VLANy a směrování mezi VLANy

VLANy

VLANy jsou založeny na logických a nikoliv na fyzických připojeních. Mohou segmentovat sítě podle funkce, kategorie pracovníků nebo aplikace. Každá VLAN je považována za samostatnou logickou síť. Pro podporu VoIP je vyžadována samostatná hlasová VLAN. Přístupový port může patřit pouze k jedné datové VLAN, ale může mít také Voice VLAN. Konfigurace VLAN s normálním rozsahem jsou uloženy v souboru vlan.dat ve flash paměti. VLANy jsou identifikovány číslem, při nezadání jména ho doplní systém.

Trunk

Trunk je spojení vrstvy 2 typu point-to-point mezi dvěma přepínači, které přenáší provoz pro všechny VLANy. Pole VLAN tag zahrnuje čtyři pole: typ sítě (dnes jen Ethernet), prioritu uživatele, jeden bit DEI (Drop Eligible Indicator, indikátor vyhození, dříve CFI – Canonical Format Indicator) a VLAN ID. Trunky budou potřebovat označení (tagging) pro různé VLANy, obvykle 802.1Q. Značení (tagging) IEEE 802.1Q umožňuje jednu nativní VLAN, která zůstane neoznačená. Rozhraní lze nastavit na trunking nebo nontrunking (access).

Vyjednávání o trunku

Trunk negotiation (vyjednávání) je řízeno protokolem Dynamic Trunking Protocol (DTP). DTP je proprietární protokol společnosti Cisco, který spravuje vyjednávání o nastavení trunku. Defaultně je dynamic auto a pak buď na obě strany nastavujeme trunk anebo stačí na jednen dát dynamic desirable. Příkazem switchport nonegotiate lze trunking stopnout.

VLAN hopping attack

Útok VLAN hopping attack umožňuje, aby rámce z jedné VLAN procházely do jiné VLAN, aniž by nejprve procházely routerem. Útočník by mohl použít útok VLAN hopping k „čichání“ provozu na jiné VLAN, od které má být počítač útočníka izolován. Na druhé straně může útočník také odeslat provoz do sítě VLAN, na kterou by počítač útočníka neměl být schopen dosáhnout. Dva hlavní způsoby provedení útoku VLAN hopping jsou switch spoofing a Double tagging.

Chcete-li zabránit útoku VLAN hopping, můžete deaktivovat trunkování na všech portech (díme mode access), které nepotřebují vytvářet trunky, a deaktivovat (nonegotiate) DTP na portech, které musí být trunky.

```
Switch1(config)# interface gigabitethernet 0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# exit
Switch1(config)# interface gigabitethernet 0/4
Switch1(config-if)# switchport trunk encapsulation dot1q
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switch port nonegotiate
```

Abyste zabránili útoku přeskakování VLAN pomocí doubletaggingu, nepoužívejte k odesílání provozu uživatelů nativní VLAN. Můžete to udělat vytvořením VLAN, která nemá přidané žádné porty. Tato nepoužívaná VLAN je pouze pro nativní přiřazení VLAN.

```
Switch1(config)# interface gigabitethernet 0/4
Switch1(config-if)# switchport trunk native vlan 400
```

Směrování mezi VLANy

Směrování mezi VLANy je proces předávání síťového provozu z jedné VLAN do jiné VLAN.Tři možnosti zahrnují starší verzi, router-on-a-stick a přepínač L3 pomocí SVI.

Chcete-li nakonfigurovat přepínač s VLAN a trunkovou sítí, proveďte následující kroky: vytvořte a pojmenujte VLANy, vytvořte rozhraní pro management, nakonfigurujte přístupové porty a nakonfigurujte porty trunkové sítě.

Metoda router-on-a-stick vyžaduje, aby bylo pro každou směrovanou VLAN vytvořeno subinterface. Aby mohlo dojít ke směrování, musí být každému podřízenému rozhraní směrovače přiřazena adresa IP v jedinečné podsíti. Po vytvoření všech podrozhraní musí být fyzické rozhraní povoleno pomocí konfiguračního příkazu bez vypnutí rozhraní.

Enterprise Campus LAN používají **přepínače vrstvy 3** k zajištění směrování mezi VLAN. Přepínače L3 využívají hardwarové přepínání k dosažení vyšší rychlosti zpracování paketů než směrovače.

Schopnosti přepínače vrstvy 3 zahrnují směrování z jedné VLAN do druhé pomocí více přepínaných virtuálních rozhraní (SVI) a převod switchportu vrstvy 2 na rozhraní vrstvy 3 (tj. směrovaný port).

Chcete-li nakonfigurovat přepínač s VLANy a trunkovou sítí, proveďte následující kroky: vytvořte VLANy, vytvořte rozhraní SVI VLAN, nakonfigurujte přístupové porty a povolte směrování IP.

Chcete-li povolit směrování na přepínači L3, je třeba nakonfigurovat routed (směrovaný) port. Směrovaný port je vytvořen na přepínači vrstvy 3 deaktivací funkce switchport na portu vrstvy 2, který je připojen k jinému zařízení vrstvy 3.

Chcete-li nakonfigurovat přepínač vrstvy 3 na směrování pomocí směrovače, postupujte takto: nakonfigurujte směrovaný port, povolte směrování, nakonfigurujte směrování, ověřte směrování a ověřte připojení.

Existuje celá řada důvodů, proč konfigurace mezi VLAN nemusí fungovat. Všechny souvisejí s problémy s připojením, jako jsou chybějící VLAN, problémy s trunkovým portem přepínače, problémy s přístupovým portem přepínače a problémy s konfigurací routeru.

VLAN může chybět, pokud nebyla vytvořena, byla omylem odstraněna nebo není na trunku povolena. Dalším problémem směrování mezi VLAN jsou nesprávně nakonfigurované porty přepínačů.