Přepínací režimy – Prořezávací

v momentu, kdy z rámce přijmu adresu, tak to rovnou začnu na danou adresu přeposílat

Modifikovaná prořezávací

poslouchám pevnou dobu, 64 bajtů, pokud nedojde ke kolizi v tu dobu, tak teprve tehdy začnu přeposílat, výhoda, že je pevně dané zpoždění, se kterým přepošlu

Store and foreward

začínám přeposílávat až ve chvíli, kdy jsem si jistý, že mi vyšlo CRC (dnes se nejvíc využívá, variablilní zpoždění nevadí, a paměť je levná)

BGP-4 – weight, local preference, AS\_path + vstupní diskriminátor (gateway)

IGMP registrace k multicastu

IGMP snooping – switch detekuje IGMP zprávy a je si s nimi schopen plnit svoji „mac tabulku“ (je to spesl snoop tabulka)

NETCONF protocol – konfigurace zařízení. Každé zařízení má ale jinou konfiguraci – Netconf to shrnuje pod jednu, aby se to dalo konfigurovat najednou

RADIUS protocol – AAA autentickace, autorizace, accounting (o koho se jedná, jaká má práva, kolik toho čerpal) pouze hesla jsou kryptovaná

DIAMETR – pro labilní sítě

CAPWAP – jednotný systém bezdrátových sítí, managuje acespointy ve wifi síti – mezi wireless controlerrem a menšími accespointy funguje právě CAPWAP

SNMP – monitoring z manažerské stanice. Na každém zařízení SNMP agent a MIB databáze  
 GetRequest – manažer se ptá na některé hodnoty uložené na zařízení  
 Response – odpověď na GetRequest, nebo SetRequest  
 SetRequest – Jako GetRequest, ale Get je read Set je write  
 Trap – Zpráva o statusu od klienta pro managera. Např když začne docházet paměť, hodnota se bube nebezpečně blížit nejaký hranici (přehřívání)  
 Inform – Ack Trap zprávy  
MIB databáze – strom, má základ, který se musí zachovat, ale muže se dál větvit  
 OID - 1.2.6.1.1.2 (urcuje vždycky patro a co na danem patre, v podstate slozky)  
 ASN.1 – textovy popis databaze  
 BER – Type/Length/Value – kodování pro přenos po síti

SYSLOG – generování, transport, sběr událostí a poruch, používá UDP, ve zprávě určeno z jekého procesu pochází. Různá stupeň akutnosti (severity) 8 stupňů

NETFLOW – shromažďuje info o prošlých packetech

Bezpečnost

Autentizace – ověření identity člověka

Autorizace – Určuje přístupová práva

Utajení – Informace jen pro autorizované objekty – šifrování

Integrita – Zjištění, zdali přenášená informace nebyla změněna, ztracena, schopnost detekce takovéto změny

WEP – pouze utajení (I to řeší špatně) nahradil ho  
TKIP – kompatibilní se starym hardware, podporuje dynamické klíče

PAP – přijde jméno/heslo a já porovnám a buďto ack (OK), nak (nope), heslo se posílá v plain textu

CHAP – periodicky kontroluje klienta pomocí 3way handshake, používá Hash Funkci MD5

802.1x – nepřímá autentizace, pocitac se pripoji na sit a router se ptá autentizačního serveru.