1. Směrovací protokoly užívané primárně v prostředí TCP/IP.

- BGP a OSPF jsou dva nejvíc používané směrovací protokoly. BGP exceluje s dynamickým směrováním pro rozsáhlé sítě a OSPF nabízí více efektivní výběr cesty a rychlou konvergence
- **RIP**
  - Metrika = počet mezilehlých směrovačů, maximálně 15
  - Směrovače posílají své směrovací tabulky sousedům každých 30s
  - Pro přenos tabulek se využívá UDP
- **IGRP**
  - Distance vector IGP protokol vyvinutý společností Cisco
  - IGRP byl vytvořen částečně proto, aby překonal omezení RIP (maximální počet skoků pouze 15 a jedna metrika směrování) při použití ve velkých sítích
- **EIGRP**
  - Distance vector IGP
  - Může provádět vyvažování zátěže cest s různou cenou
  - Pro výpočet nejkratší cesty používá difuzní aktualizační algoritmus DUAL

Protokol OSPF (znát algoritmus SPF - umět vysvětlit - příklad činnosti), metrika, typy zpráv (LSA), zapouzdření, používané adresy a porty, zvláštnosti implementace v prostředí sítí s vícenásobným přístupem - DR/BDR, postup volby.

Charakteristika

-Všechny routery si vyměňují LSA zprávy (obsahující informace o cestách) a tvoří si LSDB (databáze cest) - topologie sítě

- Je postavený na principu oblastí, výchozí oblast **area 0** (páteřní oblast), ke které se ostatní připojují
- OSPF a OSPFv2 = IPv4 OSPFv3 = IPv6
- Patří mezi nejpoužívanější protokoly
- Defaultní administrativní vzdálenost = 110

SPF (shortest-path first) = slouží k výpočtu nejkratší cesty

Princip:

1. Každý směrovač identifikuje své sousedy
   a. Zjistí cenu a port ke každému sousedu
   b. K seznámení slouží Hello pakety (lze nastavit i manuálně)
2. Každý směrovač sestaví svůj Link State Advertisement (LSA) a ten distribuuje do celé sítě
   a. Rozhlašuje cenu ke každému ze svých sousedních směrovačů a ty to posílají dále
   b. Vysílá v případě že: Nový soused, změna ceny cesty, zmizí soused

3. Směrovač přijme LSA
    a. Kontrolují se 2 věci
        i. LSA se doručí všem ostatním routerům
        ii. LSA je nejaktuálnější
    b. Databáze musí být identické pro všechny směrovače (Pokud ne, tak by vypočítávali špatné trasy – kruhové cesty)
4. Spustí SPF algoritmus
5. Vybere nejlepší cestu

Metrika

- Používá **cenu cesty** (hodnota daná přenosovou rychlostí rozhraní)
- Vzorec => referenční hodnota přenos. rychlosti (defaultně 100Mbit/s) / přenosová rychlost daného rozhraní

Typy zpráv (LSA) a zapouzdření

a) Hello paket = Pro navázání sousedství s jinými směrovači

b) Database Description (DBD) paket = obsahuje zkrácený LSDB odesílajícího směrovače pro kontrolu přijímajícího směrovače (LSDB musí být identické, aby se vytvořil přesný SPF strom)

c) Link-State Request (LSR) paket = Pro zažádání libovolného záznamu o DBD

d) Link-State Update (LSU) paket = Odpovídá na LSR (obsahuje různé typy LSA)

1. Router LSAs
2. Network LSAs
3. Summary LSAs
4. Summary LSAs (reprezentuje ASBR)
5. Externí LSAs autonomního systému
6. Multicast OSPF LSAs
7. Defined for Not-so-stubby areas (používá se ve stub oblastech místo LSA 5)
8. Externí vlastnosti LSA pro BGP

e) Link-State Acknowledgment (LSAck) paket – pokud přijde LSU odešle potvrzení LSAck

-Jedno LSU obsahuje jedno nebo více LSAs

-LSAs obsahuje informace o cestě ke konečné síti

Používané adresy a porty

- OSPF komunikace mezi routery prostřednictvím multicastových adres:
    - **224.0.0.5** = komunikace od DR k ostatní routerům
    - **224.0.0.6** = odesílání LSA zpráv od DROTHER (OSPF router, který není DR nebo BDR) do DR a BDR
- Využívá transportní protokol na portu **89**

Zvláštnosti implementace v prostředí sítí s vícenásobným přístupem - DR/BDR

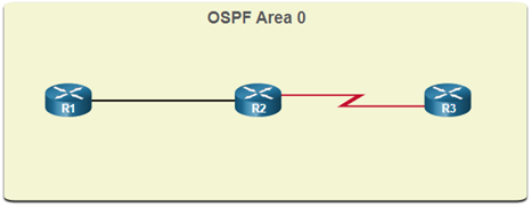
- Pokud se nejedná o P2P, tak Hello paket vybere, který router bude Designated Router (DR) a který bude Backup Designated Router (BDR)
- **DR** slouží k tomu, aby nebylo vytvořeno vícenásobné spojení vznikl spojením více sítí OSPF a zároveň snižuje zahlcování LSA pakety
    - R1 pošle LSA DR a ten pošle ostatním routerům LSA R1

Pravidla pro zvolení DR a BDR:

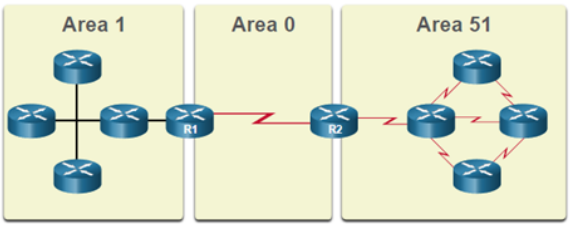
1. Router s větší prioritou OSPF se vybere jako DR
2. Pokud mají stejnou prioritu, tak se vybere router s vyšším ID
3. Router s druhou nejvyšší prioritou/ID bude BDR

Role směrovačů (interní, páteřní, ABR, ASBR)

- Aby bylo OSPF efektivnější a škálovatelnější, tak podporuje hierarchické směrování pomocí oblastí
- **Area =** množina směrovačů, které mají k dispozici identickou databázi LSA
- Pokud je vytvořeno více oblastí, vždy musí být vytvořena páteřní oblast označená area 0 a ostatní oblasti mohou být na tuto opřipojeny
    - **Single-area OSPF** – všechny routery jsou v jedné oblasti (area 0)



    - **Multi-area OSPF** – je použito více oblastí, všechny oblasti se musí napojit na páteřní oblast (area 0). Směrovače, které propojují oblast se označují jako ABR



Role

- ABR – routery, mezi jednotlivými areami
- ASBR – jsou routery, které jsou mezi OSPF síti a non-OSPF (RIP, …) sítí
- Interní směrovač – každý směrovač uvnitř oblasti
- Páteřní směrovač (backbone) – směrovač v páteřní oblasti

Pojem oblast (area)-tranzitní, regulérní; stub, not so stubby, totally stubby, totally not so stubby.

- Tranzitní (páteřní) = slouží k předávání síťového provozu z jedné oblasti do druhé

- Regulární (standartní) = zaručuje klasické směrování

- Stub (pahýl)
  - Musí být nakonfigurovány směrovače, poté nebudou vytvářet sousedství se směrovači, které nejsou typu stub
  - Zakazuje LSA typu 5 a ASBR
  - Myšlenka mnoha cest nahrazení jedinou výchozí

- Totally stubby
  - Všechno směrování závisí na jedné výchozí cestě
  - Přispívá ke snížení zátěže směrovačů v části sítě, kde není třeba úplné info o všech sítích v OSPF
  - Nesmí obsahovat ASBR (tato oblast nepovoluje zasílat LSA typ 3 a 5)

- Not-so-stubby
  - Posílá typ 7 („převlečená“ type 5 LSA)
  - Zasílá typ 3 do a z oblasti
  - ASBR je povolené

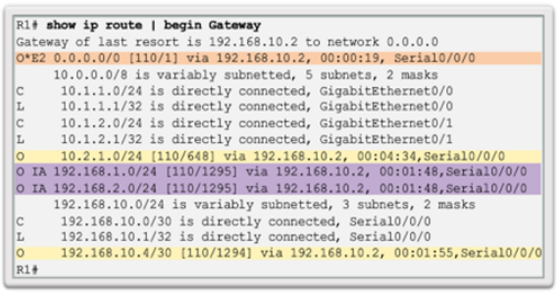
- Not-so-totally-stubby
  - Same jako not so stubby, ale je třeba konfigurovat, čímž eliminujeme typ 3

Souhrn:

- Standardní oblasti obsahují LSA 1,2,3,4,5 a mohou v nich být přítomny ASBR
- Stub oblasti obsahují LSA typ 1,2,3 a vnější cesty jsou nahrazeny výchozí cestou
- Totally stubby používají LSA 1 a 2 a jednu 3 ,která popisuje výchozí cestu mez
- NSSA implementují funkci stub, ale mohou obsahovat ASBR, LSA 7 jsou převlečené typ 5, které převádí ABR, aby mohly být šířeny záplavou

Konfigurace OSPF s více oblastmi, topologie, problémy - OSPF virtual link.

- O – říká, že routa je vnitřní
- O IA - ukazuje na Summary LSA
- O E1 nebo E2 – ukazuje na externí LSA



- OSPF virtual link
    - Řeší situace, kdy daná oblast není přímo propojená s páteřní oblastí = připojení nespojité oblasti pomocí tranzitní oblasti
    - Slouží pouze pro dočasné řešení nebo zálohy
    - Při konfiguraci se musí použít ID(odpovídá nějakému loopbacku) routeru pro virtuální linku
    - Problémy této implementace
        - Nemohou procházet přes více než 1 tranzitní oblast (pro každou další tranzitní oblast bychom potřebovali novou virt. linku)
        - Jsou závislé na stabilitě tranzitní routy (intra-area)
        - LSA záznamy naučené z virtuální linky nestárnou (neporvádí se refresh každých 30 minut, aby se nezahlcovala linka)

Redistribuce statických směrovacích záznamů do směrovacích protokolů, výchozí cesta.

- Výchozí statická cesta je třeba pro posílání paketů do sítě, která nepoužívá OSPF
- Propagace = **default-information originate** (výchozí cesta MUSÍ být nastavena)

2. Access Control List - účel, druhy, příklad konfigurace. Parametr „established“.

Účel:

- série komandů s účelem filtrovat pakety na základě obsahu jejich hlavičky
- defaultně nemá router ACL
- skládá se ze série permit/deny statementů (Access Control Entries)
- Příklady užití
    - limitace zatížení sítě pro zvýšení jejího výkonu (zákaz obsahu typu “video”)
    - řízení toku v síti = omezení jen na některé linky (zákaz některých route updatů)
    - základní bezpečnost = povolen přístup jen z určitých sítí/adres
    - filtrace provozu dle typu provozu (zákaz Telnetu)
    - screen hostra pro permit/deny ke službám sítě (filtrování práv přístupu)
    - poskytování priorit pro určité typy provozu = (př. přenos hlasu/zvuku)

Druhy:

- Standard = permit/deny pouze na základě zdrojové IPv4 adresy
- Extended
    - filtrují dle zdrojové/cílové ipv4 adresy, typu protokolu, TCP/UDP portu, atd.
- Číslované
    - 1-99 + 1300-1999 = standardní
    - 100-199 + 2000-2699 = extended
- Pojmenované = jsou lepší, jelikož jméno naznačuje účel ACL

Konfigurace:

- využívá se wildcard (0.0.0.255) = vymezení IP adres pro aplikování ACL (bity s 0 musí sedět)
- router může mít na každém rozhraní až 4 ACL (inbound/outbound IPv4/6)
- Vymazání ACL = no access-list **access-list-name/number**

- Best practise:
  - dělat ACL dle požadavku organizace
  - vypsat si, co má ACL dělat
  - využívat text editor pro práci a ukládání ACL
  - dokumentovat ACL pomocí remark komandu (poznámka)
  - testovat na development před implementaci do produkce

- Číslovaný standardní
  - access-list **access-list-number** deny/permit source

- Pojmenovaný standardní
  - ip access-list standard **access-list-name**

- Aplikování na interface:
  - když je ACL vytvořené, tak ho je potřeba nalinkovat na interface
  - **ip access-group access-list-number/name in/out** (konfigurovat v interface)
  - Odstranění = no ip access-group

Parametr extended/established:

- Číslovaný extended
  - access-list **access-list-number** deny/permit protocol source (sourceWC) (operator sourcePort) destination (destinationWC) (operator destPort)

- Pojmenovaný extended
  - ip access-list **extended access-list-name**
  - Poté vytvářet jednotlivé ACE

- Operátory (lq, gt, eq) slouží pro porovnávání portů, nejsou povinné

- Parametr established
  - Volitelný parametr, za pomocí tohoto argumentu může ACL vykonávat základní firewall funkce
  - zamezuje TCP provozu generovanému/započatému zvenčí, ale povoluje odpověď z venku
  - může být použit na povolení provozu z jen některých webovek, jiné jsou zakázány

3. Bezpečnost v počítačových sítích - druhy malware, typy útoků. Zranitelnosti a hrozby - IP, ICMP, TCP, UDP, ARP, DHC, DNS - příklady útoků

Druhy malware

Viry

-nejčastější malware, potřebuji lidskou akci k aktivaci (třeba otevření přílohy)
-dnešní době jsou vyvíjeny pro specifický účel

- Boot sector virus = útočí na boot sector, file partition table nebo file system
- Firmware virus = útočí na firmware zařízení
- Macro virus =virus zneuvyužíva např. Ms office macro pro ovládání PC
- Program virus = virus se vloží do jiného programu
- Script virus = virus utočí na interpreter OS, který je využit k vykonání scriptu

Trojský kůň

-útočník ho užívá ke kompromitaci cíle, je to program, který se tváří normálně, ale má část, která vyukonává neplechu
-často jsou součástí free online programů/her

- Remote-access = umožní útočníkovi vzdálený přístup
- Data-sending = předá útočníkovi citlivá data
- Destructive = poškodí nebo vymaže soubory
- Proxy = využívá zařízení cíle jako zdroj pro jiné ilegální aktivity
- FTP = umožní neautorizovaný přesun souborů
- Security software disabler = vypne antivirus nebo firewall
- DoS = zpomalí nebo zastaví provoz na síti
- Keylogger = snaží se ukrást citlivé informace pomocí zaznamenávání klávesnice

Adware

-obvykle přes online download SW
-zobrazuje pop-up okna v browseru nebo nečekané přesměrování na jiné webovky
-problém při rychlejším vyskakování oken, než uživatel stíhá zavírat

Ransomware

-obvykle zašifruje soubory uživatele a pak vyžaduje výkupné
-obrana zálohováním, jinak platba v kryptu

Rootkit

-využíván útočníkem pro získání admin práv
-těžké na detekci, jelikož mohou pozměnit funkce obranných prvků
-vytváření backdoor pro útočníka (instalace, upload nebo pro DDoS)
-pro odstranění je třeba speciální sw tool nebo reinstall

Spyware
-podobné adwaru, ale pro neoprávněný sběr informací o oběti

Worm
-self-replicating program, který využívá zranitelností v systému pro své šíření
-využívá síť pro nalezení obětí se stejnou zranitelností
-obvykle zpomalují nebo narušují síť organizace

Typy útoků

Průzkumné útok
-útočník chce zjistit/zmapovat oběť za účelem dalšího postupu

- Information query = útočník hledá open source informace (Google, whois)
- Ping sweep = ping adres sítě organizace pro zjištění, které jsou aktivní
- Port scan = zjištění aktivních služeb (portů) na IP (nmap, superscan, netscantools)
- Vulnerability scanner = zjištění typu a verzi aplikací + OS na hostu (př. Nipper, SAINT)
- Exploitation tools = objevení zranitelnosti pro danou verzi (SQLMAP, Metasploit)

Přístupové útoky (access attacks)

- Útok na heslo = zjištění kritického hesla pro systém (bruteforce, dictionary, …)
- Spoofing útok->útočník napodobuje jiné zařízení falšováním
  dat př. IP, MAC, DHCP spoofing
- Trust exploitation
- Port redirection
- Man-in-the-Middle
- Buffer overflow
- Sociální inženýrství = útok který se zaměřený na zranitelnost člověka (phishing, …)

DoS+DDoS
-je založen na zasílání enormního množství dat nebo škodlivě formátovaných paketů, která síť, host nebo aplikace nejsou schopny vydržet => zpomalení nebo pád systému
-DDoS je podobný DoS, ale útok je zároveň prováděn z několika míst/zařízení

Zranitelnosti a hrozby

Typy zranitelností
Technologické = zranitelnosti operačních systémů, protokolů, síťových zařízení

Konfigurační = nedostatečně zabezpečené přenosové kanály, jednoduchá hesla, …

Bezpečností politiky = špatně definovaná bezpečnostní politika, neexistující plán obnovy, …

Hrozby

- Výpadky sítě, narušení fungování služby = ztráta peněz a času
- Informační krádež = odcizení citlivých informací o zákaznících/firmě
- Poškození nebo změna dat
- Odcizení identity

IP

-IP neověřuje zda zdrojová IP v paketu opravdu přišla od zdroje = možnost padělání

- Amplification and reflection = útočník zabrání opravdovému uživateli v přístupu k informacím/službám pomocí DoS/DDoS
- Address spoofing = ukradne původní adresu z paketu pro blind spoofing
- Man in the Middle = útočník se vloží do komunikace, aby mohl monitorovat provoz
- Session hijacking = útočník dostane přístup k fyzické síti a to zneužije

ICMP

-hlavně pro zmapování sítě+DoS

-obrana pomocí ACL

-využívá se jednotlivých ICMP zpráv

- Echo request/reply = host verifikace+DoS
- Unreachable = prozkoumání/skenování sítě
- Mask reply = mapování vnitřní IP sítě
- Redirect = nalákání hosta pro zasílání provozu přes kompromitované zařízení
- Router discovery = injectování do routovací tabulky

TCP

-obvykle se útočí na 3-way handshake mechanismus pomocí control bitů

- TCP SYN Flood = útočník neustále posílá SYN-ACK paket na spoofnutou adresu a čeká na ACK (nikdy nepřijde). Nakonec je oběť zahlcena a má nedostupné TCP služby
- TCP Reset = útočník může poslat spoofnutý paket obsahující TCP RST na endpoint
- TCP session hijacking = obtížné na provedení, utočník ovládne již autentifikovaného hosta a může pouze zasílat data cíli

UDP

-nemá default encryption (otevřená všem), checksum je optional a útočník může vytvořit i novou checksum dle změn

- UDP Flood = za použití nástroje(UDP Unicorn) útočník pošle záplavu UDP paketů z spoofnutého hosta na server. Nástroj se bude snažit najít uzavřený port => server odpoví ICMP port unreachable zprávou. Jelikož má server hodně zavřených portů, tak vytvoří velký provoz na segmentu sítě, což zabere většinu kapacity (podobné DoS)

ARP
-útočník může propagovat cizí IP/MAC jako svou a vytvořit tak Man in the Middle

- ARP Cache poisoning = útočník pošle ARP odpověď s požadovanou IP a svou MAC => host nyní změní ARP cache, takže provoz jde přes útočníka a ten může jen odposlouchávat nebo měnit obsah

DHCP
- DHCP Spoofing = připojení falešného DHCP serveru do sítě, který poskytuje falešné údaje reálným klientům (špatný gateway => MitM)
- DHCP Starvation = vyčerpání poolu IP adres serveru

DNS
-definuje dvojce jméno domény/webu s jeho ip
-zabezpečení DNS je často opomíjeno

- DNS open resolver attacks (servery otevřené světu)
  - Cache poisoning = přesměrování klienta na jiný web
  - Amplification and reflection = DDoS schová útok kdy pošle open resolver s IP cíle
  - Resource utilization = DoS sebere všechny prostředky DNS open resolverů
- DNS stealth attacks
  - Fast flux = maskuje phishing/malware díky měnícím se DNS cílů
  - Double IP flux = utočník rychle změní hostname v IP mappingu (špatně se identifikuje útočník)
  - Domain generator algorithms = malware generuje doménová jména, které pak lze využít pro command and control servery
- DNS domain shadowing attack = útočník sežene credentials domény, vytvoří sub domény pro následný útok
- DNS Tunneling = útočník vloží non-DNS provoz do DNS provozu, většinou aby obešel zabezpečení a mohl komunikovat s boty uvnitř sítě nebo vytáhl data (databázi hesel)

4. Překlad adres. Statický, dynamický; pojmy pool; inside/outside, local/global, rozdíl NAT/PAT, NAT v prostředí IPv6 - ULA

Překlad adres
-NAT (Network Address Translation) = technologie která překládá privátní adresy na veřejné
-díky tomuto stačí organizaci jedna veřejná IP adresa prezentování do internetu, za kterou dokáže “schovat” vícero privátních IP adres
-hlavní důvod je šetření veřejných IP adres + bezpečnost
-NAT funguje zejména na routeru, který přistupuje do vnějšího internetu

Základní druhy adres

- Inside Local = privátní adresy stanic ve **vnitřní** síti, privátní
- Inside Global = veřejné adresy, pod nimiž jsou stanice na **vnitřní** síti vidět z vnější sítě
- Outside Local = privátní adresy stanic ve **vnější** síti
- Outside Global = veřejné adresy, pod nimiž jsou stanice **vnější sítě** vidět z vnitřní sítě

Statický překlad

- Každá inside local IP adresa má pevně danou ubsude global adresu na kterou se překládá
- Ideální pokud potřebujeme sdílet nějaké zařízení které má mít konzistentní IP adresu (např. webový server)
- Překladová tabulka je statická a v případě změny je potřeba manuální úprava

Dynamický překlad

- Jedna inside local IP může být na outside interface zastoupena vícero inside global adresami

Pool

- Sada dostupných veřejných IP adres, které jsou postupně přidělovány místním zařízením při použití dynamického překladu

Inside/Outside:

- **Inside (vnitřní)**
  -adresa jakéhokoliv zařízení **vnitřní sítě**

- **Outside (vnější)**
  -adresa jakéhokoliv zařízení **vnější sítě**

Local/Global:

- **Local (lokální)**
  -jakákoli **privátní** adresa uvnitř konkrétní sítě, překládaná pomocí NAT na globální

- **Global (globální)**
  -**veřejná** IP adresa routovatelná v rámci internetu, na okraji sítě

Rozdíl NAT/PAT:

-NAT překládá **jednu inside local** adres na **vícero** možných veřejných inside **global**
-PAT (nebo také NAT overload) překládá **vícero inside local** adres na **jednu** veřejnou **inside global** adresu, avšak každá IP dostane jiný port

- Inside local port = port, ze kterého byl paket odeslán
- Inside global port = port, na který byl původní port namapován

NAT v IPv6

-NAT pro čistě IPv6 není z důvodu dostatečného počtu adres potřeba
-Pro propojení IPv6 a IPv4 sítí slouží protokol **NAT64** pro překlad privátních a veřejných adres různého typu
-NAT64 je jeden z mechanismů usnadňující přechod od IPv4 k IPv6 (dále DualStack a Tunneling)

ULA

-ULA (Unique Local Address) adresy jsou u IPv6 “obdobou” privátních IPv4 adres
-Slouží **pouze** ke **komunikaci uvnitř** lokální sítě (nepřekládají se) => zvýšení bezpečnosti
-Mají dostatečně dlouhý prefix pro zaručení unikátnosti v rámci sítě (od /48 do /64)
-Skládají se z globálního prefixu (FC00::/7) a lokálního identifikátoru, který se generuje náhodně nebo podle vlastních pravidel organizace.

5. Globální sítě - charakteristika, terminologie, protokoly, zařízení, tier 1 ISP

Charakteristika WAN

- Poskytují síťové služeb napříč velkými geografickými oblastmi
- Slouží pro vzdálené propojení uživatelů, sítí
- Jsou vlastněný a spravovány ISP a telekomunikačními providery
- Služby jsou poskytovány za poplatek

Protokoly pro 1. a 2. Vrstvu

- Layer 1 (SDH, SONET, ..)
    - Zabývá se elektrickým a mechanickým problémem
    - ISP používají optické vlákna s velkou šířkou pásma na velké vzdálenosti
- Layer 2 (DSL, MPLS, PPP, ATM)
    - Zabývá se tím, jak data budou zakomponovány do rámce

Terminologie

- **Data Terminal Equipment** (DTE) - zařízení, které propojuje uživatelskou LAN k WAN
- **Data Communications Equipment** (DCE) - zařízení na komunikaci s providerem (zprostředkuje prostřed na propojení uživatele ke komunikační lince)
- **Customer Premises Equipment** (CPE) - DTE a DCE hw nebo sw na straně uživatele k propojení s providerem
- **Point-of-Presence** (POP) - bod připojení k síti
- **Demarcation Point** - fyzická hranice, která určuje kde jsou povinnosti providera a kde uživatele
- **Local Loop** - kabel který propojuje CPE k CO providera
- **Central Office** (CO) - místo, které propojuje CPE k síti providera

Topologie WAN

- Point-to-point = sítě propojeny napřímo, drahé řešení pokud je mnoho sítí
- Hub-and-Spoke = jeden interface na hub routeru je sdílen všemi spoke routery
- Dual-homed = všechny spoke routery napojeny do dvou hub routerů, redundance
- Fully Meshed = každá síť spojená s každou, velká fault tolerance
- Partially Meshed = propojuje mnoho, ale ne všechny sítě

Zařízení

- Modem
    - Vytáčecí modem používající telefonní linky pro přenos dat
    - Provádí převod digitálního signálu na analogové hlasové frekvence
- DSL modem, Kabelový modem
    - Vysokorychlostní digitální modemy, využívají Ethernet
    - DSL modemy se do WANky připojují pomocí tel. Linek (kabelové pomocí koaxiálu)
- CSU/DSU
    - Pronajaté linky
    - Připojení k digitálním linkám
    - Zařízení mezi poskytovatelem a naším routerem
- Optický převodník
    - Převod z optického média na el. pulzy do dvojlinky
- Bezdrátový router
    - Bezdrátové připojení k WAN providerovi
- WAN core zařízení
    - Páteřní síť - využivá spoustu vysokorychlostních routeru a L3 switchu
    - Podpora řady různých telekomunikačních rozhraní

Tier 1. ISP

- Společnosti nabízející pevné nebo bezdrátové připojení k internetu
- Tier 1 ISP poskytují **přímé** připojení k internetu a jsou nezávislé na nikom jiném, jsou známí jako globální síťoví operátoři (pod nimi Tier 2 a 3)

Přepínání okruhů/zpráv (multiplexy T/E; SONET/SDH)

Přepínání okruhů

- Vytvoří vyhrazený okruh pro uživatele
- Během komunikace se používá celou dobu stejná cesta
- Celá kapacita cesty je přidělená jednomu okruhu – neefektivní

Přepínání paketů

- Data jsou rozložena do paketů, které jsou posílány postupně za sebou
- Veškeré pakety se posílají sítí, která je sdílená - efektivnější
- Náchylná na zpoždění i přesto je uspokojivý přenos hlasové a obrazové komunikace

SDH, SONET

- ISP používají převážně používají optická vlákna, kvůli menším přeslechům a útlumu
- Používají se 2 standardy op. vláken: (v podstatě stejné)
    - SDH – globální standard
    - SONET – americký standard

DWDM

- Novější technologie, která zvyšuje tok dat
- Multiplexuje toky paprsků díky různé vlnové délce
- Podporuje SONET/SDH standardy
- Až 80 kanálů – 10Gbps, pro podmořské kabely

Varianty připojení do WAN (single - homed, ..., dual - multihomed)

- Single-homed = používá se, pokud internet není nezbytný pro operace, **jedna linka k jednomu ISP**
- Dual-homed = používá se, pokud je připojení o něco důležitější. Nabízí load balancing a má větší redundanci, **dvě linky k jednomu ISP**
- Multi-homed = pokud je připojení nezbytné (**jedna linka k více ISP**), load balance, redundantní linky, dražší
- Dual-multihomed = nejspolehlivější připojení, **dvě linky k více ISP**

Druhy optických spojů, DSL technologie, PPPoE

Druhy optických spojů

- Fiber to the Home (FTTH) = dosahuje až do residence
- Fiber to the Building (FTTB) = přivedeno do objeku, kde je rozvedeno
- Fiber to the Node (FTTN) = přivedeno do optického uzlu, kde je rozveden pomocí dvoulinky nebo koaxiálu

DSL

- vysokorychlostní technologie, která pomocí existující telefonní linky poskytuje připojení (rozlišení na základě jiných frekvencí signálů)
- ADSL = asymetrické rychlosti up a down, využívají měděnou kroucenou dvojlinku
    - Upstream = nižší rychlost
    - Downstream = vyšší rychlost
- SDSL = symetrické rychlosti
- xDSL = soubor všech různých typů DSL, různé rychlosti apod.

PPPoE

- PPP – Layer 2 protokol, který používají telefonní služby pro propojení zařízení
- Používá se s DSL pro = autentifikaci uživatele, přiřazení IP uživateli, kvalitu linky

- Host with PPPoE client
    - Hostitel spouští PPPoE, aby získal IP ze serveru od poskytovatele
    - Klient komunikuje s DSL pomoci PPPoE a DSL komunikuje se serverem pomocí PPP
- Router PPPoE client
    - Konfigurace routeru jako PPPoE klienta
    - Klienti komunikují s routerem pomocí ethernetu a nevědí o DSL připojení
    - Více klientů sdílí jedno DSL

MetroEthernet (MAN), Virtual Private LAN Service

- Metropolitní síť založená na standardech Ethernetu sloužící k připojení účastníků k větší síti nebo Internetu, nebo k propojení poboček institucí
- Výhody:
    - Snížení nákladů a náročnosti administrace
    - Jednoduchá integrace s již existujícími sítěmi (škálovatelnost)

6. Virtuální privátní sítě

-Prostředek k bezpečnému propojení několika zařízení v rámci nedůvěryhodné sítě
-Výhodami je šetření peněz, zabezpečení síťového provozu, škálovatelnost, kompatibilita
-Zároveň umožňuje omezený přístup k webům stránkám, a souborům

- Site to Site VPN
  -VPN nakonfigurována mezi VPN bránou (uživatele neví o komunikaci přes VPN)
- Remote access VPN
  -dynamicky se vytváří za účelem zabezpečného spojení mezi klientem a zařízením

Protokol GRE

Charakteristika

- Non-secure site to site tunelovací protokol
- Používá se k zapouzdření IPv4/IPv6 uvnitř IP tunelu (vytvoření virtuálního spojení)
- Neposkytuje šifrování, podporuje broadcast a multicast

GRE over IPsec

- Využívá výhodu toho, že IPsec vytvoří zabezpečený tunel
- Zapouzdříme směrovací protokoly IP do do GRE a ten následně zapouzdříme do IPsec, které se teprve pak předájí bráně

Základní konfigurace (na source i destination zařízení)

1. Vytvoří se GRE Tunnel interface
2. Konfiguruje se IP pro daný interface
3. Nastavení source IP
4. Nastavení remote destination IP

Protokol IPSec - charakteristika, módy; význam protokolů IKE (ISAKMP), algoritmus Diffie-Hellman.

Charakteristika

- Rámec standardů síťové vrstvy, který zajišťuje bezpečnou komunikaci přes sítě pomocí kryptografických služeb
- V IPv6 je jeho podpora povinná
- Není třeba modifikovat vyšší vrstvy, IPSec je ochrání
- Škálovatelný (od PC až po velké sítě)
- Složitý – citlivý na některé útoky

Funkce a význam:

- Důvěrnost = šifrování (DES, 3DES, AES, SEAL)
- Integrita = hashování (MD5, SHA)
- Ověřování původu dat = protokol IKE, cerifikáty
- Ochrana proti opětovnému vysílání paketu
- Autentizace uživatelů a zařízení
- Diffie-Hellman = výměna veřejných klíčů

Složení IPSec

- AH (Authentication Header)
    - Zajišťuje integritu, autentizaci, ochranu před opakovaným vysíláním
    - Nešifruje data
    - IP i data kontroluje
    - Nelze udělat podvrh adresy

- Protokol ESP (Encapsulated Security Payload)
    - Důvěrnost, autentizace

- Protokol IKE (Internet Key Exchange)
    - Zajišťuje vyjednávání o výměně klíčů
    - Ustavuje SA mezi IPsec partnery
        - SA (Security Association)
            - Jednosměrný vztah mezi odesílajícím a přijímajícím
            - Security parametr index (autentizace)
            - Cílová IP
            - ID bezpečnostního protokolu

Módy

- Transportní mód (default)
    - IPv4 header se nemění a šifruje, pouze data paketu
    - Přidán ESP Header a Trailer (ukazuje na TCP header)

- Tunelovací mód (ve VPN tunelech)
    - Celý IPv4 je zapouzdřen a zašifrován
    - Přidán ESP Header a Trailer (ukazuje na starý IPv4 header)
    - Přidána nová IPv4 hlavička pro zajištění dosažení cíle tunelu

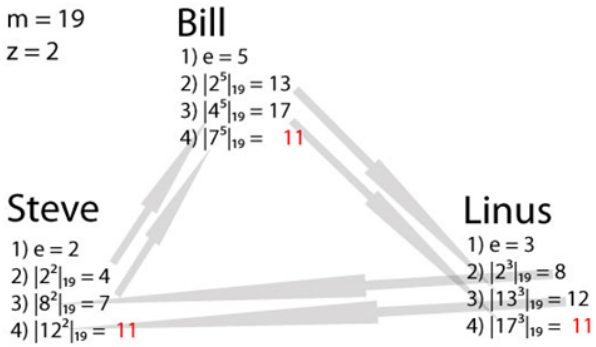
-V obou módech může být přidán ESP Auth Data pro integritu

Význam protokolů IKE (ISAKMP)

- Internet Security Association and Key Management Protocol se zabývá všemi aspekty SA a zajišťuje vyjednávání o výměně kryptografických klíčů

Algoritmus Diffie-Hellman

- Nelze na základě odposlechnutých informací zjistit klíč
- Veřejně se domluví na modulu m a základu z
- Každý účastník zvolí svůj exponent nesoudělný s modulem
- Umocní základ modulárně základ na svůj exponent a výsledek pošle dalšímu
- Červený výsledek je klíčem



7. Kvalita služeb (QoS).

Šířka pásma (přenosová rychlost), zahlcení, zpoždění

Šířka pásma

- Měří se v počtu bitů, které lze přenést za jednu sekundu (bps)

Zahlcení

- Vzniká pokud je v síti více provozu než dokáže zvládnout
    - Agregace linek (4 do 1)
    - Přechod mezi rychlostmi rozhraní (1000 do 100)
    - Přechod mezi sítěmi (WAN do LAN)
- Místa zahlcení jsou ideálními místy pro aplikaci QoS

Zpoždění (latence)

- Doba za kterou se paket dostane ze zdroje do cíle

- Druhy a jejich zdroje:
    - Fixed
        - Code delay = doba než se data zkomprimují před přenosem
        - Packetization = oba zapouzdření paketu
        - Serialization = doba přenosu rámce na drát
        - De-jitter = doba kterou potřebuje vyrovnávací paměť a jejich odeslání v rovnoměrných intervalech
    - Variable
        - Queuing = doba kterou rámec/paket čeká pro přenos na lince
        - Propagation = doba putování mezi odesílatelem a příjemcem

Kolísání zpoždění (jitter)

- Změna vzdálenosti paketů od sebe
- Za straně jsou odesílány v nepřetržitém proudu, ale díky přenosu vznikne zpoždění – přicházejí v jiných intervalech

Algoritmy obsluhy front - First-In, First-Out, Priority Queuing, Fair Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing, Low Latency Queuing.

FIFO (First In First Out)

- Kdo dřív přijde ten dřív mele
- Nejjednodušší (využívá pouze jednu frontu)
- Žádná podpora priority, agresivní proudy zvýhodněny

Priority queuing

- Pakety jsou zařazeny do prioritních tříd
- Každá priorita má svou FIFO frontu
    - Nejdříve se obslouží vyšší třída, pokud nic není ve vyšší jde na řadu nižší
- Pakety s vyšší prioritou mají přednost
- Pokud je kontinuální tok vyšší priority, tak pakety s nižší se zahodí (vyhladovění)

Weighted Fair Queuing (WFQ)

- Pakety jsou opět třízeny do front podle priority
- Frontám jsou přiřazeny váhy – čím vyšší váha tím vyšší priorita
- Obsluhují se střídavě dle váhy – čím vyšší váha tím více paketů odebráno
- Řeší problém vyhladovění

Class-Based Weighted Fair Queuing (CBWFQ)

- Obdoba WFQ ale umožňuje definovat třídy
    - Každá třída má uživatelem definovanou minimální šířku pásma

Low Latency Queuing (LLQ)

- CBWFQ, ale s prioritní frontou například pro voice pakety

Problém Tail Drop, globální synchronizace TCP

Problém Tail Drop

- Problém CBWFQ, pokud se naplní fronta (buffer) tak se všechny další pakety zahodí
- Nerozlišuje mezi třídami služeb
- Řeší Congestion avoidance

Globální synchronizace TCP

- Obě strany komunikace uzavřou své spojení a vymění si potvrzení o přijetí tohoto kroku, avšak pakety se neustále odesílají
- Fronta se plní, když je plná tak se poslední pakety zahazují

Best effort, integrované služby, diferencované služby

Best effort

- Maximální snaha doručit paket, bez záruky
- Se všemi pakety se zachází stejně, ale nemáme záruku o doručení
- + = Škálovatelnost, žádné QoS, nejjednodušší a nejrychlejší na nasazení
- - = Žádná garance doručení, může dorazit v jakémkoliv pořadí, neexistuje preference paketů s vyšší prioritou

Integrované služby (IntServ)

- Poskytuje end-to-end QoS aplikacím, které ji vyžadují
- Spravuje síťové zdroje za účelem poskytování QoS
- Umí rezervovat zdroje a má mechanismy řízení přístupu
- Používá přístup orientovaný na připojení – každá komunikace musí specifikovat descriptor a zažádat si o zdroje
    - Před odesláním dat si aplikace zažádá o určitou službu
    - Zažádá si o typ, aby pokryla zpoždění/šířku pásma, …. (RSVP – pro rezervaci potřeb)
    - Nejdříve si zažádá o rezervaci potřebné cesty – pokud se vytvoří, tak začne přenášet, pokud ne tak ani nezačne

Diferencované služby (DifServ)

- Neumí vynutit end to end záruky
- Provoz klasifikován do tříd, a poskytované příslušné QoS pro tyto třídy
- Každý paket je označen v poli type of service
- Na základě přiřazené třídy je s paketem zacházeno
- Jednoduché a žádné rezervační protokoly navíc, lehce škálovatelný mechanismus pro klasifikaci a správu

Techniky implementace QoS–klasifikace a značkování (ToS/TC, DSCP), předcházení zahlcení, řízení zahlcení - RED, WRED.

Klasifikace a značkování

- Označíme paket (přidání hodnoty do hlavičky), což určí do jaké třídy paket patří a na základě značky jsme schopni aplikovat QoS pravidla
- ToS = IPv4 TC = IPv6
- DSCP = novější verze, 3 kategorie značek
    - Best effort
    - Expedited Forwarding
    - Assured forwarding = nejvyšší priorita

Předcházení a řízení zahlcení

- Třídy provozu mají přiděleny části síťových prostředků, jak je definováno zásadami QoS
- Zásady QoS také určují, jak mohou být některé přenosy selektivně přerušeny, zpožděny nebo znovu označeny, aby se zabránilo přetížení
- Primárním nástrojem pro zamezení přetížení je WRED a používá se k regulaci datového provozu TCP způsobem šetřícím šířku pásma předtím, než dojde k výpadkům způsobeným přetečením fronty

8. Význam a charakteristika protokolů CDP/LLDP, využití, bezpečnostní rizika

CDP

- Charakteristika
  - Cisco proprietální L2 protokol, který slouží ke shromáždění informací o Cisco zařízeních, které sdílejí data na stejné lince (jsou propojené)
  - Je nazávislý na typu média (ethernet, wireless..) a běží na všech typech zařízení (routery, switche…)
- Funkce
  - V principu funguje tak, že zařízení posílá periodicky CDP advertisement připojeným zařízením (obsahuje info o jménu, typu a počtu rozhraní, typu zařízení)
- Využití
  - Slouží k mapování sítě (tvorba logické topologie když chybí dokumentace), troubleshootingum
  - Při rozhodování o designových změnách topologie a změnách zařízení

LLDP

- Charakteristika
  - L2 standardní protokol, který není omezený na Cisco zařízení
- Funkce
  - Stejná jako u CDP
- Využití
  - Stejné jako u CDP

Bezpečností rizika

- Útočník může zneužitím protokolu získat informace o síťovém rozvržení, verzích IOS systémů, IP adresách
- Z tohoto důvodu by nemělo CDP běžet globálně na všech rozhraních

9. Protokol NTP – význam, pojem stratum, možnosti uspořádání serverů, bezpečnostní rizika.

Význam

- Protokol zajišťující, že zařízení napříč sítí mají synchronizovaný čas a datum
- Zařízení komunikují s NTP serverem (veřejným nebo implementovaným na privátní síti)
- NTP používá UDP a port **123**
- Důležité z hlediska správy zařízení, bezpečnosti, řešení problémů a plánování
- Pokud by čas nebyl správný nebylo by možné určit pořadí událostí a příčiny událostí, které na zařízení nebo v síti nastaly

Stratum

- NTP sítě jsou hierarchické - > každá úroveň v hierarchii představuje **stratum**
- Úroveň stratumu je definována počtem hop countu od autoritativního zdroje
    - Stratum 0 = získává čas od zařízení jako atomické hodiny nebo GPS = zdroj nejpřesnějšího času
    - Stratum 1 = síťové zařízení připojená k autoritativním zdrojům času (stratum 0)
        - Jsou primárním síťovým standardem pro stratum 2 zařízení
    - Stratum 2 a níže = NTP klienti
- Čím nižší stratum tím spolehlivější čas
- Max stratum level je 15
- Level 16 znamená, že zařízení je nesynchronizováno

Možnosti uspořádání serverů

- **Hierarchické** = synchronizační servery na vrcholu a klienti dole
- **Peer-to-peer** = servery se vzájemně synchronizují a mají stejnou váhu
- **Hybridní uspořádání** = využívají se prvky obou předchozích uspořádání
- **Redundantní** = k dispozici více serverů a každý klient může synchronizovat čas od více serverů, což zvyšuje odolnost sítě proti výpadkům

Bezpečností rizika

- NTP aplifikační útok/ Reflekční útok
    - Útoky spočívají v posílání podvrženého požadavku na NTP server, který odpoví mnohem větší odpovědí na IP oběti => DoS útok
- Neautorizovaná manipulace času
    - Útočník může manipulovat nastavení času na cílových zařízeních => dopad na kritické systémy, kompromitace integrity dat
- Zneužití NTP serveru k monitorování trafficu, který prochází sítí

10. Protokol SNMP–základní operace, verze a rozdíly mezi nimi, hierarchie MIB-OID

Charakteristika

- Protokol na **aplikační vrstvě** umožňující administrátorům spravovat síťová zařízení
- Slouží k monitorování a správě síťového výkonu, řešení síťových problémů a k plánování růstu sítě

- Složení:
  - SNMP manager
  - SNMP agent (běží na spravovaném zařízení)
  - MIB (Management Information Base)

- SNMP manager
  - spouští SNMP management software
  - sbírá informace z SNMP agenta pomocí **get** akce a může měnit konfiguraci na agentovi pomocí **set** akce
  - Odesílá požadavky na MIB SNMP agentům na portu 161(UDP)

- SNMP agent
  - Odesílají na portu 162 (UDP) informace do manageru pomocí tzv. “Traps”
    - Trap = informace o nastalé události (ztráta spojení souseda, restart)

- MIB
  - Ukládá informace o zařízení a operační statistiky, dostupné autentifikovaných užiatelům
  - Za přistup k MIB je zodpovědný SNMP agent

- SNMP agent a MIB se nacházejí na klientských zařízeních

Základní operace

- Manažer má dva základní requesty: set a get
  - **get-request** = získá hodnotu z určité proměnné
  - **get-next-request** = získá hodnotu z proměnné v rámci tabulky; správce SNMP nemusí znát přesný název proměnné (sekvenční vyhledávání)
  - **get-bulk-request** = získává velké bloky dat, například více řádků v tabulce, které by jinak vyžadovaly přenos mnoha malých bloků dat
  - **get-response** = odpovídá na get-request, get-next-request a set-request odeslané systémem NMS
  - **set-request** = uloží hodnotu do určité proměnné
- Agent odpovídá pomocí:
  - **Get an MIB variable** = sáhne do MIB a zašle hodnotu manažerovi
  - **Set an MIB variable**

Verze a rozdíly

- SNMPv1
    - Protokol pro jednoduché správu sítě, dnes už zastaralý

- SNMPv2c
    - Používá rámec administrativy založený na komunitních řetězcích
    - Komunitní řetězec
        - autentifikační metoda pro přístup k MIB objektům
        - jedná se o heslo v plaintextu
        - dva typy (read only, read write -> práva vůči MIB)

- SNMPv3
    - Poskytuje bezpečný přístup k zařízením prostřednictvím autentizace a šifrování paketů v síti.
    - Zahrnuje tyto bezpečnostní funkce:
        - integritu
        - autentizaci, která ověří, že zpráva je z platného zdroje
        - šifrování

Porovnání

- v2c i v1 používají komunitní řetězce pro zabezpečení
- v2c narozdíl od v1 zahrnuje hromadného vyhledávání a podrobnější errory
- v1 a v2c jsou prakticky nebezpečné
- v3c poskytuje bezpečnostní modely a úrovně zabezpečení

Hierarchie MIB-OID

- MIB svoje proměnné organizuje hierarchicky
- Proměnné slouží k monitorování a kontrole nad síťovým zařízením
- Každá MIB proměnná je **object ID (OID)**, jednotlivé OID jednoznačně identifikují spravované objekty v MIB hierarchii
- Podle RFC MIB organizuje OID do hierarchie OIDs (strom)
- RFC definuje společné proměnné, které využívá většina zařízení + vendoři si tvoří své

11. Protokol syslog–historie, použití: facility/severity (priority)

Historie

- Vyvinut v 80. letech pro UNIX
- Poprvné zdokumentovaný v roce 2001 RFC 3164

Použití

- Standardizovaný protokol pro sběr, přenos a správu log záznamů o událostech v sítí nebo na zařízeních
- Používá port **514 (UDP)** k odeslání zpráv o události na sběrače zpráv
- Funkce:
    - Shromažďování logovacích informací pro monitorování a troubleshooting
    - Výběr typu zachycených logovacích informací
    - Schopnost specifikovat cíle zachycených syslogovských zpráv
- Složení:
    - Zařízení generující log záznamy (odesilatel)
    - Zařízení přijímající log záznamy (příjemce)
    - Syslog server = zodpovědný za příjem, ukládání a analýzu log záznamů

Severity/Facility

- Každá zpráva má danou úroveň závažnosti a facility určující zdroj

  Formát => %facility-severity-MNEMONIC: description

Severity

- Úrovně 0 - 7 dle kritičnosti (0 nejkritičtější)
    - Level 0 - 4 = emergency - warning (chybové zprávy od SW nebo HW)
    - Level 5 = notification (běžné, ale významné události - změna stavu rozhraní)
    - Level 6 = informational (běžné události, např při bootování)
    - Level 7 = debugging (zprávy generované debug příkazem)

Facility

- Identifikátory služeb, pro kategorizaci systémových stavových dat (hlášení chyb a událostí)
    - IF = zpráva generována rozhraním
    - IP
    - OSPF
    - SYS = operačním systémem
    - IPSEC

12. Seznam prefixů, distribuční seznamy, mapy cest

Seznam prefixů (prefix-list)

- Určují, které prefixy adres jsou povoleny nebo zakázány pro směrování dat v rámci sítě
- Každý záznam v prefix-listu obsahuje prefix IP adresy a akci, která se má na daný prefix aplikovat (permit nebo deny)
- Mají více fitrovacích možností než ACL (nastavení rozsahu adresního prostoru, který se bude filtrovat => operátor **ge** (greater) a **le** (lesser) na dané prefixy)

Distribuční seznamy (distribute-list)

- Metoda k filtrování prefixů sítí, které router pomocí **routovacího protokolu** odesílá
- Přístupové je možno aplikovat pouze na jedno rozhraní, pro případy aplikace na vícero rozhraní se hodí distribuční seznamy
- Filtrování může být inbound nebo outbound
- K samostatnému výběru prefixu může použít **ACL, Seznam prefixů** nebo **Mapy cest**

Mapy cest (route-map)

- Další metoda filtrování
- Jeho základem je buď ACL nebo prefix-list = umožňuje míchat více filtrovacích technik
- Používá k filtraci spoustu atributů (adresy, protokoly, délky prefixu) (na ty základní volá ACL)
- Funguje jako if-else-than
    - Pokud je splněna základní podmínka, tak je možné nastavit další akce, které se mají vykonat

13. Protokol BGP-4. Místo, účel, algoritmus.

Charakteristika

- Směrovací protokol pracující na základě vektoru vzdálenosti, který se používá v autonomních systémech (AS) pro směrování mezi různými síťovými doménami
- Je navržen tak, aby zajistil stabilitu směrování v celém internetu. Díky pečlivé kontrole směrovacích informací a algoritmům pro výběr cest minimalizuje BGP vznik smyček a oscilací směrování

Účel

- Klíčový protokol pro správu směrování na internetu. Používá se mezi ISP pro směrování mezi AS a také většími organizacemi, které provozují vlastní sítě.
- BGP umožňuje propojení a směrování mezi různými internetovými sítěmi, což zajišťuje efektivní a spolehlivé směrování provozu

Pojem autonomní systém (AS)

- Skupina sítí a směrovačů pod jednou administrativní doménou (společná správa a směrovací politika), ve které běží nějaký IGP (Interior Gateway Protocol) protokol
- Pro účely routování mezi různými AS slouží EGP (external gateway protocol) => BGP
- Číslo autonomního systému
    - 16 bitová hodnota, která je registrována (stejně jako veřejná IP)
    - Rozsah 1 - 64511 je globálně jedinečný
    - Rozsah 64512 - 65535 označuje privátní AS

Propojování AS

Single homed

- K jednomu ISP vede pouze jedna linka (3 možnosti linky = statická cesta / IGP / BGP)
- Výhody = cenově efektivní
- Nevýhody = chybí redundance => při výpadku ztráta spojení

Dual homed

- K jednomu ISP vedou dvě linky
- Možno zapojit všemi způsoby (1+1, 1+2, 2+1, 2+2) //počet routerů u zákazníka+ISP
- Výhody = vyšší redundance linek

Single multihomed

- Ke dvou a více nezávislým ISP vede pouze jedna linka
- Výhody = pro různé sítě použit bližší ISP, škálovatelnost, redundance poskytovatelů
- Nevýhody = potřeba dynamického směrování, chybí redundance

Dual Multihomed

- Způsob zapojení, kdy klient je připojený ke dvoum a více nezávislým ISP více linkami

Atributy– dělení, příklady atributů (AS_PATH, NEXT_HOP, LOCAL_PREFERENCE, WEIGHT, MED, ORIGIN)

- Slouží k tomu, ale podle nich BGP vybralo nejlepší cestu do cílové sítě
- Nejde o to, aby vybral nejkratší cestu jako u IGP, ale o nejideálnější kontrolu provozu

Dělení:

- **Well-known mandatory** = každá implementace BGP jim musí rozumět, připojení k cestě je povinné
- **Well-known discretionary** = každá implementace BGP jim musí rozumět, připojení k cestě není povinné
- **Optional transitive** = ne každá implementace BGP jim musí rozumět. V případě, že jim nerozumí, předává se atribut dále beze změny
- **Optional nontransitive** = ne každá implementace BGP jim musí rozumět. V případě, že jim nerozumí, atribut se dále nepředává

AS_PATH (Well Known Mandatory)

- Základ funkce algoritmu path-vector
- BGP volí cestu s nejkratší hodnotou AS_PATH
- Obsahuje postupně řetězec čísel AS, přes které vede cesta k cílové síti
- Na začátek AS_PATH přidávají AS své číslo
- Pokud se cesta dostane do AS, jehož číslo je již v AS_PATH uvedeno, cesta se ignoruje. Tímto způsobem se odstraňují **cesty obsahující smyčku**

NEXT_HOP (Well Known Mandatory)

- Když BGP směrovač obdrží aktualizaci od sousedního směrovače, prozkoumá atribut "next hop", aby určil nejlepší cestu pro přeposílání provozu.
- Určuje IP adresu dalšího směrovače, který by měl být použit k dosažení cílové sítě, která je v aktualizaci propagována
- Provádí rozhodování o nejlepší cestě na základě IP adresy Next hopu

LOCAL_PREFERENCE (Well Known Discretionary)

- Je použita uvnitř (multihomed) AS ke společné volbě cesty k vnější síti, která je dostupná přes více linek
- Vyměňuje se v rámci iBGP rout, avšak ne mimo hranice AS
- Zvolí se ta cesta s **nejvyšší** local preference hodnotou
- Výchozí hodnota je 100

WEIGHT (Well Known Mandatory)

- Volba cesty s **největší** váhou (podobné jako LOCAL_PREFERENCE, ale platí pouze pro router, nikoli pro AS)
- První BGP atribut na seznamu
- Cisco proprietary, ostatní vendoři nepoužívají
- Hodnota je lokální pro router (tuto informaci si routery nevyměnují)
- Výchozí hodnota je 0 pro všechny routy, které nepocházejí z lokálního routeru

MED (Optional Non Transitive)

- Používá se pro ovlivnění volby cesty sousedního AS pro dosažení jednotlivých sítí uvnitř našeho AS
- Preferuje se cesta s **nejnižší** hodnotou MED
- Vyměňuje se mezi AS

ORIGIN (Well Known Mandatory)

- Říká, odkud se informace o cestě vzala. Volí se **nejnižší** hodnota
    - IGP = cesta pochází z interního směrovacího protokolu; nejlepší
    - EGP = cesta získáná redistribucí z dnes už nepoužívaného protokolu EGP
    - INCOMPLETE = původ cesty není znám

Pořadí vyhodnocování atributů
1. Největší WEIGHT
2. Největší LOCAL_PREFERENCE
3. Self_Originate cesta (generováno směrovačem) = redistribuce např. z IGP
4. Nejkratší AS_PATH
5. Nejpreferovanější ORIGIN
6. Nejnižší MED
7. Cesty získané z eBGP preferovány před iBGP
8. Next-hop dostupný před kratší cestu vnitřkem AS
9. Nejnižší identifikátor ROUTER_ID (pokud není nakonfigurováno je to nejvyšší hodnota IP na některém z rozhraní routeru)

Základní konfigurace BGP, externí/interní BGP, volba cesty-„prepend“

1) Vytvoření BGP procesu pomocí **router bgp “**číslo AS**”**
2) Nastavení sousedního routeru **neighbor x.x.x.x remote-as** “číslo AS”
3) Nastavení update-source **neighbor x.x.x.x update-source** “interface”
4) Nastavení propagované sítě **network x.x.x.x**

iBGP = BGP v rámci jednoho AS, na obou roterech shodná AS

eBGP = BGP směruje mezi dvěma různými AS, AS na routerech jsou konfigurovány inverzně, je třeba propagovat sítě ven z AS pomocí 4)

Volba cesty - “prepend”
-slouží k umělému prodloužení AS_PATH -> set as-path prepend čísloAS
-opakovaným vložením čísla vlastního AS do AS_PATH se hodnota atributu zvětší => zhorší

Využití map cest při směrování v prostředí protokolu BGP

- Při směrování v prostředí protokolu BGP se využívají mapy cest (route maps) k manipulaci s cestami, které jsou vybrány a odeslány mezi BGP routery
- Mapy cest poskytují možnost aplikovat různé pravidla a transformace na směrovací informace, které BGP přijímá od sousedních routerů.
    - Filtrace tras = odmítnutí tras z určitých zdrojových AS nebo k povolení pouze tras splňujících určité podmínky
    - Transformace cest = změnit atributy cest, jako je například délka AS cesty (AS path length), váha (weight) nebo preference (local preference). Tím lze ovlivnit rozhodování BGP o výběru nejlepší cesty
    - Manipulace s komunitami = BGP komunity jsou štítky, které jsou připojeny k trasám a slouží k řízení směrování

14. Využití protokolu BGP (bezpečnost) – RTBH, uRPF.

RTBH (Remotely-Triggered Black Hole)

- Bezpečnostní nástroj pro sítě ISP který umožňuje rychlé a účinné zablokování provozu směřujícího do určitého cíle = obranný mechanismus proti (D)DoS
- Servery, který jsou pod útokem v první fázi obětujeme, pro ochranu infrastruktury
- Následně se zjistí IP adresa oběti útoku a vytvoří se statický směrovací záznam, který odvádí provoz od cíle útoku do zařízení Null0 (černá díra, fiktivní cílová adresa)
- BGP4 tuto cestu distribuje všem hraničním směrovačům

uRPF (unicast Reverse Path Forwarding)

- Bezpečnostní mechanismus, který zabraňuje spoofingovým útokům
- Provádí kontrolu zda příchozí paket má zdrojovou IP adresu v routovací tabulce, pokud ne paket zahodí
- Módy:
    - **Strict** = kontroluje shodu IP adresy v routovací tabulce a interface, ze kterého se o této source IP dozvěděl (musí se shodovát s interfacem, který je k této IP přiřazený v tabulce)
    - **Loose** = kontroluje pouze shodu IP adresy v routovací tabulce

15. Protokol MPLS. Charakteristika, L2/L3 MPLS.

Charakteristika

- Vysoce výkonná technologie směrování WAN
- Používá se na 2. nebo 3. vrstvě k vytvoření zabezpečených kanálů mezi lokalitami
- **Multi protocol** = kromě IP protokolu mohou být v rámci tunelu přeneseny i protokoly IPv6, Ethernet, PPP…
- **Label swapping** = směrování se provádí na základě “labelu” namísto vyhledání informace o cílové destinaci v routovací tabulce => snižuje se forwardovací zátěž na páteřních směrovačích
- Směrovač MPLS může být směrovač na customer edge (CE), směrovač na provider edge (PE) nebo interní směrovač providera (P)
- MPLS header se přidává mezi L2 a L3 hlavičku, proto se mu říká “2.5 layer protocol”

L2/L3 MPLS

L2

Atom

- Přenos framů (PPP,HDLC, Ethernet...) přes MPLS protokol
- Umožňuje propojit sítě, které běží na různých L2 technologiích

L3

MPLS Traffic Engineering

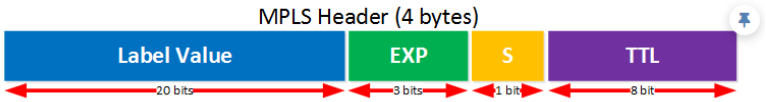
- Poskytuje speciální směrování IP provozu = optimalizace routování (vyvažování zátěže, redukce případů zahlcení)
- Automaticky kontroluje šířku pásma, QoS, poskytuje fault recovery

MPLS L3VPN

- Umožňuje rozšířit privátní sítě napříč různými geografickým oblastmi (vypadají jako by byli v jedné síti)
- Zabezpečení a izolace komunikace přes sdílenou infrastrukturu ISP

Formát labelu

- 4 byte identifikátor, který se používá pro rozhodování při dalším forwardování paketů, tím že definuje cíl a služby pro paket



- Hodnota labelu = 20 bitů, číselná hodnota labelu
- EXP = 3 bity, experimentální bity, používají se pro QoS
- S = 1 bit, příznak konce stacku, když je hodnota 1 , tak tato MPLS hlavička je poslední, pokud 0 následuje ještě více MPLS hlaviček
- TTL = 8 bitů, životnost paketu

- Paket může mít několik značek, které jsou umístěny na zásobníku - label na vrcholu je používána pro přenos paketu v MPLS síti

Možné operace routeru

- Label push = přidání labelu do paketu
- Label swap = záměny hodnota labelu
- Label pop = odstranění labelu z paketu

Účel protokolu LDP (Label Distribution Protocol)

- Protokol používaný v MPLS sítí jehož hlavním účelem je distribuce a výměna labelů mezi MPLS směrovači, aby bylo možné provádět rychlé a efektivní směrování síťového provozu
  - **Distribuce labelů** = umožňuje směrovačům distribuci a výměnu labelů pro síťové prefixy (IP adresy) a vytvořit tak MPLS popisky pro jednotlivé směrovací záznamy
  - **Rychlé přepínání na základě labelů** = Každý směrovač si udržuje tabulku labelů, která určuje, jakým směrem a přes které rozhraní pakety s určitým labelem přeposílat
  - **Podpora MPLS služeb** = podporuje různé MPLS služby, jako je L2VPN, L3VPN a Traffic Engineering (TE)

16. Protokol VRF–účel, charakteristika, varianty–VRF Lite.

Účel

- Mechanismus pro izolaci a segmentaci provozů různých zákazníků v síti (zlepšení bezpečnosti)
- Umožňuje lépe optimalizovat routovací resourcy, zlepšuje škálovatelnost sítě
- Obvykle se používá ve spojení s MPLS, ale může pracovat samostatně (VRF Lite)
- VRF funguje jako “VLAN pro routery” (vytvoření virtuálních sití na 3. vrstvě) => místo jedné globální routovací tabulky používá více virtuálních, vždy jedna pro každý interface
- Každá taková virtuální síť dopravuje pakety po svém, může používat jiný směrovací protokol apod. - to vše na společné fyzické/linkové infrastruktuře

VRF lite

- VRF bez použití MPLS, MP-BGP
- Používá se v menších sítích
- Každé směrované rozhraní (fyzické nebo virtuální) patří právě do jedné VRF instance
- Bez použití importních a exportních map nelze cesty (a pakety) přesunout z jedné instance do druhé

17. Návrh sítě–vrstvená struktura: přístupová, distribuční a páteřní vrstva, jejich účel.

Vrstvená struktura

- Model rozdělující síť na jednotlivé vrstvy plnící specifické funkce a úkoly
- Umožňuje lepší správu sítě, zvýšenou bezpečnost, snadnější rozšiřitelnost a efektivní směrování provozu v síti
- Principy
    - Hierarchie = každé zařízení na vrstvě má svou roli
    - Modularita = jednoduché rozšiřování sítě a integrování služeb
    - Flexibilita = škálovatelnost sítě
    - Bezpečnost

Přístupová vrstva

- Reprezentována zařízeními na okraji sítě (koncová zařízení) která se připojují k L2 switchům a access pointům
- Primární funkce je poskytnutí uživateli přístup k síti, PoE, zabezpečení DHCP, ARP
- Vyžaduje hodně rozhraní na připojení uživatelů

Distribuční vrstva

- Propojuje přístupovou a páteřní vrstvu
- Zajišťuje routování a řízení toku provozu
- Zajišťuje redundantní linky pro případy selhání
- Provozuje QoS, ACL a VLANy

Páteřní vrstva

- Agregátor všech zařízení na distribuční vrstvě a propojuje je s jinými sítěmi
- Poskytuje odolnost proti chybám, rychlost přenosu dat mezi různými distribučními vrstvami a konektivitu k externím sítím
- Skládá se z rychlých routerů a switchů dimenzovaných pro přenos velkého množství dat a minimalizaci zpoždění

Dva typy vrstvené struktury:

- 3 vrstvý model = obsahuje přístupovou, distribuční a páteřní vrstvu
- 2 vrstvý model = obsahuje přístupovou a sloučenou distribuční a páteřní vrstvu

18. Virtualizace serverů, hypervisor typu 1 a 2, HAL. Virtualizace v sítích, softwarově definované sítě (SDN), porovnání s tradiční architekturou.

Virtualizace serverů

- Využívá nevyužitých prostředků a konsoliduje řadu fyzických serverů
- Umožňuje běh více OS na jednom HW
- Zahrnuje redundanci (ochrana proti jednomu bodu selhání) = když hypervisor selže, VM se může znovu spustit na jiném hypervisoru
- Jedna VM může běžet souběžně na dvou hypervisorech (kopírování využité RAM a CPU mezi nimi)

Výhody virtualizace

- Snížení celkových nákladů (méně fyzických serverů/síťových zařízení, menší spotřeba energie, nižší náklady na údržbu)
- Snížení nároku na velikost datacenter
- Snadné a flexibilní poskytování virtuálních serverů
- Vyšší odolnost proti chybám (live migrace VM, migrace úložiště…)
- Jednodušší prototypování a testování sítí (jednoduchy rollback, když dojde k chybě)

Hypervisor

- Program, firmware nebo HW, který přidává abstrakční vrstvu nad HW
- Abstrakční vrstva je použita k vytvoření VM, které mají přístup HW zdrojům serveru

Typ 1 (bare metal)

- Hypervizor je instalován přímo na hardware (přímý přístup k HW prostředkům)
- Používají se na podnikových serverech a zařízeních pro datová centra
- Jsou efektivnější (zlepšují škálovatelnost, výkon a robustnost)

Typ 2

- Software, který vytváří a spouští instance virtuálních strojů (VM)
- Host = počítač, na kterém hypervizor podporuje jednoho nebo více VM
- Výhodou je absence potřeby management console a cena (většinou free)

HAL

- SW vrstva mezi OS a HW počítače nebo zařízení
- Slouží k poskytování standardizovaného rozhraní mezi OS a konkrétním HW, což umožňuje operačnímu systému komunikovat s HW bez ohledu na jeho konkrétní implementaci
- HAL poskytuje abstrakci hardwaru, což znamená, že operační systém může pracovat s různými typy hardwaru pomocí stejného rozhraní poskytovaného HAL
- Usnadnění portability OS na různá zařízení a umožňuje snadnou výměnu nebo rozšiřování HW bez potřeby úprav OS

Virtualizace v sítích

- Software-Defined Networking (SDN)
    - Síťová architektura, která virtualizuje síť a nabízí nový přístup k správě a řízení sítě, který usiluje o zjednodušení a zefektivnění správního procesu.
- Cisco Application Centric Infrastructure (ACI)
    - Hardwarové řešení speciálně navržené pro integraci cloudového počítání a správu datových center.

SDN

- Správa řadiče síťového zařízení je přesunuta do centralizovaného SDN řadiče
- Řadič SDN je logický prvek, který umožňuje síťovým správcům spravovat a řídit, jak by měly přepínače a směrovače zpracovávat síťový provoz
- Řadič orchestruje, mediuje a usnadňuje komunikaci mezi aplikacemi a síťovými prvky

- Speciální rozhraní
    - Northbound Interface
        - Rozhraní pro přístup a správu SDN řadiče (pomcí GUI, skriptů..)
    - Southbound Interface
        - Rozhraní (REST API) pro komunikaci mezi síťovým zařízením a SDN řadičem
- Komponenty
    - OpenFlow
        - správce provozu mezi zařízeními a řadičem
    - OpenStack
        - nástroj virtualizace a orchestrace pro automatizaci sítě, používá se spolu s Cisco ACI
    - THRILL, I2RS, SPB, Cisco FabricPath

19. Protokol NetFlow, účel, historie, verze.

Účel

-Síťový protokol od Cisca sloužící k monitorování sběru a analýze dat o provozu v síti
-Jeho hlavním účelem je poskytovat podrobné statistiky a informace o síťovém provozu
-Využívají se pro:

- analýzu síťového chování
- plánování kapacity
- správu bezpečnosti
- diagnostiku síťových problémů

-Implementuje se pomocí 3 komponent

- Flow exporter = exportuje záznamy do jednoho nebo více collectorů
- Flow collector = přijímá, ukládá a předběžné zpracovává data přijatá od exportéru
- Analysis application = analyzuje přijatá data

Historie

-Poprvé představen v roce 1996 jako součást Cisco IOS pro směrovače.
-Od té doby se stal široce používaným standardem v oblasti sběru datového provozu v sítích.

Verze

-**v1** (již zastaralá) poskytovala základní informace o přenosu paketů, jako jsou zdrojové a cílové IP adresy, porty a délka paketů
-**v5** nejrozšířenější verze, ale pouze pro IPv4, přinesla podporu pro sběr statistik o paketech
-**v9 a IPFIX** (IP Flow Information Export) přinesly další pokročilé funkce, včetně podpory pro export provozu do externích nástrojů. Nejpoužívanější pro IPv6, MPLS, a IPv4 BGP.

20. Správa zařízení Cisco

Uživatelské účty, úroveň privilegií

Vytvoření uživatelského účtu

- **username <jméno> password <heslo>** = účet se jménem a heslem
- **username <jméno> privilege <úroveň>** = učet se jménem a privilegiemi

Nastavení úrovně privilegií

- **privilege exec level <úroveň> <příkaz>** = úroveň privilegií pro určitý příkaz
- **enable secret <heslo>** = tajné heslo pro přechod do priv. módu (úroveň 15)

Nastavení privilegovaného módu (enable) pro uživatele

- **line vty 0 15** = nastavení vzdáleného přístupu.
- **privilege level <úroveň> <příkaz>** = úroveň privilegií pro vzdálený přístup.

Nastavení výchozí úrovně privilegií

- **privilege exec default level <úroveň>** = výchozí úroveň privilegií pro nové účty

Nastavení view (pohledů) pro omezení přístupu

- **parser view <název>** = vytvoření nového pohledu (view).
- **commands <název> include <příkaz>** = přidání povoleného příkazu do pohledu.
- **username <jméno> view <název>** = přiřazení pohledu uživatelskému účtu

Nastavení hesel–možnosti jejich ukládání. Hesla pro zabezpečení konsoly, vzdáleného přístupu, přechodu do privilegovaného módu.

Nastavení hesla pro zabezpečení konzole

- **line console 0** = nastavení konzole
- **password <heslo>**
- **login**
- **exit**

Nastavení hesla pro vzdálený přístup (SSH nebo Telnet)

- **line vty 0 15** = nastavení vzdáleného přístupu.
- **password <heslo>**
- **login**
- **exit**

Nastavení hesla pro přechod do privilegovaného módu (enable)

- **enable secret <heslo>** = šifrované heslo
- **enable password <heslo>** = plaintext heslo
- **enable password level <číslo> <heslo>** = nastavení hesla a určité úrovně oprávnění

Konfigurace protokolu SSH (jednotlivé kroky)

Generování klíčového páru pro SSH

- **crypto key generate rsa** = vygeneruje pár RSA klíčů pro SSH komunikaci

Aktivace SSH na zařízení

- **ip ssh version 2** = nastaví verzi SSH
- **ip ssh time-out <časový limit>** = časový limit pro připojení SSH
- **ip ssh authentication-retries <počet pokusů>** = počet pokusů o autentizaci při SSH připojení.
- **line vty 0 15** = nastavení vzdáleného přístupu
- **transport input ssh** = povolí pouze SSH jako povolený vstupní protokol.
- **login local** = použití lokální databáze uživatelů pro přihlašování

Nastavení uživatelských účtů pro SSH

- **username <jméno> secret <heslo>**: Vytvoří uživatelský účet s heslem pro SSH přístup.
- **username <jméno> privilege <úroveň>** = privilegia pro uživatelský účet

Ověření SSH konfigurace

- **show ip ssh**

Zálohování a obnova operačního systému a konfiguračních souborů

Zálohování konfigurace

- **copy running-config <název_souboru>** = zkopíruje běžící konfiguraci do souboru
- **copy startup-config <název_souboru>** = zkopíruje konfiguraci uloženou v paměti do souboru (startup-config)

Obnova konfigurace

- **copy <název_souboru> startup-config** = nahraje konfiguraci ze souboru do paměti (startup-config) zařízení
- **copy <název_souboru> running-config** = nahraje konfiguraci ze souboru přímo do běžící konfigurace

Zálohování operačního systému (image)

- **copy flash:<název_souboru> tftp://<adresa_TFTP_serveru>/<název_cílového_souboru>** = zkopíruje OS (image) z flash paměti na TFTP server pro zálohování
- **copy flash:<název_souboru> usbflash0:<název_cílového_souboru>** zkopíruje OS (image) z flash paměti na USB flash disk

Obnova operačního systému (image)

- **copy tftp://<adresa_TFTP_serveru>/<název_souboru> flash:<název_cílového_souboru>** = nahraje OS (image) z TFTP serveru do flash paměti zařízení
- **copy usbflash0:<název_souboru> flash:<název_cílového_souboru>** = nahraje OS (image) z USB flash disku do flash paměti zařízení

Protokol TFTP (Trivial FTP)

- Odlehčená verze FTP protokolu, obsahuje jen základní funkce
- Používá se pro přenos souborů v případech, kdy je běžné FTP nevhodné pro sovu komplikovanost (zálohování konfiguračních souborů, bootování bezdiskových PC)

Obnova neznámého hesla u směrovačů a přepínačů–podstata, jednotlivé kroky.

Podstata:

-Obnova přes **sériovou konzoli** pomocí **fyzického přístupu** k zařízení
-Proces obnovy hesla může být různý v závislosti na konkrétním modelu a verzi operačního systému zařízení Cisco => pročíst dokumentaci k danému modelu

Jednotlivé kroky:

1. **Přechod do ROMMON módu**
   -Po připojení konzole k zařízení lze během bootování přejít do ROMMON módu pomocí break sekvence (Ctrl+Break). ROMMON mód se značí rommon 1>
2. **Změna konfiguračního registru a reset**
   -ROMMON obsahuje pár základních příkazů, zejména confreg. Pomocí confreg 0x2142 nastavíme konfigurační registr tak, aby ignoroval startup-config. Poté reset zařízení.
3. **Zkopírování startup-config do running-config**
   -Pomocí copy startup-config running-config zkopírujeme startup do running, abychom zachovali konfiguraci zařízení a přešli do privilegovaného módu.
4. **Změna hesla**
   -Jelikož jsme v privileged EXEC módu, můžeme jít do globálního konfiguračního módu a zde pomocí enable secret <heslo> změnit zapomenuté heslo.
5. **Uložení running-config do startup-config**
   -Pomocí copy running-config startup-config uložíme aktuální heslo a platnou konfiguraci.
6. **Změna konfiguračního registru**
   -Pomocí config-register 0x2102 změníme konfigurační registr aby nahrával startup config.
7. **Restart zařízení**
   -Pomocí reload restartujeme zařízení pro dokončení změn.