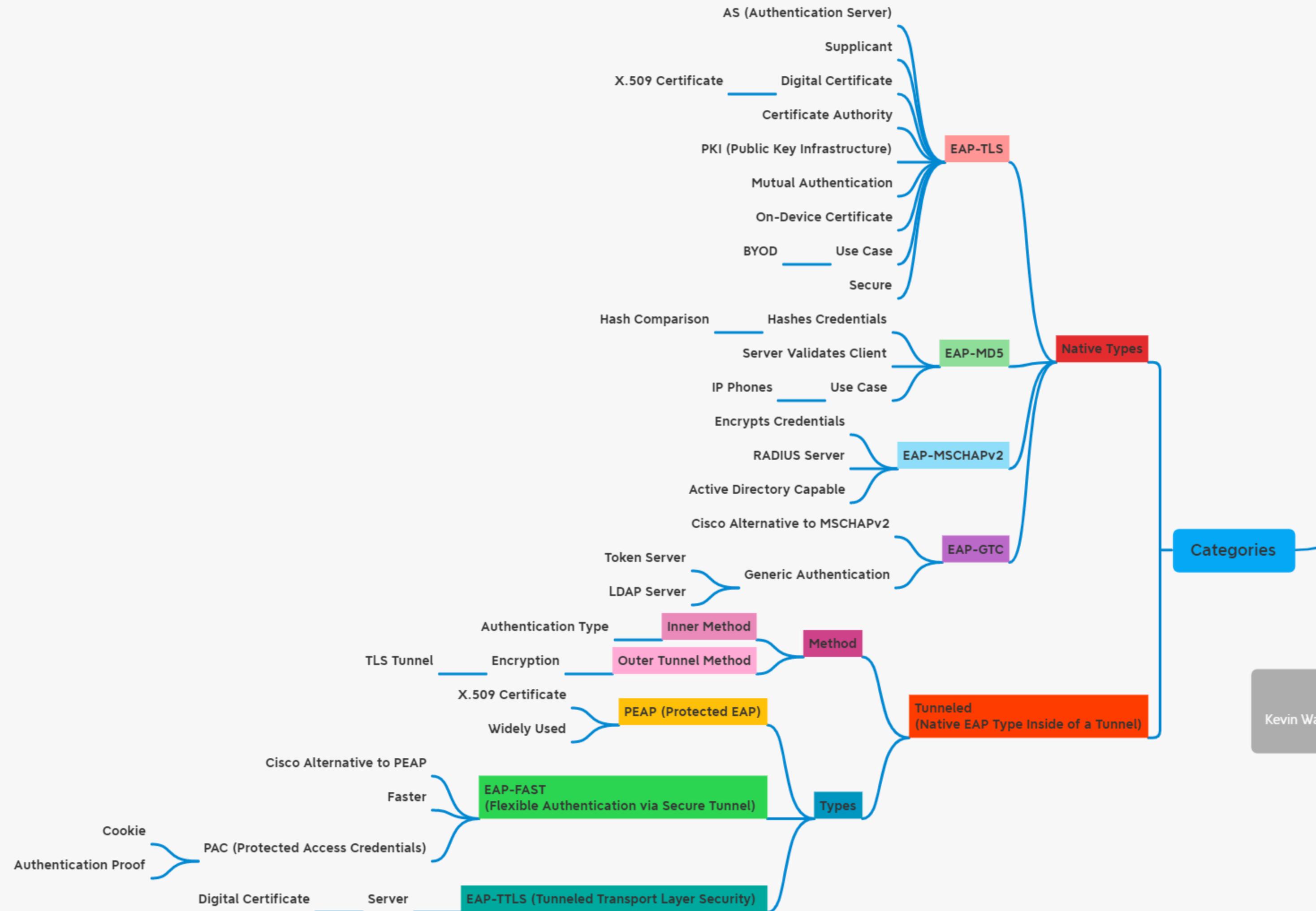


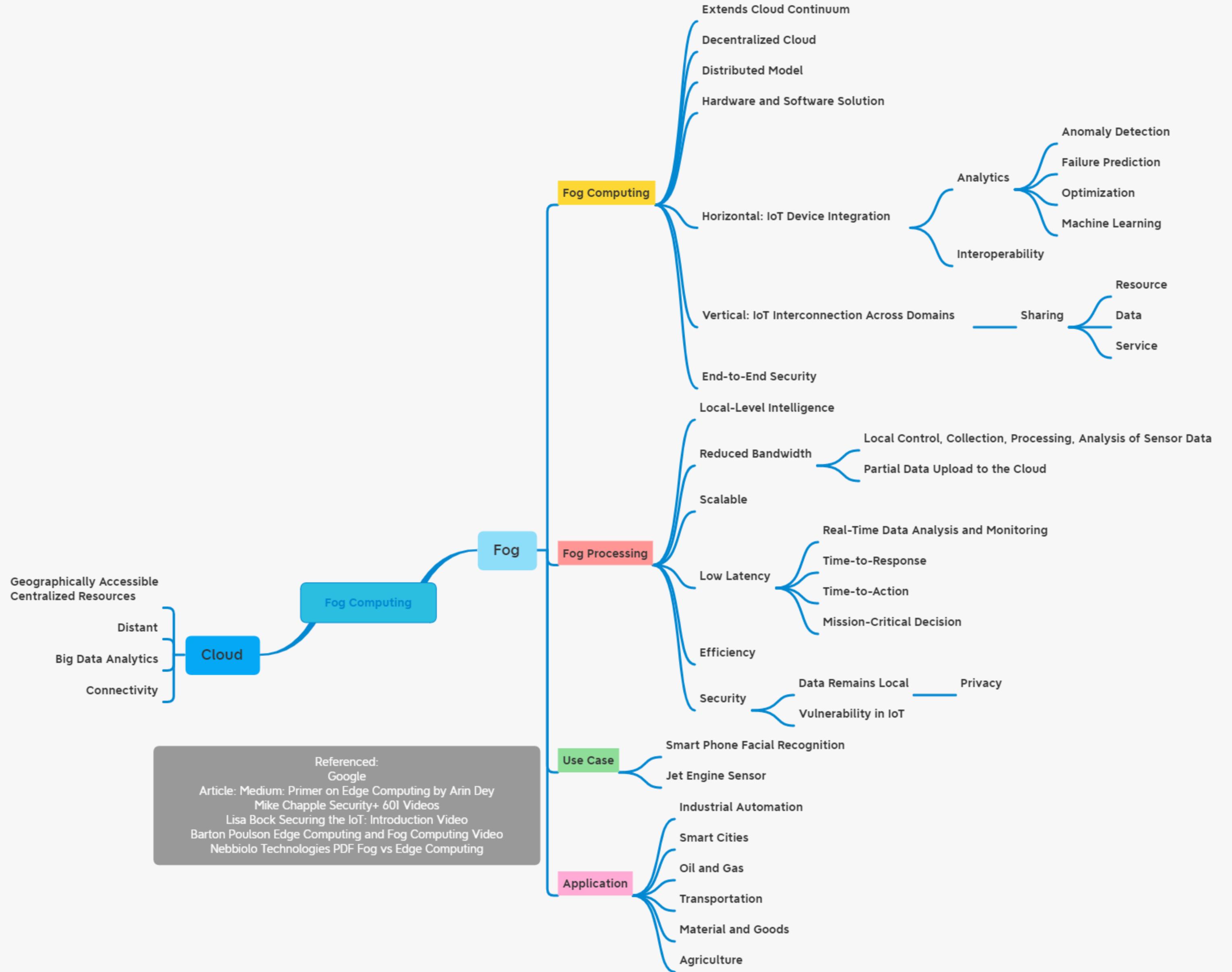


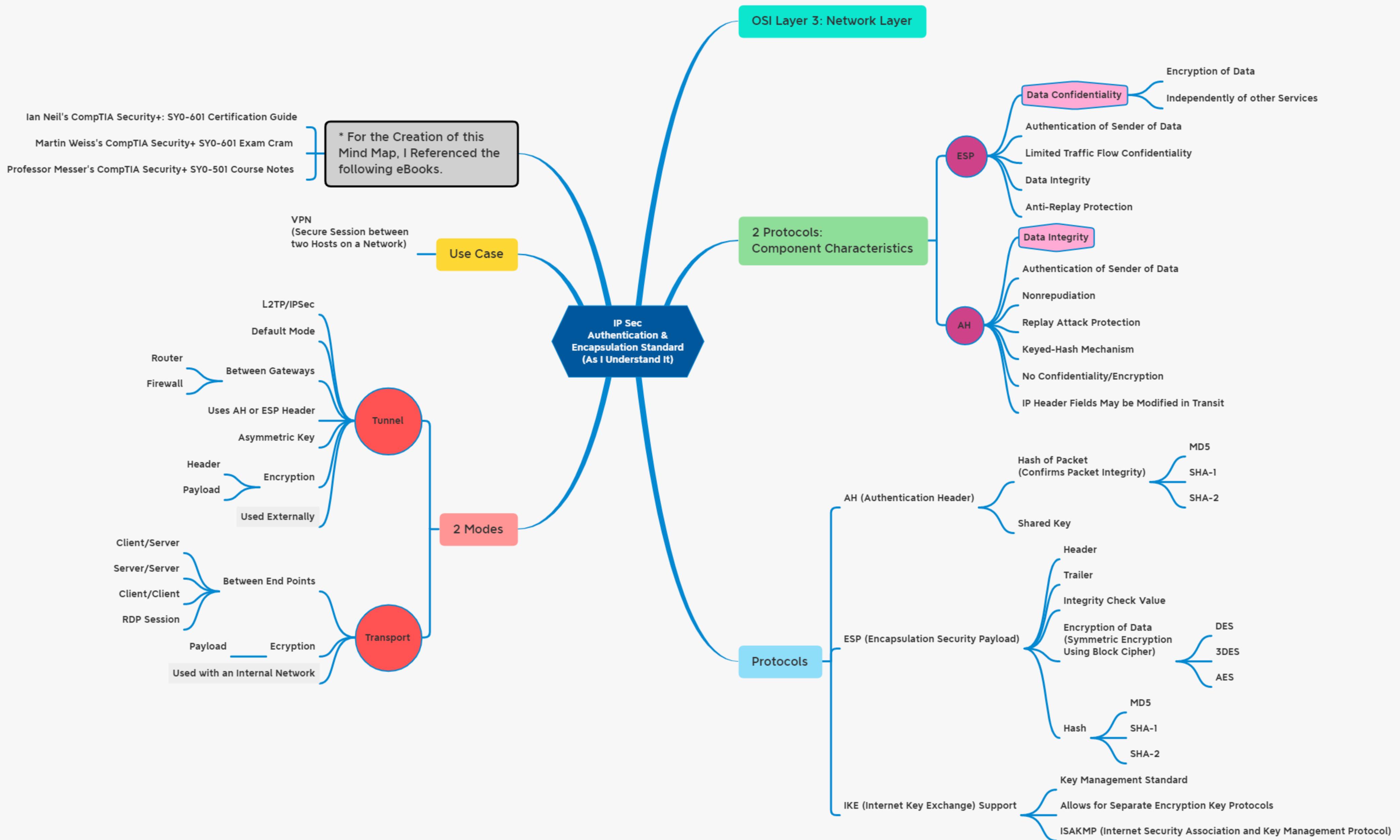





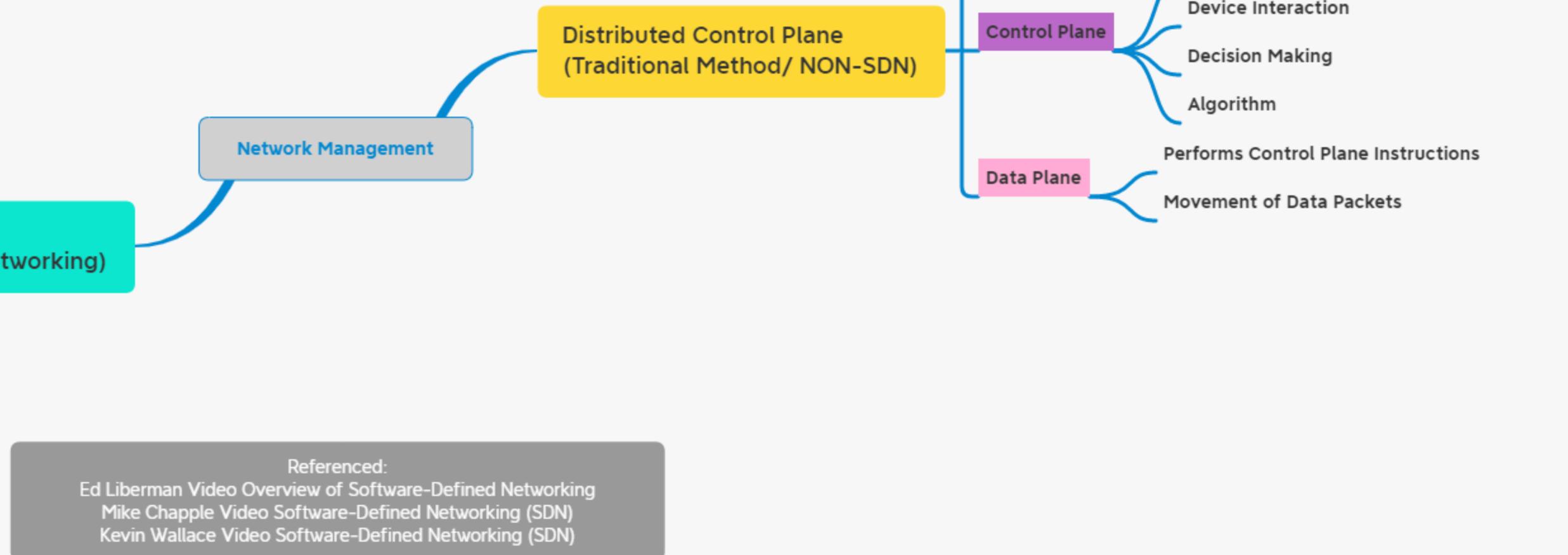
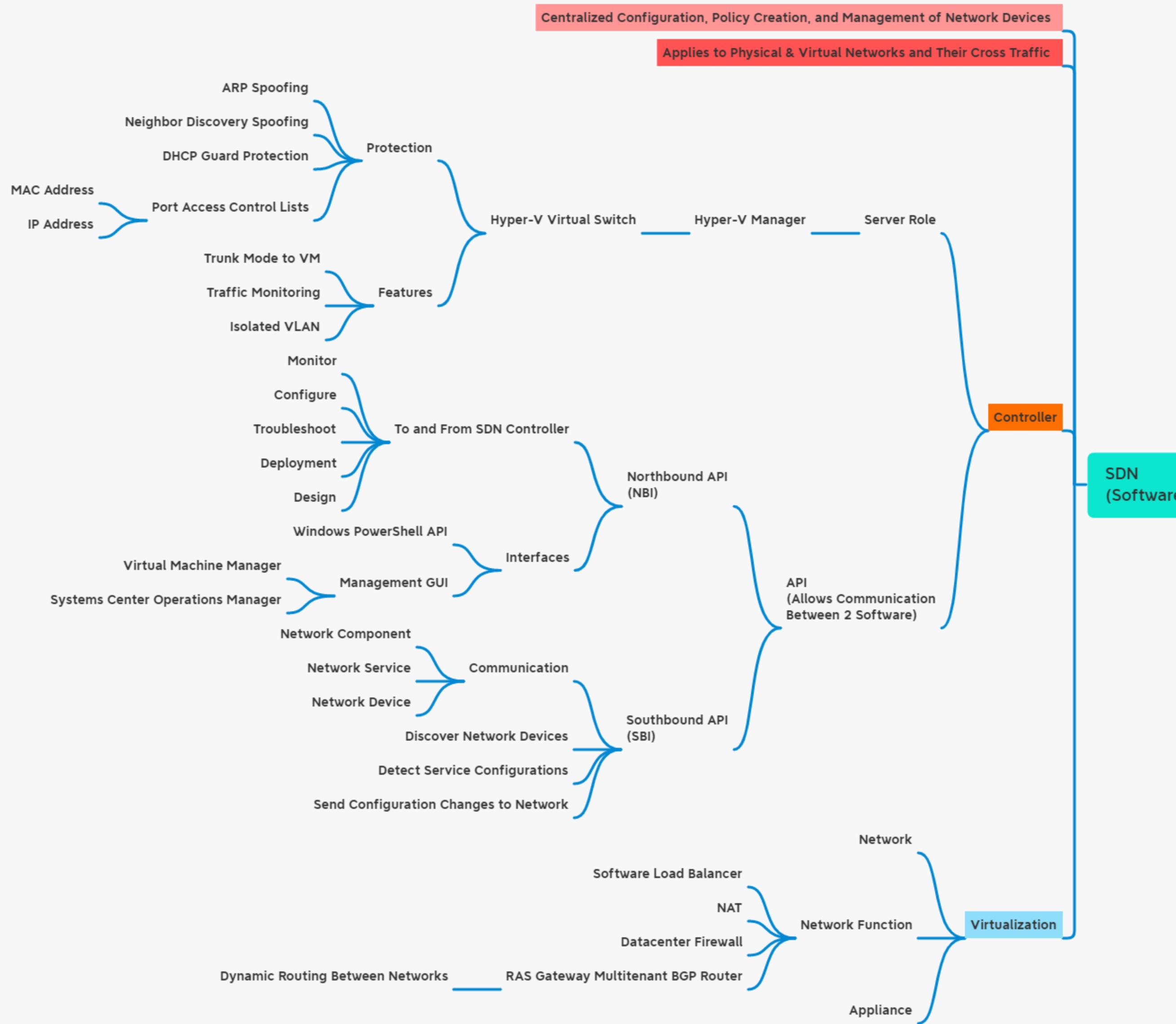


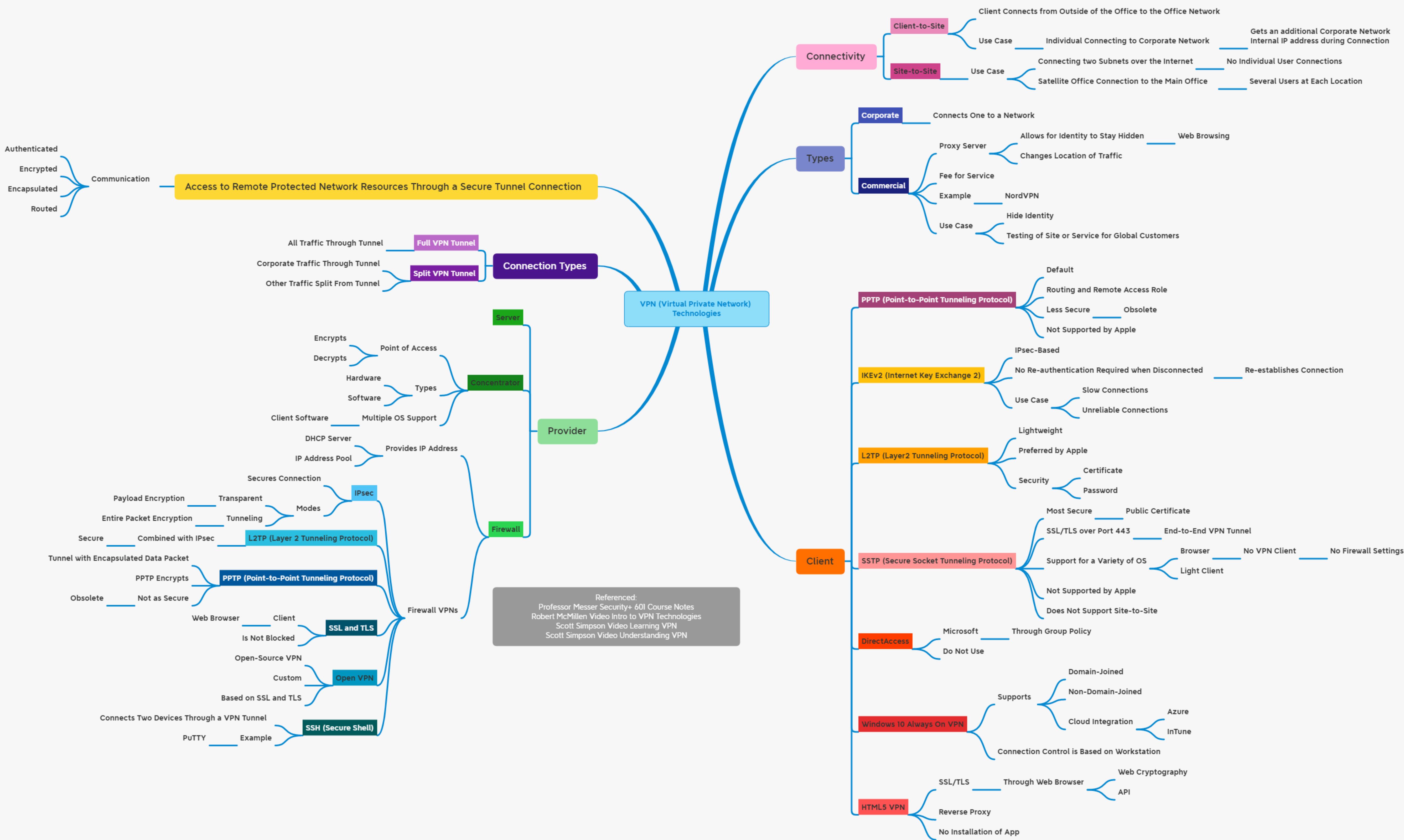


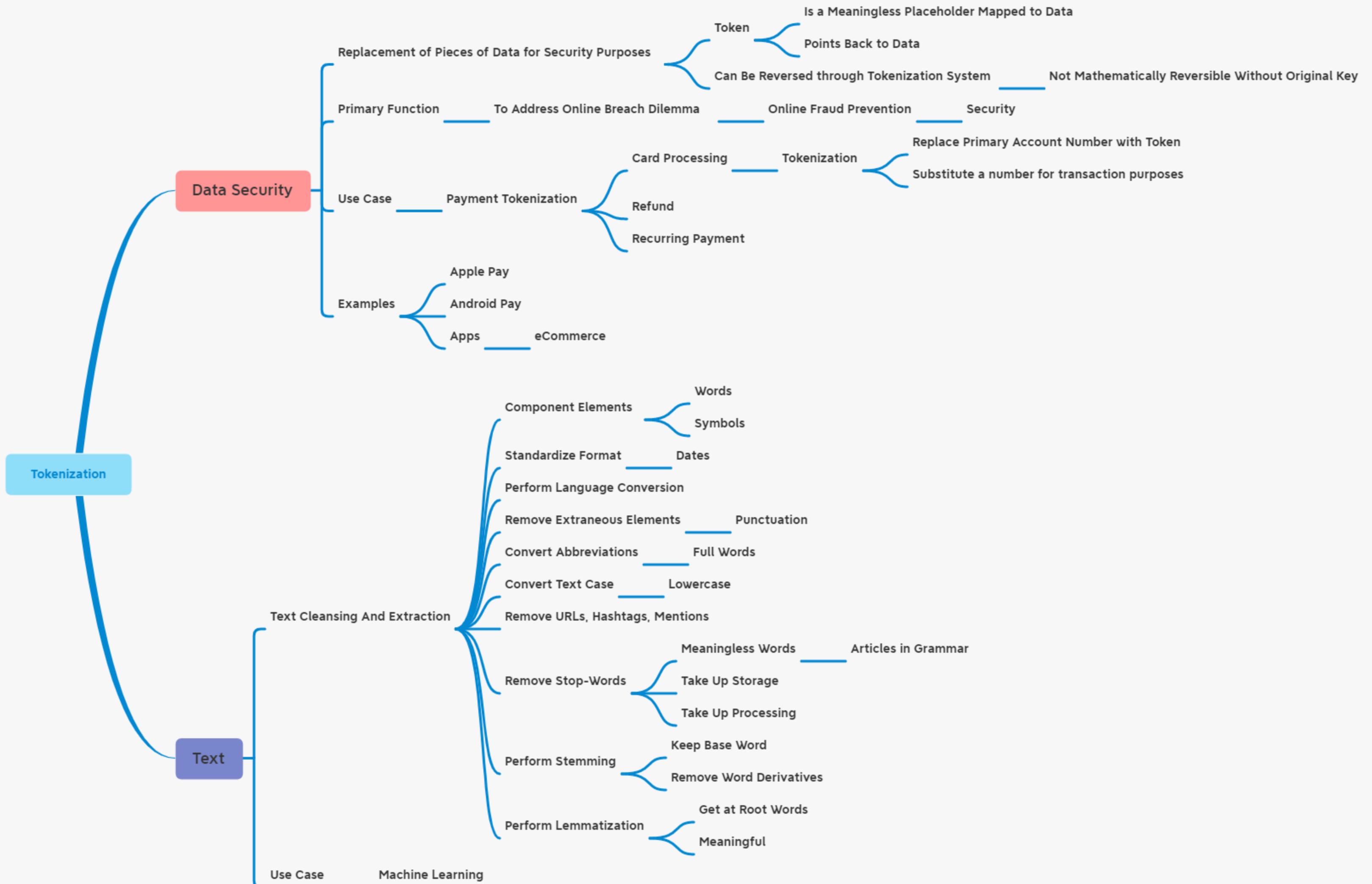






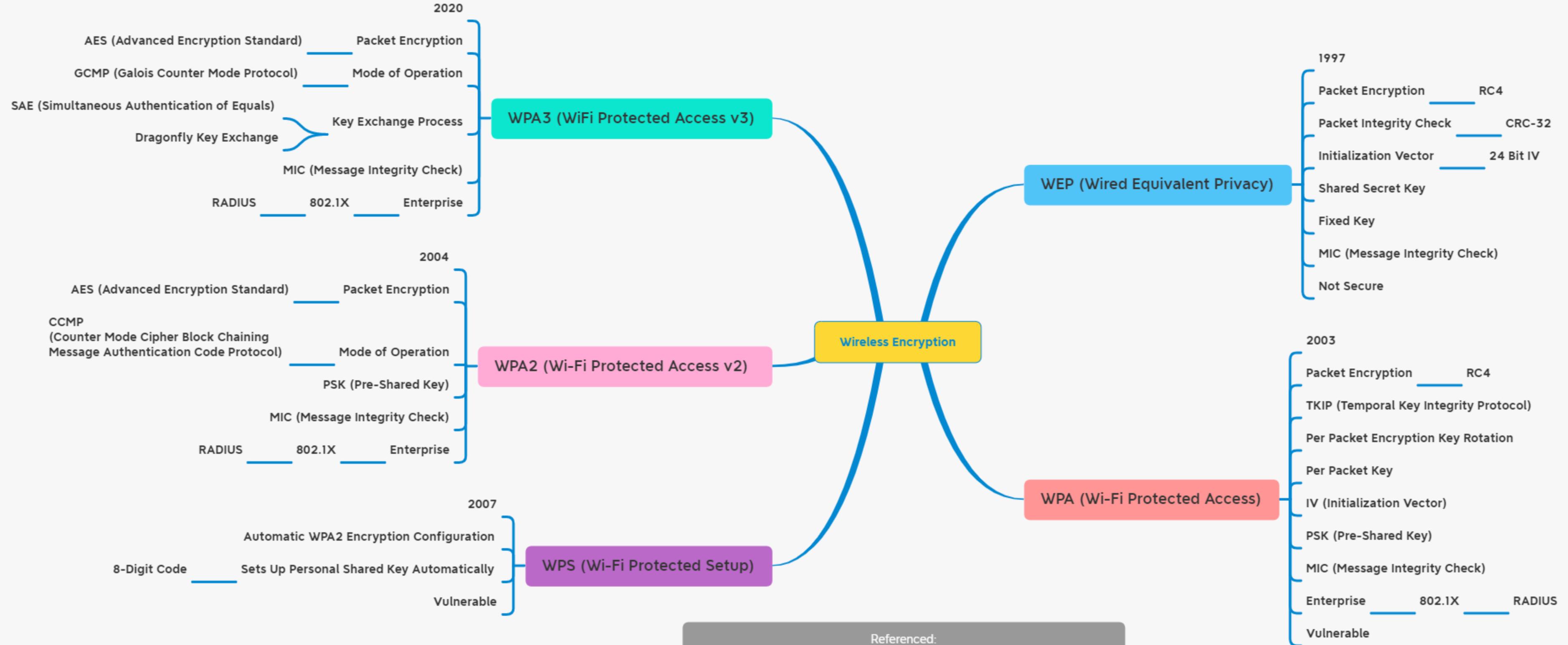






Referenced:

Professor Messer Security+ 601 Course Notes  
 Kumaran Ponnambalam Video Tokenization  
 Wikipedia Tokenization (Data Security)  
 Square Article: Payment Tokenization Explained



Referenced:  
 Professor Messer's Security+ 601 Notes  
 Mike Chapple Video Wireless Encryption  
 Mike Meyers Video Wireless Encryption  
 Mike Chapple Video WEP, WPA, WPA2  
 Cybarrior Blog Wireless Security protocols: WEP, WPA, WPA2 and WPA3  
[Wikipedia Wi-Fi Protected Access](#)

## Cryptographic Algorithms

## Cryptographic Algorithms

Block Cipher Modes					
	Methodology	Advantage	Disadvantage	Use Case	
ECB	Divide into Blocks		Weakness	Deprecated	
	Encrypt Blocks		Same Key Per Block		
CBC	Combines Block with Previous Block		Inefficient	Symmetric Block Cipher	
	IV for Randomness		Pipeline Delays		
	XOR Operation				
CTM	Block into Stream Cipher	Multiprocessing		Secure Mode of Operation	
	IV & Counter				
	Different Key Per Block				
GCM	Counter Mode Operation	Efficient		Encryption / Decryption	
	Galois Mode Authentication			Authenticity	

## Cryptographic Algorithms

Asymmetric Encryption						
	Bit	Methodology	Advantage	Disadvantage	Use Case	
RSA Rivest Shamir Adleman	2048	Prime Number Properties	Strong Security with Sufficient Key Size		Data Transmitted over Internet	
ECC Elliptic Curve Cryptography		Based on Diffie-Hellman Static Key			Email	
DHE Diffie-Hellman Ephemeral	Generates Key	Elliptical Curve	Less Resource Intensive		Low-Power Devices	
					Small Wireless Devices	
	Between 768 and 3072 Based on Group #'s 1-15  Higher Group # is More Secure	Ephemeral Key		Negotiates for Strongest Supported Group	Sharing of Symmetric Key	
ECDHE Elliptic Curve Diffie-Hellman Ephemeral	Generates Key Using ECC	Ephemeral Key		Negotiates for Strongest Supported Group	Sharing of Symmetric Key	

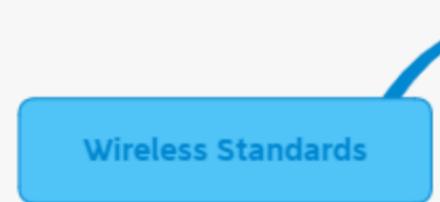
## Cryptographic Algorithms ↗

File Integrity Check				
	Output Size Bit	Algorithm	Functionality	Use Case
CRC32		Checksum	Detect Data Corruption	
MD5	128	Message Digest	Verify Data Integrity	Email
			Detect Data Corruption	File on Disk
				File Download
				Executable File
SHA Family	0 (160)	Digital Signature	Encryption	Detection of File Modification by Malware
	1 (160)		Data Integrity	HIDS
	2 (224, 256, 384, 512)			
	3 (224, 256, 384, 512)		Authenticity	Antivirus
HMAC	HMAC-MD5 (128)	Shared Secret Key for Randomness	Data Integrity	IPsec
	HMAC-SHA1 (160)		Authenticity	TLS
RIPEMD		Message Digest	Verify Data Integrity	

## Cryptographic Algorithms

### Password Hashing Algorithms

	Bit	Salt	Functionality	Use Case
Argon2		Salt	Key Derivation Function	Backend Server
		Secret Key		Cryptocurrency
Bcrypt		Salt	Blowfish Encryption	Unix/Linux Shadow Password File
PBKDF2	128, 256, 512	Salt	HMAC Function	WPA2 Apple iOS Cisco OS
Scrypt		Salt	Key Derivation Function	Wallets
				Files
				App Passwords



### IEEE 802.11 Standard

	Frequency (GHz)	Streams (Up To)	Speed (Up To)	Channel Numbers (North America)	Channel Width (MHz)	RF Modulation
802.11a	5	1	54 Mbps		20	CDMA, DSSS
802.11b	2.4	1	11 Mbps	1 through 11	20	CCK, DSSS
802.11g	2.4	1	54 Mbps	1 through 11	20	CCK, DSSS, OFDM
802.11n	2.4, 5	4 MIMO	150 x 4 = 600 Mbps	2.4: 1 through 11	20, 40	CCK, DSSS, OFDM
				5: 36, 40, 44, 48, 149, 153, 157, 161, 165		
802.11ac	5	8 MU-MIMO	866.7 x 8 = 6.933 Gbps	5: 36, 40, 44, 48, 149, 153, 157, 161, 165	20, 40, 80, 160	BPSK QPSK QAM