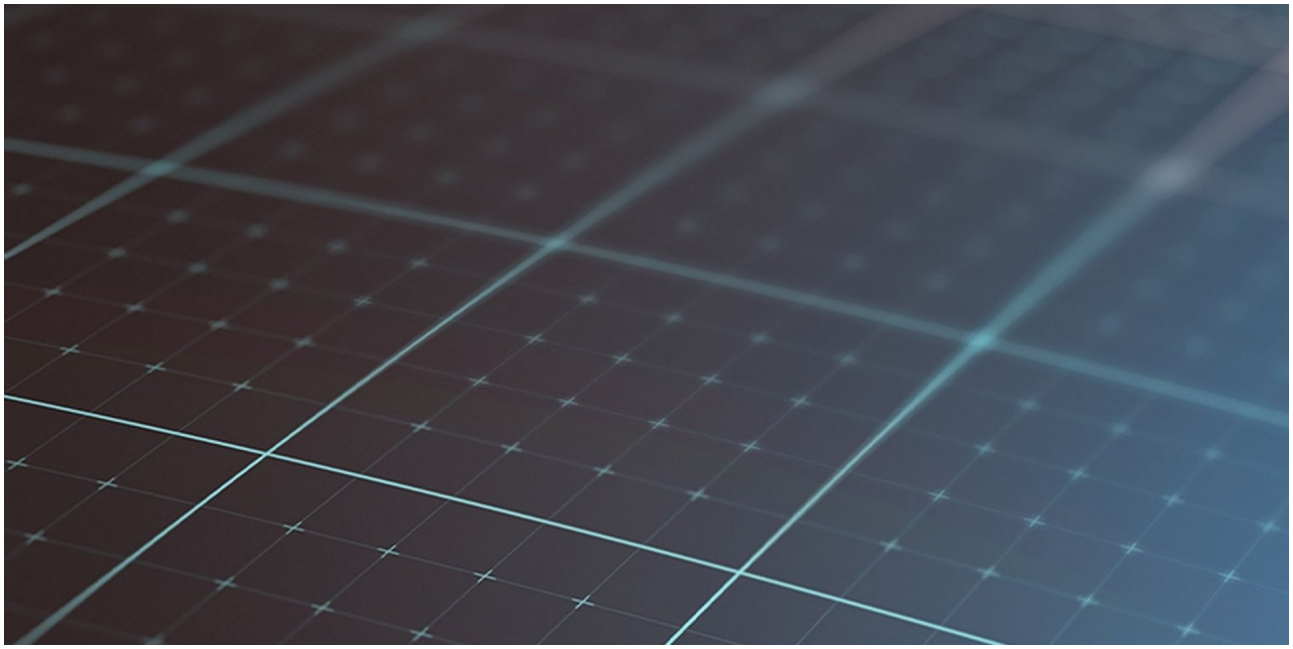


Produkt miesiąca: Extreme Fabric Connect

2021-06-09

Tradycyjny model sieci działa… Każdy, kto choć trochę siedzi w naszej branży, to potwierdzi. Zanim więc zaczniemy wyjaśniać czym Fabric Connect jest i jak działa, nasuwa się naturalne pytanie: „ale gdzie właściwie leży problem?”. Zagłębmy się na moment w rzeczywistość, w której ścinanie zakrętów wcale nie jest taką złą rzeczą!

Klasyczny, tranzytowy model dostarczania zasobów sprawdza się OK, aczkolwiek jest jedno małe „ale”. W przypadku tradycyjnych sieci proces ten staje się coraz bardziej skomplikowany z każdym kolejnym switchem czy dostarczaną usługą. Po prostu nie da się tego w żaden sposób przeskoczyć.

Za każdym razem, gdy następuje jakaś zmiana, każdy switch znajdujący się na potencjalnej ścieżce ruchu sieciowego wymaga zapewnienia środków realizacji usług – np. w sytuacji gdy dodajemy kolejne switche czy uruchamiamy dodatkowe usługi. Logicznym jest więc, że wraz z liczbą switchy i usług rośnie złożoność konfiguracji każdego przełącznika w systemie. Mówimy tu o liczbie usług do potęgi n, gdzie n odpowiada liczbie switchy…

Jakby tego było jeszcze mało, tradycyjne sieci są dość podatne na ludzki błąd podczas dostarczania zasobów. W najlepszym przypadku część lub cała sieć ulegnie awarii. W najgorszym – problem wychwyci haker, który wykorzysta błąd w konfiguracji, aby wykorzystać zasoby znajdujące się w sieci.

Aby rozwiązać ten problem, potrzebne było całkowicie nowe spojrzenie na to, jak budowana jest sieć. Konkretnie rzecz ujmując niezbędne stało się oddzielenie routingu (czyli tego jak dane dostają się z punktu A do punktu B) od usług (czyli routingu w sieci logicznej w celu spełnienia konkretnych potrzeb biznesowych). Przykładowo, routing określa nam, jak dane transportowane są od jednego biura do setek oddziałów firmy na całym świecie. Przez usługi rozumieć będziemy takie elementy, jak sieć monitoringu, która zapewnia wszystkim kamerom dostęp do serwera centralnego.

Kiedy firma otwiera nowe biuro, aktualizacji wymagać powinien jedynie routing. Dodając nową usługę lub modyfikując już istniejącą, jedyne co powinieneś wykonać to zdefiniowanie usługi na brzegu sieci. Tak to powinno wyglądać. To oddzielenie stanowi esencję przewagi, jaką Fabric Connect ma nad tradycyjnym, tranzytowym modelem dostarczania zasobów.

Rozwiązanie Extreme Fabric Connect oparte jest na standardowym protokole IEEE 802.1aq lub inaczej SPBm, czyli „Shortest Path Bridging” – technologii umożliwiającej konfigurację urządzeń sieciowych w sposób zapobiegający powstawaniu pętli. Standard ten określa dwie odrębne role dla switchy (lub „mostków”, czyli „bridges”, jak to IEEE lubi je określać): szkieletowe switche dla rdzenia sieci (Backbone Core Bridge, w skrócie BCB) które pełnią funkcję routingu, a także szkieletowe switche dla brzegu sieci (Backbone Edge Bridge, w skrócie BEB), które odpowiadają z kolei zarówno za routing, jak i usługi.

Przejdźmy dalej i zobaczmy, jak to wszystko działa w praktyce…

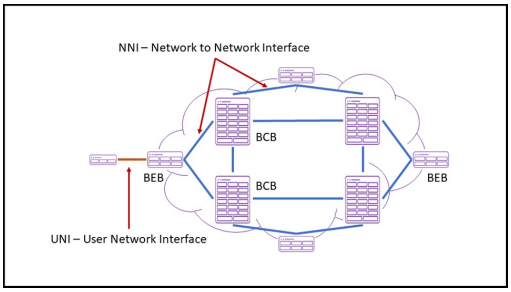
Backbone Core Bridge

Jak już wspomnieliśmy, BCB odpowiada jedynie za routing. Jego zadaniem (podobnie jak innych switchy BCB w sieci typu fabric) jest upewnienie się, że ruch pomiędzy usługami kierowany jest w sposób najbardziej efektywny. Jakby nie patrzeć, nazwa „shortest-path” (ang. najkrótsza droga) nie bierze się z niczego.

W przeciwieństwie do tradycyjnych modeli sieci, Fabric Connect nie próbuje określać ścieżek wewnątrz sieci na chybił-trafił (na przykład w oparciu o takie protokoły jak Spanning Tree). Właśnie ta autodeterminacyjna natura tradycyjnych sieci stanowi powód, dla którego takie hasła jak „zapętlenie sieci” spędzają sen z powiek wielu inżynierów.

Zamiast tego, Fabric Connect wykorzystuje oparty na otwartych standardach IS-IS protokół trasowania stanu łącza, czyli “Intermediate System to Intermediate System”. Zasadniczo mechanizm ten umożliwia grupom fizycznie połączonych węzłów SPBm (np. switchom BCB) komunikację pomiędzy sobą – po to, aby określić najlepszą możliwą ścieżkę do przesłania danych poprzez sieć. Jest to rozwiązanie nie tylko zautomatyzowane, ale też samonaprawiające się. Jeśli któryś BCB natknie się na jakiś problem, pozostałe switche BCB po prostu pominą go przy trasowaniu, tak aby zachować ciągłość działania sieci. Więcej połączeń pomiędzy switchami BCB jest więc czymś pozytywnym, a nie kolejną „tykającą bombą” w postaci pętli, jak to się ma w przypadku tradycyjnych sieci.

Mówiąc prostym językiem, każdy BCB „wie” o bezpośrednich połączeniach, jakie ma z pozostałymi switchami BCB. Połączenia te nazywamy „Network to Network Interfaces”, lub w skrócie NNI. Warto podkreślić, że każdy BCB konfigurowany jest wyłącznie z bezpośrednio połączonym NNI. Takie rozwiązanie zapobiega komplikowaniu konfiguracji za każdym razem, kiedy dodajemy nowy BCB. Każdy kolejny switch BCB wpływa na konfigurację jedynie swoich bezpośrednich „sąsiadów”. Nowy BCB „uczy się” pozostałych switchy rdzeniowych poprzez IS-IS.



Download image

Z każdym dodatkowym switchem BCB i z każdym kolejnym NNI, sieć Fabric Connect rośnie, ale co najważniejsze – staje się coraz bardziej odporna na awarie. Sieci typu fabric są co prawda w stanie obsłużyć te same topologie, co sieci tradycyjne, aczkolwiek w ich przypadku topologia tak czy inaczej schodzi na drugi plan.

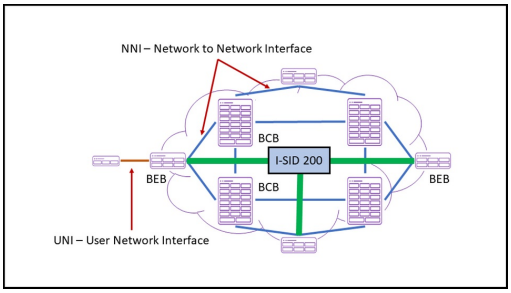
W momencie, gdy ruch związany z usługą trafia do rdzenia sieci, Fabric Connect sam oblicza najbardziej optymalną ścieżkę wewnątrz sieci. Możesz dodawać lub usuwać ścieżki (celowo lub w wyniku błędu), ale rdzeń sieci automatycznie znajdzie odpowiedni skrót.

W skrócie rzecz ujmując, dostarczanie zasobów w przypadku switchy BCB sprowadza się jedynie do routingu. Nie ma potrzeby, aby urządzenia te (ani też zespół je obsługujący) wiedziały cokolwiek na temat dostarczanych usług. Dodawanie i usuwanie usług w sieci typu Fabric Connect zachodzi całkowicie poza switchami BCB, co pozwala uprościć i usprawnić zarządzanie siecią.

Backbone Edge Bridge

Switche BEB odnoszą się zarówno do routingu, jak i do usług. Aby zwizualizować sobie usługę, najprościej wyobrazić sobie warstwę 2. sieci pomiędzy dwoma lub więcej switchami BEB. Każda usługa jest identyfikowana w sposób indywidualny za pomocą I-SID (Service Identifier / Identyfikator Usługi) – **Extreme Fabric Connect wspiera ponad 16 milionów usług na sieć.**

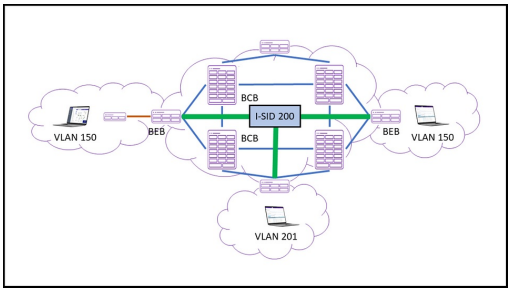
Jako że routing zawiera się w switchach BCB, rdzeń sieci możemy traktować jak swego rodzaju bańkę. Switche BEB umiejscawiane są na brzegu bańki, a połączenia pomiędzy nimi są usługami. Może to brzmieć trochę skomplikowanie, więc spróbujmy to sobie zwizualizować. Jeśli chcemy dostarczyć jakąś usługę (weźmy tu na przykład wspomniane wcześniej kamery monitoringu), musimy najpierw określić jej unikalny identyfikator. W tym przypadku użyjemy I-SID o wartości 200. W naszej sieci mamy dwie kamery, a każda z nich podłączona jest do innego switcha BEB oraz do serwera kamer. Musimy zatem ustawić trzy switche BEB tak, aby na odpowiednich portach znajdował się ten sam I-SID (jest to pewne uproszczenie, ale jeszcze do tego wrócimy).



Download image

To, jak te trzy skonfigurowane pod usługę switche BEB się komunikują, nie jest zmartwieniem dla switchy brzegowych. Są one połączone ze switchami BCB poprzez zdefiniowane NNI, a ich rola ogranicza się do oznakowania ruchu prawidłowym identyfikatorem I-SID i przekazanie go dalej do switchy BCB. Jedyną konfigurację, jakiej tutaj dokonamy, będzie dopasowanie wspieranych usług (identyfikatorów I-SID) do portów.

Jak już wcześniej wspomniałem, dopasowanie identyfikatorów I-SID do portów może być zbyt dużym uproszczeniem. Fabric Connect owszem wspiera mapowanie poszczególnych portów, aczkolwiek częstszą praktyką jest dopasowanie identyfikatorów I-SID do VLANów, jako że jest to dość elastyczny sposób na integrację sieci tradycyjnych i sieci typu fabric. Jako że w tym przypadku mapowanie uwzględnia także switche BEB, możliwe jest dopasowanie różnych VLANów do tego samego identyfikatora I-SID, tak jak prezentuje to poniższy diagram:



Download image

Istnieją jeszcze lepsze sposoby na mapowanie identyfikatorów I-SID, ale jeszcze do tego dojdziemy.

Szczególną przewagą, jaką oferuje Fabric Connect, jest fakt iż komunikacja za pośrednictwem identyfikatoró1)w I-SID przechodzi przez rdzeń sieci. Oznacza to, że każda „elastyczna” warstwa druga jest prywatna, co z kolei utrudnia potencjalnemu hakerowi poziomy ruch w obrębie sieci (typową taktyką włamywaczy w przypadku tradycyjnych sieci jest atakowanie jakiegoś prostego elementu, np. czujnika IoT, a następnie „przeskoczenie” na ważniejszą sieć).

Przewaga ta odnosi się także do warstwy 3. Jeśli chciałbyś np. skorzystać z narzędzia typu traceroute z poziomu stacji roboczej, topologia Twojej sieci będzie całkowicie niewidoczna. Często nazywa się to „hipersegmentacją”, jako że każda spośród 16 milionów wspieranych usług jest automatycznie oddzielona od pozostałych, zaś ich ścieżki istnieją tylko wtedy, kiedy usługa jest w użyciu. Fabric Connect jest więc nie tylko łatwiejszy w zarządzaniu, lecz także z definicji bardziej bezpieczny.

Korzyści płynące z zastosowania switchy BEB i identyfikatorów I-SID są dość wyraźne. Możesz dodawać nowe usługi lub modyfikować te istniejące w dowolnej chwili, bez konieczności dotykania konfiguracji rdzenia i dystrybucji. Także w czasie najbardziej intensywnego ruchu, bez potrzeby okienka serwisowego czy żmudnej rekonfiguracji i testowania. Sieć może poruszać się tak szybko, jak funkcjonuje nasz biznes, zamiast być czynnikiem dyktującym tempo naszych działań.

Nie czekaj – automatyzuj!

Teraz, kiedy omówiliśmy już kwestię routingu (poprzez nasze switche BCB) oraz usługi (w oparciu o switche BEB), pozostaje ostatni element układanki: klienci. Klienci, czyli wszystko, co wymaga dostępu do usług dostarczanych przez sieć fabric: laptopy, punkty dostępowe, czujniki, drukarki, serwery itd.

Aby zapewnić bezpieczne korzystanie z sieci, z reguły stosuje się system kontroli do sieci (Network Access Control lub w skrócie NAC) – na przykład nasz Extreme Control. W momencie, kiedy klient próbuje podłączyć się do sieci, zadaniem NACa jest jego uwierzytelnienie. Tradycyjne sieci wspierają różne metody autoryzacji określające co dany klient może zrobić, np. listy kontroli dostępu (Access Control Lists), firewalle, VLANy i tak dalej. Fabric pozwala systemowi NAC poinformować switch, z którym VLANem/identyfikatorem I-SID dany klient może się komunikować oraz która polityka bezpieczeństwa powinna zostać zastosowana. Rozwiązanie to pozwala w pełni zautomatyzować brzeg sieci typu fabric oraz scentralizować konfigurację brzegu sieci. Co więcej, jeśli dany klient porusza się w obrębie sieci, fabric może udostępnić mu te same usługi z dowolnego switcha BEB, jako że system kontroli dostępu do sieci w pełni automatyzuje dostarczanie zasobów.

Jeśli do sieci fabric podłączymy nową lokalizację, switch BEB automatycznie zyskuje dostęp do wszystkich usług. Jeżeli system NAC może uwierzytelnić próbującego się podłączyć klienta (oraz jeśli klient posiada odpowiednie autoryzacje w NAC), fabric w sposób elastyczny dostarczy wymagane usługi bez potrzeby konfiguracji.

Jeśli Twoja sieć nie jest wyposażona w urządzenia brzegowe kompatybilne z SPBm, Extreme oferuje ponadto funkcję zwaną „Fabric Attach”, dostępną w wielu switchach brzegowych i punktach dostępowych Extreme, a także urządzeniach firm trzecich, takich jak switche czy kamery przemysłowe (NEXANS, AXIS, Microsens). Fabric Attach umożliwia podłączenie klientów w taki sposób, że określają one dokładnie usługi, do których pragną uzyskać dostęp. Klientami tymi mogą być switche brzegowe, punkty dostępowe, kamery monitoringu itd. Sieć fabric może Ci także pomóc w konfiguracji urządzeń, generowaniu identyfikatorów SSID, zarządzaniu VLANami oraz przy wielu innych czynnościach, co znacząco upraszcza i automatyzuje działanie na brzegu sieci.

Fabric Connect działa z tradycyjnymi sieciami w obrębie WAN

Jedną z najczęściej spotykanych obaw dotyczących technologii Fabric Connect jest potrzeba usunięcia starej sieci, aby zrobić miejsce dla nowej (mówimy tu o tzw. modernizacji całościowej, gdzie wymianie poddaje się wszystkie elementy). Fabric Connect wspiera funkcję Fabric Extend, która umożliwia rozszerzenie sieci na IP w sieci WAN lub nawet na publiczny adres za pomocą narzędzi IPsec.

Innymi słowy, Fabric Extend umożlwia rozciągnięcie sieci typu fabric na tradycyjne sieci. Przykładowo, moglibyśmy uruchomić sieć fabric we wszystkich naszych biurach w Szwecji i w oddziałach w Tokyo, a następnie połączyć je ze sobą poprzez MPLS lub dowolny inny protokół umożlwiający przesyłanie sieci wirtualnych VLAN lub VRF.

Fabric a brzeg sieci

Brzegowe switche Fabric od Extreme w pełni wspierają bezdotykową autokonfigurację, bez potrzeby stackowania. Switche fabric automatycznie wykrywają podłączone urządzenia, takie jak inne węzły SPBm, urządzenia z funkcją Fabric Attach czy telefony VoIP za pomocą funkcji auto-sense.

Chciałbym dowiedzieć się więcej!

Mam nadzieję, że ten prosty wgląd w Fabric Connect zachęci Cię do pogłębienia swojej wiedzy o tej niesamowitej technologii. Poniżej znajdziesz kilka linków, które opisują temat sieci fabric nieco głębiej.

- Fabric Connect Key Capabilities
- Data Center Excellence with Extreme Fabric Connect
- Extending Fabric Connect to the Campus Wiring Closet with Extreme's Fabric Edge Solution
- Fabric Attach Network Automation

Ściągnij bezpłatnie "Fabric Networking For Dummies"!