MDIX → medium dependent interface crossover is a version of mdi enabling connection between corresponding devices such as switch to another switch

Bend radius → Bend radius is a concern when using fiber cables as it leads to increase reflections and decrease in signal strength.

→ Wireless B and G networks always use channels 1, 6, and 11 to ensure you're using non overlapping frequencies.

→ In ATM Network frames are called cell and it is operated 2nd layer of OSI model

SIP → Session initiation Protocol uses ports 5060 and 5061. It is a signaling protocol used for initiating, maintaining and terminating real-time sessions that include voice, video, and messaging application.

patch cable (straight-through

- patch cable has match on the Tx and Rx pin (pins 1, 2, 3, and 6) both sides of cable.

- crossover cable - pin crossing from one side to another such as pin 1 to 6.

- Rollover cable as opposite pin segment 1 to 8, 2 to 7, 3 to 6.

- Rg-6 cable has only one internal copper wire.

* MTBF - mean time between failure measure the average time between when failure occurs on a device

* MTTR - mean time to repair is average time to repair network device when it breaks

* RTO - Recovery time objective is the duration of time and service level within which a business process must be restored after a disaster to avoid unacceptable consequence associated with break in continuity

* RPO - Recovery point objective

Anycast → Anycast address is an adress that can be assigned to more than one interface A packet sent to anycast address is routed to nearest interface having that anycast address. Anycast communications are sent to nearest receives in a group of receives with the same IP. Anycast only work with IPV6.

multicast → can be used with both IPV4 and IPV6. Technique one to many over IP.

Broadcast → used only within IPV4 one to all

unicast → one to one, work with IPV4 and V6

→ TACACS+ (Terminal Access controller Access control system) was developed by proprietary protocol by CISCO.

→ RADIUS → (Remote Authentication Dial-In user service) is a network protocol that operates on port 1812 and provide centralized AAA management for users who connect and use a network.

Kerberos → is a network authentication protocol designed to provide strong mutual authentication for client/server application using secret-key cryptography developed by MIT.

CHAP → challenge-Handshake protocol is used to authenticate a user or network host to an authenticating entity. CHAP is an authentication protocol but does not provid authorization or accounting service

SDN (Software defined Network)

Three-tiered data center network
core, Distribution / aggregation / Access / edge

out-of-Band → OOB is ~~method~~ manage ment is a method of remotely controlling and managing critical IT assets and network equipment using a secure connection through a secondary interface that is physically separate from the primary network

SL authentication
strong mutual
strong encryption
supported by

2.4 GHz	5 GHz	6 GHz
802.11b	802.11a	WiFi 6E
802.11g	802.11n	unused
802.11n	802.11ac	802.11ax
	802.11ax	

↙ max speed throughput 54mbps

FQDN → Fully qualified domain name
DNS - port 53 translate FQDN to IP
DHCP - Dynamic host configuration control protocol - port 67

WINS → microsoft windows based server running the windows internet name service
WINS server maintain database of NetBIOS name to IP

→ TDR helps to determine the break into the ~~cable~~ copper cable
→ OTDR helps to determine the break into the optic fibre cable
→ optical power meter, measure the power is optical signal over fibre optic cable. It would test if the cable is broken but it cannot say where is broken

TACACS+ used

- tone generators → is used with a toner probe to accurately identify the location of a cable pairs or conductors within wiring bundle. It is only used with copper cable.

- High signal to noise signal is good thing on wireless networks and leads to faster speed and lowers retransmission,

- ## Attack

DNS spoofing or DNS poisoning
- an attack that corrupts the Domain name system data in the DNS resolver cache and cause the name server to return an Incorrect Ip address

- VLAN HOPPing
An attack where the attacker is able to send traffic from one VLAN into another by either double tagging or switch spoofing

- ARP spoofing → malicious actors sends falsified message ARP to local Area Network

- Rouge DHCP → is a DHCP server setup on a network by an attackers.