سند طراحی و تحلیل فنی

نام سند:

Technical Design and Validation of FortiGate HA over Cisco Nexus vPC

عنوان فارسی سند:

طراحی، تحلیل و اعتبارسنجی فنی FortiGate HA بر بستر Cisco Nexus vPC

نویسنده	نسخه	تاریخ	زبان
محمد ستوده نژاد	1.1	1405/02/31	فارسی

مخاطبان هدف:

مهندسان شبکه، علاقه‌مندان به طراحی دیتاسنتر، دانشجویان حوزه شبکه، متخصصان لابراتوارهای فنی، و افرادی که روی Cisco Nexus vPC، FortiGate HA و سناریوهای High Availability کار می‌کنند.

هدف سند:

این سند یک راهنمای فنی شخصی و مستقل برای طراحی، تحلیل رفتاری، بررسی خرابی، و اعتبارسنجی یک توپولوژی شبکه مبتنی بر Cisco Nexus vPC، سوئیچ‌های Access کاتالیست، و FortiGate HA است. هدف آن ارائه یک مرجع عمیق و ساختاریافته است که بتواند هم برای مطالعه شخصی و هم برای انتشار عمومی به‌عنوان یک مستند فنی قابل استفاده باشد.

محدوده سند:

- معماری vPC روی Cisco Nexus
- طراحی Access مبتنی بر Catalyst
- رفتار FortiGate HA در مجاورت vPC
- تحلیل Asymmetric Routing
- طراحی Orphan Access Switch
- طراحی STP و مکانیزم‌های حفاظتی
- طراحی Management و VRF
- روش‌های Validation و Failover Testing

فهرست مطالب

خلاصه مدیریتی

این سند به طراحی، تحلیل و اعتبارسنجی فنی یک سناریوی شبکه دیتاسنتری مبتنی بر Cisco Nexus vPC و FortiGate HA می‌پردازد. تمرکز اصلی این بررسی بر تحلیل رفتار ترافیکی، ملاحظات افزونگی، نحوه اتصال لایه‌های مختلف شبکه، و ارزیابی رفتار Failover در شرایط واقعی است.

در روند پیاده‌سازی و آزمون، مشخص شد که اگرچه طراحی اولیه از نظر ساختار منطقی قابل قبول است، اما در برخی سناریوهای خرابی، رفتار هم‌زمان Nexus vPC، LACP و FortiGate HA می‌تواند منجر به بروز اختلال در تداوم سرویس شود. به همین دلیل، علاوه بر تحلیل ریشه‌ای مسئله، طراحی اصلاحی نیز ارائه و بررسی شد.

نتایج اعتبارسنجی انجام‌شده در محیط واقعی نشان داد که با رعایت اصول کلیدی طراحی، از جمله تفکیک صحیح نقش لینک‌ها، استفاده صحیح از vPC، در نظر گرفتن رفتار Orphan Portها، جداسازی مناسب VRFها، و تعریف مسیر مدیریت مستقل، می‌توان به معماری‌ای دست یافت که از نظر پایداری، قابلیت تحلیل، و قابلیت بهره‌برداری عملیاتی، قابل اتکا باشد.

این سند با هدف ثبت تجربه فنی، مستندسازی تصمیم‌های طراحی، و ارائه یک مرجع قابل استفاده برای سناریوهای مشابه تدوین شده است.

0.دامنه و حدود سند

این سند بر طراحی، تحلیل فنی، و اعتبارسنجی یک سناریوی مشخص مبتنی بر Cisco Nexus vPC و FortiGate HA تمرکز دارد. محتوای آن شامل بررسی ساختار منطقی شبکه، نحوه اتصال اجزای اصلی، تحلیل رفتار Failover، ارزیابی ملاحظات مرتبط با LACP و vPC، و بررسی اثرات طراحی بر پایداری ارتباطات در شرایط خرابی است.

در این سند، موضوعاتی مانند طراحی Uplinkها، نقش Peer-Link و Peer-Keepalive، ملاحظات مربوط به Orphan Port، جداسازی VRFها، و مسیر مدیریت مستقل بررسی می‌شوند. همچنین، طراحی اصلاحی ارائه‌شده بر اساس مشاهدات حاصل از پیاده‌سازی و آزمون واقعی تحلیل شده است.

این سند با وجود تمرکز بر تصمیم‌های کلیدی Design و رفتار عملی اجزای اصلی، شامل جزئیات کامل همه حوزه‌های پیرامونی نیست. برای مثال، Hardening امنیتی، ظرفیت‌سنجی نهایی برای توسعه در مقیاس بزرگ، طراحی جامع سرویس‌های Routing، سیاست‌های بهره‌برداری، و برنامه مهاجرت از سناریوهای موجود، خارج از دامنه این سند هستند.

بنابراین، این مستند باید به‌عنوان یک سند فنی متمرکز بر Design Validation، Failure Analysis و Design Decision در یک سناریوی مشخص در نظر گرفته شود، نه به‌عنوان راهنمای جامع همه ابعاد یک استقرار Production.

1. مقدمه

هدف این مستند، طراحی و تحلیل رفتاری یک معماری دیتاسنتری مبتنی بر **Cisco Nexus vPC** در لایه توزیع، **Cisco Catalyst Access** در لایه دسترسی، و **FortiGate HA** به‌عنوان دروازه لایه 3 و نقطه پایان VLANها است. در این طراحی، مسیر بین Access تا Nexus و سپس تا FortiGate کاملاً **Layer 2** باقی می‌ماند و هیچ SVI یا Gateway روی Nexusهای vPC قرار نمی‌گیرد. این انتخاب مستقیماً رفتار کنترل ترافیک، همگرایی، مدل عیب‌یابی، و ریسک‌های ناشی از نامتقارن‌شدن مسیر ترافیک را تحت تأثیر قرار می‌دهد.

سناریوی حاضر پس از تحلیل و طراحی اولیه، در بستر تجهیزات واقعی نیز مورد آزمون و اعتبارسنجی قرار گرفت. بنابراین، محتوای این سند صرفاً به توصیف یک محیط آزمایشگاهی محدود نبوده و بر رفتار مشاهده‌شده در پیاده‌سازی عملی نیز تکیه دارد. به‌ویژه در محیط‌هایی که فایروال به‌عنوان نقطه ترمینیشن VLAN و policy enforcement استفاده می‌شود، استفاده از vPC در بالادست باعث می‌شود که Access بدون نیاز به STP Blocking روی Uplinkها، از هر دو Nexus به‌صورت هم‌زمان بهره ببرد و افزونگی در لایه 2 با کارایی بالا فراهم شود.

طراحی حاضر چند مسئله مهم را حل می‌کند. نخست، حذف وابستگی عملیاتی به STP Blocking در Uplinkهای دسترسی و فعال‌کردن هم‌زمان هر دو لینک بالادستی. دوم، کاهش ریسک Blackhole و Loop در مواجهه با شکست‌های جزئی. سوم، فراهم‌کردن بستر مناسب برای اتصال FortiGate HA به‌گونه‌ای که پایداری MAC و ARP در Failover حفظ شود. چهارم، فراهم‌کردن امکان تحلیل رفتاری **Orphan Port**ها که در این سناریو دو مورد از آن‌ها وجود دارد و برای عملیات واقعی بسیار مهم هستند.

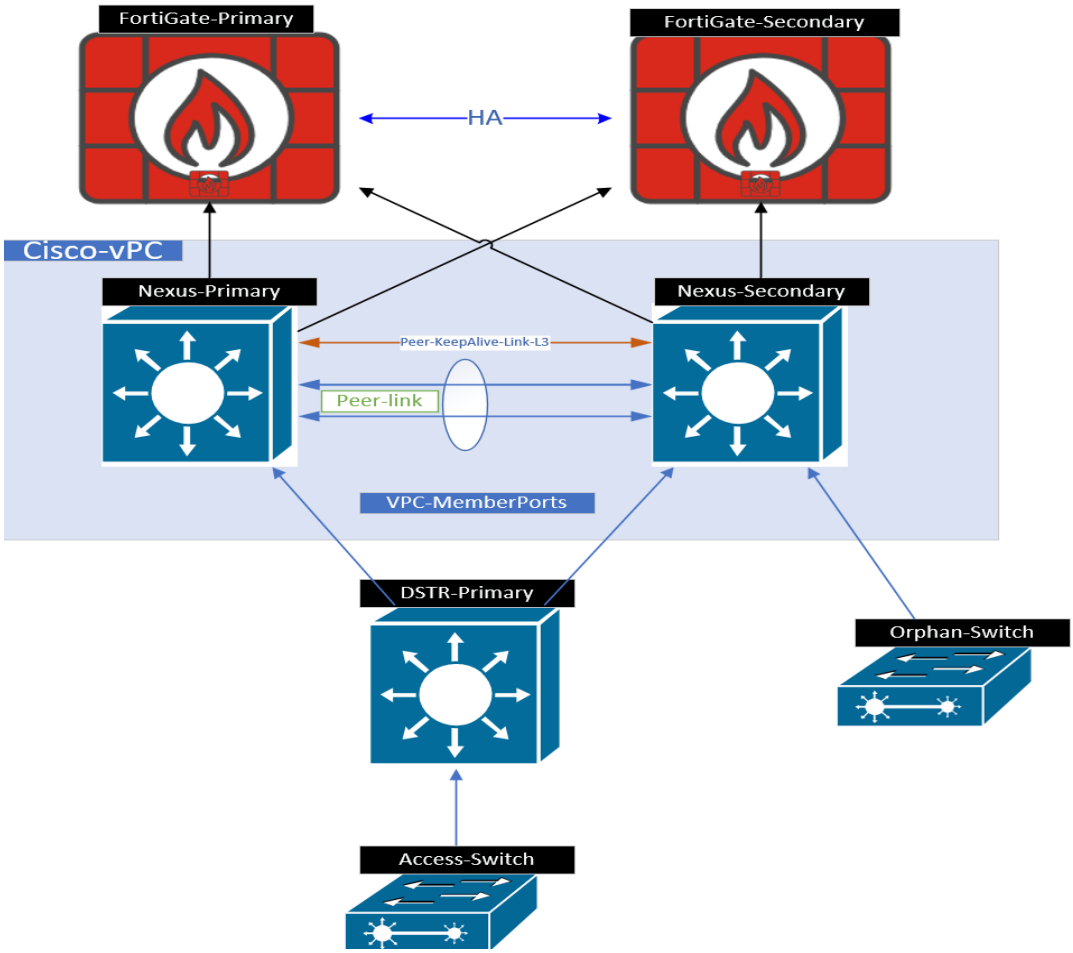
. نخست، یک **Nexus اضافی** در میانه مسیر صرفاً به‌عنوان Distribution/Transit قرار داده شده که از منظر معماری vPC الزامی نیست و صرفاً یک عنصر واسط در مسیر دسترسی به حساب می‌آید. دوم، علاوه بر Orphan Access Switch قبلی، اکنون یک **Access Switch دوم نیز به‌صورت Orphan** در سناریو وجود دارد. این دو تغییر باعث می‌شوند دامنه تحلیل Failure، STP و Orphan Protection گسترده‌تر شود و مستند باید این رفتارها را به‌صورت مجزا توضیح دهد.

2. نمای کلی توپولوژی

2.1 معماری کلی

در این سناریو، دو دستگاه **Cisco Nexus 3548** به‌عنوان **vPC Pair** عمل می‌کنند. این دو سوئیچ هسته توزیع/aggregation لایه 2 را تشکیل می‌دهند. FortiGate HA در بالادست این دو Nexus قرار دارد و VLANها روی FortiGate ترمینیت می‌شوند. در پایین‌دست، یک مسیر از طریق یک **Nexus واسط** به Access Switch اصلی می‌رسد و علاوه بر آن، یک یا چند Access Switch به‌صورت **Orphan** تنها به یکی از Nexusها متصل شده‌اند.

وجود Nexus میانی از منظر معماری کلاسیک vPC ضرورتی ندارد، زیرا معمولاً Access مستقیماً به vPC Pair متصل می‌شود. با این حال، وقتی چنین تجهیزی در سناریو قرار می‌گیرد، باید نقش آن به‌عنوان **Transit/Distribution غیر-vPC** کاملاً روشن باشد. این تجهیز نه Peer-Link است، نه عضو vPC domain، و نه مرجع STP در سطح Core. بنابراین نباید برای آن رفتارهایی فرض شود که فقط مختص دو عضو vPC هستند.



2.2 نقش لایه‌ها

نوع عملکرد	نقش فنی	تجهیز	لایه
Layer 3 / Security	Default Gateway، Security Policy، HA Failover	FortiGate HA	Gateway/Security
Layer 2	vPC Pair، L2 Aggregation، STP Root Candidate	NX-Primary / NX-Secondary	Aggregation/Distribution
Layer 2 Transit	سوئیچ واسط برای Accessاصلی	NX-DSTR-PRIMARY	Transit/Distributionاضافی
Layer 2 Access	اتصالEndpoint ها و Uplinkبه Distribution	Catalyst Access	Access
Layer 2 Access	اتصال Single-Homed به یکی ازNexus ها	Orphan Switch 1 / Orphan Switch 2	Access Orphan

2.3 جریان ترافیک

ترافیک کاربر از Access وارد Catalyst یا یکی از Orphan Switchها می‌شود و از طریق لینک لایه 2 به سمت Nexus مربوطه حرکت می‌کند. سپس از طریق vPC uplinkها یا local switching به سمت FortiGate ارسال می‌شود. در بازگشت، FortiGate بسته را بر اساس جدول MAC و ARP به سمت یکی از Nexusها می‌فرستد. اگر طراحی vPC درست انجام نشده باشد، امکان دارد برگشت ترافیک از Nexus مقابل عبور کند و اینجاست که مفاهیمی نظیر **peer-gateway** و **peer-switch** مستقیماً بر پایداری مسیر تأثیر می‌گذارند.

2.4 Control Plane و Data Plane

در این طراحی، **Control Plane** شامل STP، vPC control synchronization، Peer-Keepalive، MAC learning، HA state، logic در FortiGate و Protocolهای مدیریتی است. **Data Plane** صرفاً فورواردینگ فریم‌های لایه 2 بین Access، vPC Pair و FortiGate را شامل می‌شود. تمایز این دو مهم است، زیرا ممکن است Data Plane یک مسیر را ببیند اما Control Plane آن را معتبر نداند، یا بالعکس. بسیاری از Failureهای پیچیده دقیقاً از ناهماهنگی میان این دو حوزه ناشی می‌شوند.

2.5 دامنه‌های خرابی

دامنه خرابی	محل	اثر مستقیم	ریسک
خرابی یک Nexus عضو vPC	NX-Primaryیا-NX Secondary	قطع بخشی ازuplink ها، تغییرMAC learning	متوسط تا بالا
خرابیPeer-Link	بین دوNexus vPC	از دست‌رفتن Sync و احتمالSuspend	بسیار بالا
خرابیPeer-Keepalive	مسیرkeepalive	اثر فوری بر Data ندارد، ولی Split-Brain Logic تحت تأثیر است	بالا
خرابی FortiGate Active	Gateway Layer	بهFailover عضو Secondary	بالا
خرابی Nexus واسط	NX-DSTR-PRIMARY	قطع دسترسی Access اصلی	متوسط
خرابی Orphan Uplink	Switch Orphan	قطع کامل همان Access خاص	بالا برای همانSegment

2.6 جریان VLAN

VLAN	نقطه عبور	محل Gateway	توضیح
User VLANs	Accessواسط → Nexus مستقیم / vPC Pair → FortiGate	FortiGate	تمام مسیر تا فایروال L2 است
Management In-Band VLAN	در صورت تعریف	معمولاً SVI روی Nexus یا مسیر روت‌شده جداگانه	فقط برای دسترسی مدیریتیIn-Band
Keepalive VLAN/VRF	غیر ازmgmt0	Front-3لایهInterface درPanel مجزا VRF	فقط برایPeer-Keepalive

3. مفاهیم اصلی vPC

3.1 معماری vPC

vPC یا **Virtual Port-Channel** مکانیزمی است که اجازه می‌دهد یک دستگاه پایین‌دستی، دو لینک فیزیکی خود را به دو Nexus مجزا متصل کند اما از دید خود آن را یک EtherChannel واحد ببیند. در عمل، دو Nexus در سطح کنترل، اطلاعات لازم را با هم همگام می‌کنند تا پایین‌دست مجبور به Block کردن یکی از لینک‌ها توسط STP نشود و هر دو لینک فعال باقی بمانند.

علت وجود vPC، حل تناقض کلاسیک افزونگی و بهره‌وری است. در مدل سنتی STP، برای جلوگیری از Loop یکی از لینک‌ها Block می‌شود. در vPC، بدون نیاز به شاسی واحد یا Stack واقعی، دو سوئیچ مجزا رفتاری معادل یک نقطه تجمیع منطقی ارائه می‌دهند. اگر این هماهنگی ناقص باشد، پایین‌دست ممکن است ترافیک را به سوئیچی بفرستد که مالک محلی تصمیم فورواردینگ نیست و در نتیجه یا ترافیک از Peer-Link عبور می‌کند یا Blackhole رخ می‌دهد.

Peer-Link 3.2

Peer-Link حیاتی‌ترین جزء vPC است. این لینک بین دو Nexus عضو vPC برقرار می‌شود و برای **همگام‌سازی اطلاعات کنترلی و حمل برخی از ترافیک‌های خاص** به کار می‌رود. Peer-Link باید ظرفیت بالا، پایداری زیاد و ترجیحاً Port-Channel داشته باشد. از دست‌دادن Peer-Link مساوی با ورود طراحی به حساس‌ترین حالت Failure است.

از طریق Peer-Link معمولاً اطلاعاتی نظیر MAC table synchronization، STP state information، IGMP/ARP synchronization و پیام‌های مرتبط با وضعیت vPC بین دو Peer رد و بدل می‌شود. با این حال، Peer-Link نباید به‌عنوان مسیر عادی و دائمی برای Data Plane طراحی شود. اگر ترافیک عادی به‌صورت مداوم مجبور به عبور از Peer-Link شود، یعنی طراحی در لایه 2 بهینه نیست یا ویژگی‌هایی مثل Peer-Gateway درست پیاده نشده‌اند.

3.2.1 آنچه نباید روی Peer-Link متکی باشد

مورد	وضعیت	دلیل
مسیر عادی ترافیک Host به Gateway	نامطلوب	افزایش Hairpin و ریسکFailure
مدیریت In-Band معمول	نامطلوب	وابستگی مدیریتی به vPC Control Path
Peer-Keepalive	ممنوع	Keepaliveباید مستقل از Peer-Linkباشد
OOB Management	ممنوع	مدیریت Out-of-Band باید مستقل باشد

3.3 Peer-Keepalive

Peer-Keepalive مکانیزمی برای تشخیص زنده‌بودن Peer است و هدف اصلی آن **جلوگیری از Split-Brain** است، نه همگام‌سازی Data Plane. این نکته بسیار مهم است. برخی ادمین‌ها تصور می‌کنند Keepalive نقش کنترلی مشابه Peer-Link دارد، در حالی که عملاً Keepalive فقط برای تشخیص این استفاده می‌شود که آیا Peer واقعاً از دسترس خارج شده یا صرفاً Peer-Link قطع شده است.

اگر Peer-Link قطع شود اما Keepalive همچنان برقرار باشد، هر Nexus متوجه می‌شود که Peer هنوز زنده است ولی Sync اصلی از بین رفته، بنابراین رفتارهای حفاظتی vPC فعال می‌شوند. اگر هر دو هم‌زمان از بین بروند، هر Nexus ممکن است تصور کند طرف مقابل مرده است و این همان شرایط Split-Brain است که می‌تواند منجر به Loop، Duplicate Forwarding و MAC Instability شود.

3.4 Configured Role و Operational Role

در vPC، هر Nexus یک **Role Priority** دارد که بر اساس آن ممکن است به‌صورت **Primary** یا **Secondary** تعریف شود. این نقش پیکربندی‌شده، تضمین نمی‌کند که در هر لحظه همان نقش عملیاتی برقرار باشد. آنچه مهم است **Operational Role** است که در زمان اجرا و بر اساس وضعیت واقعی Peer-Link، Keepalive و Sequence Bring-Up تعیین می‌شود.

در عملیات، ممکن است سوئیچی که در طراحی به‌عنوان Secondary مشخص شده، به دلیل ترتیب Boot یا شرایط Failure به‌صورت عملیاتی نقش Primary را برعهده بگیرد. اگر تیم عملیاتی تفاوت این دو مفهوم را نفهمد، در زمان عیب‌یابی ممکن است تصمیم نادرست بگیرد. به همین دلیل همیشه باید هم `show vpc role` و هم وضعیت Peer adjacency بررسی شود، نه صرفاً برچسب‌های اسمی NX-Primary و NX-Secondary.

3.5 رفتار Non-Preemptive

vPC به‌صورت پیش‌فرض **Non-Preemptive** طراحی شده است. یعنی اگر یک Nexus پس از Failure دوباره بالا بیاید، صرفاً به این دلیل که اولویت بالاتری دارد، بلافاصله نقش عملیاتی را از Peer فعلی پس نمی‌گیرد. دلیل این رفتار، جلوگیری از ناپایداری و Role-Flapping در محیط Production است.

اگر Preemption وجود داشت، هر بار بازگشت تجهیز ترجیحی می‌توانست باعث جابه‌جایی نقش‌ها، تغییرات در مسیرهای کنترلی و نوسان در MAC/STP behavior شود. در شبکه دیتاسنتری، ثبات عملیاتی از ارجحیت بالاتری نسبت به بازگرداندن سریع نقش اسمی برخوردار است. بنابراین Non-Preemptive بودن، یک تصمیم مهندسی برای حفظ همگرایی پایدار است، نه یک محدودیت.

Peer-Switch 3.6

Peer-Switch قابلیتی است که باعث می‌شود هر دو Nexus عضو vPC از دید STP، رفتاری شبیه یک Root Bridge مشترک داشته باشند. در عمل، هر دو Peer قادر می‌شوند BPDUها را با ویژگی‌هایی سازگارتر به پایین‌دست ارسال کنند تا Access در مواجهه با vPC uplinkها دچار برداشت ناسازگار از Topology نشود.

3.6.1 علت وجود Peer-Switch

در غیاب Peer-Switch، یکی از Nexusها از دید STP Root واقعی خواهد بود و دیگری خود را Root نمی‌بیند. این مسئله در برخی Failureها و در طراحی‌های چندلایه می‌تواند باعث شود Access یا تجهیز میانی، Topology را ناهماهنگ درک کند. وقتی Peer-Switch فعال است، پایین‌دست دو Nexus را از منظر STP رفتاری نزدیک‌تر به یک موجودیت منطقی واحد می‌بیند.

3.6.2 رفتار MAC و STP با Peer-Switch

ویژگی	با Peer-Switch	بدون Peer-Switch
نمایش Root به Access	پایدارتر	بالقوه ناهماهنگ
رفتار STP در vPC uplink	همگن‌تر	مستعد برداشت متفاوت
Failover در Topology	تمیزتر	احتمال TCN و نوسان بیشتر
سازگاری با Access L2	بهتر	ضعیف‌تر

3.6.3 اگر Peer-Switch غیرفعال باشد چه می‌شکند

اگر Peer-Switch غیرفعال باشد، به‌ویژه در سناریویی که بین vPC Pair و Access یک Nexus واسط نیز وجود دارد، دید STP پایین‌دست ممکن است میان دو سمت تفاوت داشته باشد. این مسئله در شرایط Failure می‌تواند منجر به انتخاب نامطلوب Root Port، ارسال ناهماهنگ BPDU و تغییرات غیرقابل‌پیش‌بینی در مسیرهای لایه 2 شود. نتیجه می‌تواند از افزایش TCN تا Loop لحظه‌ای یا Blackhole متغیر باشد.

Peer-Gateway 3.7

Peer-Gateway قابلیتی است که اجازه می‌دهد هر Nexus، فریم‌هایی را که مقصد MAC آن‌ها در واقع متعلق به Gateway سمت Peer است، به‌صورت محلی بپذیرد و مجبور نباشد آن‌ها را از Peer-Link عبور دهد. این ویژگی در سناریوهای دارای فایروال، FHRP، یا تجهیزاتی که ARP/MAC آن‌ها نسبت به مسیر بازگشت حساس است، اهمیت بسیار بالایی دارد.

3.7.1 منطق ARP و MAC

در بسیاری از طراحی‌ها، Host یا فایروال ممکن است ARP را از یک سمت دریافت کند اما در مسیر واقعی فریم را به سمت دیگر بفرستد. اگر Nexus محلی نتواند فریمی را که مقصد MAC آن به‌ظاهر متعلق به Peer است قبول کند، مجبور می‌شود آن را از Peer-Link رد کند. این کار هم ناکارآمد است و هم در Failureها دردسرساز می‌شود. Peer-Gateway این وابستگی را کاهش می‌دهد.

3.7.2 نمونه Packet Walk

فرض کنید FortiGate بسته برگشتی را به NX-Secondary بفرستد، اما MAC مقصد متعلق به مسیری باشد که از دید سنتی باید به NX-Primary برسد. بدون Peer-Gateway، NX-Secondary آن را local terminate نمی‌کند و تلاش می‌کند از Peer-Link به Peer بفرستد. با Peer-Gateway، NX-Secondary همان‌جا فریم را می‌پذیرد و Local Forwarding انجام می‌دهد. این موضوع تأخیر، مصرف Peer-Link و ریسک نامتقارن‌شدن رفتار را کاهش می‌دهد.

3.7.3 اثر Peer-Gateway در طراحی مبتنی بر Firewall Gateway

وضعیت	نتیجه
Peer-Gateway فعال	فورواردینگ محلی بهتر، کاهشHairpin ، رفتار پایدارتر با FortiGate
Peer-Gateway غیرفعال	افزایش وابستگی بهPeer-Link ، ریسک نامتقارن‌شدن مسیر، حساسیت بیشتر درFailover

3.7.4 ریسک‌های Misconfiguration

خطا	پیامد
عدم فعال‌سازی Peer-Gateway در حضور Firewall Gateway	برگشت ترافیک ازPeer-Link ، MAC Instability، افزایشAsymmetry
فعال بودن vPC بدونPeer-Switch	STP inconsistencyو Root perception نامناسب
طراحی Keepalive وابسته به همان مسیرData	افزایش ریسک Split-Brain در Failure مشترک

4. طراحی STP در محیط vPC

4.1 STP چگونه vPC را می‌بیند

STP از دید پایین‌دست، vPC uplinkها را به‌عنوان یک ارتباط تجمیع‌شده می‌بیند، نه دو مسیر مستقل رقابتی. همین موضوع دلیل اصلی فعال‌ماندن هم‌زمان Uplinkها است. با این حال، STP همچنان در محیط وجود دارد و خاموش نشده است؛ بلکه نقش آن از جلوگیری فعال از Loop به **حفاظت و تشخیص ناهنجاری** تغییر می‌کند.

4.2 استراتژی Root Bridge

در این طراحی، Root Bridge باید عملاً روی vPC Pair قرار گیرد. اگر Root در جای دیگری باشد، مخصوصاً روی Nexus واسط یا سوییچ‌های پایین‌دست، مسیرهای STP می‌توانند برخلاف قصد معماری شکل بگیرند. چون vPC Pair نقطه تجمیع اصلی و اتصال به Gateway است، Root بودن آن‌ها موجب کوتاه‌ماندن مسیرهای لایه 2 و پیش‌بینی‌پذیری بیشتر Failover می‌شود.

4.3 اهمیت Peer-Switch برای STP

وقتی Peer-Switch فعال است، هر دو Nexus در تعامل با STP رفتار سازگارتر و متقارن‌تری نشان می‌دهند. این موضوع به‌ویژه زمانی مهم می‌شود که Nexus واسط در پایین‌دست وجود داشته باشد. چون تجهیز واسط، BPDUها را از دو سمت دریافت می‌کند و اگر این دو سمت در ادراک Root اختلاف داشته باشند، انتخاب Root Port و Alternate Port می‌تواند رفتاری ناپایدار پیدا کند.

4.4 رفتار در خرابی Peer-Link

در خرابی Peer-Link، STP به‌تنهایی مسئله را حل نمی‌کند. vPC منطق حفاظتی خود را فعال می‌کند و بسته به اینکه Keepalive برقرار باشد یا نه، پورت‌های خاصی را Suspend می‌کند تا از Dual-Active L2 جلوگیری شود. در این وضعیت، Access ممکن است از دید STP هنوز لینکی را Up ببیند ولی vPC آن را منطقی suspend کرده باشد. بنابراین همیشه باید STP state را کنار vPC state تحلیل کرد.

4.5 رفتار در خرابی Access Switch

اگر Access اصلی که از طریق Nexus واسط متصل است Fail شود، فقط همان Segment از دست می‌رود و تأثیری روی Peer-Link و FortiGate ندارد. اگر یکی از Accessهای Orphan Fail شود، دامنه خرابی محدود به همان سوئیچ است. اما اگر Uplink یک Orphan به Nexus بالادست قطع شود، آن Access به‌طور کامل از شبکه جدا می‌شود، زیرا برخلاف vPC host، مسیر دوم ندارد.

4.6 مکانیزم‌های حفاظتی STP

4.6.1 BPDU Guard

BPDU Guard برای پورت‌هایی است که باید فقط به Endpoint متصل باشند. اگر روی چنین پورتی BPDU دریافت شود، به معنی اتصال نادرست سوئیچ یا Loop بالقوه است و پورت Errdisable می‌شود. استفاده از آن روی Access Edge ضروری است، اما روی Uplinkها یا پورت‌های بین‌سوئیچی نباید به‌کار رود.

4.6.2 Root Guard

Root Guard روی پورت‌هایی استفاده می‌شود که نباید از سمت مقابل Root Bridge جدید معرفی شود. هدف آن جلوگیری از جابه‌جایی ناخواسته Root به سمت Access یا تجهیزات غیرمجاز است. در این سناریو، Root Guard می‌تواند روی برخی Downlinkهای Distribution به سمت لایه‌ای که نباید Root شود مفید باشد.

4.6.3 Loop Guard

Loop Guard برای جلوگیری از Forward شدن ناخواسته پورتی است که باید Blocking/Alternate بماند اما به علت از دست‌رفتن BPDU وارد وضعیت اشتباه شود. در محیط‌هایی که فیبر یک‌طرفه، خطای BPDU یا ناپایداری لینک وجود دارد، Loop Guard بسیار مهم است.

4.6.4Bridge Assurance

Bridge Assurance روی لینک‌های Network-Type بین سوئیچ‌ها استفاده می‌شود و تضمین می‌کند که اگر BPDU از سمت مقابل نرسد، پورت وارد حالت ناسالم شود و بی‌محابا Forward نکند. در محیط Nexus، این مکانیزم برای لینک‌های Core/Distribution مفید است و سطح ایمنی را بالا می‌برد.

4.7 جدول کاربرد حفاظت‌ها

مکانیزم	محل استفاده	هدف	خطر در عدم استفاده
BPDU Guard	Edge Portها	جلوگیری از اتصال سوئیچ غیرمجاز	Loopو تغییر STP Topology
Root Guard	Downlinkهای حساس	جلوگیری از جابه‌جایی Root	Root hijack
Loop Guard	لینک‌های مستعد Loss BPDU	جلوگیری از Forward اشتباه	Loopپنهان
Bridge Assurance	لینک‌های سوئیچ به سوئیچ	تشخیص Failure کنترل	Forwardingناسالم

5- FortiGate HA و Asymmetric Routing

5.1 Asymmetric Routing چیست

Asymmetric Routing زمانی رخ می‌دهد که یک جریان ترافیکی، مسیر رفت و برگشت یکسانی را طی نکند یا بسته‌های یک Session از دید فایروال از اینترفیس‌ها/Nodeهای متفاوتی عبور کنند. در شبکه‌های دارای فایروال Stateful، این موضوع مهم است چون فایروال فقط بر اساس مقصد IP تصمیم نمی‌گیرد، بلکه وضعیت Session را نیز نگه می‌دارد.

در سطح بسته، فرض کنید SYN از یک سمت وارد FortiGate Active شود اما پاسخ SYN/ACK یا ترافیک برگشتی به دلیل تفاوت در MAC learning، vPC forwarding یا Failover از مسیری برسد که فایروال آن را متعلق به همان Session نداند. در این حالت، Session lookup ممکن است شکست بخورد و ترافیک Drop شود. پس نامتقارن‌بودن صرفاً مفهوم Routing Table نیست؛ بلکه **Session Path Symmetry** نیز هست.

5.2 چرا فایروال ترافیک نامتقارن را Drop می‌کند

فایروال Stateful برای هر Session اطلاعاتی مانند Source/Destination IP، Port، Protocol، Interface، و گاه Directionality را نگه می‌دارد. اگر بسته برگشتی از مسیری بیاید که با Session state ثبت‌شده ناسازگار باشد، دستگاه به‌منظور امنیت آن را حمله یا جریان غیرمعتبر تلقی می‌کند. این رفتار درست و عمدی است، نه اشکال فایروال.

در HA نیز این موضوع حساس‌تر می‌شود. اگر Active/Passive باشد، عضو Passive معمولاً مسیر فوروارد‌ینگ اصلی نیست. اگر بخشی از ترافیک به دلیل ناپایداری لایه 2 یا MAC ambiguity به سمتی برسد که با Active session table تطابق ندارد، ریسک Drop بالا می‌رود. بنابراین طراحی vPC باید از دید فایروال، ثبات ورود و خروج فریم‌ها را حفظ کند.

5.3 رفتار FortiGate HA در Active/Passive

در Active/Passive، یک عضو Active تمام Sessionها را پردازش می‌کند و عضو Passive آماده Failover است. هنگام Failover، FortiGate معمولاً Virtual MAC، Gratuitous ARP یا مکانیسم‌های مشابهی برای اعلام تغییر مالکیت Gateway/Interface استفاده می‌کند. هدف این است که تجهیزات لایه 2 سریعاً MAC location جدید را بیاموزند و جریان ترافیک بدون نیاز به انقضای کامل ARP cache ادامه یابد.

اگر لایه 2 بالادست یعنی Nexus vPC Pair، رفتار پایدار در MAC learning نداشته باشد، Failover فایروال می‌تواند با تأخیر یا نامتقارنی همراه شود. به‌طور خاص، اگر Peer-Gateway غیرفعال باشد یا Peer-Link درگیر Hairpin ترافیک عادی شود، احتمال اینکه بسته‌های برگشتی از سمتی غیرمنتظره دیده شوند بیشتر خواهد شد.

5.4 رفتار FortiGate HA در Active/Active

در Active/Active، همچنان مفهوم Primary/Primary-Master برای کنترل وجود دارد، اما Session distribution و UTM processing ممکن است بین اعضا توزیع شود. این مدل پیچیدگی بیشتری در هم‌ترازی مسیرها دارد و به‌طور معمول در طراحی‌های لایه 2 حساس‌تر از Active/Passive است. چون اگر Flow pinning و session ownership دقیقاً با رفتار MAC و مسیرهای vPC هماهنگ نباشد، ریسک Asymmetry بیشتر می‌شود.

برای سناریوی حاضر که هدف آن پایداری و سادگی عملیاتی در محیط اعتبارسنجی بستر پیاده‌سازی‌است، **Active/Passive انتخاب مناسب‌تری** است. با این حال، در مستند باید ذکر شود که در Active/Active حساسیت به MAC stability، session ownership و مسیرهای بازگشت به‌مراتب بیشتر می‌شود.

5.5 تعامل FortiGate با Nexus vPC

MAC Learning 5.5.1

FortiGate بسته به HA state ممکن است در Failover، MAC move ایجاد کند یا Virtual MAC را از یک لینک به لینک دیگر منتقل کند. Nexusها باید این تغییر را سریع و درست یاد بگیرند. اگر بین دو Nexus و FortiGate، EtherChannel/vPC یا طراحی زوج‌لینک درست باشد، این تغییر معمولاً قابل‌پیش‌بینی‌تر خواهد بود.

ARP Reply Paths 5.5.2

ARP reply ممکن است از یک عضو فایروال یا از یک سمت خاص برگردد، اما Data packet بعدی از سمتی دیگر عبور کند. اگر vPC با Peer-Gateway و Peer-Switch به‌درستی تنظیم نشده باشد، این اختلاف کوچک در L2 می‌تواند به Session-level asymmetry تبدیل شود.

5.5.3 اثر Peer-Gateway و Peer-Switch

Peer-Switch باعث می‌شود STP در پایین‌دست رفتار سازگارتر ببیند و در نتیجه تغییرات Topology کمتر به MAC instability منجر شوند. Peer-Gateway نیز موجب می‌شود هر Nexus بتواند مقصد MAC مرتبط با Gateway path را محلی بپذیرد و نیاز به Hairpin روی Peer-Link کاهش یابد. ترکیب این دو، مخصوصاً در مجاورت فایروال Stateful، یک الزام طراحی است نه گزینه تزئینی.

5.5.4 جدول اجباری سناریوها

Scenario	vPC Config	FortiGate Behavior	MAC Stability	Asymmetric Risk
Active/Passive + Peer-Switch + Peer-Gateway	صحیح و کامل	Failoverتمیزتر	بالا	پایین
Active/Passive +بدون-Peer Gateway	ناقص	بازگشت ترافیک مستعدHairpin	متوسط	متوسط تا بالا
Active/Passive +بدون-Peer Switch	STPناهماهنگ	در Failure ها ناپایداری بیشتر	متوسط	متوسط
Active/Active +تنظیم کامل	پیچیده ولی قابل‌کنترل	Session ownershipحساس	متوسط	متوسط
Active/Active +تنظیم ناقص	پرریسک	Session ambiguity	پایین	بسیار بالا
Peer-Link Failure در حضور HA	degraded	نیازمند رفتار محافظتیvPC	پایین‌تر	بالا

5.6 جمع‌بندی Best Practice برای FortiGate

Best Practice	دلیل
استفاده از Active/Passive در این سناریو	پایداری بیشتر و تحلیل ساده‌تر
فعال‌سازیPeer-Gateway	کاهش Hairpin و جلوگیری از نامتقارنی لایه 2
فعال‌سازیPeer-Switch	STPسازگارتر و Failover تمیزتر
ثابت‌نگه‌داشتن مسیرهایL2	جلوگیری ازSession drop
کنترل MAC move درFailover	کاهش زمان بازیابی

6. طراحی Orphan Port و تحلیل Failure

6.1 Orphan Portچیست

Orphan Port در vPC پورتی است که روی یکی از Nexusهای عضو vPC قرار دارد اما Peer متناظر آن روی Nexus مقابل وجود ندارد. یعنی تجهیز پایین‌دستی به‌صورت **Single-Homed** فقط به یک Peer متصل است. از دید vPC، این پورت عضوی از یک vPC دوطرفه نیست و بنابراین منطق افزونگی و تقارن کامل vPC روی آن اعمال نمی‌شود.

در سناریوی جدید شما، دو نوع Orphan داریم. یکی Orphan Switch مستقیمی که تنها به NX-Secondary یا NX-Primary متصل است. دیگری Access Switch دوم که شما فرمودید به‌صورت Orphan در نظر گرفته شود. این یعنی بخشی از شبکه از مزیت Dual-Homing vPC بهره نمی‌برد و در Failure تحلیل آن باید جدا از Access اصلی انجام شود.

6.2 چرا Orphan خطرناک است

خطر Orphan از اینجا ناشی می‌شود که ترافیک آن Access ممکن است در شرایط عادی از یک سمت وارد شود اما در شرایط Failure، به دلیل تغییرات MAC table، STP state یا Peer-Link availability، بازگشت مناسب نداشته باشد. Orphan چون فقط یک مسیر Upstream دارد، در صورت رخداد خطا روی همان Nexus محلی، هیچ مسیر جایگزین مستقیمی در پایین‌دست ندارد.

مشکل مهم‌تر زمانی رخ می‌دهد که Peer-Link از دست برود اما Nexus محلی همچنان تا حدی Up باشد. در چنین شرایطی، Orphan ممکن است به سوئیچی متصل بماند که دیگر Sync کامل با Peer ندارد و ادامه فورواردینگ آن منجر به Blackhole یا Loop منطقی شود. به همین دلیل Cisco برای Orphan رفتارهای حفاظتی توصیه می‌کند.

6.3 orphan-port suspend

قابلیت **orphan-port suspend** باعث می‌شود وقتی شرایط مشخصی از Failure رخ دهد، پورت‌های Orphan به‌صورت خودکار Suspend شوند تا از ادامه فورواردینگ ناسالم جلوگیری شود. فلسفه این قابلیت آن است که **قطع کنترل‌شده بهتر از ادامه سرویس نادرست** است. در دیتاسنتر، Blackhole خاموش و بی‌علامت از قطع صریح خطرناک‌تر است.

Cisco این رفتار را توصیه می‌کند چون در سناریوی Peer-Link failure یا شرایطی که Nexus دیگر نمی‌تواند وضعیت واقعی Peer را با قطعیت بداند، باز نگه‌داشتن Orphan Port ممکن است باعث شود پایین‌دست هنوز شبکه را Up ببیند ولی ترافیک عملاً به مقصد نرسد. Suspend کردن، Failure domain را واضح و قابل‌تشخیص می‌کند.

6.4 سناریوهای خرابی Orphan

سناریو	رفتار محتمل	ریسک
خرابی Nexus محلیOrphan	قطع کاملAccess Orphan	مستقیم ولی قابل‌پیش‌بینی
خرابی Peer-Link با Keepaliveسالم	احتمال Suspend بر اساس منطق حفاظتی	کاهشBlackhole
خرابیPeer-Link + Keepalive	ریسک Split-Brain و نیاز شدید به Protection	بسیار بالا
STP inconsistencyدر مسیر Orphan	Block/Suspendیا ناپایداری Topology	بالا

6.5 Orphan برای Access دوم

وقتی Access Switch دوم به‌صورت Orphan تعریف می‌شود، باید آن را از همان ابتدا خارج از محدوده High-Availability واقعی در نظر گرفت. این سوئیچ از منظر عملیاتی یک **Single Point of Attachment** دارد. بنابراین اگر به هر دلیل NX میزبان آن دچار Failure شود، کل آن Access از دست می‌رود. همچنین اگر هدف مدیریت In-Band، سرویس‌دهی به NOC یا حمل VLANهای حساس از طریق این Access باشد، این انتخاب طراحی باید آگاهانه و مستندسازی‌شده باشد.

7. طراحی مدیریت و VRF

7.1 چرا ترافیک مدیریتی باید ایزوله باشد

ترافیک مدیریتی شامل SSH، SNMP، Syslog، NTP، TACACS/RADIUS و Peer-Keepalive است. این ترافیک نباید با Data Plane کاربر مخلوط شود، زیرا هم از منظر امنیت و هم از منظر عیب‌یابی مشکل‌ساز است. وقتی Management ایزوله باشد، در زمان اختلال در VLANهای کاربری یا STP، همچنان می‌توان به تجهیزات دسترسی داشت و Root Cause را دقیق‌تر بررسی کرد.

7.2 چرا mgmt0 + VRF معمولاً بهترین انتخاب است

روی Nexus، اینترفیس **mgmt0** ذاتاً برای مدیریت Out-of-Band طراحی شده و در **VRF management** قرار می‌گیرد. این اینترفیس از Data Plane front-panel جدا است و همین جداسازی باعث می‌شود دسترسی مدیریتی وابسته به Peer-Link، VLANهای کاربری یا STP نباشد. به همین دلیل در طراحی Production، mgmt0 انتخاب ارجح است.

7.3 اگر ادمین بخواهد به Nexusهای vPC شده SSH بزند ولی OOB نباشد چه درگیر می‌شود

اگر SSH به Nexusها **In-Band** باشد، یعنی مسیر مدیریتی از همان شبکه Data یا از VLAN/Interfaceهای جلویی عبور کند، چند مسئله ایجاد می‌شود. نخست، دسترسی مدیریتی دیگر مستقل از خرابی‌های لایه 2/لایه 3 نیست. اگر VLAN مسیر مدیریت، STP، vPC state، یا FortiGate policy دچار مشکل شود، ممکن است دقیقاً در زمانی که بیشترین نیاز به مدیریت دارید، SSH از دست برود.

دوم، در محیط vPC اگر آدرس مدیریتی روی SVI یا روی رابطی تعریف شود که Reachability آن از هر دو Nexus باید برقرار باشد، باید مراقب بود که مسیر بازگشت، ARP و ACLها متقارن بمانند. در غیر این صورت ممکن است از یک مسیر به سوییچ برسید ولی پاسخ از مسیر یا VRF دیگری برگردد و ارتباط مدیریتی ناپایدار شود.

سوم، اگر OOB نباشد، امنیت مدیریت نیز پیچیده‌تر می‌شود. شما باید ACL، Control Plane Policing، AAA، route leaking احتمالی، و جداسازی از User VLANها را دقیق طراحی کنید. در غیر این صورت SSH Nexus تبدیل به یک سرویس قابل‌دسترسی از بستر عملیاتی عمومی می‌شود که از منظر امنیتی پذیرفتنی نیست.

7.4 چگونه می‌توان SSH In-Band داشت

برای SSH In-Band چند روش وجود دارد، ولی در Nexus vPC بهترین روش این است که **یک VRF مجزا برای مدیریت In-Band** ساخته شود و یک اینترفیس لایه 3 یا SVI اختصاصی در آن VRF قرار گیرد. این VRF باید Route، ACL، NTP، Syslog و AAA خودش را داشته باشد یا حداقل از طریق Route Leaking به مقاصد مدیریتی برسد. نباید آن را در VRF پیش‌فرض و در دل VLANهای کاربر رها کرد.

اگر سوییچ Nexus در این سناریو L2-only برای سرویس‌دهی است و SVI برای VLANهای کاربر روی FortiGate ترمینیت می‌شود، هنوز هم می‌توان یک **VLAN/Transit مدیریتی جداگانه** تعریف کرد که فقط برای دسترسی به خود Nexus استفاده شود. در این حالت، آن VLAN نباید نقش Gateway کاربر داشته باشد و باید با ACL و FortiGate policy به‌شدت محدود شود. این یعنی Nexus از دید سرویس کاربران همچنان L2 است، اما برای مدیریت خودش یک حضور کنترل‌شده لایه 3 دارد.

7.5 چرا مدیریت نباید از Peer-Link عبور کند

Peer-Link برای هماهنگی داخلی بین دو عضو vPC طراحی شده است و نقش اصلی آن حمل ترافیک‌های کنترلی همگام‌سازی، برخی فریم‌های خاص، و سناریوهای ضروری Data Plane در شرایط مشخص است. این لینک نباید به‌عنوان مسیر عادی مدیریت In-Band در نظر گرفته شود، زیرا هرگونه وابستگی مدیریتی به Peer-Link باعث می‌شود در زمان خرابی همان لینکی که مرکز حساسیت vPC است، دسترسی عملیاتی شما نیز مختل شود.

اگر SSH، SNMP یا Syslog به‌گونه‌ای طراحی شود که برای رسیدن به یکی از Nexusها ناخواسته از Peer-Link عبور کند، در رخدادهایی نظیر Peer-Link failure، dual-active suspicion، suspend شدن vPCها، یا MAC instability، مسیر مدیریت نیز هم‌زمان غیرقابل‌اعتماد می‌شود. این وضعیت از منظر عملیاتی بسیار خطرناک است، زیرا درست در لحظه‌ای که شبکه نیازمند بررسی دقیق است، تیم عملیات ممکن است دید مدیریتی خود را از دست بدهد.

از منظر معماری، Peer-Link باید یک **dependency sink** باشد نه یک **service transit path**. یعنی سایر سرویس‌ها نباید برای بقای خود به Peer-Link وابسته شوند. هرچه تعداد سرویس‌های وابسته به Peer-Link بیشتر شود، دامنه خرابی این لینک از یک مشکل محدود در vPC به یک بحران چندلایه در Data، Control و Management تبدیل می‌شود.

7.5.1 پیامدهای عبور مدیریت از Peer-Link

وضعیت	پیامد مستقیم	ریسک عملیاتی
SSH از مسیر وابسته به Peer-Link	قطع دسترسی مدیریتی در Failure	بالا
Syslog از مسیر Peer-Link	از دست‌رفتن لاگ‌های زمان حادثه	بالا
SNMP Polling وابسته به Peer-Link	NMS وضعیت غلط یا مبهم می‌بیند	متوسط تا بالا

7.6 طراحی پیشنهادی برای مدیریت In-Band روی Nexusهای vPC

اگر ادمین بخواهد بدون OOB به Nexusهای vPC شده SSH بزند، طراحی باید به‌صورت کنترل‌شده و از قبل مهندسی شود. راه‌حل صحیح این نیست که صرفاً یک IP روی هر SVI گذاشته شود و از همان بستر کاربری به آن SSH شود. راه‌حل درست این است که یک **Management VRF مجزا** ایجاد شود و دسترسی In-Band فقط در همان VRF تعریف شود.

در این مدل، هر Nexus یک Interface لایه 3 یا SVI مدیریتی در VRF اختصاصی خود دارد. مسیر رسیدن NMS، Jump Server یا Bastion Host نیز باید به همین VRF ختم شود. این VRF باید از User VLANها جدا باشد و از طریق ACL، CoPP و Firewall Policy فقط از مبدأهای مجاز اجازه SSH، SNMP، NTP و Syslog را بپذیرد.

اگر FortiGate در این سناریو Gateway اصلی VLANها است، می‌توان VLAN مدیریتی مخصوص Nexusها را نیز تا FortiGate ترانک کرد و Gateway همان VLAN را روی FortiGate قرار داد. در این حالت، FortiGate مسیر و Policy مدیریت را کنترل می‌کند، اما باید دقت شود که دسترسی مدیریتی در زمان Failover فایروال نیز پایدار بماند و Sessionهای مدیریتی در اثر HA Transition قطع نشوند یا حداقل قابل‌پیش‌بینی باشند.

7.6.1 گزینه‌های پیاده‌سازی مدیریت In-Band

روش	پیاده‌سازی	مزیت	محدودیت
SVIمدیریتی در VRF مجزا	VLANمدیریت SVI + روی Nexus	ساده و استاندارد	نیازمند L3 روی Nexus برایManagement
Routed Interfaceدر VRFمجزا	Interface no switchport	تمیزتر و قابل‌کنترل	نیازمند لینک L3 مستقل
Loopbackدر VRF + Reachabilityاز Transit	مناسب برای مانیتورینگ	پایداری خوب برای سرویس‌ها	نیازمند Route Design دقیق
استفاده از VRF پیش‌فرض	سریع ولی نامطلوب	پیاده‌سازی ساده	ریسک امنیتی و عملیاتی بالا

7.7 اگر نخواهیم Peer-Keepalive روی mgmt0 باشد چه باید کرد

در Nexus، استفاده از **mgmt0** برای Peer-Keepalive بسیار رایج و توصیه‌شده است، زیرا به‌صورت طبیعی از Data Plane جدا است. اما اگر شما بخواهید Peer-Keepalive را روی mgmt0 نبرید، راه‌حل معتبر این است که برای Keepalive یک **VRF مجزا** روی یکی از Interfaceهای Front-Panel لایه 3 ایجاد کنید.

این طراحی زمانی کاربرد دارد که OOB در اختیار نیست، یا mgmt0 در سناریو ما به هر دلیل قابل‌استفاده نیست، یا سیاست طراحی شما اقتضا می‌کند تمام سرویس‌های خاص روی Fabric جلویی ولی در VRFهای مجزا حمل شوند. در این حالت، باید دقت شود که مسیر Keepalive از Data و Management عادی جدا باشد و تا حد امکان تنها بین دو Nexus reachability داشته باشد.

Peer-Keepalive نباید روی همان VLANها و همان مسیری قرار گیرد که بار اصلی Data یا SSH In-Band از آن عبور می‌کند. چون در این صورت یک Failure مشترک می‌تواند هم Peer-Link را از بین ببرد، هم Keepalive را، و سیستم وارد شرایطی شود که تشخیص دقیق مرگ Peer ممکن نباشد. بنابراین اگر mgmt0 استفاده نمی‌شود، VRF اختصاصی Keepalive باید با دقت طراحی شود.

7.8 طراحی VRF اختصاصی برای Peer-Keepalive

راه‌حل صحیح این است که یک VRF مستقل، مثلاً `VRF-PKA`، ساخته شود و روی هر Nexus یک Interface لایه 3 در این VRF قرار گیرد. دو اینترفیس می‌توانند مستقیماً Back-to-Back به هم وصل شوند یا از طریق یک VLAN Transit اختصاصی تنها بین دو Nexus برقرار شوند. این VRF نباید Route عمومی داشته باشد مگر در صورت نیاز بسیار مشخص.

منطق این طراحی آن است که Keepalive فقط باید یک موضوع را تشخیص دهد: آیا Peer زنده است یا نه. بنابراین بهترین طراحی، یک ارتباط ساده، مستقیم، مستقل و کم‌وابستگی است. هرچه این مسیر به زیرساخت‌های بیشتری وابسته باشد، ارزش تشخیصی Keepalive کمتر می‌شود.

7.8.1 اصول طراحی VRF برای Keepalive

اصل	دلیل
VRFاختصاصی فقط برایKeepalive	جلوگیری از تداخل با Data وManagement
رابط لایه 3 مستقل	حذف وابستگی به STP و VLAN کاربر
ترجیحاً لینک مستقیم بین دوNexus	کمینه‌کردنFailure Domain
عدم عبور از FortiGate یاAccess	جلوگیری ازcircular dependency
عدم اشتراک باSSH In-Band	جلوگیری از هم‌بستگی خطاها

7.9 نمونه منطق پیاده‌سازی Peer-Keepalive روی VRF غیر از mgmt0

در این روش، شما روی هر دو Nexus یک VRF می‌سازید، یک اینترفیس Front-Panel را `no switchport` می‌کنید، روی آن IP قرار می‌دهید، سپس در vPC domain، مقصد keepalive را در همان VRF معرفی می‌کنید.

نمونه پیکربندی مفهومی

```
vrf context VRF-PKA

interface Ethernet1/10
  no switchport
  vrf member VRF-PKA
  ip address 10.255.255.1/30
  no shutdown
```

روی Nexus دوم:

```
vrf context VRF-PKA

interface Ethernet1/10
  no switchport
  vrf member VRF-PKA
  ip address 10.255.255.2/30
  no shutdown
```

سپس در vPC domain:

```
vpc domain 10
  peer-keepalive destination 10.255.255.2 source 10.255.255.1 vrf VRF-PKA
```

و روی Nexus مقابل:

```
vpc domain 10
  peer-keepalive destination 10.255.255.1 source 10.255.255.2 vrf VRF-PKA
```

این مدل از نظر طراحی کاملاً معتبر است، به شرط آنکه لینک مذکور واقعاً مستقل از Peer-Link و مستقل از سرویس‌های کاربری باشد. اگر شما همین Keepalive را از داخل یک VLAN مشترک با Data عبور دهید، اگرچه از لحاظ Syntax پیکربندی ممکن است کار کند، اما از منظر طراحی مهندسی انتخاب ضعیفی خواهد بود.

7.10 تفاوت mgmt0 با Front-Panel VRF برای Keepalive

معیار	mgmt0 + management VRF	Front-Panel + VRF اختصاصی
استقلال از Data Plane	بسیار بالا	متوسط تا بالا
وابستگی به Fabric جلویی	ندارد	دارد
مناسب برای Lab	گاهی محدود	بسیار مناسب
مناسب برای Production	بهترین انتخاب	قابل‌قبول با طراحی درست
پیچیدگی عیب‌یابی	کمتر	بیشتر
ریسک هم‌بستگی خرابی	کمتر	بیشتر

7.11 استفاده هم‌زمان از Management VRF و Keepalive VRF

در سناریوی شما، یک طراحی بسیار خوب این است که **دو VRF مجزا** تعریف شود:

- یک VRF برای **مدیریت In-Band**
- یک VRF جداگانه برای **Peer-Keepalive**

این تفکیک باعث می‌شود اگر مشکل در مسیر مدیریت رخ دهد، Keepalive همچنان مستقل باشد، و اگر Keepalive قطع شد، الزاماً به این معنی نباشد که مسیر مدیریت نیز مشکل دارد. این جداسازی برای عیب‌یابی و کاهش خطای تحلیلی بسیار مهم است.

7.11.1 جدول پیشنهادی VRFها

کارایی	VRF	Interface	دلیل طراحی	Best Practice
SSH / SNMP / Syslog / NTP In-Band	VRF-MGMT-INBAND	Routed Portیا SVI	جداسازی مدیریت از User Traffic	فقط از منابع مجاز
Peer-Keepalive	VRF-PKA	Routed Front-Panel Link	استقلال از Peer-Link و Mgmt	فقط بین دو Nexus
OOB Management در صورت وجود	management	mgmt0	بیشترین پایداری	انتخاب ارجح در Production

8. Configuration Cheat Sheet

8.1 تنظیمات پایه vPC

قابلیت	نمونه دستور	هدف
فعال‌سازی feature	feature vpc	فعال‌سازی vPC
vPC domain	vpc domain 10	تعریف دامنه vPC
role priority	role priority 1000	تعیین اولویت نقش
peer-keepalive	peer-keepalive destination x source y vrf VRF-PKA	تشخیص سلامت Peer
peer-link	`vpc peer-link` روی Port-Channel	لینک حیاتی vPC

8.2 تنظیمات Peer-Switch و Peer-Gateway

قابلیت	نمونه دستور	هدف
Peer-Switch	peer-switch	سازگاری STP
Peer-Gateway	peer-gateway	پذیرش محلی MAC های Gateway-style

8.3 تنظیمات Orphan Protection

قابلیت	نمونه دستور	هدف
Auto Recovery	auto-recovery	بازیابی کنترل‌شده پس از Failure
Orphan Port Consideration	طراحی Policy و	جلوگیری از Blackhole
Suspend Behavior	وابسته به سناریو و vPC consistency	توقف سرویس ناسالم

8.4 تنظیمات STP

قابلیت	نمونه دستور	هدف
Root Primary	spanning-tree vlan X priority ...	تثبیتRoot
BPDU Guard	spanning-tree bpduguard enable	محافظتEdge
Root Guard	spanning-tree guard root	جلوگیری ازRoot hijack
Loop Guard	spanning-tree guard loop	جلوگیری از Loop ناشی از BPDU loss
Bridge Assurance	روی لینک‌هایnetwork-type	ایمنی لینک سوئیچ‌به‌سوئیچ

8.5 تنظیمات VRF مدیریت

قابلیت	نمونه دستور	هدف
ساختVRF	vrf context VRF-MGMT-INBAND	جداسازی مدیریت
SVIمدیریتی	`interface vlan XXX` + `vrf member`	SSH/SNMP/NTP
Routed Portمدیریتی	`no switchport` + `vrf member`	مسیر لایه 3 تمیز
Static Route	ip route vrf VRF-MGMT-INBAND ...	مدیریتReachability

8.6 دستورات بررسی و صحه‌گذاری

بررسی	دستور
وضعیتvPC	show vpc
Keepaliveو Role	`show vpc role` / `show vpc peer-keepalive`
Peer-Link	show vpc peer-link
MAC Table	show mac address-table
STP Root/Ports	show spanning-tree
هاVRF Interface	`show vrf` / `show ip interface brief vrf all`
VRFدرRoute	show ip route vrf VRF-PKA
SSH Status	show ssh

9. Validation Checklist

Check Item	Command	Expected Result	Status
vPC domain up	show vpc	Peer adjacency formed	**Failed:**☐ **Successful:**☐
Peer-Link healthy	show vpc peer-link	Up, consistency success	**Failed:**☐ **Successful:**☐
Peer-Keepalive via VRF-PKA	show vpc peer-keepalive	Alive, reachable	**Failed:**☐ **Successful:**☐
Peer-Switch enabled	`show vpc` / running-config	Enabled	**Failed:**☐ **Successful:**☐
Peer-Gateway enabled	running-config / `show vpc`	Enabled	**Failed:**☐ **Successful:**☐
STP Root on vPC pair	show spanning-tree root	Root = Nexus pair design target	**Failed:**☐ **Successful:**☐
Access uplinks forwarding	show spanning-tree root	Correct forwarding state	**Failed:**☐ **Successful:**☐
Orphan ports identified	`show interface status` + topology review	Properly documented	**Failed:**☐ **Successful:**☐
Management VRF reachable	ping vrf VRF-MGMT-INBAND ...	Success	**Failed:**☐ **Successful:**☐
SSH to both Nexuses	`ssh` from jump host	Success and stable	**Failed:**☐ **Successful:**☐
FortiGate HA healthy	FortiGate HA status	Primary/Secondary expected	**Failed:**☐ **Successful:**☐
MAC relearn after failover	show mac address-table	Stable relearn	**Failed:**☐ **Successful:**☐

10. Failover Test Matrix

Scenario	Action	Expected Behavior	Result
Peer-Link failure	Shutdown Peer-Link Port-Channel	vPC protective action, orphan behavior per design	**Failed:**☐ **Successful:**☐
Peer-Keepalive failure only	Cutoff VRF-PKA link	Data remains up, alarm/visibility needed	**Failed:**☐ **Successful:**☐
Primary Nexus reload	Reload NX-Primary	Secondary carries service, vPC recovers after return	**Failed:**☐ **Successful:**☐
Secondary Nexus reload	Reload NX-Secondary	Primary continues service	**Failed:**☐ **Successful:**☐
FortiGate failover	Force HA failover	Gateway MAC/ARP updates, short disruption only	**Failed:**☐ **Successful:**☐
Access main switch failure	Shutdown Access or its uplink	Only that access domain impacted	**Failed:**☐ **Successful:**☐
Orphan switch uplink failure	Shutdown orphan uplink	Complete isolation of orphan switch	**Failed:**☐ **Successful:**☐
DSTR Nexus Failure	Reload NX-DSTR-PRIMARY	Access behind it disconnected	**Failed:**☐ **Successful:**☐
STP inconsistency simulation	Inject BPDU anomaly	Guard feature triggers as designed	**Failed:**☐ **Successful:**☐
SSH via In-Band failure path	Cutoff Management Vlan/Route	OOB absent -> management impact observable	**Failed:**☐ **Successful:**☐

11. Design Best Practices

11.1 Peer-Switch باید فعال باشد

Peer-Switch صرفاً یک بهینه‌سازی نیست، بلکه در طراحی vPC که پایین‌دست آن Access و تجهیز واسط وجود دارد، برای پایداری برداشت STP از Topology ضروری است. بدون آن، پایین‌دست ممکن است دو Peer را از منظر Root behavior یکسان نبیند و در Failureها ناپایداری افزایش یابد.

11.2 Peer-Gateway در مجاورت فایروال ضروری است

در حضور FortiGate به‌عنوان Gateway، احتمال بروز سناریوهایی که ARP، MAC destination و مسیر بازگشت کاملاً هم‌راستا نباشند زیاد است. Peer-Gateway کمک می‌کند هر Nexus رفتار محلی‌تری در فورواردینگ نشان دهد و ترافیک برای رسیدن به Peer دچار Hairpin غیرضروری روی Peer-Link نشود.

11.3 Keepalive را از Data و از Peer-Link جدا نگه دارید

ارزش Peer-Keepalive به استقلال آن است. اگر روی همان زیرساختی قرار گیرد که Data یا Peer-Link را حمل می‌کند، در زمان Failure تشخیص زنده‌بودن Peer مبهم می‌شود. بهترین حالت mgmt0 است، اما اگر ممکن نیست، VRF اختصاصی روی Front-Panel انتخاب درست بعدی است.

11.4 مدیریت In-Band باید VRF مجزا داشته باشد

اگر OOB ندارید، هرگز مدیریت Nexus را در VRF پیش‌فرض و میان VLANهای کاربری رها نکنید. VRF مجزا باعث می‌شود مسیرها، ACLها، سرویس‌ها و عیب‌یابی مدیریتی ساختارمند و امن باشد. این موضوع مخصوصاً وقتی اهمیت دارد که خود Nexusها عضو vPC Pair باشند و Failureهای لایه 2 روی دسترسی مدیریتی اثر بگذارند.

11.5 Orphan را آگاهانه و محدود استفاده کنید

هر Orphan Port یک Trade-Off است. شما سادگی یا اجبار فیزیکی را در ازای کاهش High Availability می‌پذیرید. بنابراین Orphan باید کاملاً مستند، محدود، و در Failure Matrix دیده شود. Orphan برای سرویس‌های حساس یا مسیرهای مدیریتی انتخاب مناسبی نیست مگر با پذیرش صریح ریسک.

12. جمع‌بندی نهایی طراحی

این طراحی از منظر دیتاسنتری یک الگوی معتبر برای اتصال **Access لایه 2** به **FortiGate HA Gateway** از طریق **Cisco Nexus vPC Pair** است. مزیت اصلی آن، حفظ افزونگی و بهره‌وری هم‌زمان در لایه 2 بدون نیاز به STP blocking در Uplinkهای اصلی است. با این حال، این مزیت فقط زمانی واقعاً پایدار و Production-Grade خواهد بود که قابلیت‌های کلیدی vPC به‌درستی فعال و فهمیده شده باشند.

Peer-Switch در این طراحی عملاً الزامی است، زیرا STP در پایین‌دست باید vPC Pair را با رفتاری سازگار و قابل‌پیش‌بینی ببیند. به‌ویژه وقتی یک Nexus واسط نیز در میانه توپولوژی قرار گرفته، نبود Peer-Switch می‌تواند درک ناهماهنگی از Root و Topology ایجاد کند و Failure behavior را نامطمئن سازد.

Peer-Gateway در حضور FortiGate نه‌فقط مفید، بلکه حیاتی است. چون Gateway واقعی روی فایروال قرار دارد و رفتار ARP/MAC در Failover یا در بازگشت ترافیک می‌تواند حساس باشد. Peer-Gateway کمک می‌کند هر Nexus بسته‌هایی را که به‌ظاهر متعلق به MAC سمت Peer هستند به‌صورت محلی بپذیرد و از عبور غیرضروری از Peer-Link جلوگیری شود. این موضوع مستقیماً ریسک Asymmetric Routing و Session Drop روی فایروال را کاهش می‌دهد.

VRF مدیریت یک الزام غیرقابل‌مذاکره است، به‌خصوص اگر مدیریت OOB در دسترس نباشد. SSH زدن به Nexusهای vPC به‌صورت In-Band بدون VRF مجزا، بدون کنترل مسیر برگشت، و بدون ACL/CoPP مناسب، از نظر عملیاتی و امنیتی طراحی ضعیفی خواهد بود. اگر OOB ندارید، باید یک VRF مجزا برای مدیریت In-Band طراحی شود و آن را از Data Plane کاربران جدا نگه دارید.

Orphan Protection نیز در این سناریو اهمیت بالایی دارد، زیرا اکنون بیش از یک Access/Segment به‌صورت Single-Homed در طراحی حضور دارد. Orphan Portها ذاتاً بخشی از مزایای High Availability vPC را دریافت نمی‌کنند و در Failureها می‌توانند باعث Blackhole یا رفتار مبهم شوند. مستندسازی دقیق، محدود نگه‌داشتن دامنه آن‌ها، و پیش‌بینی suspend/protection behavior برای عملیاتی‌شدن این طراحی ضروری است.

تأثیر حالت HA بر طراحی vPC و Uplinkها

نوع پیاده‌سازی FortiGate HA نقش مستقیمی در نحوه طراحی Uplinkها و مدل vPC Grouping در لایه Nexus دارد. در سناریوهای Active-Active، به دلیل مشارکت هم‌زمان هر دو نود در Forwarding، طراحی لینک‌ها معمولاً با تمرکز بر تقارن ارتباطی، توزیع بار، و استفاده هم‌زمان از مسیرهای فعال انجام می‌شود. در این حالت، تجمیع لینک‌ها در قالب ساختارهای مشترک می‌تواند با منطق عملکرد HA هم‌راستا باشد، مشروط بر آنکه الزامات فنی هر دو Vendor به‌درستی رعایت شده باشد.

در مقابل، در سناریوهای Active-Passive، تنها یکی از نودها در هر لحظه مسئول عبور ترافیک است و نود دوم در وضعیت Standby قرار دارد. به همین دلیل، هرگونه ابهام در وضعیت Uplinkها، یا هم‌راستا نبودن رفتار LACP و vPC با منطق Failover فایروال، می‌تواند منجر به بروز اختلال در زمان جابه‌جایی نقش‌ها شود. در چنین شرایطی، استفاده از Uplinkهای

مستقل، Port-Channelهای جداگانه، یا vPC Grouping تفکیک‌شده می‌تواند رفتار طراحی را شفاف‌تر، قابل پیش‌بینی‌تر و از نظر عملیاتی مطمئن‌تر کند.

در این سناریوی مشخص، با توجه به Active-Passive بودن HA و رفتار مشاهده‌شده در زمان Failover، طراحی تفکیک‌شده برای Uplinkها انتخاب شد تا وابستگی‌های مبهم کاهش یابد و کنترل دقیق‌تری بر رفتار ارتباطی نود فعال و نود Standby فراهم شود.

13.نتیجه‌گیری

این بررسی نشان داد که طراحی شبکه‌های دیتاسنتری مبتنی بر Cisco Nexus vPC و FortiGate HA، صرفاً با تکیه بر صحت ظاهری Configuration یا اتصال فیزیکی صحیح قابل جمع‌بندی نیست، بلکه رفتار واقعی اجزای مختلف در سناریوهای خرابی و جابه‌جایی نقش‌ها باید به‌صورت دقیق تحلیل و اعتبارسنجی شود.

در این سناریو، مسئله اصلی از جایی آغاز شد که رفتار LACP و vPC در لایه سوئیچینگ، با منطق عملکرد FortiGate HA در زمان Failover کاملاً هم‌راستا نبود. همین موضوع نشان داد که در طراحی چنین معماری‌هایی، شناخت رفتار مستقل هر Vendor به‌تنهایی کافی نیست و تحلیل برهم‌کنش واقعی آن‌ها اهمیت تعیین‌کننده دارد.

بررسی انجام‌شده همچنین نشان داد که طراحی صحیح توانست وابستگی‌های مبهم را کاهش دهد، رفتار لینک‌های مؤثر را شفاف‌تر کند، و قابلیت پیش‌بینی وضعیت شبکه را در زمان Failover افزایش دهد. این موضوع از منظر پایداری سرویس، سهولت عیب‌یابی، و اطمینان‌پذیری عملیاتی دارای اهمیت مستقیم است.

در نهایت، این سناریو صرفاً در سطح طراحی باقی نمانده و در بستر واقعی نیز پیاده‌سازی و اعتبارسنجی شده است. نتایج این اعتبارسنجی نشان می‌دهد که در صورت رعایت اصول کلیدی طراحی، از جمله Peer-Switch، Peer-Gateway، جداسازی صحیح VRFها، مدیریت مستقل و تحلیل دقیق Orphanها، این معماری می‌تواند به‌عنوان یک الگوی فنی معتبر و قابل اتکا برای استقرارهای عملیاتی مورد استفاده قرار گیرد.

بدین‌وسیله از مهندس عرفان نواب بابت راهنمایی‌ها، تبادل نظرهای فنی و ارائه دیدگاه‌های ارزشمند در فرایند تهیه و تکمیل این سند صمیمانه قدردانی می‌شود. مشارکت و نظرات ایشان نقش مؤثری در بهبود کیفیت فنی این مستند داشته است.

14.منابع رسمی

1. Design and Configuration Guide: Best Practices for Virtual Port Channels (vPC) on Cisco Nexus Series Switches
2. Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide — Configuring vPCs
3. Understand and Configure Nexus 9000 vPC with Best Practices

15.جدول کلمات مخفف

Acronym	Full Form	Description
HA	High Availability	Network design approach that ensures service continuity and minimal downtime during failures.
vPC	Virtual Port Channel	Cisco technology that allows links connected to two different Nexus switches to appear as a single logical port-channel.
STP	Spanning Tree Protocol	Layer-2 protocol used to prevent switching loops by creating a loop-free logical topology.
VRF	Virtual Routing and Forwarding	Technology that allows multiple independent routing tables to coexist on the same device.
MAC	Media Access Control	Hardware address used to uniquely identify a network interface at Layer 2.
ARP	Address Resolution Protocol	Protocol used to map an IP address to its corresponding MAC address.
BPDU	Bridge Protocol Data Unit	STP control frame used to exchange topology information between switches.

SSH	Secure Shell	Cryptographic protocol used for secure remote device management.
OOB	Out-of-Band Management	Dedicated management network used to access devices independently from production traffic.
LACP	Link Aggregation Control Protocol	IEEE protocol used to dynamically create and manage port-channels.
TCN	Topology Change Notification	STP message indicating a change in the Layer-2 topology.
SYN	Synchronize	TCP flag used to initiate a TCP connection.
SYN/ACK	Synchronize / Acknowledgment	TCP response used in the second step of the three-way handshake.
SVI	Switched Virtual Interface	Logical Layer-3 interface associated with a VLAN.
ACL	Access Control List	Set of rules used to filter network traffic.
AAA	Authentication Authorization Accounting	Security framework controlling device access and logging activities.
NTP	Network Time Protocol	Protocol used to synchronize clocks across network devices.