کتاب

CCNA (Data Center)
DCICT & DCICN
Fast Track

به زبان فارسی

CCNA Data Center

Fast Track

نویسنده:
مهندس ابوالفضل هاشمی

به نام خدا

CCNA Data Center
Fast Track

مهندس ابوالفضل هاشمی

a.hashemi70@gmail.com

Introduction – ۱

دوره CCNA DC یکی از دوره‌های شرکت سیسکو است. این دوره هیچ پیش‌نیازی ندارد و برای افرادی که قصد گرفتن مدرک CCNA DC را دارند و یا افرادی که می‌خواهند از Data Center اطلاعاتی داشته باشند مفید است. CCNA DC شامل دو زیر مجموعه Introducing Cisco Data Center Networking (DCICN) و Introducing Cisco Data Center Networking Technologies (DCICT) است.

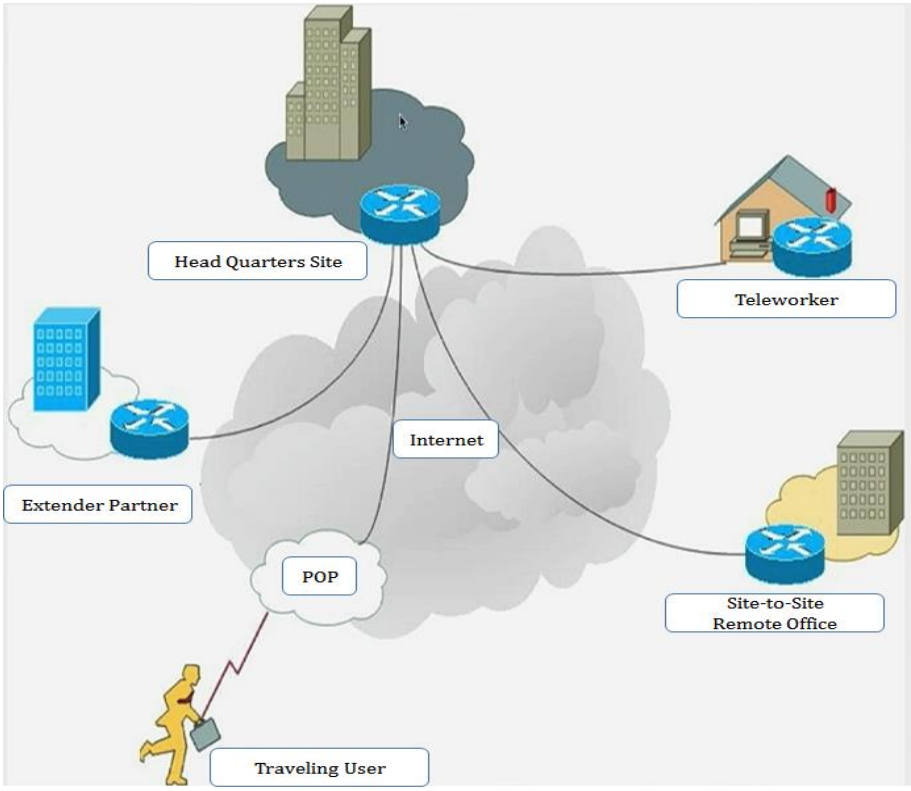
در مجموعه DCICN، مباحث عملکرد شبکه، مدل ارتباطی Host-to-Host، استانداردهای ارتباطی و اتصالات Ethernet، مفاهیم لایه TCP/IP Transport و IP، پردازش تحویل بسته و عملکرد Switch، آشنایی با سیستم‌عامل NX-OS، کار با سیستم‌عامل NX-OS، VLAN و Trunk، توپولوژی افزونگی Switch، IPv4 Subnetting، IPv6 Transition و تبدیل IPv4 به IPv6، پروتکل‌های Routing، ACL و امنیت آنها شرح داده می‌شود.

در مجموعه DCICT، مباحث تجهیزات سخت‌افزاری و قابلیت‌های نرم‌افزاری در مرکز داده شرح داده می‌شود. این مباحث شامل لایه‌های مرکز داده، تجهیزات Nexus، تجهیزات MDS، مشاهده و بررسی Switchهای Nexus، Fabric path، Virtual Port Channel (vPC)، Overlay Transport Virtualization (OTV)، Virtual Device Context (VDC)، Fabric Extender (FEX)، مجازی‌سازی منبع ذخیره‌سازی، مجازی‌سازی سرور، مجازی‌سازی شبکه Nexus 1000v Switch، انواع ذخیره‌سازها در مرکز داده، Fabric Channel (FC) و مقایسه آن با Fiber Channel over Ethernet (FCoE)، تجهیزات Unified Computing System (UCS) و مقایسه آنها، Blade Server و پروفایل‌های سرویس UCS هستند.

افرادی که توانایی استفاده از تجهیزات این دوره را ندارند می‌توانند از نرم‌افزارهایی مانند GNS3، EVE-NG و دیگر موارد استفاده نمایند. این نرم‌افزارها تجهیزاتی مانند Nexus 7000 و Nexus 9000 را شبیه‌سازی می‌کنند. همچنین نرم‌افزار UCS Platform Emulator برای شبیه‌سازی تجهیزات UCS قابل استفاده است.

Introduction to Network -۲

دلیل ایجاد شبکه برای برقرار کردن ارتباط بین سیستم‌ها از جمله سرویس‌دهنده‌ها و سرویس گیرنده‌ها است. هدف از به وجود آمدن شبکه به اشتراک‌گذاری اطلاعات است. در شکل زیر در قسمت Head Quarters Site ممکن است اتاق سرور و یا مرکز داده وجود داشته باشد. این سایت از طریق اینترنت ممکن است به کاربران در حال سفر، کارمندان اداری از راه دور و مشتریان دیگر سرویس دهد.به طور مثال Site-to-Site remote Office ممکن است از پروتکل VPN برای اتصال استفاده نماید.



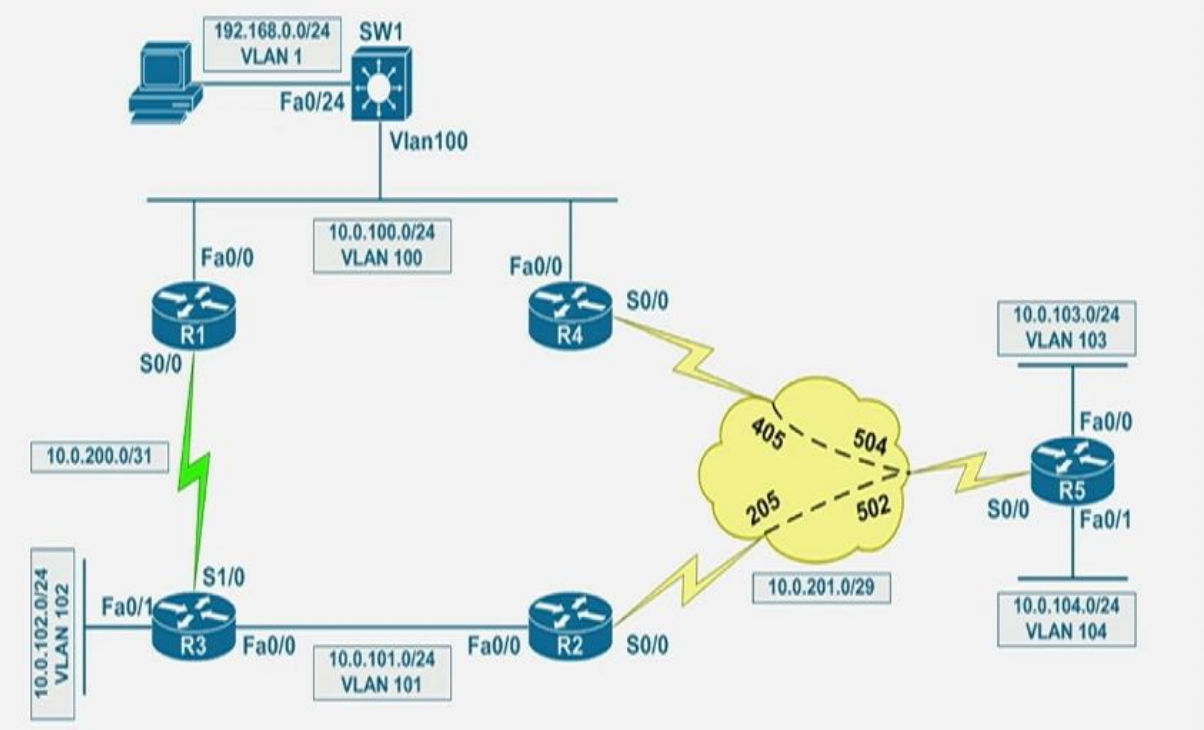
Physical Components of a Network -۱-۲

مؤلفه‌های شبکه شامل موارد زیر هستند:

۱. کامپیوتر یا MAC: کاربران آخر یا End User بیشتر از کامپیوتر یا MAC استفاده می‌کنند.
۲. Network Interface Card (NIC): هر دستگاه برای ورود به شبکه به کارت شبکه نیازمند است.
۳. Switch: این دستگاه چندین پورت دارد که دستگاه‌های دیگر را به هم متصل می‌کند.
۴. Router: وظیفه Routerی و یا ارتباط بین VLANها را برعهده دارد. ممکن است یک Switch لایه سه باشد. این دستگاه ممکن است وظیفه ارتباط با خارج از شبکه را نیز برعهده داشته باشد.

در شکل زیر کامپیوتر شماره ۱ از طریق Switch به VLAN شماره ۱ متصل است. پورت بعدی این Switch به VLAN شماره ۱۰۰ متصل شده است. از طریق این VLAN به دو Router که هر یک به شبکه دیگر متصل شده است، ارتباط دارد. Router سمت چپ از طریق پورت سریال که Point-to-Point است، به Router دیگر

متصل شده است. Router سمت راست از طریق دستگاه Frame Relay که Point-to-Multi Point به شبکه دیگر متصل شده است.



۲-۲- Sharing of Resources

به اشتراک‌گذاری در شبکه ممکن است یکی از موارد زیر باشد:

۱. به اشتراک‌گذاری می‌تواند شامل برنامه‌ها باشد. مانند E-mail، Data Base، Web Service و یا موارد دیگر باشد.
۲. اشتراک‌گذاری ممکن است دستگاه Printer باشد.
۳. ممکن است دستگاه ذخیره‌ساری به اشتراک‌گذاشته شود. دستگاه ذخیره‌سازی می‌تواند Network Attached Storage (NAS) که براساس File است و از پروتکل FTP یا CIFS استفاده می‌شود باشد. یا می‌تواند Storage Area Network (SAN) که بر اساس Block است باشد.
۴. ممکن است یک دستگاه Backup که از Tape استفاده می‌کند به اشتراک گذاشته شود.

۲-۳- Application Interactions

ارتباط برنامه‌ها با یکدیگر در شبکه می‌تواند یکی از موارد زیر باشد:

۱. Batch Application: این برنامه‌ها نیازمند پهنای‌باند است ولی این پهنای‌باند اهمیت زیادی ندارد. مانند FTP.
۲. Interactive Application: در این نوع برنامه‌ها زمان پاسخ دهی مهم است ولی حیاتی نیست. مانند Data Base Update.

۳. Real Time Application: تأخیر در این برنامه‌ها مهم و حیاتی است. مانند Voice.

۲-٤- Network Characteristics

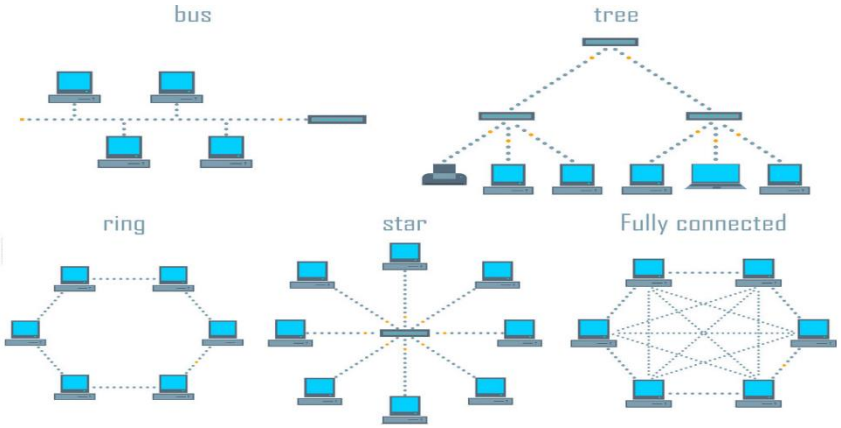
مشخصات یک شبکه ممکن است یکی از موارد زیر باشد:

۱. Availability: دسترسی‌پذیری اندازه‌گیری میزان UP Time است. این مدت زمان را می‌توان با Resiliency یا انعطاف‌پذیری و Redundancy یا افزونگی افزایش داد.
۲. Scalability: مقیاس‌پذیری در واقع پتانسیل رشد شبکه است. شبکه به گونه‌ای باید طراحی شود که با رشد کاربرها، سرورها و ... خللی در عملکرد شبکه پیش نیاید. بطور مثال با افزایش یک اسلات به Switch، تعداد سرورها را افزایش داد. این یک اصل در طراحی شبکه است.
۳. Reliability: قابلیت اطمینان به میانگین زمان برای تعمیر و رفع خرابی گویند.
۴. Security: حفاظت از اطلاعات یک اصل مهم در شبکه است. این نیز یک اصل در طراحی شبکه است.
۵. Speed: سرعت یا نرخ جابه‌جایی داده است. معمولاً اتصال Switchها به یکدیگر یا Up Link ممکن است 1GB، 10GB، 40GB و یا بیشتر باشد.
۶. Cost: هزینه‌ها در شبکه ممکن است هزینه سرمایه‌گذاری CapEx و یا هزینه عملیاتی یا OpEx باشد.

۲-۵- Network Topologies

توپولوژی یا ساختار شبکه می‌تواند یکی از موارد زیر باشد:

۱. Bus: در این نوع شبکه پهنای‌باند بین دستگاه‌ها به اشتراک گذاشته می‌شود.
۲. Star: در این نوع ساختار یک Switch چندین دستگاه را به هم متصل می‌نماید.
۳. Extended Star: در این نوع ساختار تعدادی Switch، تعدادی دستگاه دیگر را به یکدیگر متصل می‌نماید.
۴. Wireless: در این نوع ساختار یک Access Point تعدادی کاربر را بصورت بیسیم پشتیبانی می‌کند.



Host-to-Host Communications -۶-۲

مدل‌های اولیه ارتباط Host-to-Host وابسته به شرکت سازنده تجهیزات بوده است. تجارت و تکنولوژی شرکت‌های سازنده را به سمت نوآوری برای مطابقت تجهیزات با شرکت‌های دیگر سوق داد. یکی از دلایل ایجاد مدل Open Systems Interconnection (OSI) این امر می‌تواند باشد. هدف از ایجاد مدل OSI می‌تواند یکی از عوامل زیر باشد:

۱. یکی از اهداف ایجاد مدل OSI کاهش پیچیدیگی است.
۲. این مدل ارتباط بین شرکت‌های سازنده و اینترفیس‌ها را استاندارد می‌کند.
۳. باعث ایجاد مهندسی ماژولار گردید.
۴. قابلیت همکاری بین چندین سازنده وجود دارد.
۵. نوآوری ترویج داده شد.
۶. آموزش و یادگیری ساده‌تر شد.

OSI Model -۷-۲

این مدل از هفت لایه تشکیل شده است که به ترتیب از لایه یک پایین‌ترین لایه تا لایه هفت بالاترین لایه توضیح داده می‌شود.

Physical Layer -۱-۷-۲

لایه فیزیکی یا Physical Layer لایه یک مدل OSI است. در این لایه عملکرد شبکه و پردازش‌های مکانیکی و الکترونیکی برای فعال‌سازی، تعمیرات و غیرفعال‌سازی تعریف می‌شود. کابل‌های فیزیکی و قطعات سخت‌افزاری مانند Hub، Network Interface Card (NIC) و Host Bus Adapter (HBA) که مربوط به سیستم ذخیره‌سازی می‌شود در این لایه قرار دارند. در این لایه وابستگی الکترونیکی و ارسال باینری وجود دارد.

Data Link -۲-۷-۲

چگونگی فرمت‌بندی داده برای ارسال و کنترل شبکه و جریان در طول مسیر وجود دارد. در این لایه تشخیص خطا و تکنولوژی نحوه دسترسی به رسانه از طریق سیم، بیسیم و ... در این لایه صورت می‌گیرد. در این لایه Switch و آدرس MAC کارایی دارند.

Network -۳-۷-۲

ارسال بسته‌های Routerی، آدرس دهی IPv4 و IPv6، انتخاب بهترین مسیر برای ارسال بسته در این لایه صورت می‌گیرد. Routerها یا routers در این لایه کارآمد هستند.

Transport ۲-۷-٤

وظیفه رسیدگی ارسال بین برنامه‌ها با استفاده از پورت‌های TCP و UDP را بر عهدا دارد. این لایه مطمئن می‌شود که ارسال بسته بصورت مطمئن و یا نامطمئن صورت گرفته است. وظیفه دیگر این لایه ایجاد، حفظ و خاتمه یک حلقه مجازی ارتباطی بین میزبان‌ها است.

Session ۲-۷-۵

این لایه وظیفه ایجاد، مدیریت و خاتمه جلسه و همچنین همگام‌سازی گفت‌وگو بین برنامه‌ها و هاست‌ها را برعهده دارد.

Presentation ۲-۷-٦

این لایه وظیفه فرمت‌بندی، ساختاردهی و گفت‌وگوی نحوه ارسال داده را برعهده دارد. همچنین این لایه مطمئن می‌شود که داده‌ای که از سیستم دریافت شده است قابل خواندن باشد. رمزگذاری نیز در این لایه صورت می‌گیرد.

Application ۲-۷-۷

این لایه سرویس شبکه را برای پردازش برنامه فراهم می‌سازد. احراز اصالت کاربران در این لایه صورت می‌گیرد. برنانمه‌ها می‌تواند E-mail، اشتراک‌گذاری فایل و یا فراهم نمودن محیط دسترسی مانند ترمینال یا SSH باشد.

تجهیزات نیازدارند تا فقط به لایه خودشان اهمیت دهند و این دلیل استفاده از مدل چند لایه‌ای OSI است. بطور مثال یک سرویس‌دهنده وب اهمیت نمی‌دهد که بسته از طریق سیم و یا بیسیم ارسال می‌شود و یا Switch اهمیت نمی‌دهد که آدرس دهی بصورت IPv4 و یا IPv6 است.

Protocol Data Unit ۲-۸-

هر لایه برای ارتباط با لایه دیگر باید از یک فرمت خاص برای بسته‌بندی استفاده نماید که به این فرمت Protocol Data Unit (PDU) گفته می‌شود.

Encapsulation ۲-۸-۱

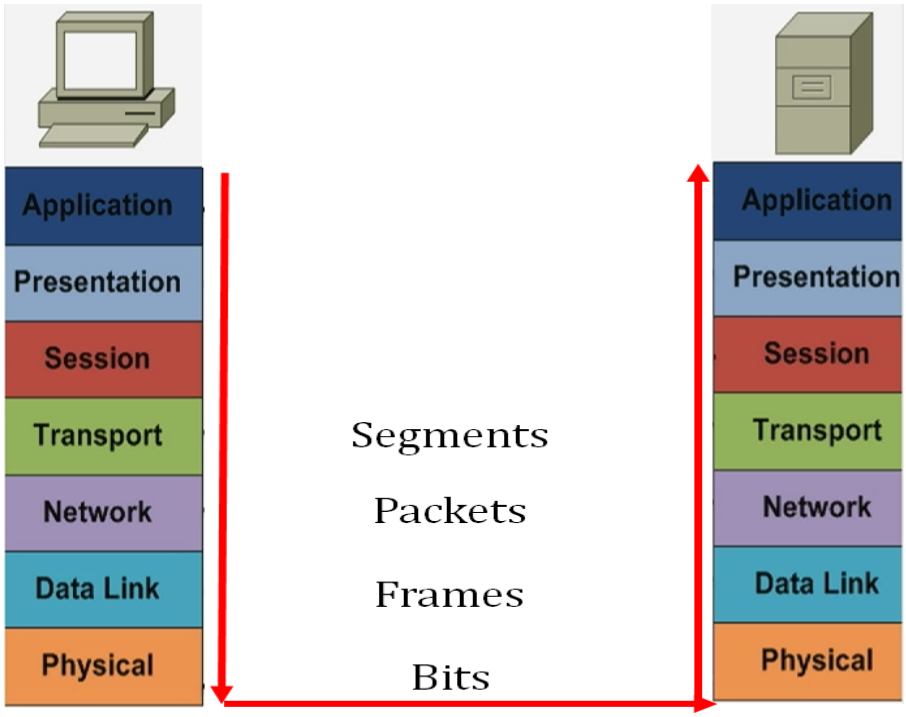
به عملیات اضافه نمودن فرمت خاصی از داده در قالب PDU برای ارسال به یک میزبان Encapsulation گفته می‌شود. وقتی داده از لایه بالا به پایین OSI انتقال می‌یابد این عملیات صورت می‌گیرد. در واقع لایه بالایی داده‌ای به داده اصلی اضافه می‌نماید و آن را به لایه پایینی ارسال می‌کند. اگر داده جدیدی که به داده اصلی اضافه می‌شود در جلوی داده اصلی قرار گیرد Header و اگر در پشت داده اصلی قرار گیرد Trailer گفته می‌شود. روند Encapsulation تا زمان ارسال به لایه فیزیکی ادامه می‌یابد.

Decapsulation ۲-۸-۲

به عملیات حذف فرمت داده اضافی در قالب PDU هنگام دریافت از یک میزبان Decapsulation گفته می‌شود. وقتی داده از لایه پایین به بالا OSI انتقال می‌یابد و هر لایه Header و یا Trailer مربوط به خود را حذف می‌کند. در واقع لایه پایینی فرمت مخصوص به خود را حذف می‌کند و بسته را به لایه بالایی انتقال می‌دهد. روند Decapsulation تا زمان ارسال به لایه کاربردی ادامه می‌یابد.

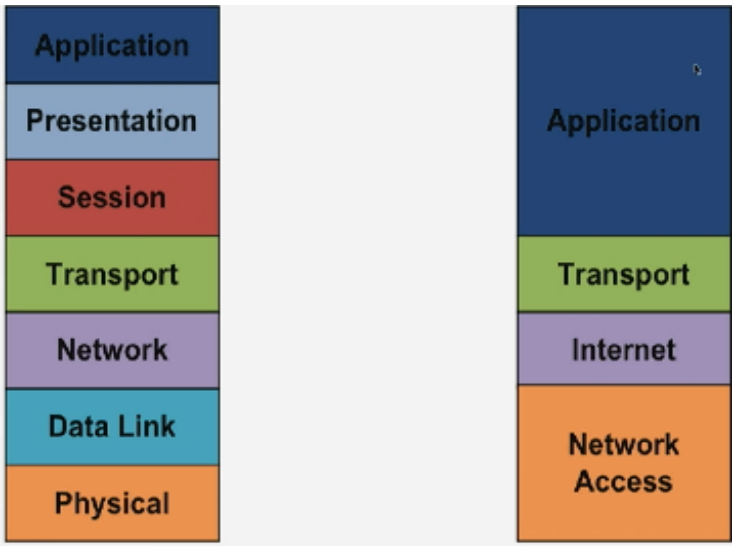
هر لایه PDU و نام مربوط به خود را دارد. به PDU لایه انتقال Segment، لایه شبکه Packet، لایه پیوند داده Frame و به لایه فیزیکی Bit گفته می‌شود.

در ارتباط نظیربه‌نظیر شکل زیر نحوه ارسال یک داده از یک طرف به طرف دیگر نمایش داده شده است.



TCP/IP Model ۲-۹-

مدل Transmission Control Protocol (TCP) / Internet Protocol (IP) شبیه مدل OSI است با این تفاوت که چهار لایه دارد. شکل زیر نشان‌دهنده قالب این پروتکل است.



Ethernet Connections ۲-۱۰-

ارتباط Ethernet از طریق کارت شبکه(NIC)، یک درگاه(Connector) و یک کابل(Cable) صورت می‌گیرد. در جدول زیر بعضی از استانداردها آورده شده است.

10/100 Ethernet Media			
Standard	Cable	Connector	Distance
10BASE-2	RG-58 Coax	BNC	185M
10BASE-5	RG-50 Coax	AUI	500M
10BASE-T	Cat 3	RJ-45	100M
10BASE-TX	Cat 5	RJ-45	100M
100BASE-FX	MMF	SC, ST, LC, MTRJ	400M

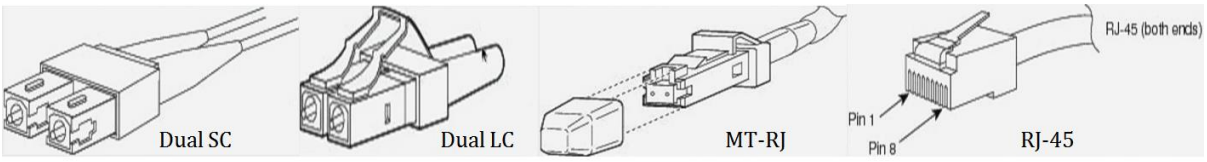
در جدول بالا سطر اول و دوم مربوط به کابل‌های Coaxial است. سطر سوم و چهارم کابل‌های مسی زوج به هم تابیده و در سطر آخر کابل‌های فیبر نوری Multi-Mode Fiber است. درگاه‌ها برای هر کابل متفاوت است و هر استاندارد فاصله خاصی را پشتیبانی می‌کند. در جدول زیر می‌توان 1G Ethernet را مشاهده نمود.

1G Ethernet Media			
Standard	Cable	Connector	Distance
1000BASE-SC	Twinax	DE-9 or 8P8C	25M
1000BASE-SX	MMF	Dual LC	200-500M
1000BASE-LX	MMF	Dual LC	550M
1000BASE-T	Cat 5	RJ-45	100M
1000BASE-TX	Cat 6a	RJ-45	100M

کابل‌های Twinax پر هزینه هستند و معمولاً داخل و یا بین رک استفاده می‌شوند. کابل‌های Cat 6a از محبوبیت زیادی برخوردار هستند و قیمت مناسبی دارند. در جدول زیر 10G Ethernet قابل مشاهده است.

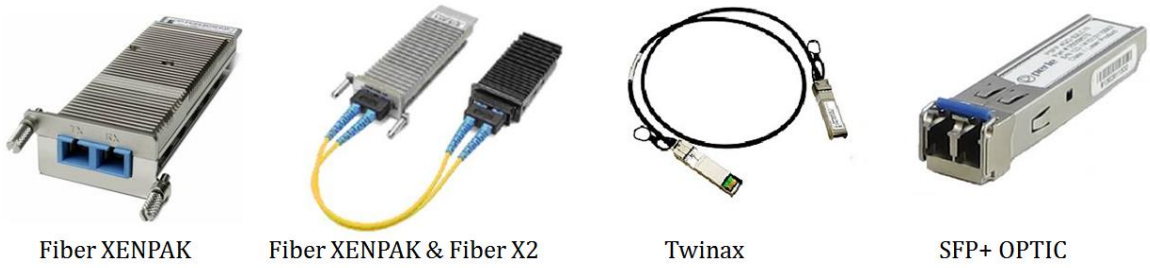
1G Ethernet Media			
Standard	Cable	Connector	Distance
10GBASE-SR	MMF	Dual LC / SC	26-300M
10GBASE-LR	SMF	Dual LC	10Km
10GBASE-CX4	CX4	Infiniband 4X	15M
10GBASE-T	Cat 6a	RJ-45	100M
10GBASE-T	Twinax (Passive)		1-5M
10GBASE-T	Twinax (Active)		7-10M

کابل‌های فیبر Single-Mode Fiber فواصل بسیار طولانی را نسبت به Multi-Mode Fiber پشتیبانی می‌کنند. ارتباطات یا Ethernet Connections در شکل زیر نمایش داده شده‌اند.



در شکل زیر انواع درگاه‌های یک گیگی یا 1G Transceivers نمایش داده شده است.

در شکل زیر انواع درگاه‌های ده گیگی یا 10G Transceivers نمایش داده شده است.



اختصار تجهیزات بالا بصورت Gigabit Interface Converter (GBIC)، Small Form-factor Pluggable (SFP)، Mechanical Transfer Registered Jack (MT-RJ)، Standard Connector (SC)، Lucent Connector (LC) است.

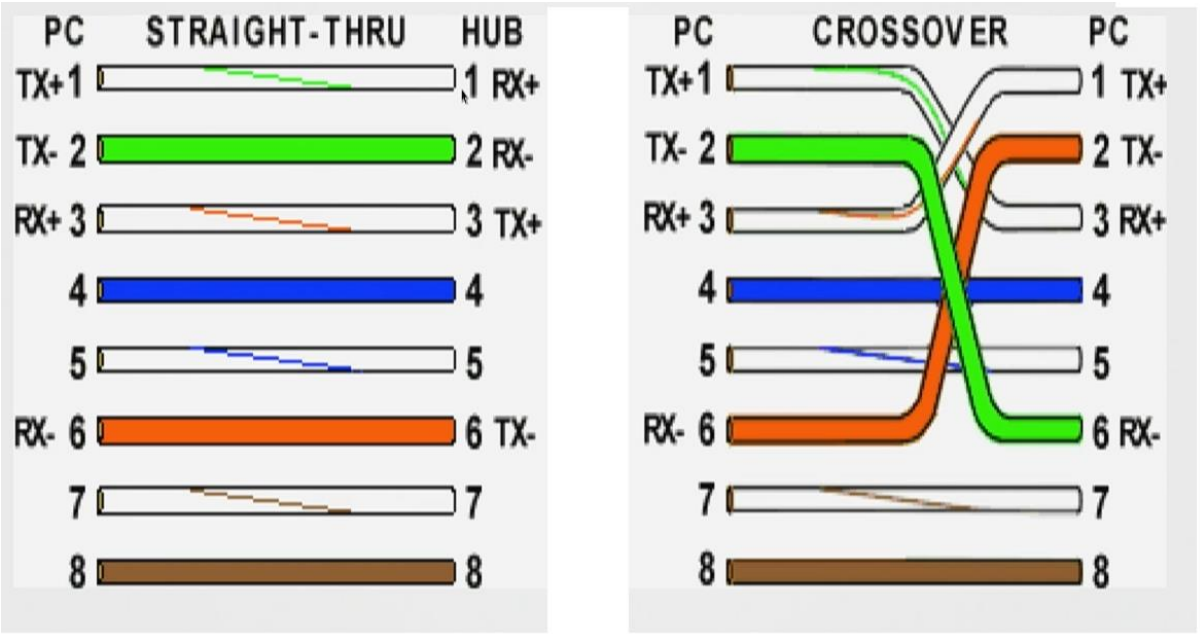
کابل‌های قدیمی هزینه بالایی نسبت به کابل‌های جدید دارند. کابل‌های زوج به هم تابیده بدون روکش یا Unshielded Twisted Pair که سرعت آنها بین 10Mbps تا 1Gbps است، هزینه نسبتاً پایینی دارند. این کابل‌های بین ۱ تا ۱۰۰ متر را پشتیبانی می‌کنند. به این نوع کابل‌ها با متراژ کوتاه Patch Cord گفته می‌شود که معمولاً در یک رک یا بین رک استفاده می‌شود. این نوع کابل‌ها از ۸ سیم که ۴ زوج سیم به هم تابیده است تشکیل شده‌اند. رنگ‌های این کابل‌ها استاندارد و به رنگ نارنجی، سبز، آبی و قهوه‌ای است. ۴ سیم دیگر ترکیب رنگ سفید و این رنگ‌ها است. انواع کابل‌های UTP در ادامه شرح داده می‌شود.

۱. Cat1: این کابل استاندارد برای سیم‌های تلفن است. داده برروی آن ارسال نمی‌شود و از درگاه RJ-11 برای ارتباط استفاده می‌شود.
۲. Cat3: این کابل نیز برای تلفن است و داده ارسال نمی‌شود ولی سرعت آن تا 10Mbps است و به نام 10Base-T شناخته می‌شود.
۳. Cat5: از این کابل به بعد برای ارسال داده است و سرعت آن تا 100Mbps است.
۴. Cat5e: این کابل نیز برای داده است و تا سرعت 1Gbps را پشتیبانی می‌کند.
۵. Cat6: این کابل تا سرعت 1Gbps را پشتیبانی کرده و از سیم مسی 24-gauge استفاده می‌کند.

۶. Cat6a: این کابل عملکرد زیادی در برابر نویزهای بالا دارد و سرعت آن تا 10Gbps است.

RJ-45 Jack Plug RJ-45 Jack Face

کابل‌های UTP بصورت Straight و یا Crossover هستند. کابل‌های Straight برای ارتباط بین Switch و Router و یا بین Switch یا Hub و کامپیوتر و سرور است. کابل‌های Crossover بین Switch و Switch، Router و Router، کامپیوتر و کامپیوتر، Hub و Hub، Router به کامپیوتر و Switch به Hub است. در واقع باید طرف دیگر از نوع کابل پشتیبانی کند. بعضی از تجهیزات شرکت سیسکو نوع کابل را تشخیص داده و با توجه به آن سیم ارسال و دریافت را انتخاب می‌کند که به این قابلیت Auto Medium Dependent Interface (MDI-X) گویند.



Local Area Network ۲-۱۱-

Local Area Network (LAN) به شبکه محلی گفته می‌شود که این شبکه می‌تواند کوچک در حد یک Switch و چند کامپیوتر باشد. همچنین می‌تواند بزرگ در حد چند Switch یا Router و تعداد بسیاری کامپیوتر باشد.

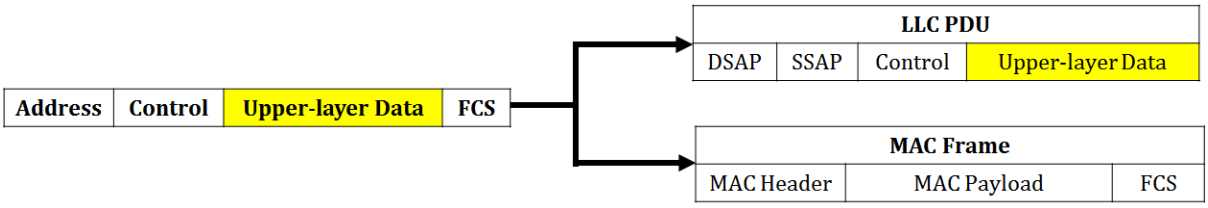
اجزای یک شبکه LAN می‌تواند شامل کامپیوترهای شخصی و سرویس‌دهنده، ارتباطات داخلی مانند کارت شبکه و رسانه‌های دیگر، تجهیزات شبکه مانند Switch و Router و پروتکل‌ها مانند Ethernet، Internet Protocol (IP)، Dynamic Host Configuration Protocol (DHCP) و Address Resolution

Protocol (ARP) باشد. کارایی و استفاده از یک شبکه LAN می‌تواند دسترسی به داده‌ها را فراهم کند، منابع دستگاه‌های I/O مانند پرینتر را به اشتراک بگذارد، ارتباط بین اینترنت و شبکه‌های دیگر را فراهم کند.

در تعریف Ethernet می‌توان گفت یک خانواده‌ای از تکنولوژی یا پروتکل‌های شبکه‌های کامپیوتری است که در شبکه‌های محلی، کلان‌شهری و یا شبکه‌های وسیع استفاده می‌شود. تاریخچه Ethernet در جدول زیر قابل مشاهده است.

Year	Activity
1973	Ethernet invented at Xerox
1982	DIX release 10Mbps Ethernet (Version II)
1983	IEEE approves 802.3 (10Base-5)
1985	IEEE approves 802.3a (10Base-2)
1990	IEEE approves 802.3i (10Base-T)
1995	IEEE approves 802.3u (10Base-TX)
1998	IEEE approves 802.3z (1Gbps)
2002	IEEE approves 802.3ae (10Gbps)
2010	IEEE approves 802.3ba (40Gbps & 100Gbps)

در جدول بالا DIX به معنی Digital Intel and Xerox است. در 10Base-5 و 10Base-2 از کابل‌های Coaxial و 10Base-T از کابل مسی استفاده می‌شود. پروتکل Ethernet برای دولایه فیزیکی و پیوند داده برای کابل و سیگنال استفاده می‌شود. در داخل Ethernet استاندارد IEEE 802.3 نهفته است. این استاندارد خود به دو زیرلایه تقسیم می‌شود. زیرلایه Logical Link Control (LLC) ارتباط بین لایه بالاتر یعنی IP و زیرلایه زیرین یعنی MAC را برعهده دارد. زیرلایه Media Access Control (MAC) وظیفه دسترسی به لایه فیزیکی را برعهده دارد.



داخل Ethernet یک پروتکل دسترسی به رسانه به نام Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) وجود دارد. وظیفه این پروتکل مدیریت سیگنال در داخل شبکه، با استفاده از شنود لینک، دسترسی چندگانه و تشخیص برخورد است. با استفاده از این پروتکل هر زمان می‌توان از لینک برای ارسال داده استفاده نمود، ولی قبل از آن ایستگاه‌ها تشخیص می‌دهند که شبکه توسط ایستگاه دیگری در حال استفاده نباشد. اگر شبکه در حال استفاده بود CSMA/CD منتظر می‌ماند. در صورتیکه شبکه در حالت سکوت باشد CSMA/CD داده را ارسال می‌کند. اگر دو ایستگاه چیزی شنود نکنند و هر دو در یک زمان داده ارسال نمایند برخورد ایجاد می‌شود. پس از برخورد ایستگاه‌ها مجدد داده را ارسال می‌کنند.

Ethernet Frame ۲-۱-۱۱-

قالب یک Ethernet Frame در شکل زیر امده است:

Ethernet Frame Format					
Preamble 8 Byte	Destination MAC Address 6 Byte	Source MAC Address 6 Byte	Type/Length 2 Byte	Payload 46-1500 Byte	Frame Check Sequence (FCS) 4 Byte

در Ethernet Type II از EtherType برای شناسایی پروتکل لایه بالاتر استفاده می‌شود و لی در Ethernet 802.3 از Length برای مشخص نمودن طول داده استفاده می‌شود. همچنین در 802.3 از Start Of Frame (SOF) برای محدود کردن شروع Frame مقدار 1 Byte از Preamble گرفته می‌شود. در 802.3 اطلاعات پروتکل زیرلایه LLC را بین Length و Payload ذخیره می‌کند. این اطلاعات شامل Destination Service Access Point (DSAP)، Source Service Access Point (SSAP) و LLC CTL است.

Network Connections ۲-۱۲-

انواع ارتباطات در شبکه بصورت یکی از موارد زیر است:

۱. Unicast: ارسال نمودن Frame از طرف یک میزبان به یک میزبان دیگر را ارسال Unicast گویند. در این ارسال فقط آدرس MAC میزبان مقابل در آدرس گیرنده قرار می‌گیرد.
۲. Broadcast: ارسال نمودن Frame از طرف یک میزبان به همه میزبان‌های دیگر را ارسال Broadcast گویند. در این ارسال آدرس MAC Broadcast در آدرس گیرنده قرار می‌گیرد.
۳. Unicast: ارسال نمودن Frame از طرف یک میزبان به یک گروه میزبان دیگر را ارسال Multicast گویند. در این ارسال آدرس MAC Multicast گروه در آدرس گیرنده قرار می‌گیرد.

Ethernet Address ۲-۱۳-

آدرس Ethernet یا همان آدرس MAC بروی کارت شبکه توسط سازنده آن الحاق می‌شود. به این آدرس الحاق Burned-in Address یا BIA نیز گویند. آدرس MAC از دو قسمت 24 Bit که در کل 48 Bit است تشکیل شده است. 24 Bit اول از سمت چپ به نام Organizational Unique Identified (OUI) است که از آدرس آن می‌توان اطلاعاتی از سازنده بدست آورد. 24 Bit دوم یا سمت راستی به نام Vendor-Assigned است.

Cisco UCS MACC Address = 00:25:B5:00:11:00

با استفاده از دستور ipconfig در سیستم‌عامل ویندوز و ifconfig در سیستم‌عامل لینوکس می‌توان این آدرس و اطلاعات کارت شبکه را مشاهده نمود.

با استفاده از دستور ping می‌توان از صحت برقراری ارتباط بین دو دستگاه مطمئن شد. برگشت این دستور شامل مدت زمان ارسال و دریافت بسته، Time To Live (TTL) و حجم بسته است. قابلیت‌های دستور ping در زیر آورده شده است:

۱. t–: این قابلیت برای ارسال بی‌نهایت بسته ping است. تا زمانی که دستور توقف (Ctrl+c) وارد نشود این بسته‌ها ارسال و جواب برگردانده می‌شود. بصورت پیش‌فرض ۴ بسته ارسال می‌شود.
۲. l–: با استفاده از این قابلیت حجم بسته یا Maximum Transmission Unit (MTU) را می‌توان مشخص نمود.
۳. f–: در صورتیکه بسته‌ها از حجم معینی بیشتر باشند، بعضی از تجهیزات آنها را به حجم‌های استاندارد تکه تکه و ارسال می‌نمایند. این قابلیت از تکه‌تکه شدن بسته‌ها جلوگیری می‌نماید.
۴. a–: این قابلیت نام آدرس دستگاه مقابل را نمایش می‌دهد.

دستور tracert مسیر ارسال بسته را نقطه به نقطه نمایش می‌دهد.

۰دستور arp جدول Address resolution Protocol را نمایش می‌دهد. این پروتکل وظیفه بدست آوردن آدرس MAC و IP دستگاه‌ها را برعهده دارد و در جدولی ذخیره می‌کند. در برگشت این دستور آدرس‌های

```
                ›ping 192.168.1.1 -l 1300 -f

Pinging 172.29.8.1 with 1300 bytes of data:
Reply from 172.29.8.1: bytes=1300 time<1ms TTL=255
Reply from 172.29.8.1: bytes=1300 time<1ms TTL=255
Reply from 172.29.8.1: bytes=1300 time<1ms TTL=255
Reply from 172.29.8.1: bytes=1300 time=6ms TTL=255

Ping statistics for 172.29.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

                 >arp  -a

Interface:              --- 0xb
  Internet Address      Physical Address      Type
                        00-00-0c-9f-f2-a7     dynamic
                        40-55-39-08-51-41     dynamic
                        6c-9c-ed-45-b7-41     dynamic
                        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

               .>tracert

Tracing route to                  over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms
  2    <1 ms    <1 ms    <1 ms
  3    10 ms    11 ms    10 ms
  4    10 ms    10 ms    10 ms
  5    10 ms    10 ms    10 ms
  6    12 ms    12 ms    12 ms
  7    10 ms    10 ms    10 ms

Trace complete.
```

Static و Dynamic قابل مشاهده است. با استفاده از قابلیت s- می‌توان ردیف جدیدی به جدول بصورت دستی اضافه نمود. با استفاده از قابلیت d- می‌توان آن آدرس را حذف نمود.

IP Addressing -۱٤-۲

عملکرد و کارایی آدرس‌های IP در لایه سه مدل OSI است. پروتکل IP یک پروتکل غیر اتصال‌گرا است، بدین معنی که اگر مقصد آماده دریافت نباشد، یا مقصد وجود نداشته باشد یا خطایی رخ دهد بسته از سمت مبدأ به سمت مقصد ارسال می‌شود. در واقع از رسیدن بسته به مقصد اطمینانی حاصل نمی‌شود. پروتکل IP از یک ساختار سلسله مراتبی برای آدرس‌دهی استفاده می‌کند. این سرویس‌دهی بصورت انتخاب بهترین تلاش یا Best Effort است و هیچ ضمانتی برای آن وجود ندارد. ضمانت این سرویس برعهده لایه‌های بالاتر است. این پروتکل از هیچ ابزاری برای ترمیم داده در صورت وجود خطا استفاده نمی‌کند و بسته پس از دریافت توسط مقصد به مبدأ ارسال می‌شود. آدرس IP یک آدرس دیجیتالی یا منطقی یکتا است که در شبکه تعریف می‌شود. این آدرس شامل 32 Bit است که بصورت خودکار یا دستی قابل تنظیم است. این آدرس به شکل صفر و یک یا باینری است. خواندن این آدرس به این شکل سخت است که برای راحتی آن را به نقطه دسیمال یا Dotted Decimal تبدیل می‌کنند. این تبدیل بصورت ۴ قسمت ۸ بیتی بین ۰ تا ۲۵۵ است.

Binary	Decimal
11000000.10101000.00000001.00000001	192.168.1.1

آدرس IP از دو قسمت آدرس شبکه (Network) و آدرس میزبان (Host) تشکیل شده است. آدرس شبکه و میزبان بصورت سلسله مراتبی هستند. بطور مثال آدرس شبکه مانند شماره خیابان اصلی است و آدرس میزبان مانند شماره پلاک خانه است. در واقع برای آدرس دهی ابتدا باید شماره خیابان و سپس شماره خانه وارد شود.

IP Address Classes -۱-۱٤-۲

آدرس IP به ۵ کلاس A، B، C، D و E تقسیم می‌شود. برای شناسایی نوع کلاس از ۴ بیت ابتدایی آن از سمت چپ به راست استفاده می‌شود.

Class Name	Start With Binary	Start With Decimal	Network Bit	Host Bit
A	0xxxxxxx	0 – 127	8 Bit	24 Bit
B	10xxxxxx	128 – 191	16 Bit	16 Bit
C	110xxxxx	192 – 223	24 Bit	8 Bit
D	1110xxxx	224 – 239	Reserved	
E	1111xxxx	240 – 255	Reserved	

کلاس‌های A، B و C برای استفاده شبکه و میزبان هستند. کلاس‌های D و E برای آدرس‌های چند پخشی و پروتکل‌های خاص استفاده می‌شود. کلاس A برای شبکه‌های بزرگ، کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک استفاده می‌شود. اگر این کلاس‌ها از قانون گفته شده در جدول برای آدرس شبکه و میزبان استفاده کنند، Classful نامیده می‌شوند. اگر از این قانون پیروی نشود و از IP Subnetting استفاده

شود، Classless نامیده می‌شود. آدرس Mask، آدرسی است که مشخص می‌کند کدام قسمت Network و کدام قسمت Host باشد یا به عبارتی چند بیت برای شبکه و چند بیت برای میزبان استفاده شود. در آدرس‌دهی Classful بصورت زیر Mask تعریف می‌شود.

Classful Name	Default Mask
A	255.0.0.0/8
B	255.255.0.0/16
C	255.255.255.0/24

IP Subnetting ۲-۱٤-۲

اگر در آدرس‌دهی IP، مدیر شبکه قسمت مربوط به میزبان یا Host را به یک زیر مجموعه از آدرس‌ها که مورد نیاز است تقسیم کند به این تقسیم کردن IP Subnetting گویند. در واقع به معنی قرض گرفتن قسمتی از آدرس میزبان و اضافه کردن آن به آدرس شبکه است. نتیجه این تبدیل آدرس، بیشتر شدن تعداد آدرس‌های شبکه و کمتر شدن آدرهای میزبان است. دو آدرس در هر زیر شبکه غیز قابل استفاده است. یکی آدرس شبکه و دیگری آدرس ارسال همه پخشی یا Broadcast است. این عمل با نام Variable length Subnet Masking (VLSM) نیز شناخته می‌شود.

Classful	Classless
Network Address = 192.168.1.0 / 24 11000000.10101000.00000001.xxxxxxxx Network = 24 Bit Host = 8 Bit First Host = 192.168.1.1 Last Host = 192.168.1.254	192.168.1.0 / 26 11000000.10101000.00000001.00xxxxxx Network = 26 Bit Host = 6 Bit First Host = 192.168.1.1 Last Host = 192.168.1.62

همانطور که گفته شد از سه کلاس اول برای آدرس‌دهی در شبکه استفاده می‌شود. به آدرس‌هایی که برای استفاده از اینترنت استفاده می‌شوند عمومی یا Public و به آدرس‌هایی که بصورت محلی برای شبکه‌های داخلی استفاده می‌شود خصوصی یا Private گویند. در جدول‌های زیر آدرس‌های عمومی و خصوصی آمده است.

Class	Public Range
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

آدرس 127.x.x.x رزرو شده برای Loopback و تست شبکه است.

Class	Private Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255

C	192.168.0.0 to 192.168.255.255

باید توجه داشت که می‌توان از کلاس آدرس‌های محلی متفاوت در یک شبکه استفاده نمود. بطور مثال یک سمت شبکه از کلاس C و یک سمت دیگر از کلاس B استفاده نمود.

Dynamic Host Configuration Protocol (DHCP) -۳-۱٤-۲

وظیفه این پروتکل آدرس‌دهی بصورت خودکار به میزبان است. پروتکل DHCP با استفاده از قابلیت‌ها می‌تواند آدرس IP، Subnet Mask، Default Gateway، DNS Server و تنظیمات دیگر را برای میزبان ارسال نماید. DHCP را می‌توان برروی Router نیز تنظیم نمود. این پروتکل توسعه یافته پروتکل Bootstrap (BooTP) است. هر دو پروتکل وظیفه آدرس‌دهی خودکار به میزبان در شبکه را دارند. این پروتکل در لایه Application قرار دارد و از پورت‌های UDP 67, 68 استفاده می‌نماید و ساختار کلاینت سروری دارد. بسته‌های DHCP و مراحل آن بصورت زیر است:

۱. DHCP Discover: ابتدا کلاینت درخواست DHCP Discover را بصورت broadcast ارسال می‌کند. این بدان معنی است که به جست‌وجوی سرور برای دریافت آدرس می‌پردازد.
۲. DHCP Offer: سپس سرور پاسخ DHCP Offer را ارسال می‌کند. در واقع سرور به کلاینت تنظیمات را پیشنهاد می‌دهد.
۳. DHCP Request: بعد از آن کلاینت درخواست DHCP Request را به دو دلیل ارسال می‌کند، یکی برای مشخص کردن یک سرور از بین چند سرور و دیگری درخواست برای گرفتن آدرس IP.
۴. DHCP Acknowledge: در آخر سرور پاسخ DHCP Acknowledge را ارسال و برای کاربر تنظیم می‌کند.

Dynamic Name Service (DNS) -٤-۱٤-۲

این پروتکل برای ترجمه آدرس‌های IPv4 و IPv6 به نام و بالعکس است. سیستم نامگذاری سلسله مراتبی دارد. بطور اصلی به عنوان سرویس‌دهنده Berkeley Internet Name Domain (BIND) پیاده‌سازی می‌شود. حدود ۷۰٪ از سرویس‌دهنده‌های DNS از BIND استفاده می‌کنند.

Transport Layer -۱۵-۲

وظایفی که لایه چهارم برعهده دارد می‌توان به موارد زیر اشاره نمود:

۱. Session Multiplexing: این لایه با استفاده از پورت‌های TCP و UDP می‌تواند چندین جلسه برگزار نماید.
۲. Segmentation: با استفاده از پروتکل TCP می‌تواند بسته‌های تقسیم شده را به هم متصل نماید.

۳. Flow Control: کنترل جریان در لایه‌های دیگر به شکل‌های متفاوتی صورت می‌گیرد. در این لایه به این صورت است که پروتکل TCP مطمئن می‌شود که ترافیک بصورت end-to-end خیلی سریع فرستاده نشود و در دو طرف یکسان باشد.
۴. Connection Oriented: در واقع پروتکل TCP یک ارتباط پایدار end-to-end ایجاد می‌کند. از 3 way handshake برای این عمل استفاده می‌شود.
۵. Reliability: این وظیفه موقعی که نیاز باشد، هنگام خطا در Segment توسط پروتکل TCP صورت می‌گیرد و Segment دوباره ارسال می‌شود.

۲-۱۵-۱- Transmission Control Protocol (TCP)

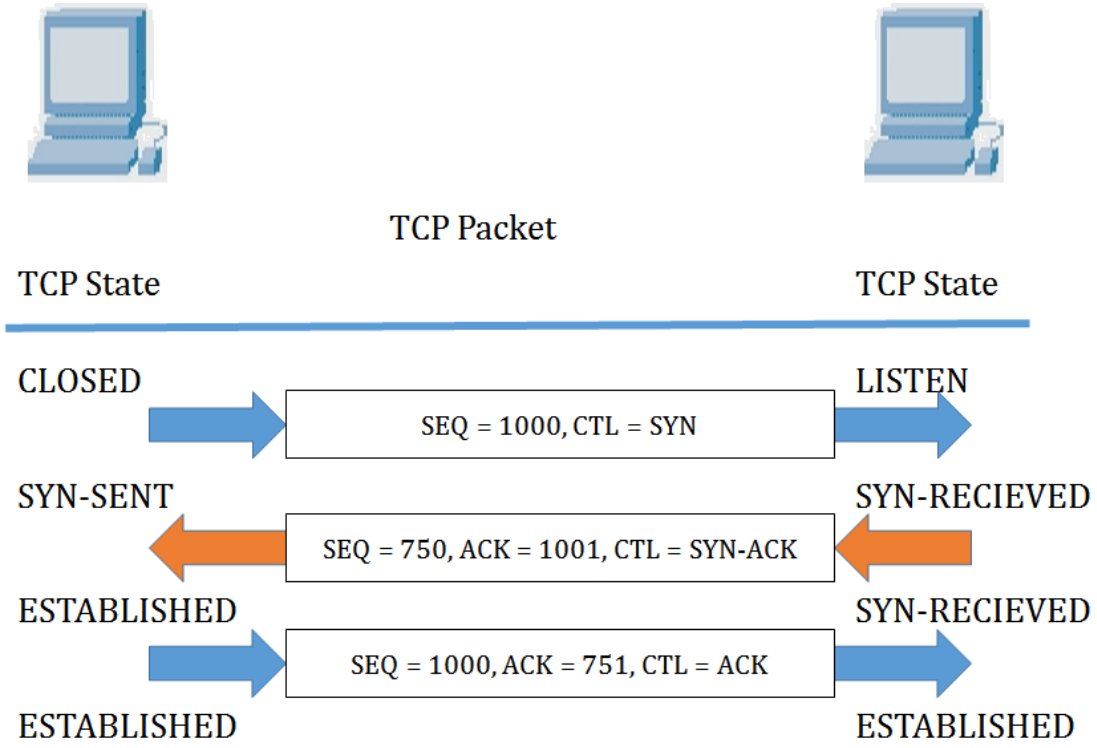
پروتکل TCP یک پروتکل مطمئن در لایه چهارم است. این پروتکل از صف بندی (Sequencing) و تأیید بسته‌ها (Acknowledgment) استفاده می‌کند. زمانی که فرستنده داده‌ای را ارسال می‌کند به این داده یک شماره صف اختصاص می‌دهد. گیرنده پس از دریافت، یک شماره تأییدیه و یک شماره صف که فرستنده انتظار آن را دارد ارسال می‌کند. این روند برای تشخیص از بین رفتن داده یا عدم ترتیب درست آن مفید است. پروتکل‌هایی مانند Email استفاده از SMTP port 25، Web استفاده از HTTP port 80 و SSH استفاده از port 22 نمونه‌هایی از TCP هستند. سربار یا هدر TCP بصورت جدول زیر است.

<table>
<tr><td colspan="4">TCP Header</td></tr>
<tr><td colspan="3">Destination Port
16 Bit</td><td>Source Port
16 Bit</td></tr>
<tr><td colspan="4">Sequence Number
32 Bit</td></tr>
<tr><td colspan="4">Acknowledgment Number (if ACK set)
32 Bit</td></tr>
<tr><td>Data Offset</td><td>Reserved
3 Bit</td><td>Control Bit</td><td>Windows Size
16 Bit</td></tr>
<tr><td colspan="3">Urgent
16 Bit</td><td>Checksum
16 Bit</td></tr>
<tr><td colspan="4">Options (if data offset > 5. Padded at the end with "0" bytes if necessary)
0-32 Bit</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Control Bit می‌تواند به معنی Setup، Congestion، Termination و ... باشد. Windows Size یک شماره است که باید دستگاه‌ها بین هم توافق نمایند. Checksum برای بررسی خطا در داده و سربار است. Urgent نشان دهنده انتهای داده ضروری است. Options حداکثر اندازه TCP-SEQ است. اندازه Data بستگی به لایه بالاتر دارد و ممکن است متغیر باشد.

TCP 3 Way Handshake ۲-۱-۱-۱۵

برای برقرار ارتباط در TCP، ابتدا کاربر بسته‌ای را به نام SYN که شامل شماره صف است برای سرویس‌دهنده ارسال می‌کند. سرویس دهنده بسته را دریافت و پاسخ آن را به نام SYN-ACK که شامل شماره صف کاربر و شماره تأییدیه خودش است را ارسال می‌نماید. کاربر پس از دریافت بسته SYN-ACK، بسته ACK را به نشان تأیید ارسال می‌کند. بعد از این سه مرحله کاربر و سرویس‌دهنده می‌توانند ترافیک داده را انتقال نمایند.



Flow Control ۲-۱-۱-۱۵-۲

کنترل جریان از سرریز شدن فضای صف یا Buffer جلوگیری می‌کند. زمانی که فرستنده ارسال انجام می‌دهد، گیرنده در صورت عدم آمادگی پیام Not Ready ارسال می‌نماید تا فرستنده ارسال را متوقف کند. زمانی که Buffer گیرنده آماده دریافت باشد پیام Ready از سمت گیرنده به فرستنده ارسال می‌شود و فرستنده ارسال را ادامه می‌دهد.

TCP Acknowledgment ۲-۱-۱-۱۵-۳

پروتکل TCP در فرستنده صفی از Segmentها را دارد تا در صورت رسیدن Acknowledgment آنها را ارسال نماید. بسته ACK از سمت فرستنده به گیرنده ارسال می‌شود تا فرستنده بسته‌ای را که گیرنده منتظر آن است را ارسال نماید. در بسته ACK شماره ACK وجود دارد که این شماره برابر با SEQ+1 است.

TCP Windowing ۲-۱-۱-۱۵-٤

در پروتکل TCP، پنجره‌بندی برای ارسال داده تنظیم و ثابت نگه می‌دارد تا از ازدحام یا از بین رفتن داده جلوگیری نماید. اگر اندازه پنجره ۴ باشد، به معنی این است که فرستنده می‌تواند چهار Segment را بدون دریافت ACK ارسال نماید. در صورت گرفتن ACK چهارتای بعدی را ارسال می‌کند.

User Datagram Protocol (UDP) ۲-۱۵-۲

این پروتکل نیز در لایه چهارم است. پروتکل UDP یک پروتکل نامطمئن یا Connectionless و بر مبنای بهترین تلاش یا Best Effort است. بدین معنی است که بهترین تلاش بر مبنای ترافیک فعلی، تأخیر، از بین رفتن بسته و ... را برای ارسال بسته انجام می‌دهد ولی تضمینی برای دریافت و ترتیب آن ندارد. این پروتکل دسترسی به لایه شبکه را بدون سربار فراهم می‌کند. این پروتکل سریع و سبک است، تشخیص و بررسی خطا ندارد، ابزاری برای ترمیم داده ندارد و از شماره صف و تأییدیه استفاده نمی‌کند. بررسی موارد گفته شده به عهده برنامه کاربردی است. پروتکل‌هایی مانند SNMP استفاده از port 161، TFTP استفاده از port 69 و DNS استفاده از port 53 (البته در DNS ممکن است از TCP نیز استفاده شود) نمونه‌هایی از UDP هستند. بطور مثال در پروتکل SNMP اگر بسته Set فرستاده شود، نمی‌توان مطمئن شد که آیا این بسته تنظیم شده است یا خیر. سربار یا هدر UDP بصورت جدول زیر است. اندازه Data بستگی به لایه بالاتر دارد و ممکن است متغیر باشد.

UDP Header	
Destination Port 16 Bit	Source Port 16 Bit
Length 16 Bit	Checksum 16 Bit
Data	

Mapping IP Layer to Transport Layer ۲-۱۵-۳

سربار یا هدر پروتکل IP در لایه سوم از شماره پروتکل برای مشخص نمودن پروتکل لایه بالاتر یا Upper Layer Protocol (ULP) که قرار است به لایه چهارم برود استفاده می‌کند. بطور مثال اگر شماره پروتکل برابر ۶ باشد به معنی این است که IP باید بسته را به TCP و اگر شماره پروتکل ۱۷ باشد به معنی این است که IP باید بسته را به UDP در لایه چهارم بسپارد.

Mapping Transport Layer to Application Layer ۲-۱۵-٤

همانطور که گفته شد اگر از TCP Port 20,21 استفاده شود، به معنی این است که از برنامه کاربردی FTP استفاده شده است. برای دیگر برنامه‌ها نیز بدین شکل است و پورت استفاده شده نشان دهنده نوع برنامه است. Internet Assigned Numbers Authority (IANA) در رابطه به تخصیص پورت‌ها استانداردی را طراحی نموده است. طبق این استاندارد پورت‌های ۰ تا ۱۰۲۳ برای برنامه‌های شناخته شده، ۱۰۲۴ تا ۴۹۱۵۱ برای برنامه‌های تعریف شده توسط کاربر و ۴۹۱۵۲ تا ۶۵۵۳۵ برای استفاده متغیر در طول جلسه ارتباطی استفاده می‌شود.

Packet Delivery Process ۲-۱٦

فرآیند تحویل بسته یا Packet Delivery Process به نحوه تحویل بسته در لایه دو شبکه اشاره دارد. همانطور که توضیح داده شده در لایه یک Ethernet و NIC وجود دارد. در لایه دو دستگاه‌هایی مانند NIC، Bridge و Switch وجود دارد. همچنین آدرس MAC نیز در لایه دو قرار دارد. در لایه سه شبکه نیز دستگاه‌هایی مانند Router و Switch Layer 3 وجود دارد. در لایه سه نیز از پروتکل IP برای آدرس‌دهی استفاده می‌شود.

میزبان‌ها باید در رابطه با این که کدام آدرس IP به کدام آدرس MAC اختصاص دارد اطلاعاتی جمع‌آوری کنند و آن را در داخل جدولی ذخیره نمایند تا بتوانند با استفاده از آن بسته لایه دو ایجاد نمایند. پروتکل ARP به میزبان‌ها کمک می‌کند تا آدرس IP نگاشت شده به آدرس MAC را بدست آورند. این پروتکل اینگونه عمل می‌کند که میزبان درخواست کننده آدرس MAC، آدرس IP را در داخل Ethernet Frame با آدرس همه پخشی FFFF:FFFF:FFFF قرار می‌دهد و آن را ارسال می‌کند. به این بسته ARP Request گویند. موقعی که میزبانی آدرس IP خود را در داخل بسته مشاهده می‌کند با استفاده از بسته ARP Reply پاسخ می‌دهد که آدرس MAC درخواستی آدرس من است و آدرس خود را ارسال می‌کند. نحوه عملکرد ARP زمانی که باید Routerی صورت گیرد کمی متفاوت است. اگر آدرس IP دو میزبان در داخل یک شبکه باشند، طبق روال قبل این عمل انجام می‌شود. در غیر اینصورت بسته ARP Request به default gateway یا Router پیش‌فرض ارسال می‌شود. این Router به دلیل این که میزبان داخل یک شبکه دیگر است و باید بسته را به اینترفیس دیگری منتقل کند، یک بسته Ethernet Frame جدید ایجاد می‌کند و آن را با توجه به جدول Routerی خود ارسال می‌کند. این روند تا زمانی که به شبکه مقصد برسد بصورت Hop-By-Hop انجام می‌شود. در نهایت گیرنده مورد نظر بسته را دریافت و پاسخ را به Router مورد نظر خود می‌دهد. Router نیز بسته را بصورت بازگشتی به همان Router اولیه ارسال می‌کند و بسته در نهایت به مبدأ اصلی ارسال می‌شود.

۳- Introduction to Switch

در این بخش اطلاعات و مطالب مربوط به Switch در مرکز داده توضیح داده می‌شود و به مفهوم و عملکرد Switch و سپس به اطلاعات مختصری مربوط به Nexus Switch پرداخته می‌شود.

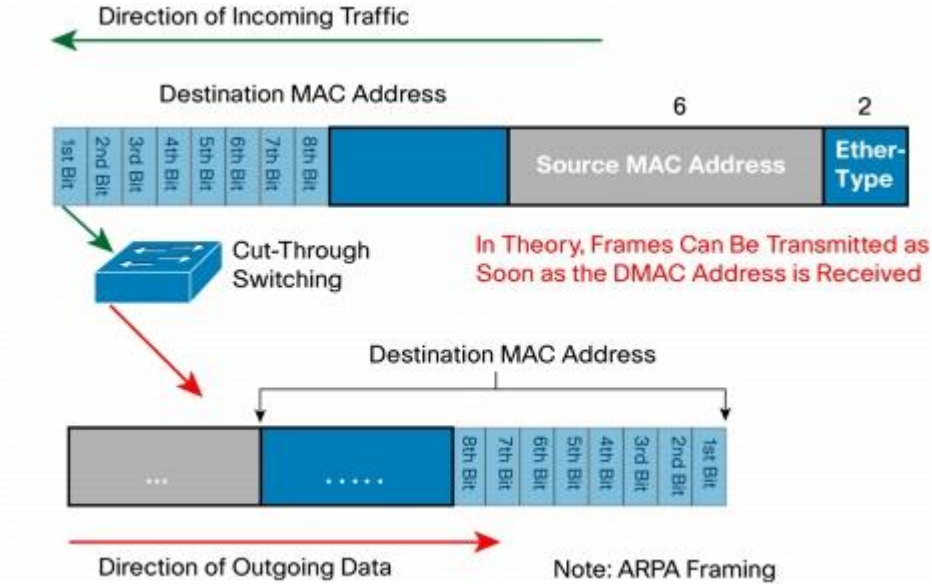
۳-۱- Introduction

در قسمت LAN معمولاً از کابل‌های ۱۰۰ متر استفاده می‌شود. این کابل‌ها می‌تواند از نوع Cat 5 یا Cat 5e و یا بالاتر باشد. برای افزایش یا گسترش شبکه یا برای جابه‌جایی داده می‌توان از Hub و یا Switch استفاده نمود. در شبکه‌های قدیمی از Hub و در شبکه‌های مدرن از Switch استفاده می‌شود. در قسمت LAN زمانی که از Hub استفاده شود، پهنای‌باند به اشتراک گذاشته می‌شود. در Switch هر پورت از پهناب‌باند جداگانه‌ای استفاده می‌شود. اگر از Hub استفاده شود از تعداد بسیاری دستگاه و متعاقباً از پهنای‌باند اشتراکی بیشتری استفاده می‌شود که در نتیجه به دلیل گسترش شبکه Collision Domain نیز افزایش می‌یابد. اگر از Switch استفاده شود Collision Domain نیز کاهش می‌یابد، زیرا برروی هر پورت فقط یک Collision اتفاق می‌افتد. در Switch در واقع اگر هر پورت تنها به یک سیستم متصل باشد Collision رخ نمی‌دهد. بطور مشابه با گسترش شبکه Network Congestion اتفاق می‌افتد، زیرا باید حجم داده بسیاری در شبکه انتقال یابد.

اگر به یک لایه بالاتر نگاه شود، Bridge قرار دارد. Bridge باهوش‌تر از Hub است. این دستگاه می‌تواند عمل Forwarding، Filter و Flood را انجام دهد. این دستگاه می‌تواند بین LANهای مختلف Buffering یا فضای صف اختصاصی ایجاد کند. این دستگاه همچنین Collision Domainها را افزایش می‌دهد. زیرا هر پورت از Bridge یک Collision Domain را ایجاد می‌کند. همچنین این دستگاه جدول آدرس MAC را در خود ذخیره و از آن برای ارسال Frame استفاده می‌کند. Bridge از تعداد پورت کمی پشتیبانی می‌کند.

اگر پیشرفته‌تر نگاه شود Switchها قابلیت‌های بیشتری دارند. Switchها علاوه بر کارایی Bridge از پورت‌های بیشتری نیز پشتیبانی می‌کند. تعداد این پورت‌ها ۲۴ یا ۴۸ و یا ۵۰۰ می‌تواند باشد. Switchها نیز Forwarding، Filter و Flood انجام می‌دهند و جدول MAC را در خود ذخیره می‌کنند. علاوه بر این از فضای Frame Buffer بزرگ، انتقال بسته بین Switch ها و Back Plane و سرعت 1Gbps تا 100Gbps پشتیبانی می‌کنند.

روش‌های ارسال Frame در Switch می‌تواند به دو صورت Cut-Through یا Store-and-Forward باشد. در Cut-Through دستگاه Switch بدون آنکه منتظر دریافت کامل Frame شود، به محض دیدن آدرس MAC مقصد، هر چه را دریافت کرده است، ارسال می‌کند. خطا در این مورد بررسی نمی‌شود. شکل زیر نشان دهنده روش Cut-Through است.



در روش Store-and-Forward دستگاه Switch منتظر دریافت همه Frame می‌ماند و آنها را ذخیره می‌کند. پس از دریافت کامل Frame آن را به آدرس MAC مقصد ارسال می‌کند. در این روش خطا بررسی می‌شود.

روش‌های ارتباطی در Switch می‌تواند Unicast، Multicast و Broadcast باشد. زمانی که یک Frame وارد Switch می‌شود، آدرس مبدأ در جدول MAC ذخیره می‌شود و این را به خاطر می‌سپارد که این آدرس مربوط به این پورت است. در ارسال Unicast زمانی که Frame به پورت Switch وارد می‌شود، اگر آدرس مبدأ و مقصد برروی یک پورت باشد آن را حذف می‌کند، زیرا Switch آن را حلقه تشخیص می‌دهد و به این

عمل Filtering گویند. اگر آدرس مبدأ و مقصد متفاوت باشد آن را برروی پورت مقصد ارسال می‌کند و به این عمل Forwarding گویند. اگر آدرس مقصد برای Switch ناشناخته باشد آن را برای همه پورت‌ها به غیر از مبدأ ارسال می‌کند و به این Flooding گویند. در روش Broadcast همانند روش ناشناخته، Frame برای همه پورت‌ها به غیر از مبدأ ارسال می‌شود.

معمولاً گروه کاربران بر مبنای محل فیزیکی آنها تعریف می‌شود. اگر تعداد کاربران به گونه‌ای افزایش یابد که Switch قابلیت پشتیبانی آن را نداشته باشد و یا نیاز به پورت‌ها بیشتری احساس شود، باید یک Switch دیگر به شبکه اضافه نمود. Switchهای داخل شبکه باید از طریق کابل به یکدیگر متصل شوند. برای اتصال روش‌های متفاوتی بطور مثال Stack وجود دارد. باید توجه داشت بین Switchها باید از لینک با سرعت بالاتری استفاده نمود.

۳-۲- Nexus Switch

در این بخش به نحوه Boot شدن و دستورات ابتدایی سیستم Nexus Switch پرداخته می‌شود.

در ابتدا برای مشاهده صفحه Switch باید از طریق کابل Console به پورت Console سیستم مورد نشر متصل شد. پس از اتصال در هنگام Boot شدن، یک سری بررسی‌ها صورت می‌گیرد و بعد از آن از کاربر خواسته می‌شود که تنظیمات را بصورت خودکار از DHCP دریافت کند یا تنظیمات را دستی وارد نماید. اگر حالت دستی انتخاب شود سوال‌های متعددی جهت تنظیم پرسیده می‌شود که در زیر به توضیح هر یک پرداخته می‌شود. در هنگام Boot شدن سیستم از دو Image در سیستم‌های Nexus استفاده می‌شود. یک فایل به نام kickstart و دیگری به نام system است. فایل kickstart فایل سبک و کم حجمی است که برای Load شدن ابتدایی سیستم به کار برده می‌شود و پس از آن برای تنظیمات، سیستم‌عامل اصلی به نام system اجرا می‌شود که این سیستم سنگین‌تر و بزرگتر است.

حافظه‌هایی که در این Switchها وجود دارد در زیر شرح داده شده است:

۱. Flash: این حافظه برروی آن سیستم‌عامل سیسکو است. می‌توان آن را به‌روزرسانی نمود و با خاموش یا روشن شدن تغییری نمی‌کند.
۲. Random-Access Memory (RAM): برروی این حافظه تنظیمات در حال اجرای سیستم قرار دارد و مانند حافظه کامپیوتر اگر ذخیره نشود اطلاعات آن هنگام خاموش و روشن شدن از بین می‌رود. با دستور show running-config می‌توان آن را مشاهده نمود.
۳. Non-Volatile Random-Access Memory (NVRAM): برروی این حافظه تنظیمات سیستم قرار دارد و اطلاعات آن هنگام خاموش و روشن شدن از بین نمی‌رود. با show startup-config می‌توان آن را مشاهده نمود. برای انتقال RAM به NVRAM از دستور copy running-config startup-config استفاده می‌شود.

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

پرسیده می‌شود آیا پیغام تنظیمات در ادامه نشان داده شود که برای تنظیم از yes استفاده می‌شود.

Do you want to enforce secure password standard (yes/no) [y]: yes

Create another login account (yes/no) [n]: yes

Enter the User login Id: cisco

Enter the password for "cisco":

Confirm the password for "cisco":

Enter the user role [network-operator]:

در دستورات بالا کاربر، پسورد و نقش آن تعریف می‌شود.

Configure read-only SNMP community string (yes/no) [n]: no

Configure read-write SNMP community string (yes/no) [n]: no

در دستورات بالا تنظیمات مربوط به SNMP وارد می‌شود.

Enter the switch name: N7K

در دستور بالا نام دستگاه وارد می‌شود.

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: yes

Mgmt0 IPv4 address: 192.168.1.10

Mgmt0 IPv4 netmask: 255.255.255.0

در دستورات بالا پورت مدیریتی Mgmt0 تنظیم می‌شود. این پورت برای مدیریت سیستم است و عملیات Routing، Switching و ... برروی آن انجام نمی‌شود.

Enable the http-server? (yes/no) [y]: n

Configure clock? (yes/no) [n]: n

Configure timezone? (yes/no) [n]: n

Configure summertime? (yes/no) [n]: n

Configure the ntp server? (yes/no) [n]: n

Configure default switchport interface state (shut/noshut) [shut]:

Configure default switchport trunk mode (on/off/auto) [on]:

Configure default switchport port mode F (yes/no) [n]:

Configure default zone policy (permit/deny) [deny]:

Enable full zoneset distribution? (yes/no) [n]:

Configure default zone mode (basic/enhanced) [basic]:

دستورات بالا بخشی از تنظیمات است که بنا به نیاز شبکه وارد می‌شود.

```
The following configuration will be applied:
password strength-check
switchname N7K
no feature ssh
no feature telnet
system timeout congestion-drop default mode F
system timeout congestion-drop default mode E
no feature http-server
system default switchport shutdown
system default switchport trunk mode on
no system default zone default-zone permit
no system default zone distribute full
no system default zone mode enhanced
Do you like to edit the configuration? (yes/no) [n]:
Exiting the basic config setup.
```

در آخر تأییدیه برای انجام تغییرات پرسیده می‌شود.

برای پاک نمودن تنظیمات می‌توان از دستور write erase استفاده نمود.

دستور pwd نشان دهنده مسیری است که کاربر در آن محل دستورات را وارد می‌نماید.

```
N7K# pwd
bootflash:
N7K#
```

دستور dir فایل‌های موجود در مسیر فعلی را نمایش می‌دهد. بطور مثال فایل‌های kickstart و system در مسیر bootflash را نشان می‌دهد.

```
n7k-kickstart.7.3.0.D1.1.bin
n7k-.7.3.0.D1.1.bin
```

با وارد نمودن کاراکتر ? می‌توان از دستورات موجود در همان خط فرمان کمک گرفت و اطلاعات مربوط به آن را مشاهده نمود. با وارد نمودن کلید tab می‌توان از قابلیت کامل نمودن خودکار دستور استفاده نمود.

بطور مثال برای به‌روزرسانی نسخه سیستم‌عامل Nexus از دستور زیر می‌توان استفاده نمود.

```
N7K# copy ftp://anonymouse@192.168.1.50/n7k- kickstart-7.4.bin bootflash: ?
  bootflash:///
  bootflash://module-1/
  bootflash://sup-1/
  bootflash://sup-active/
  bootflash://sup-local/
```

همانطور که مشاهده می‌شود کاراکتر ? ادامه دستورات را کمک می کند.

برای نصب از دستور زیر استفاده می‌شود.

```
N7K#install all kickstart bootflash://n7k-7.4.bin bootflash
```

با استفاده از دستور show module می‌توان ماژول‌های سخت‌افزاری نصب شده برروی تجهیز را مشاهده نمود. با استفاده از دستور show interface brief می‌توان اطلاعات خلاصه تمامی اینترفیس‌ها را مشاهده نمود. بطور خاص می‌توان از دستور show interface ethernet 2/1 یک اینترفیس خاص را مشاهده نمود. با استفاده از عبارت " " in | انتهای دستور می‌توان خروجی دستور را بر اساس عبارت مورد نظر فیلتر نمود. با استفاده از دستور show boot می‌توان متغیرهای Boot را مشاهده نمود.

تنظیمات در تجهیزات سیسکو بصورت سلسله مراتبی است. برای انجام تنظیمات عمومی باید از دستور configure terminal استفاده نمود. پس از آن برای تنظیمات اینترفیس باید از دستور interface استفاده نمود. همچنین با وارد نمودن دکمه ترکیبی Ctrl+c می‌توان از تنظیمات خارج شد.

```
N7K# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
N7K(config)# interface ethernet 2/1
N7K(config-if)#
```

NX-OS ۳-۳

این سیستم‌عامل برای مرکز داده طراحی شده است و از قابلیت‌های Switching، Routing و Storage Networking پشتیبانی می‌کند. در واقع برای ارسال بسته‌ها در لایه دو، مسیریابی و شبکه‌های ذخیره‌سازی استفاده می‌شود. می‌توان از طریق Command Line Interface (CLI) و یا فایل Extensible Markup Language (XML) به این سیستم‌عامل دسترسی داشت و تنظیمات را برروی آن اعمال نمود. این سیستم عامل بر اساس SAN-OS که مخصوص تجهیزات Cisco MDS است، طراحی شده است. در واقع قسمتی از تیمی که خانواده Cisco MDS 9000 را در سال ۲۰۰۲ توسعه داده، Nexus 7000 NX-OS را نیز توسعه داده است. بطور ساده به نسخه Cisco MDS 9000 SAN-OS 4.1 سیستم‌عامل NX-OS گفته می‌شود.

همانطور که گفته شد در ساختار نرم‌افزاری NX-OS سه قابلیت Switching، Routing و SAN Networking نهفته شده است. هسته NX-OS بر پایه Linux Kernel 2.6 است. سرویس‌ها و قابلیت‌های این سیستم‌عامل بصورت ماژولار، قابل اضافه و حذف است. در صورت نیاز به یک سرویس می‌توان با دستور feature آن را اضافه و یا حذف نمود. این سیستم‌عامل شامل دو فایل Image است. این فایل‌ها Kickstart و System است. پایه Protocol Stack بر اساس IPv4، IPv6 و Layer2 است.

قابلیت‌های مهمی که در لایه دو دارد شامل VLAN، RAPID STP، MST، LACP، vPC، OTV و FCoE است. قابلیت‌های مهمی که در لایه سه دارد شامل OSPF، EIGRP، PIM، HSRP، VRRP و OTV است. در

هر دو لایه هر کدام جدول Forwarding اختصاص خود را دارند که بر اساس سخت‌افزار توزیع شده است. همچنین از قابلیت‌های امنیتی ACL، Port Security و Cisco Trustsec پشتیبانی می‌کند.

قابلیت‌های که در طراحی به کار برده شده است می‌توان استفاده از نرم‌افزار ماژولار، جداسازی قسمت Control Plane و Data Plane، استفاده از Inservice Software Upgrade (ISSU) برای به‌روزرسانی و قابلیت‌های مجازی‌سازی را نام برد. قابلیت به‌روزرسانی در همه پلتفورم‌ها پشتیبانی نمی‌شود و بستگی به نوع تجهیز دارد. همچنین از قابلیت‌های مجازی‌سازی می‌توان Virtual Device Context (VDC) و Virtual Routing and Forwarding (VRF) را نام برد.

این سیستم‌عامل از قابلیت‌های بازیابی پردازش در لایه دو و سه پشتیبانی می‌کند. در لایه دو با استفاده از Persistent Storage Service (PSS) خطاهای لایه دو مدیریت می‌شود. باید توجه داشت که برای بعضی از پروتکل‌ها این امکان فراهم شده است. زمانی که خطا رخ می‌دهد، سرویس مجدد از نو راه‌اندازی می‌شود و این در صورتی است که قسمت Data Plane در حال ارسال ترافیک است. در لایه سه راه‌اندازی مجدد نسبتاً خوبی به کار گرفته شده است. بطور مثال قسمت Control Plane پایگاه داده OSPF را ذخیره می‌کند و در صورت رخ داد خطا در پردازش OSPF قسمت Data Plane ارسال بسته‌ها را ادامه می‌دهد.

همانطور که گفته شد پس از راه‌اندازی کامل سیستم‌عامل NX-OS دستور Setup بصورت خودکار اجرا می‌شود، زیرا هیچ تنظیمی هنوز برروی سیستم انجام نشده است. در این قسمت پسورد، آدرس IP مدیریتی، Telnet، SSH و دیگر موارد قابل تنظیم است. نام کاربری پیش‌فرض admin است. نقش‌های پیش‌فرض Network-Admin (دسترسی خواندن و نوشتن) و network-Operator (دسترسی فقط خواندنی) هستند.

برای مشاهده کاربر و نقش آن از دستور show user-account و show role می‌توان استفاده نمود.

```
N7K# show user-account
user:admin
    this user account has no expiry date
    roles:network-admin
N7K# show role
Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule   Perm   Type      Scope          Entity
  ------------------------------------------------------------------
  1      permit  read-write
Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
```

```
-------------------------------------------------------------------
Rule   Perm   Type      Scope          Entity
-------------------------------------------------------------------
1      permit  read
```

حالت‌های مختلفی برای اجرای دستور وجود دارد که به ترتیب توضیح داده می‌شود.

۱. Exec Mode: در این حالت بیشتر نمایش تنظیمات قابل مشاهده است. در زیر این حالت نمایش داده شده است

```
switch#
switch# show interface
switch# show running-config
switch# show ip arp
switch# ping 192.168.1.1
switch# traceroute 192.168.1.1
switch# clear cli history
switch# clear user admin
switch# copy running-config startup-config
switch# copy running-config tftp://10.10.10.10/N7K.cfg
```

۲. Global Configuration: در این حالت تنظیمات سیستمی، اینترفیس، تفییر feature و دیگر موارد انجام می‌شود. برای رفتن به این حالت از دستور configure terminal استفاده می‌شود.

```
switch# configure terminal
switch(config)#
switch(config)# interface ethernet 2/1
switch(config-if)#
```

کلیدهایی که در وارد نمودن دستورات کمک می‌کنند به شرح زیر است:

Ctrl+a	رفتن به ابتدای خط فرمان
Ctrl+e	رفتن به انتهای خط فرمان
Ctrl+z	رفتن به حالت Exec
Ctrl+c	خارج شدن از وارد نمودن دستور
Tab	کامل شدن خودکار دستور
?	نشان دادن توضیحات یا قابلیت‌های دستور
Backspace	پاک نمودن عبارت‌ها در دستور(delete کارایی ندارد)

VLAN & Trunk ۳-٤-

برروی هر پورت از Switch یک Collision Domain وجود دارد و اگر Switch چندین پورت داشته باشد چندین Collision Domain دارد. همه پورت‌ها بصورت پیش‌فرض برروی یک Broadcast Domain هستند و با گسترش شبکه این دامنه بزرگ شده و با ارسال یک بسته همه پخشی سرعت شبکه کاهش می‌یابد. بنابراین برای جداسازی دامنه‌های همه پخشی از مفهمومی به نام Virtual LAN یا VLAN استفاده می‌شود. معمولاً در این جداسازی آدرس‌های شبکه جداگانه‌ای استفاده می‌شود که البته ضروری و یا پیش‌نیاز نیست. هر VLAN یک Broadcast Domain جداگانه دارد. فوایدی که VLAN ارائه می‌کند به شرح زیر است:

۱. جداسازی شبکه: معمولاً پورت‌های Switch بر مبنای فیزکی جداسازی و در یک VLAN قرار می‌گیرند.
۲. انعطاف‌پذیری: می‌توان بر مبنای عملکردهای مختلف پورت‌های Switch را عضو VLANهای مختلف نمود. بطور مثال برای Voice از یک VLAN و برای Data از یک VLAN دیگر استفاده نمود.
۳. امنیت: می‌توان برای جداسازی ترافیک شبکه دستگاه‌ها را در VLANهای متفاوت قرار داد.

با گسترش و افزایش VLANها مدیریت VLANها دچار مشکل می‌شود. پروتکل Virtual Trunking Protocol (VTP) این اجازه را به Switchها می‌دهد تا اسم و شماره VLANها را بصورت خودکار یاد بگیرند و آنها را حذف، تغییر و یا ایجاد نمایند و کاربران را با استفاده از VTP Advertisement یا بسته‌های اطلاعاتی VTP در VLANهای مخصوص به خودشان قرار دهند. VTP پروتکلی است که برای کمک به مدیریت VLANها استفاده می‌شود و یک امر ضروری در شبکه نیست. VTP حالت‌های مختلفی برای یک Switch دارد و به آن VTP Mode گویند که به شرح زیر است:

۱. Client: در این حالت Switch نمی‌تواند VLAN را ایجاد، تغییر و حذف نماید. تنها بسته‌های اطلاعاتی مربوط به VTP را دریافت، ارسال و بین Switchها جابه‌جا می‌نماید و اطلاعات خود را Server مطابقت می‌دهد.
۲. Server: در این حالت Switch اجازه ایجاد، تغییر و حذف VLAN را دارد. بسته‌های اطلاعاتی مربوط به VTP را دریافت، ارسال و بین Switchها جابه‌جا می‌نماید و اطلاعات خود را با دیگر Switchها مطابقت می‌دهد.
۳. Transparent: در این حالت Switch اجازه ایجاد، تغییر و حذف VLAN را دارد. بسته‌های اطلاعاتی مربوط به VTP را دریافت، ارسال و بین Switchها جابه‌جا می‌نماید ولی اطلاعات خود را با دیگر Switchها مطابقت نمی‌دهد و فقط بسته‌های VTP Advertisement را از خود عبور می‌دهد. برای تنظیم این حالت باید بصورت دستی آن را تنظیم نمود و از VTP Mode پیروی نمی‌کند.

مفهموم دیگری که در VTP استفاده می‌شود، VTP Pruning است. این مفهوم در واقع عملیاتی است که با استفاده از اطلاعات VTP، VLANهایی که در Trunk هستند ولی در Switchهای همسایه استفاده نمی‌شوند را حذف می‌کنند. در واقع عملیات حرص کردن را برای VLANهای اضافی انجام می‌دهد.

بصورت پیش‌فرض همه پورت‌ها عضو VLAN 1 هستند. شماره VLANهای ۲-۳۹۶۷ قابل استفاده و شماره‌های ۳۹۶۸-۴۰۹۴ رزرو شده‌اند. پروتکل‌های CDP و VTP از VLAN 1 برای ارسال بسته‌های خودشان استفاده می‌کنند. VTP برای ایجاد و یا حذف VLAN باید در حالت Server یا Transparentباشد.

پورت Switch برای جابه‌جایی VLANها باید در حالت Trunk باشد تا بتواند هم زمان چندین VLAN را از خود عبور دهد. در واقع Trunk اجازه می‌دهد میزبان‌هایی که در Switchهای متفاوت ولی در یک VLAN و در یک Broadcast Domain هستند، اطلاعات خود را به اشتراک بگذارند. شماره VLAN یک Tag در داخل Ethernet Frame است که Trunk می‌تواند آن را تغییر دهد. Native VLAN بصورت Untagged است. پروتکل‌های Ethernet جدید شماره VLAN را برروی Trunk، Encode می‌کنند. IEEE 802.1q یا Dot1q یک پروتکل استاندارد است که برای این عمل طراحی شده است و برای جابه‌جایی VLANها استفاده می‌شود.

۳-۵- Redundant Switch Topologies

زمانی که یک مسیر اضافه در لایه دو وجود داشته باشد، جدول آدرس MAC در هم می‌شکند و باعث سر در گمی می‌شود. به عبارت دیگر از چندین اینترفیس آدرس MAC یکسان وارد می‌شود و آن را همانند آدرس ناشناخته هدایت می‌کند و باعث ارسال Frameها به اینترفیس اشتباهی می‌شود. در این حالت به دلیل وجود حلقه یا Loop میزات مصرف لینک‌های ارتباطی افزایش و گاهی به ۱۰۰٪ می‌رسد. به همین دلیل از مکانیزمی برای جلوگیری حلقه به نام Spanning-Tree Protocol (STP) استفاده می‌شود و پورت‌های Switch را به حالت Disable و یا Blocking می‌برد تا با مدیریت مسیرهای فیزیکی در قسمت‌های مختلف شبکه از حلقه جلوگیری کند. استانداردی که برای STP تعریف شده است IEEE 802.1D است. این پروتکل به این گونه عمل می‌کند که همه دستگاه‌ها با یک Switch اصلی به نام Root Bridge به توافق می‌رسند. بطور خلاصه روند این پروتکل به این صورت است که اگر Root Bridge بالاترین Switch در نظر گرفته شود، پورتی که از Switchهای پایین دستی به آن متصل است و کمترین هزینه تا آن را دارد، Root Port نامیده می‌شود. بقیه پورت‌های که به Root Bridge متصلند و هزینه بیشتری دارند غیر فعال یا Block می‌شوند. پورت‌های Switchهای پایین دستی با انجام همین روند به حالت Designating می‌روند. این روند یک به یک انجام شده تا در شبکه هیچ حلقه‌ای وجود نداشته باشد. برای این که پورت‌ها بتوانند حالت‌های خود را انتخاب کنند باید ویژگی‌های لینک و Bridge بین سیستم‌ها به اشتراک گذاشته شود. به اطلاعاتی که در STP تبادل می‌شود STP Advertisement یا Bridge Protocol Data Unit (BPDU) گفته می‌شود. این بسته‌ها بصورت آدرس چند پخشی

0180.C200.0000 ارسال می‌شود. داخل بسته‌های BPDU ویژگی‌های Root ID، Root Path Cost، Bridge ID، Port ID و Timers وجود دارند. دو نوع بسته BPDU وجود دارد که Configuration و Topology Change Notification (TCN) هستند.

۳-۵-۱- Root Bridge Election

کمترین Bridge ID (BID) به عنوان Root انتخاب می‌شود. BID ۸ بایت است که شامل Bridge Priority که عددی بین ۰ و ۶۵۵۳۵ و آدرس MAC است. بصورت پیش فرض Bridge Priority برابر ۳۲۷۶۸ است. استانداردهای جدید Bridge Priority را به دو قسمت تقسیم می‌کنند که شامل Bridge Priority به اندازه ۴ بیت و System ID Extended که همان شماره VLAN است به اندازه ۱۲ بیت می‌شود. کمترین BID به عنوان Root انتخاب می‌شود.

Legend: C= changeable; U= unchangeable
CCCCUUUUUUUUUUUU 16 bits
0001UUUUUUUUUUUU 1*2^12 = 4096
0111UUUUUUUUUUUU Default: 32768
0111000000000001 Default for VLAN 1: 32769

۳-۵-۲- Root Port Election

پورتی است که کمترین هزینه تا رسیده به Root Bridge را دارد. در واقع کمترین هزینه یا بیشترین پهنای‌باند برای رسیدن به Root Bridge را Root Port گویند. اگر هزینه‌ها برابر باشد آنگاه به BID و در صورت برابری مجدد به شماره پورت نگاه می‌شود.

۳-۵-۳- Designated Port Election

به پورت‌های پایین دستی از Root Bridge گفته می‌شود و همانند Root Port انتخاب می‌شوند. همانند Root Port اگر هزینه‌ها برابر باشد آنگاه به BID و در صورت برابری مجدد به شماره پورت نگاه می‌شود.

همه پورت‌های دیگر به حالتن Blocking می‌روند. در این حالت فقط BPDU دریافت می‌شود و همه ترافیک‌ها حذف می‌شوند و اجازه ارسال ترافیک وجود ندارد. در واقع کلید حل مشکل حلقه در شبکه پورت‌های Block هستند.

در جدول زیر نقش پورت‌ها در STP نمایش داده شده است.

Port Role	BPDU Behavior	Port State
Root	Receiving	Forwarding
Designated	Sending	Forwarding
Non-Designated	Receiving	Blocking
Listening	Receiving/Sending	Listening
Learning	Receiving/Sending	Learning

هزینه پورت‌ها در جدول زیر نمایش داده شده است.

Bandwidth	Short Path Cost Method Port Cost	Long Path Cost Method Port Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1-Gigabit Ethernet	4	20,000
10-Gigabit Ethernet	2	2,000

STP Timers ۳-۵-٤-

زمانی که Switch راه‌اندازه و کامل Boot می‌شود، برای همگرایی STP مدت زمانی صرف می‌شود. این مدت زمان به زمانی که برای انتخاب حالت‌های پورت‌ها صرف می‌شود، بستگی دارد.

Disable (Shutdown) -> Listening (Exchange BPDU) -> Learning (Build MAC table) -> Forwarding (Normal Loop-free traffic forward)

در حالت Blocking بسته BPDU دریافت می‌شود ولی داده در شبکه ارسال نمی‌شود. در صورت تغییر نقشه شبکه ممکن است حالت زیر رخ دهد.

Blocking (Receive BPDU) -> Listening (Exchange BPDU) -> Learning (Build MAC table) -> Forwarding (Normal Loop-free traffic forward)

سه زمان در STP استفاده می‌شود که در یر توضیح داده شده است.

۱. Hello: مدت زمانی است که بصورت دوره‌ای بسته‌های BPDU ارسال می‌شود. این زمان بصورت پیش‌فرض ۲ ثانیه است.
۲. MaxAge: به مدت زمانی که پورت در حالت Block منتظر باشد و بسته BPDU دریافت نکند، گفته می‌شود. این زمان بصورت پیش‌فرض ۲۰ ثانیه است.
۳. Forward Delay: مدت زمانی است که برای هر کدام از Listening و Forwarding به طول می‌انجامد. این مدت زمان بصورت پیش‌فرض ۱۵ ثانیه است.

همانطور که گفته شده اگر خطایی در یکی از پورت‌ها رخ دهد و پورتی بخواهد جایگزین آن شود ۵۰ ثانیه زمان صرف می‌شود.

Topology Change Notification (TCN) ۳-۵-۵-

TCN نوع دوم از بسته BPDU است. این بسته زمانی که تغییری در شبکه رخ دهد ارسال می‌شود تا جدوا MAC دستگاه‌ها به روز شود. بطور مثال اگر یک پورت فعال به حالت خاموش برود، یک پورت Block به حالت Designated می‌رود. این بسته از سوی یک Root Port دستگاه به سمت Root Bridge ارسال می‌شود. Switch بالادستی پس از دریافت این بسته، پیغام TCNAck به فرستنده ارسال می‌کند. این روند تا زمانی که بسته به Root Bridge برسد ادامه می‌یابد. پس از دریافت بسته توسط Root Bridge، پیغام TCN به همه پورت‌ها ارسال می‌شود. در نهایت زمان نگهداری آدرس MAC که پیش‌فرض ۵ دقیقه است به ۱۵ رثانیه کاهش می‌یابد.

Rapid STP ۳-۵-۶-

این پروتکل در استاندارد IEEE 802.1w تعریف شده است. RSTP قابلیتی را فراهم کرده است که همگرایی از 802.1D سریع‌تر باشد. این پروتکل با 802.1D سازگار است. شرکت سیسکو همچنین RSTP را پیشرفته‌تر کرده و به نام ST Instance Per VLAN یا +RSTP نام‌گذاری نموده است.

تفاوت نقش پورت دو پروتکل در جدول زیر شرح داده شده است.

802.1D		802.1w	
Port Role	Port State	Port Role	Port State
Root	Forwarding	Root	Forwarding
Designated	Forwarding	Designated	Forwarding
Non-Designated	Blocking	Alternate/Backup	Discarding
Listening	Listening	Discarding	Discarding
Learning	Learning	Learning	Learning

همچنین حالت پورت‌ها در RSTP متفاوت است.

۱. Edge Port: پورتی است که برای میزبان استفاده می‌شود و روی آن STP اجرا نشده است. این پورت حالت Listening و Learning ندارد و مستقیم به حالت Forwarding می‌رود.
۲. Network Port: پورتی است که در STP شرکت می‌کند. این پورت با حالت Discarding شروع می‌شود تا بتواند حلقه را تشخیص دهد. در صورت دریافت BPDU تشخیص می‌دهد که پورت به حالت Root برود و یا در Discarding بماند.

Multiple STP ۳-۵-۷-

این پروتکل در استاندارد IEEE 802.1s تعریف شده است. در این پروتکل می‌توان چندین درخت Spanning-tree داشت و با تعریف هر شماره یا Instance برای هر درخت، VLANها را به آن نگاشت کرد. هر VLAN که در Instance تعریف شده است یک قسمتی از Common Instance یا CIST است. پروتکل MSTP با 802.1D و RSTP سازگار است.

برای تنظیم یک Switch به عنوان Root Bridge از دستورات زیر استفاده می‌شود. البته باید توجه داشت که مدیر شبکه باید از ST مطمئن باشد. برای تنظیم می‌توان STP Priority را با دستور STP Priority برروی Switchها فعال نمود.

```
switch(config)# spanning-tree vlan 10 priority ?
 <0-61440>  Bridge priority in increments of 4096
switch# show spanning-tree
```

Port Channel ۳-۵-۸-

زمانی که چندین مسیر ارتباطی بین Switchها باشد، از افزونگی یا redundancy استفاده می‌شود. Port Channel تکنولوژی است که چندین لینک فیزیکی را باهم ترکیب کرده و یک لینک منطقی ایجاد می‌کند.

همچنین این امکان را فراهم می‌کند تا در صورت وجود خطا در یکی از لینک‌ها انعطاف‌پذیری وجود داشته باشد. امکان دیگری را که فراهم می‌کند Load Balancing یا توازن بار بین لینک‌ها است. Load balancing بر اساس شاخص Hashing انجام می‌شود. لینک‌ها باید در دو Switch مختلف باشند. پروتکلی که بین لینک‌ها جهت گفت‌وگو یا Negotiation استفاده می‌شود، Link Aggregation Control Protocol (LACP) است. مکانیزم Hashing می‌تواند بر اساس Frame لایه دو source and Destination MAC، Packet لایه سه MAC و source and Destination IP، PDU لایه چهار source and Destination MAC و IP و Port باشد. این پروتکل بصورت Global در داخل یک Switch تنظیم می‌شود.

۳-۶- IPv4 Networks

آدرس‌های IPv4 به دو صورت نام‌گذاری می‌شوند.

۱. Binary: در این آدرس‌گذاری از دو عدد ۰ و ۱ استفاده می‌شود و هر قسمت از IP، ۸ تا عدد در خود جای می‌دهد.
۲. Decimal: در این آدرس گذاری اعداد بین ۰ و ۹ ولی در هر قسمت بین ۰ تا ۲۵۵ قابل جایگذاری است.

برای تبدیل Binary به Decimal اگر عدد نظیر با Decimal برابر ۰ باشد ۰ گذاشته می‌شود. اگر عدد نظیر برابر ۱ باشد، اعداد هر قسمت با همدیگر جمع می‌شود.

Value	128	64	32	16	8	4	2	1
Binary	1	0	1	0	0	1	1	0
Decimal	128	0	32	0	0	4	2	0

10100110 -> 128+32+4+2=166

11000000.10101000.00000001.00000001 = 192.168.1.1

تفاوت بین شبکه‌های لایه دو تخت یا Flat Layer 2 با زیرشبکه‌ها یا Subnets این است که در شبکه‌های تخت همه دستگاه‌ها Broadcast Domain اشتراکی دارند و پهنای‌باند نیز به اشتراک گذاشته می‌شود. همچنین در شبکه‌های تخت اعمال سیاست‌های امنیتی مشکل است. در شبکه‌های Subnets اعمال سیاست‌ها آسان‌تر و پهنای‌باند بیشتری در دسترس است.

Subnet Mask نیز همانند IPv4 بصورت Decimal و Binary هستند. آدرس Mask نمایش دهنده نقطه بین شبکه و میزبان است. در جدول زیر نمونه‌ای از آدرس‌دهی نمایش داده شده‌است.

Value	128	64	32	16	8	4	2	1	Long Mask	
Binary	1	1	1	0	0	0	0	0		
192.168.	128	64	32	0	0	0	0	0	224	192.168.224.
Binary	1	1	1	1	0	0	0	0		
192.168.	128	64	32	16	0	0	0	0	240	192.168.240.
Binary	1	1	1	1	1	0	0	0		

192.168.	128	64	32	16	8	0	0	0	248	192.168.248.
Binary	1	1	1	1	1	1	0	0		
192.168.	128	64	32	16	8	4	0	0	252	192.168.252.
Binary	1	1	1	1	1	1	1	0		
	128	64	32	16	8	4	2	0	254	

در جدول زیر نمونه‌ای از تعداد شبکه و میزبان در کلاس C نشان داده شده است.

تعدا بیت X	تعداد بیت شبکه 2^X	تعدا بیت باقیمانده برای میزبان Y	تعداد میزبان قابل استفاده2^Y-2 (دو آدرس برای شبکه و همه پخشی کسر می‌شود)
1	2	7	126
2	4	6	62
3	8	5	30
4	16	4	14
5	32	3	6
6	64	2	2
7	128	1	0
8	256	0	0

بطور مثال در 192.168.10.0 اگر چهار بیت از قسمت میزبان قرض و به قسمت شبکه اضافه شود Subnet Mask بصورت زیر است. همچنین آدرس شبکه و آدرس همه پخشی نیز نمایش داده شده است.

NNNNNNNN. NNNNNNNN. NNNNNNNN.NNNNHHHH
11000000. 10101000.00001010.00000000 = 192.168.10.0
11111111.11111111.11111111.11110000 = 255.255.255.240 یا /28

Subnet 1:
Network Address: 192.168.10.0/28
Host Range: 192.168.10.1 – 14
Broadcast Address: 192.168.10.15
Subnet 2:
Network Address: 192.168.10.16/28
Host Range: 192.168.10.17 – 30
Broadcast Address: 192.168.10.31

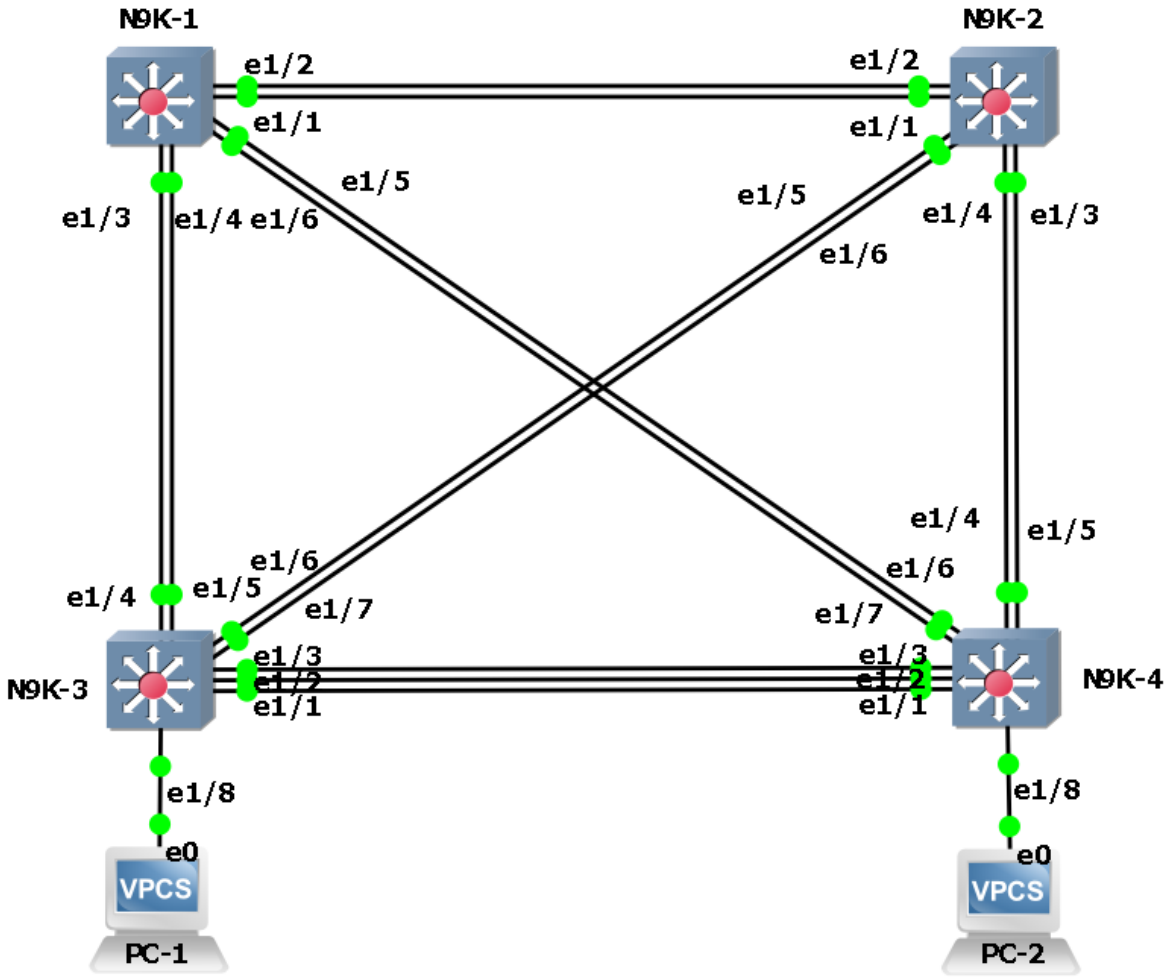
این روند تا انتهای آدرس‌دهی ادامه دارد.

۳-۷- STP Commands

با استفاده از نقشه شبکه زیر دستورات STP وارد می‌شود. در هر قسمت ورودی دستور و خروجی آن نمایش داده می‌شود. دستورات برای تنظیم برروی هر Switch به شرح زیر است.

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan)# name V10
```

```
switch(config-vlan)# exit
switch(config)# interface ethernet 1/1-8
switch(config-if-range)# switchport mode trunk
switch(config-if-range)# no shutdown
switch(config-if-range)# exit
```



با وارد کردن دستور زیر Priority مربوط به Switch N9K-1 را تغییر داده که باعث Root شدن آن می‌شود.

```
N9K-1(config)# spanning-tree vlan 10 priority 0
```

پس از وارد کردن دستوررات بالا خروجی دستورات برروی N9K-3 به شرح زیر است:

```
N9K-3# show spanning-tree vlan 10
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Eth1/1           Altn BLK 4         128.1    P2p
Eth1/2           Altn BLK 4         128.2    P2p
Eth1/3           Altn BLK 4         128.3    P2p
Eth1/4           Root FWD 4          128.4    P2p
Eth1/5           Altn BLK 4         128.5    P2p
```

```
Eth1/6        Desg FWD 4       128.6   P2p
Eth1/7        Desg FWD 4       128.7   P2p
Eth1/8        Desg FWD 4       128.8   Edge P2p
```

همچنین خروجی برروی N9K-1 به شرح زیر است.

```
switch# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    10
             Address     0caf.6ffa.3907
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     0caf.6ffa.3907
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Eth1/1          Desg FWD 4         128.1    P2p
Eth1/2          Desg FWD 4         128.2    P2p
Eth1/3          Desg FWD 4         128.3    P2p
Eth1/4          Desg FWD 4         128.4    P2p
Eth1/5          Desg FWD 4         128.5    P2p
Eth1/6          Desg FWD 4         128.6    P2p
Eth1/7          Desg FWD 4         128.7    P2p
Eth1/8          Desg FWD 4         128.8    P2p
```

برای سریع‌تر شدن و شرکت نکردن در STP پورت مربوط به کامپیوترهای PC-1 و PC-2 می‌توان از دستور spanning-tree port type edge استفاده نمود.

```
switch(config-if)# spanning-tree port type ?
  edge     Consider the interface as edge port (enable portfast)
  network  Consider the interface as inter-switch link
  normal   Consider the interface as normal spanning tree port
switch(config-if)# spanning-tree port type edge
```

قسمتی از خروجی دستور show interface trunk برروی N9K-1 به شرح زیر است.

```
--------------------------------------------------------------------------------
Port          STP Forwarding
--------------------------------------------------------------------------------
Eth1/1        1,10
Eth1/2        1,10
Eth1/3        10
```

```
Eth1/4      10
Eth1/5      1,10
Eth1/6      10
Eth1/7      1,10
Eth1/8      1,10
```

با دستور زیر می‌توان هزینه مسیر را بصورت long مشاهده نمود.

```
switch(config)# spanning-tree pathcost method long
switch# show spanning-tree vlan 10
Interface       Role Sts Cost     Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Eth1/4          Root FWD 20000     128.4    P2p
Eth1/5          Altn BLK 20000     128.5    P2p
Eth1/8          Desg FWD 20000     128.8    Edge P2p
```

برای تغییر حالت STP به پروتکل MSTP از دستورات زیر استفاده می‌شود.

```
switch# configure terminal
switch(config)# spanning-tree mode mst
switch(config)# spanning-tree mst configuration
switch(config-mst)# name CCNA-DC
```

شماره Revision باید در همه Switchها یکسان باشد. MST برای منطقه کارکرد خود از ترکیب NAME + Revision Number استفاده می‌کند.

```
switch(config-mst)# revision 2
```

نگاشت VLAN به پروتکل MSTP به شرح زیر است.

```
switch(config-mst)# instance 1 vlan 10
switch(config-mst)# exit
```

انتخاب Switch به عنوان Root به شرح زیر است.

```
switch(config)# spanning-tree mst 1 root primary
switch# show spanning-tree vlan 10
switch# show spanning-tree mst 1
##### MST1    vlans mapped:   10
Bridge      address 0caf.6f22.6f07  priority     32769 (32768 sysid 1)
Root        address 0caf.6ffa.3907  priority     24577 (24576 sysid 1)
          port    Eth1/4          cost         40000    rem hops 18
Interface       Role Sts Cost     Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Eth1/4          Root FWD 20000     128.4    P2p
Eth1/5          Altn BLK 20000     128.5    P2p
Eth1/8          Desg FWD 20000     128.8    Edge P2p
```

Introduction to IPv6 -۸-۳

به دلیل کمبود فضای IPv4، IPv6 طراحی شده است. حداکثر تعداد آدرس IP که در IPv4 استفاده می‌شود 2^{32} است که برابر با ۴،۲۹۴،۹۶۷،۲۹۶ آدرس می‌شود. ۳۲ تعداد بیت استفاده در IPv4 است. تعدا بیت مورد استفاده در IPv6 برابر با ۱۲۸ است. حداکثر تعداد آدرس در IPv6 برابر با 2^{128} که بیتر از ۳۴۰۲۸۲۳۶۶۹۲۰۹۳۸۴۶۳۴۶۳۳۷۴۶۰۷۴۳۱۷۷۰۰۰۰۰+ آدرس است. در آدرس‌دهی IPv4 بصورت Dotted Decimal یا نقطه دسیمال از ۴ قسمت ۸ بیتی استفاده می‌شود. در IPv6 از بصورت Hexadecimal و از ۸ قسمت ۱۶ بیتی استفاده می‌شود. در IPv6 هر دو کاراکتر برابر یک بایت است.

آدرس‌دهی در IPv6 بصورت زیر است.

۱. Global Unicast: برای استفاده در محیط عمومی اینترنت استفاده می‌شود. شروع آن با 2000 است.
۲. Link-Local Unicast: هر اینترفیسی که فعال می‌شود، بصورت خودکار آدرس‌دهی می‌شود. این آدرس فقط برای این لینک قابل استفاده است و با FE80 شروع می‌شود.
۳. Unique Local: برای آدرس‌های خصوص یا درون سازمانی استفاده و با FC00 شروع می‌شود.
۴. Multicast: این آدرس‌ها چندپخشی است و با FF شروع می‌شود.

آدرس‌دهی EUI-64 نوعی آدرس‌دهی با استفاده از آدرس MAC است. آدرس MAC از ۴۸ بیت تشکیل شده است. پروتکل IPv6 از دو قسمت ۶۴ بیتی تشکیل شده است که ۶۴ بیت دوم مربوط به میزبان می‌شود. برای آدرس‌دهی EUI-64 ابتدا MAC را به دو قسمت ۲۴ بیتی تقسیم کرده و مابین آن از FF:FE استفاده می‌شود. ۴۸ بیت به اضافه ۱۶ بیت برابر ۶۴ بیت میزبان می‌شود. پس از آن باید بیت شماره ۷ از سمت چپ را به ۱ تبدیل نمود. بطور مثال MAC = 1034:5678:9012 تبدیل به 1234:56FF:FE78:9012 می‌شود.

آدرس‌دهی در IPv6 به سه صورت انجام می‌گیرد.

۱. Static: برای آدرس‌دهی می‌توان بصورت دستی توسط کاربر و یا دستی از EUI-64 استفاده نمود.
۲. Stateless Auto configuration: بدون وجود سرور هر نود با استفاده از اطلاعاتی که توسط Router یا هر دستگاه دیگری روی لینک قرار می‌گیرد، آدرس‌دهی را انجام می‌دهد.
۳. DHCPv6: این روش همانند IPv4 است. یک سرور به همه نودها آدرس می‌دهد. این مدل از Stateless قابلیت‌های بیشتری مانند DDNS دارد.

عملکرد IPv6 به این شکل است که نودی که به Router متصل است، اگر Router در دسترس باشد و بتواند به نودها IP دهد، از آن آدرس می‌گیرد. در صورتی که Router در دسترس نباشد و یا DHCP Server در شبکه وجود داشته باشد، Router پیام درخواست IP را برای همه DHCP Serverها بصورت Multicast یا چندپخشی ارسال می‌کند. باید توجه داشت که نودها از آدرس Link-Local به عنوان مبدأ برای ارسال بسته استفاده می‌کنند.

برای تبدیل IPv4 به IPv6 و بالعکس از روش‌های Tunneling استفاده می‌شود.

۱. Dual Stack: نودها به هر دو IPv6 و IPv4 متصل هستند. هر نود دو جدول IP دارد و برای شبکه IPv4 از جدول IPv4 و برای شبکه IPv6 از جدول IPv6 استفاده می‌کند.
۲. Manual Tunneling: نیاز به Dual Stack است و بسته‌های IPv6 را داخل بسته‌های IPv4 قرار می‌دهد.
۳. Dynamic 6to4 Tunneling: IPv4 داخل بسته‌های IPv6 قرار می‌گیرد و تونل را بصورت خودکار انجام می‌دهد. این روش برای ارتباط بین سایت‌های مختلف و در بستر اینترنت انجام می‌گیرد.
۴. Intra-Site Automatic Tunnel Addressing (ISATAP): تونل را بصورت خودکار بین دو سایت داخلی که وسط آن IPv4 است قرار می‌دهد. این روش برای استفاده در داخل سایت‌های یک سازمان است.

٤- Introduction to Routing

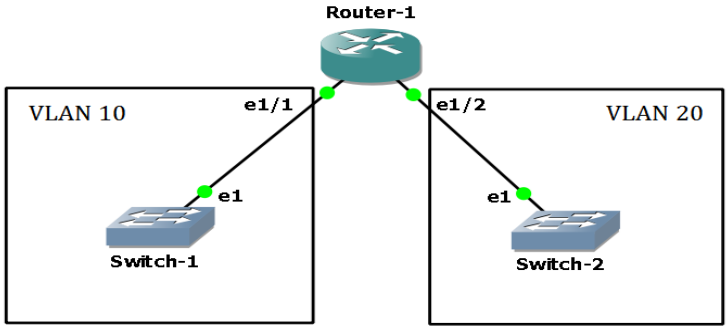
Switchهای لایه دو Frameها را تغییر نمی‌دهند و فقط آنها را انتقال می‌دهند. این Switchها عملکرد مشابه Bridge را انجام می‌دهند و ارتباط میزبان‌هایی که در یک VLAN هستند از طریق آدرس MAC موجود در جدول MAC برقرار می‌کنند. در واقع در لایه دو فقط ارتباط Broadcast Domain محلی را برقرار می‌کنند و ارتباطی که بین VLANها باید برقرار شود وظیفه Routerها است. Routerها یا Switchهای لایه سه بسته‌های لایه دو را از نو ایجاد می‌کنند. این عملیات به این صورت انجام می‌شود که هدر لایه دو حذف شده و بسته جدیدی ایجاد می‌شود. آدرس‌های IP مبدأ و مقصد هیچ تغییری نمی‌کنند، ولی آدرس MAC لایه دو به دلیل انتقال از یک اینترفیس به یک اینترفیس دیگر تغییر می‌کند. باید توجه داشت که ترافیک بین VLANها باید از طریق Router یا Switch لایه سه انجام گیرد.

٤-١- Switch and Router Connectivity

برای ارتباط بین Switch و Router و همچنین ارتباط بین VLANها چندین راه حل وجود دارد که در ادامه به آن توضیح داده می‌شود.

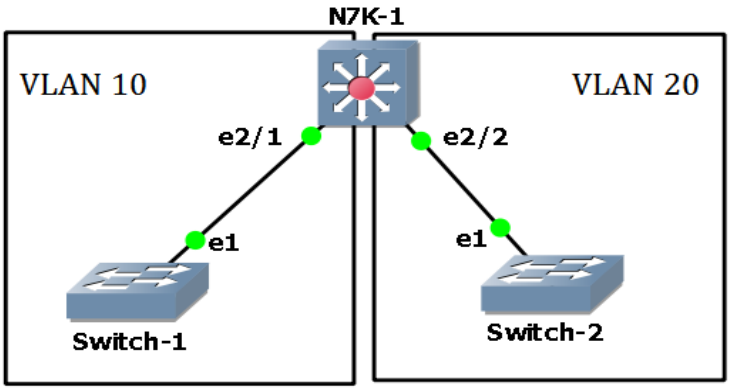
٤-١-١- Multi-Link Connection

برای ارتباط بین VLANها یک راه حل این است که برای هر VLAN یک لینک فیزیکی بین Switch لایه دو و Router استفاده شود. بطور مثال برای ارتباط بین VLAN 10 و VLAN 20، Frame از طریق لینک e1/1 در VLAN 10 ارسال می‌شود. Router، Frame را به آدرس MAC که در VLAN 20 است، تغییر می‌دهد و آن را از طریق لینک e1/2 ارسال می‌کند. در واقع Switch از طریق MAC موجود در VLAN 20 به مقصد دسترسی پیدا می‌کند. در این بحث هم از Switch لایه سه و هم از Router می‌توان استفاده نمود.



٤-١-٢- Switch Virtual Interface (SVI)

راه حل بهتری که برای ارتباط بین VLANها وجود دارد، استفاده از ترکیب Switch لایه دو و Router لایه سه است. بطور مثال استفاده از Switch چند لایه و یا لایه سه است. در این نوع، ارتباط بین Switch و Router و بازنویسی بسته‌ها در داخل Switch و یا Backplane صورت می گیرد. برای پیاده‌سازی از interface vlan <#> در Switch لایه سه استفاده می‌شود. برای فعال‌سازی برروی Nexus Switch باید قابلیت آن با دستور switch(config)# feature interface-vlan فعال شود. این راه حل سریع‌تر، آسان‌تر، انعطاف‌پذیرتر و مدیریت آن آسانتر است. باید توجه داشت interface vlan یک اینترفیس منطقی است و فزیکی نیست. برای هر VLAN باید یک اینترفیس منطقی ایجاد کرد و با استفاده از پروتکل‌های مسیریابی ارتباط بین آنها را برقرار نمود. در واقع هیچ لینک فیزیکی در لایه سه وجود ندارد.



٤-١-٣- Native Layer 3 Router Port

این پورت‌ها در تضاد با SVI که مجازی هستند، پورت‌های فیزیکی هستند. در این نوع پورت‌ها باید از لایه دو به لایه سه تبدیل شوند. برای تنظیم باید از دستور no switchport استفاده شود. پورت‌های لایه سه Native همانند پورت‌های Ethernet در Router هستند که برروی آن IP، ACL، QoS و دیگر موارد قابل تنظیم است. در طراحی معمولاً به پورتی که عملیات مسیریابی Uplink انجام می‌دهد، متصل می‌شود. بطور مثال برای Uplinkهای مسیریابی لایه Access به Distribution و یا Distribution به Core استفاده می‌شود. اگر

Uplink برای مسیریابی نباشد از این نوع اینترفیس استفاده نمی‌شود. در این نوع اینترفیس‌ها زمان همگرایی STP وجود ندارد و STP که مخصوص لایه دو است حذف می‌شود. همگرایی در این نوع برعهده پروتکل مسیریابی در لایه سه است. اگر چندین لینک از نوع Native Layer 3 بین دستگاه‌ها باشد می‌توان از port Channel استفاده نمود. باید توجه داشت که STP در لایه سه وجود ندارد.

۲-٤ Dynamic Routing Protocols

پروتکل‌های مسیریابی یا به شکل Dynamic Routing Protocol یا پروتکل‌های مسیریابی پویا هستند و یا بصورت دستی یا Static هستند. وظیفه پروتکل‌های مسیریابی برقراری ارتباط بین پورت‌های لایه سه، ارسال آدرس‌های شبکه بین Routerها و انتخاب بهترین مسیر برای مقصد است. در این بخش پروتکل‌های مسیریابی پویا به اختصار توضیح داده می‌شود. در پروتکل مسیریابی از تنظیمات پردازشی، الگوریتم‌ها و ارسال پیام‌ها برای جابه‌جایی و انتشار اطلاعات مسیریابی استفاده می‌شود. هر پروتکل مسیریابی، مسیرهای ممکن برای رسیدن به مقصد را مشخص می‌کند و بهترین مسیر را در جدول مسیریابی یا Routing Table قرار می‌دهد. دقت داشته باشید که فقط بهترین مسیر در جدول مسیریابی قرار می‌گیرد. اگر مسیری یا لینکی در یک دامنه مسیریابی حذف شود، پروتکل مسیریابی جدول مسیریابی را با استفاده از اطلاعات مسیریابی به‌روزرسانی می‌کند. اگر لینکی حذف و یا اضافه شود، زمانی برای همگرایی صرف می‌شود تا پروتکل مسیریابی بهترین مسیر را پیدا و آن را در جدول مسیریابی قرار دهد.

Autonomous System یا AS مجموعه‌ای از شبکه‌هایی است که در یک دامنه مدیریتی قرار دارند. به عبارت دیگر گروهی از شبکه‌ها است که مدیر شبکه آنها را در یک مجموعه مدیریتی قرار می‌دهد.

پروتکل‌های مسیریابی به دو دسته تقسیم می‌شوند. پروتکل‌های Interior Gateway Protocol (IGP) که اطلاعات مسیریابی در یک AS تبادل می‌شود. OSPF، EIGRP و RIP نمونه‌ای از این پروتکل‌ها هستند. از این پروتکل‌ها معمولاً در داخل یک سازمان استفاده می‌شود. پروتکل‌های Exterior Gateway Protocol (EGP) که اطلاعات مسیریابی بین ASها تبادل می‌شود. BGP نمونه‌ای از این پروتکل است. معمولاً از این پروتکل‌ها داخل اینترنت و یا بین Service Providerها استفاده می‌شود.

پروتکل‌های مسیریابی IGP به چند کلاس تقسیم می‌شوند. در ادامه به توضیح هر یک پرداخته می‌شود.

۱. Distance Vector (DV): این پروتکل‌ها به بردار مسافت نیز معروف هستند. Routing Information Protocol (RIP) نمونه‌ای از این پروتکل است. RIP جهت و مسافت را با استفاده از تعداد Hopها برای رسیدن به مقصد در شبکه مشخص می‌کند.
۲. Link State (LS): این پروتکل‌ها با استفاده از اطلاعات وضعیتی لینک‌ها، توپولوژی یا نقشه شبکه را می‌سازند و سپس با استفاده از الگوریتم دایجسترا یا Dijkstra بهترین مسیر را با استفاده از هزینه محاسبه می‌کنند. Open Shortest Path First (OSPF) نمونه‌ای از این پروتکل است.

۳. Advanced Distance Vector (ADV): در واقع این پروتکل ترکیبی از DV و LS است. Enhanced Interior Gateway Routing Protocol (EIGRP) نمونه‌ای از این پروتکل است.

Routing Metric یا معیار مسیریابی، مقداری است که با استفاده از آن بهترین مسیر برای رسیدن به مقصد محاسبه می‌شود. بطور مثال در پروتکل RIP معیار Hop Count یا تعداد Router است، در OSPF معیار Cost of Link است، در EIGRP مجموعه‌ای از Bandwidth، Delay، Load، Reliability و MTU است.

Administrative Distance یا AD یک قابلیتی است که توسط آن Routerها در هنگام وجود چندین مسیر یکسان با استفاده از چندین پروتکل مسیریابی، بهترین مسیر را انتخاب می‌کنند. در واقع AD قابلیت اطمینان یک پروتکل مسیریابی را تعیین می‌کند. برای هر پروتکل مسیریابی AD متفاوتی وجود دارد. اگر بیشتر از یک پروتکل مسیریابی برای رسیدن به یک مقصد وجود داشته باشد AD این اختلاف را حل می‌کند و از AD کمتر استفاده می‌شود. جدول زیر AD پروتکل‌های مختلف را نشان می‌دهد

Administrative Distance	Routing Protocol
0	Directly connected interface
1	Static route out an interface
1	Static route to next-hop address
3	DMNR - Dynamic Mobile Network Routing
5	EIGRP summary route
20	External BGP
90	Internal EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	Routing Information Protocol (RIP)
140	Exterior Gateway Protocol (EGP)
160	On Demand Routing (ODR)
170	External EIGRP
200	Internal BGP
250	Next Hop Resolution Protocol (NHRP)
254	Default static route learned via DHCP
255	Unknown and unused

٤-۲-۱- Distance Vector Protocol – RIP

در این پروتکل معیار یا Metric تعداد Hop یا دستگاه است. در واقع Distance یا مسافت تعداد Hop است و Vector یا بردار به معنای سمت یا Router یا اینترفیسی است که بسته از آن خارج می‌شود. در این پروتکل همه جدول مسیریابی بصورت دوره‌ای و بر اساس Hop-By=Hop انتشار داده می‌شود. Routerها فقط اطلاعات همسایه‌هایی را که به آنها متصل هستند، دارند. به این پروتکل در بعضی مواقع مسیریابی توسط شایعه نیز گفته می‌شود. پروتکل RIP Version 2 در استاندارد باز RFC 2453 تعریف شده است. پروتکل‌های

Distance Vector از الگوریتم Bellman-Ford استفاده می‌کنند. RIP Version 2 از UDP 520 و IP Multicast 224.0.0.9 برای ارسال اطلاعات مسیریابی استفاده می‌کند. همگرایی در این پروتکل زمانی انجام می‌شود که همه مسیریاب‌ها با بهترین مسیر برای رسیدن به مقصد به توافق رسیده باشند. در صورتی که خطایی در لینک یا Router رخ دهد، زمانی برای رسیدن به بهترین مسیر جدید صرف می‌شود که به آن Reconvergence Time گفته می‌شود. این زمان بستگی به طراحی شبکه دارد که ممکن است یک عملیات سریع و یا کند باشد.

تفاوت RIP v1 و RIP v2 به این صورت است که در نسخه یک آدرس‌ها حتماً باید Classful باشند و اطلاعات مسیریابی هر ۳۰ ثانیه یکبار بصورت Broadcast ارسال می‌شود. در نسخه دو از Classless و یا VLSM پشتیبانی می‌شود همچنین اطلاعات بصورت Multicast ارسال می‌شود. Nexus Switchها از نسخه دو پشتیبانی می‌کنند. از احراز اصالت یا Authentication پشتیبانی می‌شود. زمانی که نیاز باشد به‌روزرسانی صورت می‌گیرد و به عبارتی Triggered Update است.

Link State Protocol – OSPF ۲-۲-٤-

OSPF و ISIS هر دو توسط Service Provider استفاده می‌شوند. در پروتکل‌های Link State (LS) نقشه کاملی از شبکه ساخته می‌شود. پروتکل‌های Link State از Cost به عنوان Metric استفاده می‌کنند. بهترین مسیر برای همه مقصدها در نقشه شبکه با استفاده از دایجسترا SPF استفاده می‌شود. از Classless یا VLAM و Summarization پشتیبانی می‌کند. به دلایل زیر از OSPF استفاده می‌شود:

۱. این پروتکل ضمانت می‌کند که یک نقشه بدون حلقه از شبکه داشته باشد. همه مسیریاب‌ها یک نقشه کامل و یکسان از شبکه دارند که از الگوریتم دایجسترا استفاده می‌کنند.
۲. یک پروتکل استاندارد است که بین شرکت‌های مختلف می‌توان استفاده نمود.
۳. مقیاس‌پذیری بزرگی دارد. ساختار سلسله مراتبی بر اساس Area یا ناحیه دارد.
۴. همگرایی سریعی دارد. همسایه‌های مجاور خود را بصورت فعال بررسی می‌کند. بر اساس هر رخ داد بسته‌های به‌روزرسانی را ارسال می‌کند.
۵. به‌روزرسانی کارآمدی دارد. به‌روزرسانی بصورت Multicast و Unicast مطمئن استفاده می‌کند.
۶. معیار یا Metric آن بر اساس هزینه پهنای‌باند یا Bandwidth Based Cost Metric است. این معیار انعطاف‌پذیری بیشتری نسبت به Hop Count که بصورت دستی است، دارد.

در پروتکل OSP نحوه عملکرد بیدن شکل است که هر مسیریاب ئاخل خود یک پردازش اجرا می‌کند و بعد از آن بر اساس لینک‌هایی که برروی آن OSPF فعال است، همسایه‌های خود را پیدا و اطلاعات را بین یکدیگر جابه‌جا می‌کنند. باید توجه داشت که بستگی به نوع شبکه بطور مثال، Peer-to-Pere، Frame Relay، Non-Broadcast و دیگر موارد، ارتباط بین همسایه‌ها متفاوت است. در مرحله بعد با استفاده از Shortest Path

First (SPF) بهترین مسیر انتخاب می‌شود. در آخر جدول همسایه‌ها و جدول نقشه شبکه یا Topology Table ذخیره و نگهداری می‌شود.

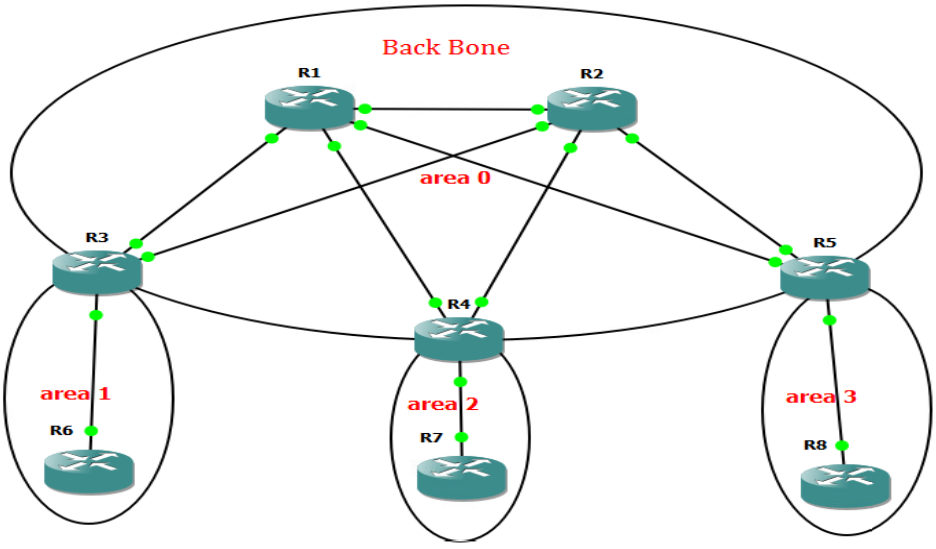
بسته‌های OSPF Hello در مسیریاب‌ها بصورت دوره‌ای برروی لینک فعال OSPF ارسال می‌شود. در داخل بسته‌های Hello اطلاعات زیر نهفته است:

۱. Router ID: این مؤلفه معمولاً بر اساس Loopback IP انتخاب می‌شود.
۲. Local Area-ID: زمانی که OSPF تنظیم می‌شود، این عدد نیز وارد می‌شود. در واقع ناحیه مورد استفاده برای OSPF است.
۳. Local Interface Subnet Mask
۴. Local Interface Priority
۵. Hello Interval: زمان ارسال بسته‌های Hello بصورت دوره‌ای است.
۶. Dead Interval: معمولاً ۴ برابر زمان Hello است که بعد از آن به معنای از بین رفتن لینک است.
۷. Authentication and Password
۸. Designated Router (DR) and Backup Designated Router (BDR)
۹. Options (flag, stub, ...)
۱۰. Router ID همسایه‌ها که برروی لینک هستند.

OSPF هزینه لینک را بصورت جدول زیر در نظر می گیرد.

Link Speed	Cost
100MBps	400
1Gbps	40
10Gbps	4
40Gbps	1

OSPF یک ساختار سلسله مراتبی دارد که باعث تقسیم کردن شبکه و انعطاف‌پذیری و محلی کردن تغییرات شبکه در یک ناحیه می‌شود.



نقاط ضعف پروتکل‌های Link State شامل موارد زیر است:

۱. نیاز به حافظه موقتی زیادی دارد، زیرا چندین جدول (Adjacency، Topology و Forwarding) را باید در خود ذخیره کند.
۲. سربار CPU زیادی دارد، زیرا از الگوریتم دایجسترا استفاده می‌کند.
۳. تنظیمات بسیار پیچیده‌ای دارد.

۳-۲-٤ Advanced Distance Vector – EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) یک پروتکل برای جانشینی IGRP است. این پروتکل اختصاصی شرکت سیسکو است که ترکیبی از دو پروتکل DV و LS است. در واقع پیشرفته بردار مسافت یا Advanced Distance Vector است. خصوصیات این پروتکل به شرح زیر است:

۱. از Classless یا VLSM پشتیبانی می‌کند.
۲. شبکه بدون حلقه را ضمانت می‌کند.
۳. سرعت همگرایی بالایی دارد و از همه پروتکل‌های IGP در یک طراحی مشخص سریع‌تر است.
۴. با استفاده از الگوریتم Diffusing Update (DUAL) به‌روزرسانی را انجام می‌دهد.
۵. به‌روزرسانی کارآمد و مطمئنی دارد، به این صورت که بسته‌های به‌روزرسانی را همسایه‌های مجاور فعال تشکیل می‌دهند.
۶. با استفاده از پروتکل Reliable Transport Protocol (RTP) رسیدن بسته‌ها را تضمین می‌کند.
۷. بسته‌های به‌روزرسانی به همسایه‌هایی که نیاز ندارند ارسال نمی‌شود.
۸. از چندین پروتکل مسیریابی مانند IPv4، IPX و AppleTalk پشتیبانی می‌کند.
۹. از چندین معیار برای Metric استفاده می‌شود.
۱۰. تنها پروتکل IGP است که بین مسیرها با هزینه‌های متفاوت توازن یا Load Balancing انجام می‌دهد.
۱۱. از MD5 برای احراز اصالت استفاده می‌کند.

نحوه عملکرد EIGRP شبیه OSPF است که با همسایه‌ها ارتباط برقرار و اطلاعات شبکه را جابه‌جا می‌کند. بهترین مسیر را با استفاده از DUAL انتخاب می‌کند. جدول همسایه‌ها یا Neighbors و شبکه یا Topology را ذخیره و نگهداری می‌کند.

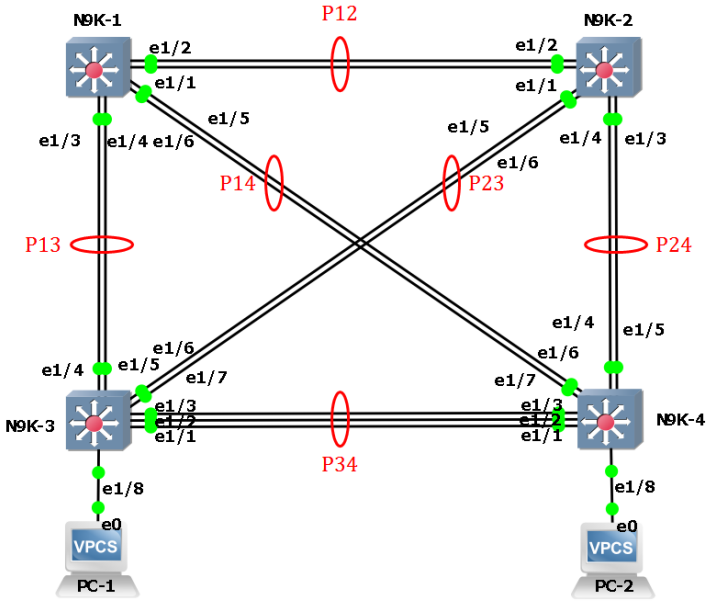
۳-٤ Port Channel Commands

برای تنظیمات مربوط به Port Channel اگر از LCAP استفاده شود باید آن را در قسمت feature فعال نمود. با زدن دستور feature می‌توان قابلیت‌هایی را مشاهده نمود که در زیر نشان داده شده است.

```
switch(config)# feature ?
eigrp           Enable/Disable Enhanced Interior Gateway Routing
interface-vlan  Enable/Disable interface vlan
```

lacp Enable/Disable LACP
ospf Enable/Disable Open Shortest Path First Protocol

با توجه به شکل زیر دستورات مربوط به Port Channel تنظیم می‌شود.



ابتدا دستورات مربوط به Switch N9K-1 وارد می‌شود.

```
N9K-1# configure terminal
N9K-1(config)# feature lacp
N9K-1(config)# interface ethernet 1/1-2
N9K-1(config-if-range)# channel-group 12 mode ?
  active   Set channeling mode to ACTIVE
  on       Set channeling mode to ON
  passive  Set channeling mode to PASSIVE
N9K-1(config-if-range)# channel-group 12 mode active
```

اگر از LACP استفاده شود آن را در حالت active قرار می‌دهیم و اگر از static port-channel استفاده شود گزینه on وارد می‌شود. در ادامه یکی از Port Channelها در حالت on قرار داده می‌شود.

```
N9K-1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
```

```
Group Port-      Type     Protocol  Member Ports     Channel
--------------------------------------------------------------------------------
12   Po12(SD)   Eth      LACP      Eth1/1(s)   Eth1/2(s)
N9K-1(config-if-range)#
```

همانطور که قابل مشاهده است از LACP استفاده شده است. در این قسمت s یا I در Eth1/1(s) نشان دهنده غیر فعال بودن است و باید طرف دیگر لینک تنظیم و بررسی شود. S در Po12 (SD) به معنای Switch بودن لینک است و D به معنای غیر فعال بودن Port Channel است. در ادامه دستورات مربوط برروی لینک‌های دیگر وارد می‌شود.

```
N9K-1(config)# interface ethernet 1/3-4
N9K-1(config-if-range)# channel-group 13 mode on
N9K-1(config-if-range)# interface ethernet 1/5-6
N9K-1(config-if-range)# channel-group 14 mode active
N9K-1(config-if-range)# show port-channel summary
--------------------------------------------------------------------------------
Group Port-      Type     Protocol  Member Ports     Channel
--------------------------------------------------------------------------------
12   Po12(SD)   Eth      LACP      Eth1/1(s)   Eth1/2(s)
13   Po13(SD)   Eth      NONE      Eth1/3(s)   Eth1/4(s)
14   Po14(SD)   Eth      LACP      Eth1/5(s)   Eth1/6(s)
```

همانطور که قابل مشاهده است در Po13(SD) حالت on استفاده شده است که پروتکل NONE است.

تنظیمات مربوط به Switch N9K-2 به شرح زیر است.

```
N9K-2# configure terminal
N9K-2(config)# feature lacp
N9K-2(config)# interface ethernet 1/1-2
N9K-2(config-if-range)# channel-group 12 mode active
N9K-2(config-if-range)# interface ethernet 1/3-4
N9K-2(config-if-range)# channel-group 24 mode active
N9K-2(config-if-range)# interface ethernet 1/5-6
N9K-2(config-if-range)# channel-group 23 mode active
```

تنظیمات مربوط به Switch N9K-3 به شرح زیر است.

```
N9K-3# configure terminal
N9K-3(config)# feature lacp
N9K-3(config)# interface ethernet 1/1-3
N9K-3(config-if-range)# channel-group 34 mode active
N9K-3(config-if-range)# interface ethernet 1/4-5
N9K-3(config-if-range)# channel-group 13 mode on
N9K-3(config-if-range)# interface ethernet 1/6-7
```

```
N9K-3(config-if-range)# channel-group 23 mode active
```

تنظیمات مربوط به Switch N9K-4 به شرح زیر است.

```
N9K-4# configure terminal
N9K-4(config)# feature lacp
N9K-4(config)# interface ethernet 1/1-3
N9K-4(config-if-range)# channel-group 34 mode active
N9K-4(config-if-range)# interface ethernet 1/4-5
N9K-4(config-if-range)# channel-group 24 mode active
N9K-4(config-if-range)# interface ethernet 1/6-7
N9K-4(config-if-range)# channel-group 14 mode active
N9K-4(config-if-range)# show port-channel summary
--------------------------------------------------------------------------------
Group Port-      Type     Protocol  Member Ports
    Channel
--------------------------------------------------------------------------------
14   Po14(SU)   Eth     LACP     Eth1/6(P)   Eth1/7(P)
24   Po24(SU)   Eth     LACP     Eth1/4(P)   Eth1/5(P)
34   Po34(SU)   Eth     LACP     Eth1/1(P)   Eth1/2(P)   Eth1/3(P)
```

همانطور که قابل مشاهده است، همه پورت‌ها فعال هستند.

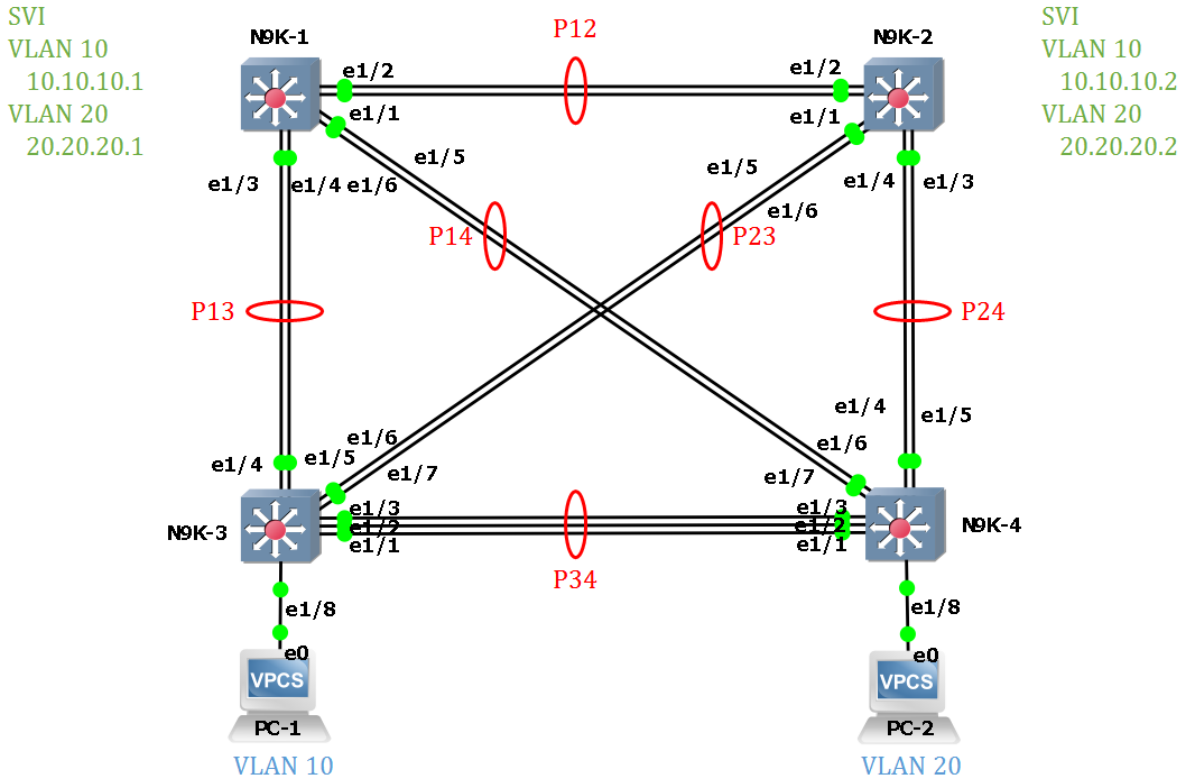
دستورات دیگر برای مشاهده تنظیمات به شرح زیر است:

```
N9K-2# show spanning-tree vlan 10
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po12             Root FWD 3         128.4107 P2p
Po23             Desg FWD 3         128.4118 P2p
Po24             Desg FWD 3         128.4119 P2p
N9K-2# show interface port-channel 12 brief
--------------------------------------------------------------------------------
Port-channel VLAN   Type Mode   Status  Reason               Speed   Protocol Interface
--------------------------------------------------------------------------------
Po12         1      eth  trunk  up      none                 a-1000(D)  lacp
```

Switch Virtual Interface (SVI) Commands ٤-٤-

دستورات مربوط به مسیریابی بین VLANها توسط SVI طبق شکل زیر تنظیم می‌شود. ارتباط بین PC-2 که در VLAN 20 است و PC-1 که در VLAN 10 است توسط SVI برقرار می‌شود. برای تنظیم ابتدا باید قابلیت آن را در Switch تنظیم نمود. پس از تنظیم باید داخل اینترفیس رفت و به آن آدرس IP داده شود.

```
switch(config)# feature interface-vlan
```




```
N9K-1(config)# interface vlan 10
N9K-1(config-if)# ip address 10.10.10.1/24
N9K-1(config-if)# no shutdown
N9K-1(config-if)#exit
N9K-1(config)# vlan 20
N9K-1(config-vlan)#exit
N9K-1(config)# interface vlan 20
N9K-1(config-if)# ip address 20.20.20.1/24
N9K-1(config-if)# no shutdown
N9K-1(config)#spanning-tree mode mst
N9K-1(config)#spanning-tree mst configuration
N9K-1(config-mst)#instance 1 vlan 10,20
```

به همین ترتیب در Switch N9k-2 نیز این دستورات وارد می‌شود. در همه Switchها باید دستورات STP مربوط به VLAN 10,20 را نیز اضافه نمود. باید توجه داشت که Default Gateway نیز باید در PC-2 آدرس 20.20.20.2 و در PC-1 نیز آدرس 10.10.10.1 تنظیم شود. در این تنظیمات هیچ‌گونه پروتکل مسیریابی تنظیم نمی‌شود و ارتباطات بین VLANها از طریق SVI صورت می‌گیرد.

```
switch# show ip interface brief
IP Interface Status for VRF "default"(1)
Interface         IP Address      Interface Status
Vlan10            10.10.10.1      protocol-up/link-up/admin-up
```

```
Vlan20          20.20.20.1     protocol-up/link-up/admin-up
```

مسیر ارتباطی را می‌توان در زیر مشاهده نمود.

```
PC-2> trace 10.10.10.101
trace to 10.10.10.101, 8 hops max, press Ctrl+C to stop
 1  20.20.20.2   24.904 ms  23.156 ms  23.633 ms
 2   * * *
 3  *10.10.10.101   41.978 ms (ICMP type:3, code:3, Destination port unreachable)
```

جدول مسیریابی در زیر قابل مشاهده است.

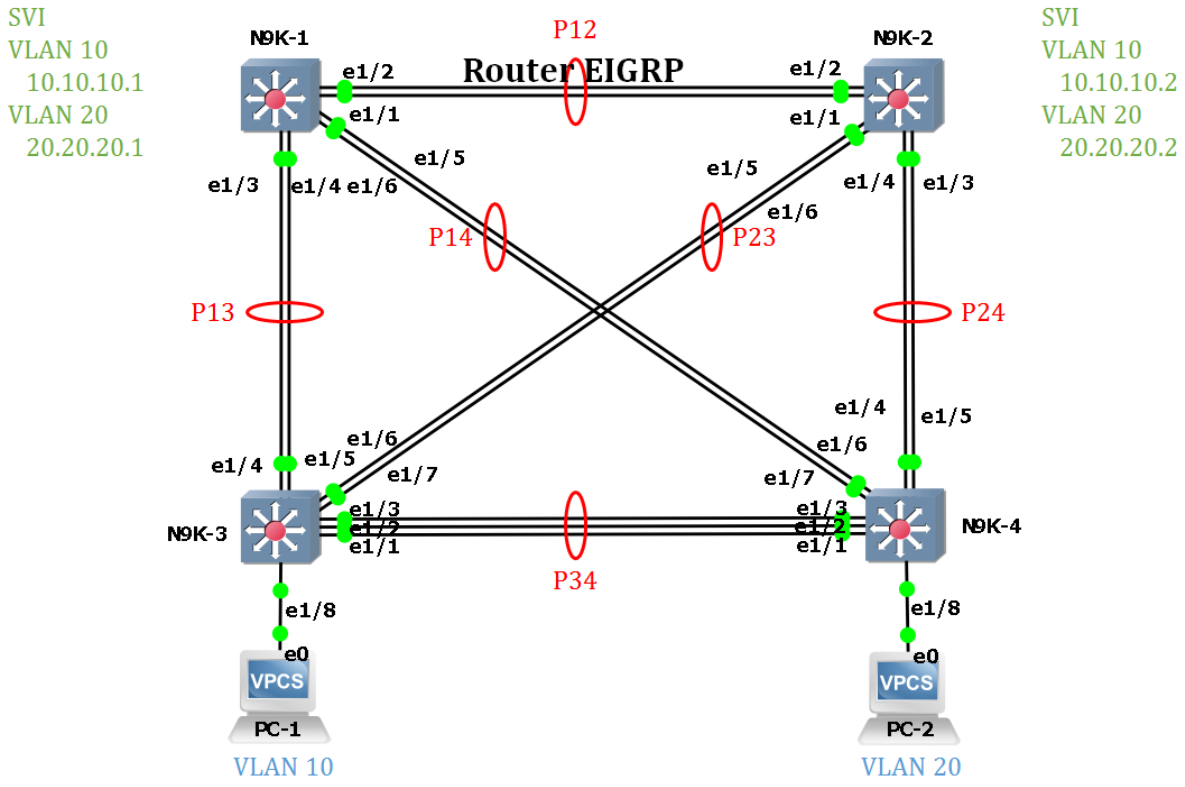
```
switch# sho ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
10.10.10.0/24, ubest/mbest: 1/0, attached
   *via 10.10.10.1, Vlan10, [0/0], 00:29:18, direct
10.10.10.1/32, ubest/mbest: 1/0, attached
   *via 10.10.10.1, Vlan10, [0/0], 00:29:18, local
20.20.20.0/24, ubest/mbest: 1/0, attached
   *via 20.20.20.1, Vlan20, [0/0], 00:29:18, direct
20.20.20.1/32, ubest/mbest: 1/0, attached
   *via 20.20.20.1, Vlan20, [0/0], 00:29:18, local
```

Routing EIGRP Commands ٤-٥-

برای فعال نمودن پروتکل مسیریابی ابتدا باید قابلیت آن را برروی دستگاه فعال نمود. پس از آن یک اینترفیس loopback ساخته و به آن آدرس داده می‌شود. این آدرس جهت Router-ID استفاده می‌شود. پس از آن پروتکل مسیریابی با استفاده از دستور Router فعال می‌شود. سپس Router-ID که همان آدرس Loopback است به عنوان Router-ID پردازش پروتکل داده می‌شود. در نهایت برروی اینترفیس یا لینک مورد نظر پروتکل مسیریابی تعریف می‌شود. بطور مثال برروی Port Channel ابتدا پورت از نوع Switch به route تبدیل شده و سپس پروتکل مسیریابی برروی آن تنظیم می‌شود. دستورات برای نقشه شبکه زیر در ادامه آمده است.

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 1.1.1.1/32
switch(config-if)# no shutdown
switch(config-if)#exit
switch(config)# feature eigrp
switch(config)# router eigrp 1
switch(config-router)# router-id 1.1.1.1
```

switch(config-router)# no shutdown
switch(config-router)# exit



N9K-1(config)# no interface port-channel 12
N9K-1(config)# interface ethernet 1/1-2
N9K-1(config-if-range)# no switchport
N9K-1(config-if-range)# channel-group 12 mode active
N9K-1(config-if-range)# no shutdown
N9K-1(config-if-range)#exit
N9K-1(config)# interface port-channel 12
N9K-1(config-if)# ip address 12.12.12.1/24
N9K-1(config-if)# no shutdown
N9K-1(config-if-range)# show port-channel summary

```
--------------------------------------------------------------------------------
Group Port-      Type     Protocol  Member Ports
    Channel
--------------------------------------------------------------------------------
12   Po12(RU)   Eth     LACP      Eth1/1(P)   Eth1/2(P)
13   Po13(SU)   Eth     NONE      Eth1/3(P)   Eth1/4(P)
14   Po14(SU)   Eth     LACP      Eth1/5(P)   Eth1/6(P)
```

همانطور که قابل مشاهده است Port Channel 12 به Routing تبدیل شده است.

N9K-1(config)# interface vlan 10
N9K-1(config-if)# ip router eigrp 1

```
N9K-1(config-if)# interface vlan 20
N9K-1(config-if)# ip router eigrp 1
N9K-1(config-if)# interface port-channel 12
N9K-1(config-if)# ip router eigrp 1
switch(config)# interface loopback 0
N9K-1(config-if)# ip router eigrp 1
```

برروی Switch N9K-2 نیز همین دستورات پیاده‌سازی می‌شود.

```
N9K-1# show running-config eigrp
router eigrp 1
  router-id 1.1.1.1
interface Vlan10
  ip router eigrp 1
interface Vlan20
  ip router eigrp 1
interface port-channel12
  ip router eigrp 1
N9K-1# show show ip route
N9K-1# show ip eigrp neighbors
IP-EIGRP neighbors for process 1 VRF default
H   Address             Interface     Hold  Uptime  SRTT   RTO  Q  Seq
                            (sec)       (ms)      Cnt Num
0   10.10.10.1          Vlan10        13   00:02:26  675  4050  0   12
2   12.12.12.1          Po12          13   00:02:01  7    50    0   10
1   20.20.20.1          Vlan20        13   00:02:08  835  5000  0   11
N9K-1# show ip eigrp 1
IP-EIGRP AS 1 ID 2.2.2.2 VRF default
  Process-tag: 1
  Instance Number: 1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  metric version: 32bit
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Active Interval: 3 minute(s)
  Number of EIGRP interfaces: 4 (1 loopbacks)
  Number of EIGRP passive interfaces: 0
```

```
  Number of EIGRP peers: 3
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/0
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
  MMODE: Initialized
  Suppress-FIB-Pending ConfiguredN9K-1(config)# show ip interface brief
IP Interface Status for VRF "default"(1)
Interface         IP Address     Interface Status
Vlan10            10.10.10.1     protocol-up/link-up/admin-up
Vlan20            20.20.20.1     protocol-up/link-up/admin-up
Lo0               1.1.1.1        protocol-up/link-up/admin-up
Po12              12.12.12.1     protocol-up/link-up/admin-up
```

Routing OSPF Commands ٤-٦-

این دستورات همانند دستورات EIGRP است با این تفاوت که در قسمت اینترفیس‌ها ناحیه مورد نظر نیز باید وارد شود. بطور مثال در Port Channel 12 پروتکل OSPF بصورت زیر تنظیم می‌شود.

```
N9K-1(config-if)# interface port-channel 12
N9K-1(config-if)# ip router ospf CCNA-DC area 0
```

دستورات زیر برای مشاهده انجام این پروتکل است.

```
N9K-2# show ip ospf neighbors
 OSPF Process ID CCNA-DC VRF default
 Total number of neighbors: 3
 Neighbor ID     Pri State            Up Time  Address         Interface
 1.1.1.1           1 FULL/DR          00:00:49 12.12.12.1      Po12
 1.1.1.1           1 FULL/DR          00:00:58 10.10.10.1      Vlan10
 1.1.1.1           1 FULL/DR          00:00:48 20.20.20.1      Vlan20
N9K-2# show ip route ospf-CCNA-DC
1.1.1.1/32, ubest/mbest: 1/0
    *via 12.12.12.1, Po12, [110/21], 00:02:10, ospf-CCNA-DC, intra
```

در این قسمت نشان داده شده است که مسیر 1.1.1.1 از طریق آدرس 12.12.12.1 و از طریق لینک Po12 امکان‌پذیر است. در EIGRP اگر شماره پردازش را به جای 1 به CCNA-DC تغییر داده شود پروتکل در حالت Shutdown می‌ماند.

با دستور clear ip eigrp neighbors می‌توان پردازش دوباره همسایه‌ها را شروع کرد.

۵- Access Control List (ACL)

لیست کنترل دسترسی مکانیزمی برای فیلتر کردن بسته‌های عبوری از Switch یا Router است که اجازه و یا عدم اجازه عبور ترافیک را می‌دهد. این لیست دسترسی قابلیت‌های زیادی برای فیلتر کردن ترافیک جریان عبوری دارد. ACL می‌تواند برروی جریان ورودی یا خروجی اینترفیس اجرا شود. بطور پیش‌فرض در آخر همه ACLها عدم اجازه عبور بسته‌ها یا Deny Any وجود دارد. به دلایل زیر می‌توان از ACL استفاده نمود:

۱. مکانیزم امنیتی یا کنترل کردن دسترسی میزبان یا شبکه‌ای به شبکه دیگر است.
۲. تعریف می‌شود که چه نوع ترافیکی اجازه عبور دارد.
۳. می‌توان با استفاده از ACL ترافیک شبکه را محدود کرد تا عملکرد شبکه بهبود یابد. بطور مثال به نوعی از ترافیک اجازه عبور داده نمی‌شود تا عملکرد شبکه بهتر شود.

در موارد زیر می‌توان از ACL استفاده نمود:

۱. فقط به مبدأهای خاص اجازه داده شود تا بتوانند به دستگاه‌های مدیریت شبکه متصل شوند.
۲. برای کلاس‌بندی ترافیک Voice می‌توان استفاده نمود. ترافیک در یک دسته قرار داده شوند تا بتوان سیاست‌های QoS را برروی آنها پیاده‌سازی نمود.
۳. از ACL برای کنترل نمودن مسیرها نیز استفاده می‌شود. بطور مثال می‌توان مشخص نمود که کدام مسیر از کدام Router عبور داده شود. همچنین در Redistribution نیز می‌توان استفاده نمود.
۴. برای تست کردن شبکه و مشاهده Logها قابل استفاده است.

در ACL شماره صف وجود دارد که ترتیب سیاست‌ها را مشخص می‌کند. پیشنهاد می‌شود که در هنگام تعریف، بین شماره صف‌ها فضای خالی ایجاد تا در آینده بتوان از این فضاها استفاده نمود. بطور مثال شماره صف‌ها بصورت ۱۰، ۲۰، ۳۰ و ... تعریف شود تا در آینده بتوان شماره صف ۲۵ را بین ۲۰ و ۳۰ قرار داد.

برای تنظیمات ACL باید به نکات زیر توجه نمود:

۱. خطی که بیشتری تطابق را با ترافیک داده دارد باید بالای صف قرار گیرد و به همین ترتیب تطابق‌های کمتر در پایین صف قرار گیرند.
۲. در آخر ACL بصورت پیش‌فرض Deny Any نهفته است و در صورت اجازه عبور بسته‌ها باید Permit استفاده شود.
۳. ACL باید در نزدیک‌ترین دستگاه به مقصدی که می‌خواهد حمایت شود پیاده‌سازی شود.
۴. برای مدیریت آسان‌تر تنها یک لیست دسترسی برای هر پروتکل، هر سمت ترافیک و یا هر اینترفیس باید تعریف شود، ولی امکان تعریف چندین ACL وجود دارد.

تعریف ACL در سیستم NX-OS به یکی از روش‌های زیر است:

۱. Routed ACL: این نوع برروی لایه سه بصورت in یا out تعریف می‌شود. با استفاده از دستور ip access-list و دستور permit یا deny قابل پیاده‌سازی است.
۲. VLAN ACL: با استفاده از access-map پیاده‌سازی می‌شود، با استفاده از match ترافیک مورد نظر تعیین می‌شود و عملیات آن با استفاده از forward و یا drop اجرا می‌شود.
۳. Port ACL: این لیست برروی اینترفیس لایه دو بصورت in یا out اجرا می‌شود.

در ACL می‌توان گروهی از اشیاء مانند پروتکل‌ها، شبکه‌ها و دیگر موارد را تعریف نمود. به این گروه Object Group گفته می‌شود. می‌توان برای این گروه نام تعریف کرد و آنها را در چندین ACL استفاده نمود. Object Group فقط برای IPv4، اینترفیس لایه سه یا Routed ACL قابل پیاده‌سازی است. با دستور object-group network <name> قابل پیاده‌سازی است.

٦- Data Center Layers

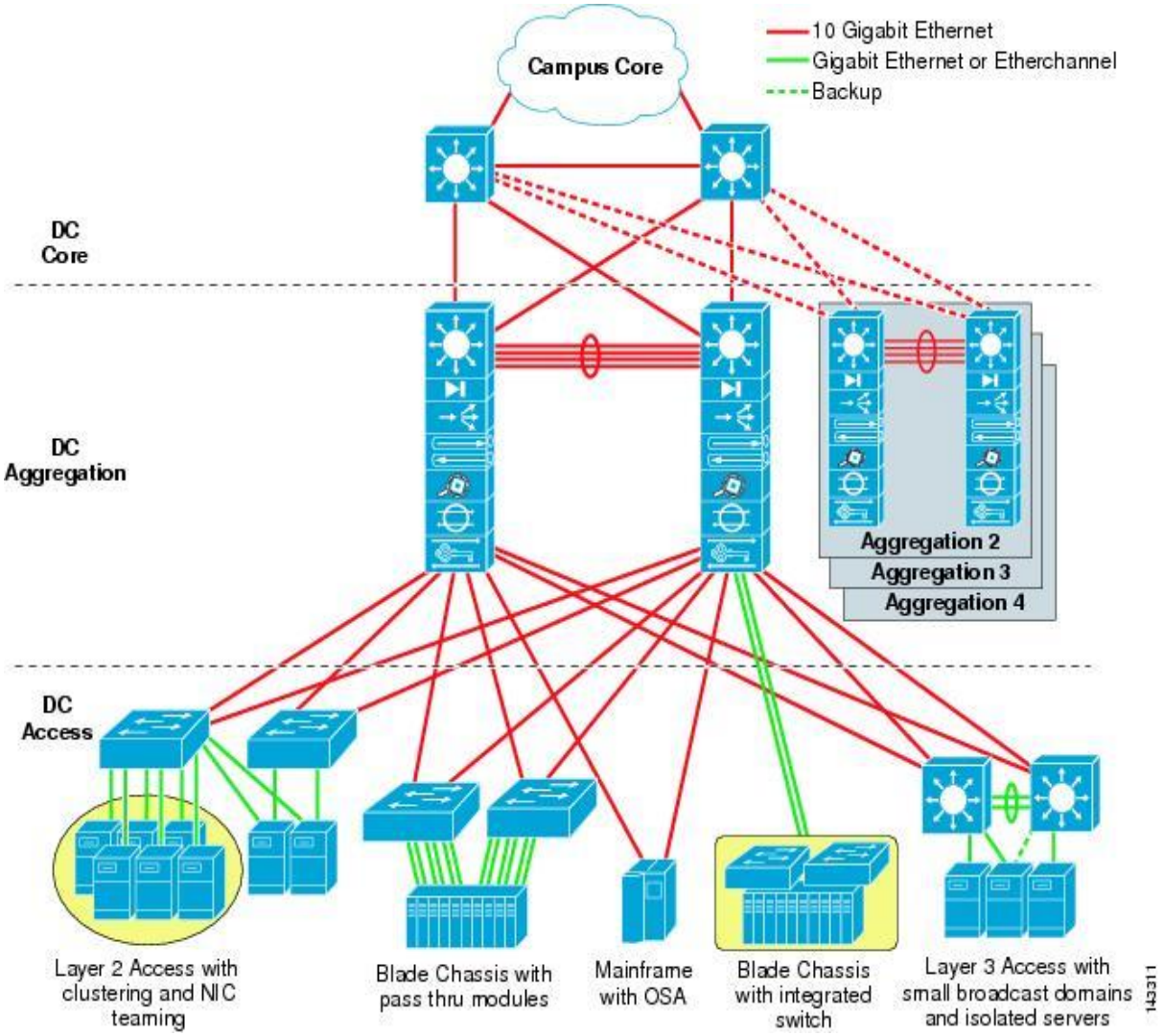
قبل از این که به لایه‌های مرکز داده پرداخته شود توضیح مختصری در رابطه با شبکه‌های Storage Area Network(SAN) داده می‌شود. شبکه‌های SAN مربوط به اطلاعات ذخیره‌سازی برای ارتباط بین سیستم‌های ذخیره‌سازی و سرورها است. در شبکه‌های SAN از تجهیزات سخت‌افزاری خاص مانند، HBA، SAN Switch، SAN Storage و دیگر موارد استفاده می‌شود. به دلایل مختلفی شبکه‌های SAN از LAN جداسازی می‌شود که در ادامه به دلایل آن پرداخته می‌شود.

۱. Security: برای جلوگیری از حمله‌های امنیتی و بهبود امنیت و جداسازی اطلاعات ذخیره‌سازی از دیگر اطلاعات از این نوع شبکه استفاده می‌شود.
۲. Bandwidth: شبکه‌های SAN نیاز به سرعت بیشتری نسبت به شبکه‌های LAN دارند که این خود موجب می‌شود پهنای‌باند اختصاصی برای این نوع شبکه در نظر گرفته شود.
۳. Flow Control: در شبکه‌های LAN پس از رخ داد خطا از مکانیزم‌های جبران خطا استفاده می‌شودو در شبکه‌های SAN خطا رخ نمی‌دهد. در واقع در شبکه‌های SAN منبع ذخیره‌سازی به عنوان یک دیسک به سرور متصل می‌شود. سرور از طریق کارت Host Bus Adapter(HBA) و کابل Fiber Channel به SAN Switch متصل می‌شود و منبع‌ذخیره‌ساز نیز از طریق کابل FC به SAN Switch متصل می‌شود که در نتیجه خطایی رخ نمی‌دهد.
۴. Performance: در شبکه‌های SAN نیاز به عملکرد بالایی نسبت به شبکه‌های LAN احساس می‌شود و سرعت بیشتری از طریق FC تأمین می‌شود.

از شبکه‌های LAN نیز می‌توان برای ارسال بسته‌های ذخیره‌سازی از پروتکل‌های FCoE یا iSCSI استفاده نمود ولی باید توجه داشت که سرعت شبکه باید بسیار بالا باشد بطور مثال 10G باشد. در واقع بسته‌های FC ویا SCSI برروی Ethernet کپسوله و ارسال می‌شوند.

Flow Control در شبکه‌های SAN کمی با شبکه‌های LAN متفاوت است. در شبکه‌های LAN مکانیزم کنترل جریان به این صورت است که مبدأ بسته‌های شبکه را بدون هیچ محدودیتی ارسال می‌کند تا این که Buffer یا فضای دریافت کننده سرریز شود. پس از آن مقصد Puase Frame را به مبدأ ارسال می‌کند تا از ارسال مبدأ جلوگیری شده و Buffer مقصد خالی شود. پس از آن مبدأ دوباره شروع به ارسال بسته می‌نماید. در این بین بسته‌هایی که از بین می‌روند دوباره ارسال می‌شوند. در شبکه‌های SAN مکانیزم کنترل جریان بر مبنای مقصد است به این صورت که ابتدا مبدأ درخواست ارسال بسته را به مقصد ارسال می‌کند. در صورت خالی بودن Buffer مقصد پیام تأیید برای مبدأ ارسال می‌شود و مبدأ شروع به ارسال بسته‌های ذخیره‌سازی می‌کند و در غیر این صورت هیچ بسته‌ای ارسال نمی‌شود. در واقع مقصد با ارسال سیگنال Ready به مبدأ اطلاع می‌دهد که می‌تواند بسته ارسال نماید. این مکانیزم در واقع به Lossless بودن شبکه SAN کمک می‌کند.

در طراحی کلاسیک شرکت سیسکو مراکز داده به سه بخش تقسیم می‌شوند. این سه بخش شامل لایه بالایی یا Core Layer، لایه میانی یا Aggregation Layer و لایه پایینی یا Access Layer می‌شود. مهندسین شبکه بیشتر در لایه پایین کار می‌کنند زیرا تغییرات در لایه Core و Aggregation کمتر اتفاق می‌افتد.



٦-١- Core Layer

اتصال به شبکه دیگر یا اینترنت از طریق لایه Core صورت می‌گیرد. اگر بطور خاص لایه Core بررسی شود موارد زیر در آن قابل مشاهده است.

۱. از کابل‌های با سرعت حداقل 10G استفاده می‌شود.
۲. از ساختار ارسال توزیع شده یا Distributed Forwarding استفاده می‌شود.
۳. دامنه‌های مدیریتی و سیاست‌های استاندارد در این لایه صورت می‌گیرد.
۴. از دامنه‌های چند پخشی یا Multicast Domain پشتیبانی می‌شود.
۵. این لایه برای رشد شبکه بطور مثال 40G و یا 100G باید آماده باشد.

٦-٢- Aggregation Layer

وظیفه این لایه ارتباط بین لایه پایینی و بالایی است. همچنین در این لایه پروتکل‌های مسیریابی، Ethernet و دیگر پروتکل‌های شبکه استفاده می‌شود. در لایه Aggregation موارد زیر قابل مشاهده است.

۱. ارسال ترافیک لایه Access به Core و بالعکس.
۲. سرویس‌های پیشرفته لایه چهار تا هفت مانند: Load Balancing، SSL Offloading، Firewalls، IPS و IDS و دیگر دستگاه‌ها را ارائه می‌دهد. همچنین طلاعات وضعیتی دستگاه‌ها نیز در این لایه نگهداری می‌شود.پ
۳. از پردازش‌های STP، HSRP، FHRP و دیگر موارد پشتیانی می‌کند.

٦-٣- Access Layer

سرورها در لایه Access قرار می‌گیرند. در این لایه موارد زیر قابل مشاهده است.

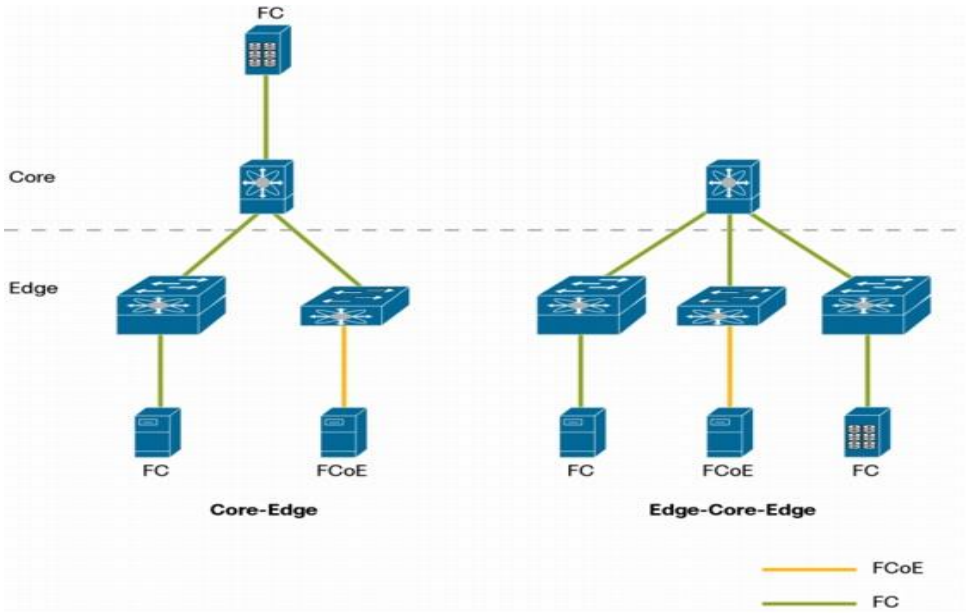
۱. از لایه دو و لایه سه مسیریابی پشتیبانی می‌کند.
۲. پورت‌های متعددی به سرورهای متعدد ارائه می‌کند.
۳. ارتباط یک سرور با یک یا چندین Switch را برقرار می‌کند.
۴. عملکرد بالا و تأخیر پایین را در Switching ارائه می‌کند.
۵. از چندین Uplink و قابلیت‌های اشتراکی بیش از حد یا Oversubscription پشتیبانی می‌کند.

در ساختار مراکز داده ابزارها و سرویس‌های زیر قابل مشاهده است.

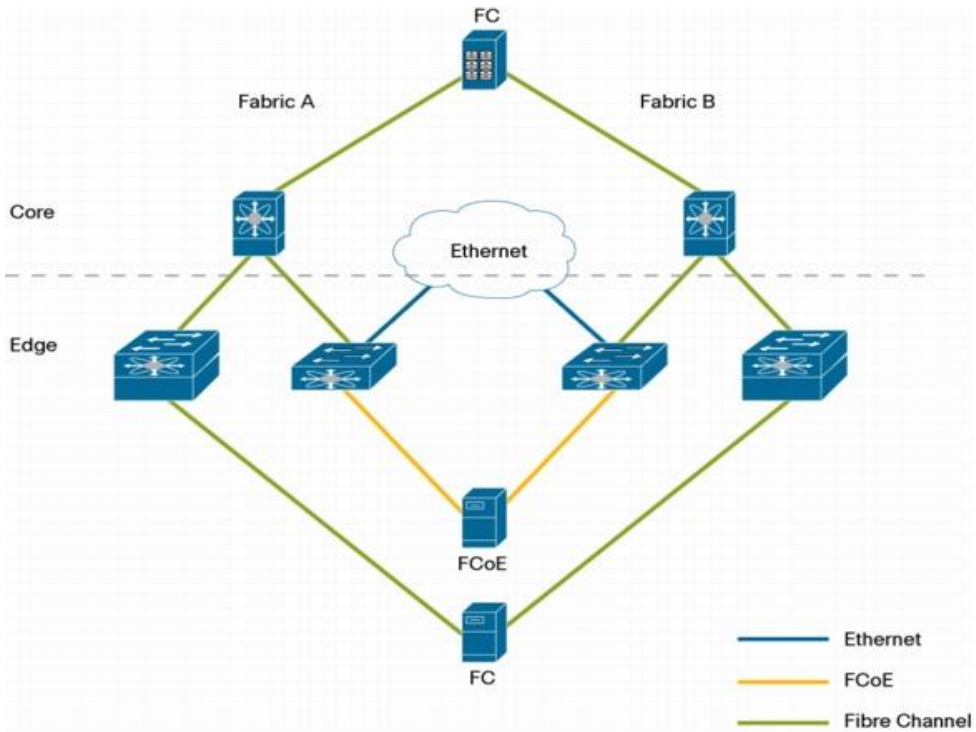
۱. ارتباطات لایه دو و لایه سه
۲. تراکم پورت‌ها
۳. Firewall، ACL، IPS و دیگر سرویس‌ها و تجهیزات امنیتی
۴. Load Balancing و SSL Offloading
۵. استفاده از HA برای جلوگیری از خطا در یک نقطه یا Single Point Of Failure

٦-٤- SAN Topology

نقشه شبکه SAN بسیار ساده‌تر از شبکه LAN است. این شبکه از دو بخش Core و Edge تشکیل شده است. در لایه Core تجهیزات SAN Switch قوی‌تری وجود دارد و این تجهیزات بصورت مستقیم با دستگاه‌های ذخیره‌سازی در ارتباط هستند. این تجهیزات همچنین ارتباط بین Edge Switchها را برقرار می‌کنند. Edge Swirtch با سرورها در ارتباط هستند که ممکن است از پروتکل FC یا FCoE استفاده کنند. در این شبکه دو توپولوژی Core-Edge و Edge-Core-Edge وجود دارد که Core-Edge از لحاظ مدیریتی و عللکرد بهتر است.



برای پیاده‌سازی HA در شبکه‌های SAN معمولاً از توپولوژی زیر استفاده می‌شود.

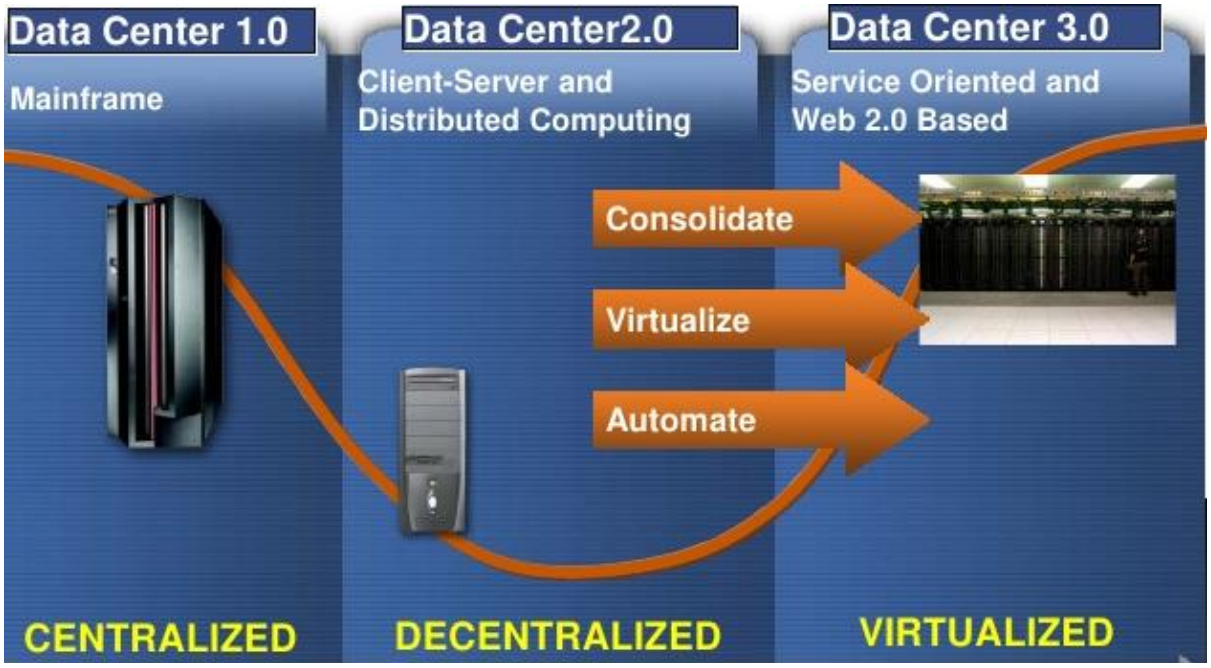


در این توپولوژی هر دستگاه ذخیره‌ساز به دو Core Switch و هر Core Switch به دو Edge Switch و هر سرور به دو Edge Switch متصل است. هر سرور از طریق کارت HBA به Switch متصل می‌شود و از پروتکل FC استفاده می‌کند. در صورت نداشتن کارت HBA می‌توان از پروتکل FCoE استفاده نمود.

مواقعی از توپولوژی Core-Edge استفاده می‌شود که تعداد دستگاه‌ها و ارتباطات ISL زیاد باشد. در این مورد مقیاس‌پذیری بزرگتر، تأخیر کمتر و اشتراک‌گذاری بیش از حد یا Oversubscription زیادی وجود دارد. همچنین افزونگی و اثر بخشی زیادی برای شبکه‌های بزرگ SAN دارد.

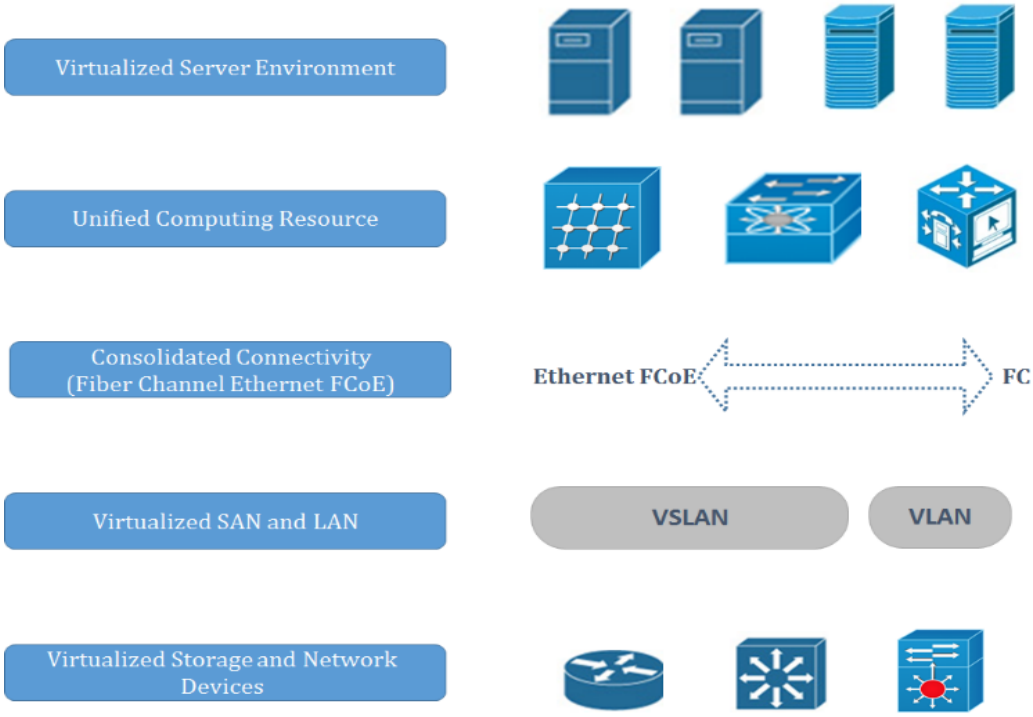
در مواقعی که از SAN کاهش یافته یا ترکیب Edge و Core استفاده می‌شود و یا به عبارت دیگر تنها یک بخش به نام Core وجود دارد، دیگر لینک ISL وجود ندارد. در این موارد مدیریت آسان‌تر اما تجهیزات گران‌تر است. عملکرد بالا و تراکم پورت‌ها بیشتر است. بطور مثال یک Switch Nexus 9000 فقط وجود دارد که با از بین رفتن دستگاه ممکن است ارتباطات از بین برود.

مراکز داده با مرور زمان پیشرفت نموده است که پیشرفت مراکز داده در شکل زیر قابل مشاهده است.



در ابتدا Data Center 1.0 است که یک سیستم قدرتمند و یا یک Mainframe وجود دارد که برروی این سیستم چندین برنامه اجرا شده و به کاربران بصورت مرکزی در یک مکان سرویس می‌دهد. در Data Center 2.0 مرکزیت برداشته شده و ساختار Client-Server ایجاد می‌شود. چندین سرور که برروی آنها چندین برنامه وجود دارد به کاربران سرویس می‌دهد. در Data Center 3.0 از تکنولوژی ابر یا Cloud و مجازی‌سازی یا Virtualization استفاده می‌شود و بر مبنای سرویس است. به این صورت که هر کاربر در هر زمان و مکانی با استفاده از Web می‌تواند سرویس مورد نیاز خود را دریافت نماید.

مؤلفه‌های یک مرکز داده را می‌توان به سه بخش Virtualization، Unified Fabric و Unified Computing تقسیم نمود. در قسمت مجازی‌سازی یا Virtualization سرویس‌هایی مانند VLAN، VRF، VDC و دیگر سرویس‌ها را می‌توان نام برد. همچنین Switch 1000v شرکت سیسکو در این بخش قرار می‌گیرد. در قسمت Unified Fabric تجهیزاتی مانند Nexus Switch که از پروتکل‌های FC، Ethernet و FCoE پشتیبانی می‌کند وجود دارد. در قسمت Unified Cmputing نیز می‌توان محصولات Cisco Unified Computing System را نام برد. اگر نقشه مرکز داده از بالا نگاه شود می‌توان قسمت‌های زیر را در آن مشاهده نمود.



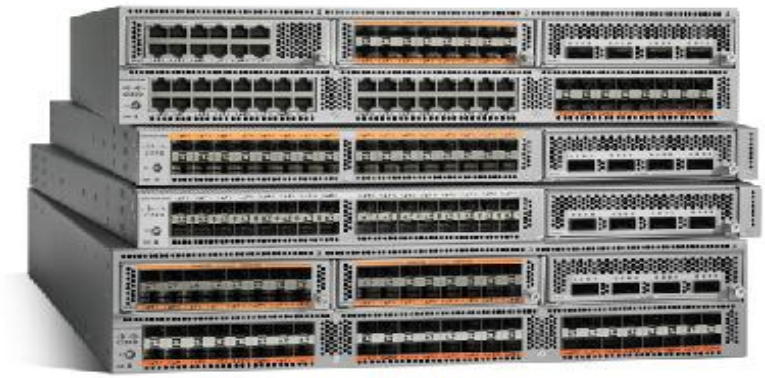
Nexus Switches -۷

همانطور که بیان شد تجهیزات Nexus مربوط به مراکز داده است. با توجه به تقسیم مراکز داده به سه بخش Virtualization، Unified Fabric و Unified Computing، تجهیزات فیزیکی Nexus در بخش Unified Fabric قرار می‌گیرد. شرکت سیسکو این تجهیزات را بر مبنای راه‌حل‌ها و سیاست‌های سازمان در سه لایه Core، Aggregation و Access ارائه می‌نماید. بطور مثال از تجهیزات سری Nexus 7000 در لایه Core، از تجهیزات سری Nexus 7000 در لایه Aggregation و از تجهیزات سری Nexus 2000 در لایه Access می‌توان استفاده نمود. باید توجه داشت که انتخاب هر محصول در هر لایه بر مبنای راه‌حل و یا سیاست سازمان متفاوت است. در لایه Access تجهیزات Nexus به اصطلاح در بالای Rack یا Top Of Rack در مراکز داده قرار می‌گیرند تا ارتباطات تجهیزات داخل Rack را به Switch متصل نمایند. در لایه Aggregation تجهیزات Nexus در انتهای هر ردیف از Rack یا End Of Row قرار می‌گیرند تا ارتباطات بین یک ردیف Rack را برقرار نمایند. در انتها نیز تمامی سر Rackها به باید با هم در ارتباط باشند که به عنوان

لایه Core در نظر گرفته می‌شود. پورت‌های پیشنهادی برای 10G است ولی می‌توان از 1G نیز استفاده نمود. همچنین می‌توان از کابل‌های FC یا Copper و یا از ماژول‌های 40G و یا 100G نیز استفاده نمود. در ادامه لیست محصولات Nexus Switch به اختصار توضیح داده می‌شود.

Nexus 7000 Series

Nexus 5000 Series



Nexus 2000 Series

Nexus 1010 & 1000v -۱-۷

این تجهیزات به عنوان نرم‌افزار یا Appliance بصورت مجازی در مراکز داده به کار برده می‌شود. Switch 1000v را می‌توان برروی سیستم‌عامل مجازی‌ساز ESXi اجرا یا Deploy نمود.

Nexus 2000 -۲-۷

این سری از تجهیزات در بالای Rack در لایه Access کاربرد دارند. برروی این تجهیزات سیستم‌عاملی وجود ندارد و شبیه یک ماژول توسط تجهیز بالاتر از خود که N5K یا N7K می‌تواند باشد مدیریت می‌شوند. این تجهیزات به Nexus 2000 FEX یا Fabric Extenders نیز معروف هستند و از سرعت‌های 100M، 1G، 10G و از FCoE برروی 10G پشتیبانی می‌کنند.

Nexus 3000 -۳-۷

این تجهیزات مانند N2K در بالای Rack قرار می‌گیرند. دارای سیستم‌عامل NX-OS و قابل برنامه‌نویسی هستند. همچنین تأخیر و مصرف برق کمتری را فراهم می‌کنند.

Nexus 4000 -٤-۷

این Switchها برای دسترسی Blade Serverها یا سرورهای تیغه بطور مثال IBM Blade Center طراحی شده‌اند. همچنین به داشتن Switchها و کابل‌های بیشتر در یک شاسی واحد، پیاده‌سازی جابه‌جایی ماشین‌های مجازی، پهنای‌باند بیشتر و مصرف برق کمترکمک می‌کند.

Nexus 5000 & 5500 -٥-۷

N5k به عنوان نسل اول این سری از Switchها است. در نسل دوم Nexus 5500 معرفی شد. این تجهیزات برای یکپارچه‌سازی شبکه‌های LAN و SAN و در لایه Aggregation قابل استفاده هستند. از 1G، 10G، FC و در صورت داشتن سرعت 10G از FCoE پشتیبانی می‌کنند که هر گزینه بر مبنای سیاست‌های سازمان است. بطور مثال تجهیزات Nexus 5548 به عنوان نسل دوم با داشتن پورت‌های Unified Fabric (پورت‌هایی که هم از FC و هم از Ethernet پشتیبانی می‌کنند) دو مدل دارند که انتهای آنها P و یا UP است. در تجهیزات Nexus 5000 بر خلاف Nexus 5500 از پورت‌های Unified Fabric پشتیبانی نمی‌شود. البته با استفاده از ماژول‌های Generic Expansion Module (GEM) می‌توان نوع پورت را تغییر داد. در Nexus 5000 در صورت استفاده از سرعت 10G می‌توان از FCoE استفاده نمود.

Nexus 6000 -٦-۷

این سری از تجهیزات برای سرعت‌های بالای 40G، کارآیی بالا و مصرف برق پایین طراحی شده‌اند. همچنین مجموعه‌ای از ویژگی‌های لایه دو و سه را ارائه می‌نمایند. این تجهیزات در مکان‌هایی با فضاهای محدود با تراکم و کارایی بالا و همچنین در محیط‌های سنتی، مجازی و ابری قابل استفاده هستند.

Nexus 7000 -۷-۷

این تجهیزات کاملاً ماژولار و در لایه Aggregation و Core قابل استفاده هستند. سرعت این Switchها تا 18Tb/s را پشتیبانی می‌کنند و از گزینه‌های متفاوتی بر مبنای شاسی انتخابی استفاده می‌شود که می‌توانند تا ۹، ۱۰ و یا ۱۸ اسلات را پشتیبانی کنند. در ۹ و ۱۸ اسلات، Line Cardها یا همان ماژول‌ها بصورت افقی و در ۱۰ اسلات، Line Cardها بصورت عمودی جانمایی می‌شوند.

Nexus License -۸-۷

در مدل N7K لایسنس‌های زیر مورد استفاده قرار می‌گیرند.

۱. لایسنس Base: این نوع لایسنس بدون پرداخت هزینه است و از قابلیت‌های زیادی مانند vPC، پروتکل‌ها و ابزارهای لایه دو پشتیبانی می‌کند. به غیر از این نوع بقیه لایسنس‌ها با پرداخت هزینه همراه است.
۲. لایسنس Enterprise LAN: زمانی که از پروتکل‌های مسیریابی Dynamic و چند پخشی یا Multicast استفاده شود از این نوع لایسنس استفاده می‌شود.
۳. لایسنس Advanced LAN Enterprise: در مواقعی کاربرد دارد که از VDC و Trustsec استفاده شود.
۴. لایسنس MPLS and XL Module
۵. لایسنس Transport مانند OTV و LISP
۶. لایسنس Enhanced Layer 2 مانند Fabricpath
۷. لایسنس Data Center Network Management برای LAN و SAN
۸. لایسنس FCoE و Storage Enterprise یا Inter-VSAN Routing (IVR)

در مدل N5K یا N5500 لایسنس‌های زیر مورد استفاده قرار می‌گیرند.

۱. لایسنس Storage Product مانند FC، FCoE و N-Port Virtualization (NPV)
۲. لایسنس FCoE NPV مانند اجرای FCoE در حالت NPV یا غیر فعال نمودن FC
۳. لایسنس VM_FEX مانند VM Fabric Extender یا VNtag. VNtag مواقعی استفاده می‌شود که برروی یک سرور مجازی کارت شبکه vNIC یک برچسب منحصر به فرد تولید نماید.
۴. لایسنس Data Center Network Management برای LAN و SAN

لایسنس‌های زیر فقط برروی N5500 استفاده می‌شود.

۱. لایسنس Enhanced Layer 2 مانند Fabricpath
۲. لایسنس Layer 3 Base: استفاده از بی‌نهایت مسیریاب static و ۲۵۶ پروتکل مسیریابی Dynamic (RIPv2، OSPF، EIGRP Stub) را ارائه می‌دهد.
۳. Layer 3 Enterprise: استفاده از Full EIGRP، OSPF 8K و BGP را فراهم می‌کند.

تجهیزات Nexus 2000 FEX بدون لایسنس و کاملاً رایگان اجرا می‌شوند. این Switchها توسط Switch بالادستی مدیریت می‌شوند و در واقع شبیه یک ماژول از راه دور عمل می‌کنند. پیاده‌سازی این نوع تجهیزات به سه صورت امکان‌پذیر است که در ادامه به آن پرداخته می‌شود.

۱. Static Pinning: اتصال دستی فقط برای اتصال به N5K است که یک یا چند uplink به N5K متصل می‌شود. برای این که از چندین uplink استفاده نمود باید حداکثر تعداد آن را در Switch با دستور pinning max-links تنظیم نمود.

۲. Dynamic Pinning: این نوع اتصال برای اتصال به Switchهای N5K و N7K قابل استفاده است. این نوع اتصال از مکانیزم Port Channel برای اتصال به Switch بالادستی و از الگوریتم Hashing برای Load Balancing استفاده می‌کند.
۳. Active Active vPC: این نوع اتصال فقط برای اتصال به N5K است. از تکنیکی برای اتصال به دو Switch بالادستی استفاده می‌کند تا افزونگی را فراهم نماید.
۴. تجهیزات N2K FEX برای اتصال به Switchهای بالادستی یا Parent Switches می‌توانند به هر Line Card از N7K یا N5K متصل شوند. بطور مثال به Line Cardهایی از قبیل M1(32P 10G) و M2 و یا سری F می‌توانند متصل شوند. در تجهیزات N5K می‌توان تا 24 FEX و در N7K می‌توان تا 32 FEX متصل نمود.

با رفتن در سایت سیسکو می‌توان انواع Supervisors، Modules و Chassis مدل N7K را مشاهده نمود.

Supervisors | M-Series I/O Modules | F-Series I/O Modules | Chassis

	Nexus 7700 Supervisor 3E	Nexus 7700 Supervisor 2E	Nexus 7000 Supervisor 2E	Nexus 7000 Supervisor 2	Nexus 7000 Supervisor 1
CPU	Intel Broadwell DE (8 cores)	Dual Quad-Core Xeon	Dual Quad-Core Xeon	Quad-Core Xeon	Dual-Core Xeon
Speed (GHz)	2.0	2.13	2.13	2.13	1.66
Memory (GB)	64	32	32	12	8
Flash memory	USB	USB	USB	USB	Compact Flash
SSD	240 GB	No	No	No	No
Fibre Channel over Ethernet on F2 module		Yes	Yes	Yes	No
CPU share		Yes	Yes	Yes	No
Virtual Device Contexts (VDCs)	8+1 admin VDC	8+1 admin VDC	8+1 admin VDC	4+1 admin VDC	4
Cisco Fabric Extender (FEX) support	64 FEX/3072 ports	64 FEX/3072 ports	64 FEX/3072 ports	32 FEX/1536 ports	32 FEX/1536 ports
Connectivity Management Processor (CMP)	Not supported	Not supported	Not supported	Not supported	Supported

Supervisors | M-Series I/O Modules | F-Series I/O Modules | Chassis

	N7K-M224XP-23L	N7K-M206FQ-23L	N7K-M202CF-22L	N7K-M348XP-25L	N7K-M324FQ-25L	N77-M348XP-23L	N77-M324FQ-25L	N77-M312CQ-26L
Line card family	M2	M2	M2	M3	M3	M3	M3	M3
Chassis supported	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7700	Cisco Nexus 7700	Cisco Nexus 7700
Ports (number and type)	24 x 10 GE	6 x 40 GE	2 x 40/100 GE	48 x 1/10 GE	24 x 40 GE	48 x 1/10GE	24 x 40GE	12 x 100G
Interface type	SFP+	QSFP+	CFP	SFP, SFP+	QSFP+	SFP, SFP+	QSFP+	QSFP28
Fabric bandwidth (Gbps)	240	240	200	480	550	480	960	1200
Performance (Mpps)	120	120	120	720	1440	720	1440	1800
NetFlow	Full/	Full/	Full/					
	sampled	sampled	sampled	Sampled	Sampled	Sampled	Sampled	Sampled
Virtual Port Channel (vPC) support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FabricPath	No	No	No	Yes	Yes	Yes	Yes	Yes
VXLAN	No	No	No	Yes	Yes	Yes	Yes	Yes
BGP-EVPN	No	No	No	Yes	Yes	Yes	Yes	Yes
Encryption	128-bit	128-bit	128-bit	128- and 256-bit	128- and 256-bit	128- and 256-bit	128- and 256-bit	128- and 256-bit
Cisco TrustSec	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Supervisors | M-Series I/O Modules | F-Series I/O Modules | Chassis

	N7K-F248XP-25E	N7K-F312FQ-25	N7K-F306CK-25	N77-F348XP-23	N77-F324FQ-25	N77-F312CK-26	N77-F430CQ-36
Line card family	F2e	F3	F3	F3	F3	F3	F4
Chassis supported	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7000	Cisco Nexus 7700	Cisco Nexus 7700	Cisco Nexus 7700	Cisco Nexus 7700
Ports (number and type)	48 ports, 1 and 10 GE	12 port 40 GE	6 port 100 GE	48 port 1 and 10 GE	24 port 40 GE	12 port 100 GE	30 Port 100GE
Interface type	SFP, SFP+	Quad Small Form Factor Pluggable Plus (QSFP+), Bidirectional (Bidi)	Cisco CPAK	SFP, SFP+	QSFP+, Bidi	Cisco CPAK	QSFP28
Fabric bandwidth (Gbps)	480	480	600	480	960	1200	2400
Performance (Mpps)	720	720	900	720	1440	1800	3450
NetFlow	Sampled	Sampled	Sampled	Sampled	Sampled	Sampled	Sampled
Cisco Fabric Extender (FEX) support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Port Channel (vPC) support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FabricPath support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 3 interface	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fibre Channel over Ethernet (CoE), FabricPath support	Yes	Yes	Yes	Yes	Yes	Yes	No

Supervisors | M-Series I/O Modules | F-Series I/O Modules | Chassis

	7000 4-slot	7000 9-slot	7000 10-slot	7000 18-slot	7700 2-slot	7700 6-slot	7700 10-slot	7700 18-slot
Supervisor redundancy	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
I/O module slots	2	7	8	16	1	4	8	16
Bandwidth per slot (Gbps)	440 Gbps	550 Gbps	550 Gbps	550 Gbps	1.3 Tbps	2.8 Tbps	2.8 Tbps	1.3 Tbps
Switching capacity (Tbps)	1.92	7.7	8.8	17.6	5	23	45	90
1 GE port density	96	336	384	768	48	192	384	768
10 GE port density	96	336	384	768	48	192	384	768
40 GE port density	24	84	96	192	60	120	240	480
100 GE port density	12	42	48	96	60	120	240	480
Rack space (RU)	7	14	21	25	3	9	14	26
Airflow	Side-rear	Side-side	Front-back	Side-side	Front-back	Front-back	Front-back	Front-back

با رفتن در سایت سیسکو می‌توان انواع N5600 را مشاهده نمود.

10-Gbps platforms | 40-Gbps Platforms

	Cisco Nexus 5672UP	Cisco Nexus 5672UP-16G	Cisco Nexus 56128P
			
Rack unit (RU)	1	1	2
Switching capacity	1.44 Tbps	1.44 Tbps	2.56 Tbps
Expansion slots	None	None	2
Unified ports	Yes	Yes	Yes
Fixed, built-in ports	48 (10 GE)	48 (10 GE)	48 (10 GE)
1/10 GE, 10-Gbps FCoE port density	Up to 72	Up to 72	Up to 128
40-GE, FCoE port density	N/A	N/A	N/A
1/10-Gb BASE-T	No	No	No
40 GE uplinks	6	6	Up to 8 (through expansion module)
100 GE ports	No	No	No
Fibre Channel port density (8/4/2/1 Gbps)	16	24	Up to 48 (through expansion modules only)
16-Gbps Fibre Channel	No	Yes, up to 24 ports	No
Fabric extender support	Yes, up to 24 (L2, L3)	Yes, up to 24 (L2, L3)	Yes, up to 24 (L2, L3)
Hot-swappable power supplies and fan trays	Yes	Yes	Yes

10-Gbps platforms | 40-Gbps Platforms

	Cisco Nexus 5624Q	Cisco Nexus 5648Q	Cisco Nexus 5696Q
			
Rack unit (RU)	1	2	4
Switching capacity	1.92 Tbps	3.84 Tbps	7.68 Tbps
Expansion slots	1	2	8
Unified ports	No	No	Yes
Fixed, built-in ports	12 (40 GE)	24 (40 GE)	N/A
1/10 GE, 10-Gbps FCoE port density	96	192	384
40-GE, FCoE port density	24	48	96
1/10-Gb BASE-T	No	No	No
40 GE uplinks	N/A	N/A	N/A
100 GE ports	No	No	Upto 32 (through expansion module)
Fibre Channel port density (8/4/2/1 Gbps)	No	No	60
16-Gbps Fibre Channel	No	No	No
Fabric extender support	Yes, up to 24 (L2, L3)	Yes, up to 24 (L2, L3)	Yes, up to 48 (L2), 32 (L3)
Hot-swappable power supplies and fan trays	Yes	Yes	Yes

بطور نمونه N2K 1G FEX نیز در تصویر زیر قابل مشاهده است.

1 GE Fabric Extender | 10GBASE-T Fabric Extender | 10G SFP+ Fabric Extender

	Cisco Nexus 2224TP	Cisco Nexus 2248TP	Cisco Nexus 2248TP-E
Fabric extender host interfaces	24	48	48
Fabric extender host interface types	100BASE-T/1000BASE-T ports: RJ-45 connectors	100BASE-T/1000BASE-T ports: RJ-45 connectors	100BASE-T/1000BASE-T ports: RJ-45 connectors
Fabric extender fabric interfaces	2	4	4
Fabric speed	20 Gbps in each direction (40 Gbps full duplex)	40 Gbps in each direction (80 Gbps full duplex)	40 Gbps in each direction (80 Gbps full duplex)
Oversubscription	1.2:1	1.2:1	1.2:1
Performance	Hardware forwarding at 88 Gbps or 65 mpps	Hardware forwarding at 176 Gbps or 131 mpps	Hardware forwarding at 176 Gbps or 131 mpps
Cisco parent switch	Cisco Nexus 5000, 6000, 7000, or 9000 Series*	Cisco Nexus 5000, 6000, 7000, or 9000 Series*	Cisco Nexus 5000, 6000, 7000, or 9000 Series*
FCoE support	No	No	No
Airflow	Port-side exhaust and port-side intake	Port-side exhaust and port-side intake	Port-side exhaust and port-side intake
Buffers	8 MB	8 MB	32 MB

MDS SAN Switches -۸

MDS Switchها برای شبکه‌های SAN طراحی شده‌اند. این تجهیزات دسترسی‌پذیری بالا(High Availability)، مقیاس‌پذیری(Scalability)، امنیت(Security)، قابلیت مدیریت(Managability) و پشتیبانی از چند پروتکل مانند FCoE، FCIP، iSCSI و دیگر پروتکل‌ها را فراهم می‌سازند. سری مربوط به این تجهیزات با نام MDS 9000 شناخته می‌شوند. این Switchها برای دو دسته Small/Medium Business و Enterprises and Service Providers طراحی شده‌اند که سری 9100، 9200 و 9300 مربوط به دسته Small/Medium Business و سری 9500 و 9700 مربوط به دسته Enterprises and Service Providers هستند. باید توجه داشت که مدل‌هایی مانند 9222i، 9216/9216A، 9216i، 9148 و تمامی MDS 9500ها از خط تولید خارج شده‌اند. همچنین تجهیزاتی وجود دارد که برروی شاسی‌های HP and IBM Blade جانمایی می‌شوند. تمامی تجهیزات MDS از سیستم‌عامل NX-OS استفاده می‌کنند.

Switchهای مدل MDS 9700 دارای ۶، ۱۰ و ۱۸ اسلات هستند که هر کدام از داشتن دو Supervisor برای افزونگی پشتیبانی می‌کنند. این تجهیزات تا پهنای‌باند 48Tbps و از سرعت‌های 2/4/8، 4/8/6/32 و 10Gbps برای FC پشتیبانی می‌کنند. همچنین از سرعت‌های 10/40 برای FCoE و FCIP نیز پشتیبانی می‌شوند. از ۱۹۲، ۳۸۴ و ۷۶۸ پورت برای هر شاسی و ۱۱۵۲ پورت برای هر Rack پشتیبانی می‌کنند. این تجهیزات همچنین از قابلیت چند پروتکلی مانند FC، FCoE، FCIP، iSCSI و دیگر پروتکل‌های امنیتی مانند Role Based Access Control(RBAC)، VSAN، ACL، SNMPv3، SFTP، SSH و Trustsec پشتیبانی می‌کنند. در مورد HA در تجهیزات MDS از افزونگی در Supervisor، Power، Fan و دیگر موارد پشتیبانی می‌شود. در تصاویر زیر مقایسه‌ای از انواع MDS 9700 صورت گرفته است.

Cisco Model	Cisco MDS 9718 multilayer director	Cisco MDS 9710 multilayer director	Cisco MDS 9706 multilayer director
			
Configuration	Chassis, dual Supervisor-1E Module, and up to 16 x 3000-Watt (W) power supplies	Chassis, dual Supervisor-1 Module, and up to 8 x 3000W power supplies	Chassis, dual Supervisor-1 Module, and up to 4 x 3000W power supplies
Maximum 2/4/8/10/16/32-Gbps Fibre Channel ports per chassis	768	384	192
Maximum 10-Gbps Fibre Channel over Ethernet (FCoE) ports per chassis	768	384	192
Maximum 40-Gbps FCoE ports per chassis	384	192	96
Maximum Fibre Channel over IP (FCIP) ports per chassis	128 x 1/10 Gigabit Ethernet 32 x 40 Gigabit Ethernet[1]	64 x 1/10 Gigabit Ethernet 16 x 40 Gigabit Ethernet[1]	32 x 1/10 Gigabit Ethernet 8 x 40 Gigabit Ethernet[1]
Port speed	2/4/8/10/16/32-Gbps Fibre Channel 10/40-Gbps FCoE 1/10/40-Gbps[1] FCIP		
Port modules and Cisco part numbers	48-port 4/8/16/32-Gbps Fibre Channel switching module		DS-X9648-1536K9
	48-port 2/4/8/10/16-Gbps Fibre Channel switching module		DS-X9448-768K9
	24-port 2/4/8/10/16-Gbps Fibre Channel, 8-port 1/10 Gigabit Ethernet for FCIP, and 2-port 40 Gigabit Ethernet[1] for FCIP		DS-X9334-K9
	24-port 40-Gbps FCoE module		DS-X9824-960K9
	48-port 10-Gbps FCoE module		DS-X9848-480K9
Licenses and Cisco part numbers	SAN Insights Package for MDS 9700 32G Directors		L-D-M97S-AXK9=
	Enterprise package license for 1 MDS9700 switch		M97ENTK9
	DCNM for SAN License for MDS 9700		DCNM-SAN-M97-K9
	Mainframe package license for 1 MDS 9700 Series Multilayer Director switch		M97FIC1K9
	IOA License for 24/10 Module (1x engine) on MDS 9700		M97IOA2410=
	IOA License Pack for 24/10 Module (2X engines) on MDS 9700		M97IOA24102X=
IBM Fibre Connection (FICON) certification	No	Yes	Yes
Expandability	16 module slots	8 module slots	4 module slots
Rack units	26	14	9
Chassis per rack	1	2	3
Crossbar switching fabric module	DS-X9718-FAB1	DS-X9710-FAB1	DS-X9706-FAB1
Supervisor	DS-X97-SF1E-K9	DS-X97-SF1-K9	DS-X97-SF1-K9
Power supply	DS-CAC97-3KW AC PSU, DS-CDC97-3KW= DC PSU, DS-CHV-3.5KW HVDC PSU	DS-CAC97-3KW AC PSU, DS-CDC97-3KW= DC PSU, DS-CHV-3.5KW HVDC PSU	DS-CAC97-3KW AC PSU, DS-CDC97-3KW= DC PSU, DS-CHV-3.5KW HVDC PSU
Features	• Data center SAN consolidation • Business continuance • Centralized SAN management • Advanced SAN security for compliance and regulation • Centralized backup, recovery, and archiving through intelligent fabric applications • Native switch-based programming and Representational State Transfer (REST) API support		

در قسمت Small/Medium Business در سری MDS 9200 تنها مدل MDS 9250i تولید می‌شود که دارای ۵۰ پورت ثابت است و قابلیت کارآیی بالا و مقیاس‌پذیری برای همگرایی بین LAN و SAN را فراهم می‌کند. در تصویر زیر سری MDS 9100 با یکدیگر مقایسه شده‌اند.

Cisco Model	Cisco MDS 9132T 32G Multilayer Fabric Switch	Cisco MDS 9148T 32G Multilayer Fabric Switch	Cisco MDS 9396T 32G Multilayer Fabric Switch
			
Configuration	Semi-modular 1RU chassis; configurable to 8, 16, 24 or 32 ports enabled	Fixed 1RU chassis; configurable to 24, 32, 40 or 48 ports enabled	Semi-modular 2RU chassis; configurable to 48, 64, 80 or 96 ports enabled
Ports	• 16 X 4/8/16/32-Gbps Fibre channel (line rate) base switch • 16X 4/8/16/32-Gbps Fibre channel (line rate) expansion module	• 48 X 4/8/16/32-Gbps Fibre channel (line rate) fixed switch	• 96 X 4/8/16/32-Gbps Fibre channel (line rate) semi-modular switch
Port speed	4/8/16/32-Gbps Fibre Channel	4/8/16/32-Gbps Fibre Channel	4/8/16/32-Gbps Fibre Channel
License keys	L-D-M91S-AXK9= M9100ENT1K9 DCNM-SAN-M91-K9 DCNM-S-M91XK9=	L-D-M91S-AXK9=[2] M9100ENT1K9 DCNM-SAN-M91-K9 DCNM-S-M91XK9=	M9300ENT1K9 DCNM-SAN-M93-K9 DCNM-SAN-M93X-K9 M93ENTDCNMX-K9 M93ENTDCNM-K9
Features	• Modular high availability • Autozone capable • Integrated SAN Telemetry • FC-NVMe ready • Slow drain detection and link isolation • Sophisticated Diagnostics • Virtual Machine awareness • Up to 8270 Buffer-to-Buffer (B2B) credits per port (up to 612-km native 32-Gbps Fibre Channel SAN extension capability) • Native on-switch REST API and PYTHON interpreter • FC Link encryption • 16-member port channel • Power-On Auto Provisioning (POAP) and intelligent diagnostics • Cisco In-Service Software Upgrade (ISSU) and dual redundant hot- swappable power supplies for high availability • High-performance ISLs with multipath load balancing • Smart zoning and VOQ • Anti-counterfeit technology		

MDS License ۸-۱-

بیشتر لایسنس‌ها در MDS Switch بر مبنای قابلیت و یا ماژول است. باید توجه داشت که سخت‌افزار MDS باید از لایسنس خریداری شده پشتیبانی نماید. لایسنس رایگان استاندارد یا Standard Package از قابلیت‌های بسیاری مانند FC، iSCSI، iSLB، VSAN، Zoning، Port Channel، RBAC، SNMPv3، SSH، Radius، TACACS و دیگر موارد پشتیبانی می‌کند.

لایسنس‌های خاص دیگر نیز وجود دارد که ممکن است شامل مواردی مانند Enterprise Package (IVR, QoS, FCSP, Port Security, IPSec, TrustSec)، SAN Extender IP (FCIP)، Mainframe (FICON)، Cisco Fabric Manager Server که البته نسخه جدید آن Cisco Data Center Network Manager است و برای مدیریت یکپارچه Routing، Switching و Storage در مراکز داده استفاده می‌شود، Data Mobility Manager (DMM) که سرویسی برای جابه‌جایی داده‌ها بین آرایه‌های ذخیره‌سازی ناهمگن است و نیاز به راه‌حل‌های مختلف مهاجرت را برطرف می‌کند، On-Demand Port Activation، Storage Media Encryption (SME) و در آخر لایسنس Storage Service Enabaler Package (SSN-16) باشد.

۹- Virtual Port Channel (vPC)

Virtual Port Channel یا به اختصار vPC اجازه می‌دهد تا لینک‌های فیزیکی بین دو دستگاه Nexus Switch به عنوان یک Port Channel واحد برای دستگاه سوم ظاهر شود. در واقع دستگاه سوم این دو دستگاه را که برروی آنها vPC اجرا شده است به عنوان یک دستگاه تشخیص می‌دهد. دستگاه سوم می‌توان Switch، Nexus 2000 FEX، سرور و یا هر دستگاه دیگری باشد. به اصطلاح به دو دستگاهی که برروی آن vPC اجرا شده است vPC Peers گویند.

این قابلیت اجازه می‌دهد تا از همه لینک‌ها بدون STP Blocking استفاده شود و از تکنیک‌های Hashing برای Load Balancing استفاده کنند. در واقع برروی vPC پروتکل STP در حال اجراست ولی به لینک‌های عضو vPC اجازه عبور داده می‌شود. به عبارت دیگر وظیفه جلوگیری از حلقه برعهده vPC است. این قابلیت شبیه به استفاده از چند شاسی به عنوان Etherchannel، Stack در Switch 3750 و یا VSS در 6500 Switch است.

در نگاه سطح بالا به vPC باید توجه داشت که فقط دو دستگاه به فیزیکی که به نام vPC Peers شناخته می‌شوند می‌توان استفاده نمود. vPC Peers باید در یک دامنه هم شماره باشند. حداکثر تعداد vPC Peers برای هر دستگاه یا VDC یک است. به عبارت دیگر تنها یک شریک در vPC وجود دارد. بین هر دو دستگاه باید لینک‌های فیزیکی وجود داشته باشد که به Peer Links شناخته می‌شوند. علاوه بر این Peer Links باید باید لینک جداگانه‌ای برای Keepalive یا تشخیص زنده بودن وجود داشته باشد که به آن Peer Keepalive Link گفته می‌شود. در نهایت باید پورت‌هایی را به عنوان عضو در vPC مشخص نمود که به این پورت‌ها vPC Member Ports گفته می‌شود.

۹-۱- vPC Peer Link

این لینک‌ها از نوع Layer 2 Trunk هستند و اطلاعات مربوط به بخش Control Plane یا اطلاعات مدیریتی شبکه را بین دو دستگاه همگام‌سازی می‌کنند.این اطلاعات می‌تواند شامل MAC Table، ARP Cash، IGMP

Snooping DB و دیگر موارد باشد. برای ارسال اطلاعات از پروتکل Cisco Fabric Service Over Ethernet (CFSOE) استفاده می‌شود. انتخاب نقش‌های vPC Primary و Secondary نیز برعهده این لینک‌ها است. بصورت معمول از این لینک‌ها برای Data Plane یا اطلاعات ترافیک ارسالی استفاده نمی‌شود. این لینک‌ها معمولاً پهنای‌باند کمتری نسبت به پورت‌های عضو vPC دارند. برای Peer Link باید حداقل از دو لینک با سرعت 10G استفاده نمود.

۹-۲- vPC Peer Keepalive Link

این لینک از نوع Layer 3 است که از ضربان قلب یا Heartbeat در Control Plane برای تشخیص صحت دستگاه‌ها استفاده می‌شود. برروی این لینک می‌توان از هر پروتکل مسیریابی استفاده نمود ولی باید توجه داشت که حداقل Ping بین آنها وجود داشته باشد. این لینک از وضعیت Active/Active یا به اصطلاح Split Brain یا فکر نامتمرکز جلوگیری می‌کند. این لینک نیز برای Data Plane استفاده نمی‌شود و می‌تواند یکی از پورت‌های MGMT0، لینک مسیریابی لایه سه و یا Port Channel باشد.

۹-۳- vPC Member Port

این پورت‌ها مربوط به عبور ترافیک Data Plane هستند که با استفاده از Port Channel به Switchهای پایین دستی خود متصل هستند. هر vPC Peer باید حداقل یک Member Port داشته باشد. از دید Switchهای پایین دستی vPC Peerها یک Switch دیده می‌شوند. VLANهایی که برروی vPC Memberها هستند باید برروی vPC Peer Links که Trunk هستند اجازه عبور داشته باشند.

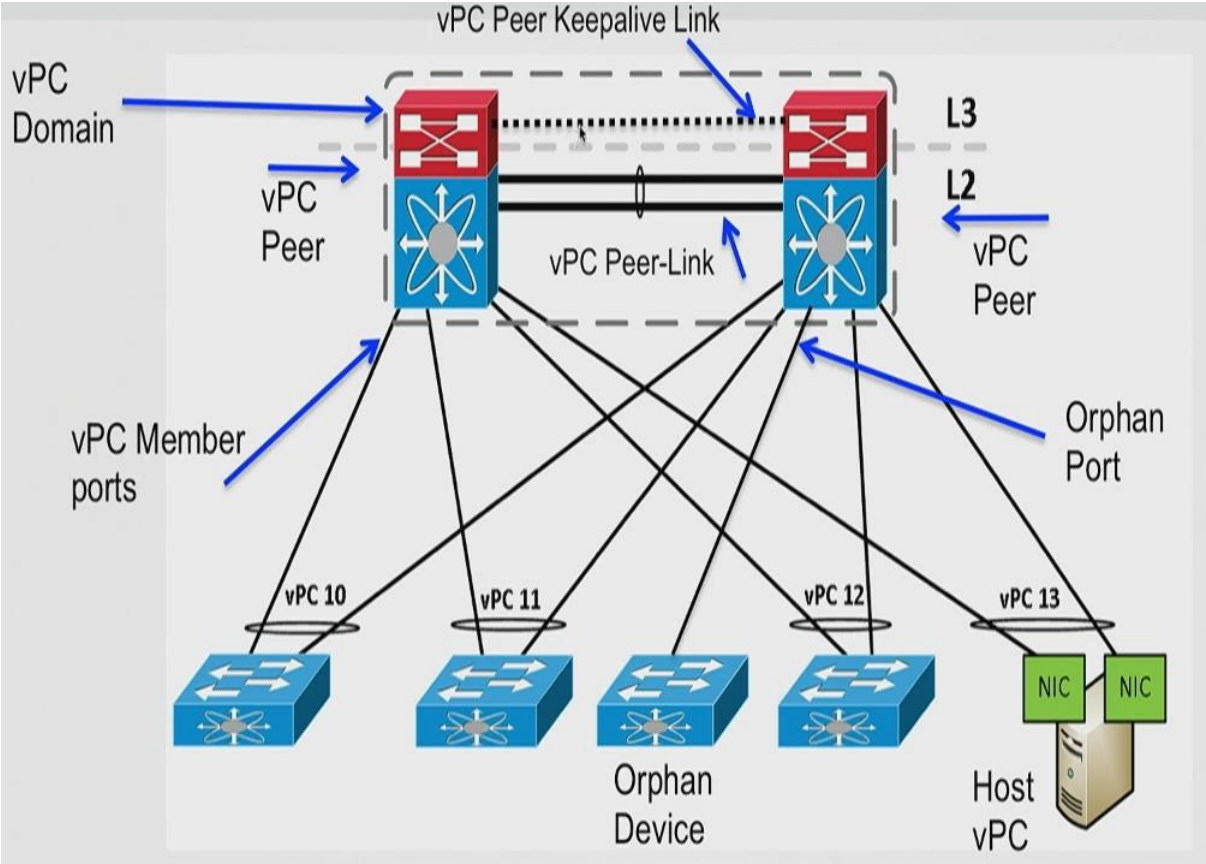
۹-٤- vPC Orphan

دستگاه Orphan یا یتیم به دستگاهی گفته می‌شود که تنها به یکی از vPC Peerها متصل شده باشد. Orphan Port نیز به پورتی برروی vPC Peer گفته می‌شود که Switchport است و به دستگاه Orphan متصل است. مشکل زمانی به وجود می‌آید که خطایی در vPC Peer رخ دهد که Orphan Port برروی آن است. در این حالت این دستگاه از شبکه جدا می‌شود. حال اگر خطا برروی vPC Peer دیگر رخ دهد قسمت دوم شبکه را از دست می‌دهد. در نتیجه پیشنهاد می‌شود که حداقل از دو پورت برای vPC Member برای هر vPC Peer استفاده نمود.

۹-۵- vPC Loop

هدف از vPC این است که افزونگی لینک‌ها یا Redundant Link را از دید STP پنهان نماید. نتیجه این عمل ایجاد سیلی از حلقه‌های لایه دو می‌شود. پس مکانیزم جلوگیری از حلقه برعهده vPC است که به آن vPC Check گفته می‌شود. زمانی که Frameهای لایه دو از vPC Peer Link دریافت می‌شوند، از پورت‌های vPC Member دستگاه vPC Peer طرف دیگر که یک vPC Member فعال در همان شماره vPC دارد، ارسال نمی‌شوند. به زبان ساده‌تر اگر بسته‌ای از Switch پایین دستی با شماره vPC 12 وارد vPC Peer Link

شود، دستگاهی که این بسته را دریافت می‌کند، بسته را به همان vPC Member با شماره vPC 12 ارسال نمی‌کند. استثنائی که در vPC Check وجود دارد این است که اگر پورت vPC Peer Member غیر فعال شود، یعنی به حالت Orphan رود، آنگاه vPC Check برروی آن غیر فعال می‌شود. باید توجه داشت که این اطلاعات بصورت مکرر از طریق vPC Peer Link جابه‌جا می‌شوند.



۱۰- FabricPath

در طراحی شبکه از ویژگی افزونگی مانند vPC در زیرساخت‌های فیزیکی و تجهیزات استفاده می‌شود. در شبکه های لایه ۲ با ایجاد افزونگی در لینک‌های ارتباطی یکی از مشکلات وجود پروتکل STP است. استفاده از این پروتکل دارای معایبی همچون از دست رفتن بخشی از پهنای‌باند به دلیل غیر فعال شدن برخی لینک‌ها و زمان‌بر بودن STP در صورت فعال یا غیرفعال شدن یک لینک است. در برخی طراحی‌ها پروتکل STP جای خود را به مکانیزم‌هایی مانند Port Channel و vPC می‌دهد. به منظور حل مشکل STP و استفاده از مزایای شبکه‌های لایه ۲ قابلیت جدیدی در Nexus Switches بوجود آمده که FabricPath نامیده می‌شود. این ویژگی با استفاده از ترکیب بهترین جنبه‌های لایه دو و لایه سه، افزونگی و جلوگیری از حلقه را فراهم می‌کند. اساس FabricPath استفاده از قابلیت‌های مسیریابی در لایه دو یا Layer 2 Routing است. در واقع Frameهای Ethernet را برروی شبکه مسیریابی شده عبور می‌دهد. در مورد vPC توپولوژی بصورت مثلثی یا Triangle است که دو vPC Peer و یک دستگاه سوم وجود دارد. در FabricPath این اجازه داده می‌شود که توپولوژی

دلخواه مانند Full Mesh، Partial Mesh، Triangle، Square و دیگر موارد طراحی شود. در واقع FabricPath جایگزینی برای vPC و STP است.

۱۰-۱- FabricPath Terminology

قبل از این که به عملکرد پروتکل FabricPath پرداخته شود باید با اصطلاحات زیر آشنا شد.

۱. Classical Ethernet: اگر دستگاهی برروی آن Ethernet با STP و Flooding عادی اجرا شود به اصطلاح گفته می‌شود برروی آن Classical Ethernet(CE) اجرا شده است.
۲. Leaf Switch: این Switch با دستگاهی که برروی آن Classical Ethernet اجرا شده است در ارتباط است. دستگاه‌های که برروی آن CE اجرا می‌شود، می‌تواند Server، Host، End Device و یا هر دستگاه دیگری باشد.
۳. Spine Switch: این Switch با هیچ Host، End Device و یا هر دستگاهی که برروی آن STP باشد در ارتباط نیست و فقط با Leaf Switch در ارتباط است.
۴. FabricPath Core Port: این پورت ارتباط بین Leaf با Spine و یا Spine با Spine را برقرار می‌کند. با دستور switchport mode fabricpath می‌توان این پورت را به حالت FabricPath تغییر داد. البته باید توجه داشت که Switch مورد نظر از لحاظ سخت‌افزاری FabricPath را پشتیبانی نماید. تجهیزاتی که از FabricPath پشتیبانی می‌کنند شامل Nexus 5500 و ماژول‌های سری F مربوط به Nexus 7K هستند.
۵. Classical Ethernet Edge Port: پورتی است که ارتباط Leaf را به یک دامنه CE برقرار می‌کند.

۱۰-۲- FabricPath Control Plane

همانطور که گفته شد در واقع از پروتکل مسیریابی برروی لایه دو استفاده می‌شود. در این مسیریابی لایه دو FabricPath از پروتکل IS-IS استفاده می‌شود. هدف این پروتکل محاسبه درخت بهینه مسیریابی بین تمامی گره‌های FabricPath است. پروتکل IS-IS نیز از الگوریتم دایجسترا برای پیدا کردن درخت بهینه استفاده می‌کند. باید توجه داشت که از IS-IS برای اعلام آدرس MAC یا MAC Advertisement در FabricPath استفاده نمی‌شود و فقط برای اعلام Switch-ID و مسیرهای بین آنها استفاده می‌شود. در IS-IS نیاز به لایه سه IP وجود ندارد. در FabricPath از Equal-Cost Multipath (ECMP) و تا ۱۶ لینک فعال پشتیبانی می‌شود. به عبارت ساده‌تر از Load Balancing در لایه دو بدون STP، Port Channel و یا vPC استفاده می‌شود. باید توجه داشت که نیازی به Port Channel در FabricPath وجود ندارد ولی می‌توان آن را فعال نمود.

FabricPath Data Plane -۳-۱۰

بسته‌های Classical Ethernet در هدر جدید FabricPath کپسوله می‌شوند. FabricPath یک استاندارد Ethernet و یا استاندارد باز Transparent Interconnection of Lots of Links (TRILL) نیست. TRILL بصورت نرم‌افزاری است و نیازمند سخت‌افزار خاص نیست که این برعکس FabricPath است.

Feature	FabricPath	TRILL
Frame Routing (ECMP, TTL, RPFC, ...)	Yes	Yes
vPC+	Yes	NO
FHRP Active/Active	Yes	NO
Multiple Topologies	Yes	NO
Conversational Learning	Yes	NO
Inter-Switch Links	Point-To-Point Only	Point-To-Point Or Shared

در هدر FabricPath مقدارهای Switch-ID مبدأ و مقصد جانمایی شده است که با استفاده از آنها ترافیک لایه دو توسط درخت STP از Switch مبدأ به Switch مقصد ارسال می‌شود. در واقع مانند پروتکل‌های مسیریابی IS-IS و OSPF در لایه سه عمل می‌کند.

FabricPath MAC Learning -٤-۱۰

یادگیری آدرس‌های MAC و ذخیره‌سازی آنها در جدول MAC به دو صورت انجام می‌گیرد.

۱. Traditional یا سنتی: در این روش آدرس‌های MAC مبدأ از تمامی ترافیک‌های دریافتی یاد گرفته می‌شود. پس از آن سیلی از درخواست‌ها برای استخراج آدرس‌های MAC مقصد ارسال می‌شود. با توجه به بسته پاسخ‌ها مبدأ MAC به عنوان مقصد در جدول MAC ذخیره می‌شود. این نوع فقط برای Classical Ethernet استفاده می‌شود.

۲. Conversational یا مکالمه‌ای: در این حالت فقط آدرس‌های MAC که در حال گفت‌وگو هستند در جدول MAC ذخیره می‌شوند که این باعث کاهش اندازه جدول MAC می‌شود. برای هر VLAN می‌توان حالت مکالمه‌ای را فعال نمود. در Classical Ethernet نیز می‌توان از این روش استفاده نمود ولی در FabricPath تنها از روش مکالمه‌ای استفاده می‌شود. همانطور که گفته شد فقط برای ماژول‌های سری F قابل استفاده است.

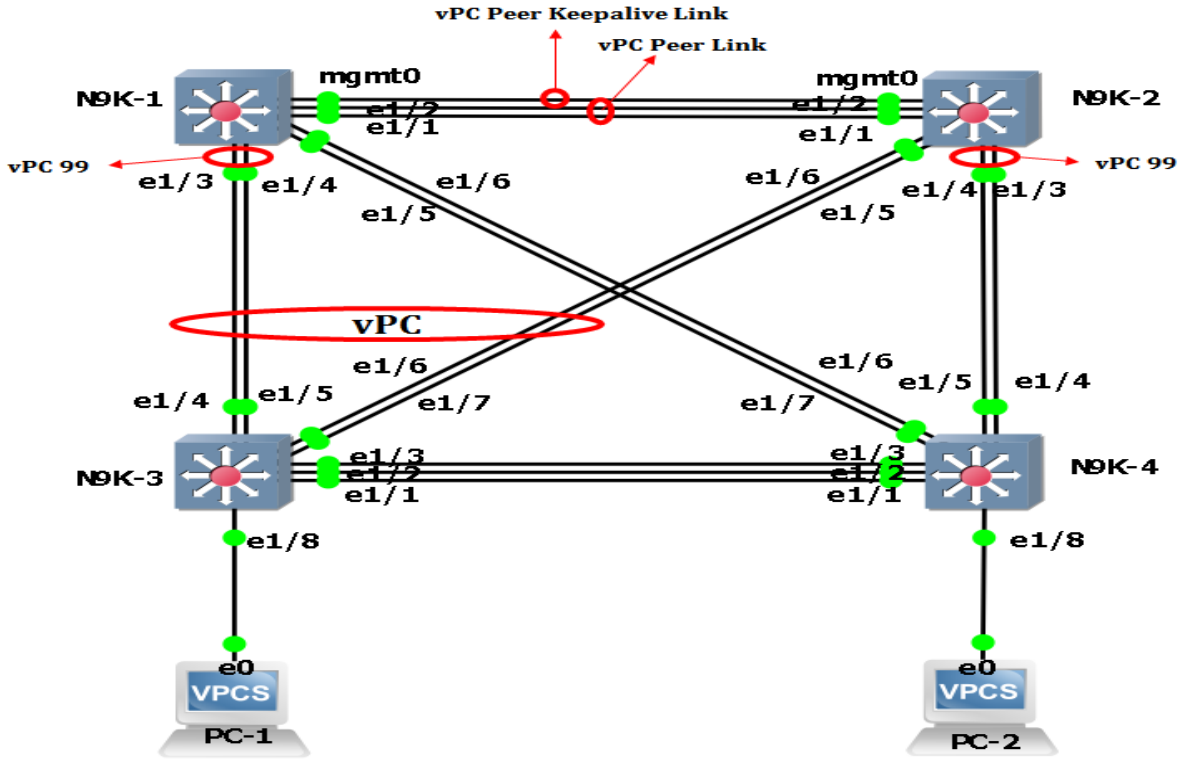
vPC and FabricPath Commands -۱۱

vPC -۱-۱۱

ابتدا به دستورات مربوط به تنظیمات vPC پرداخته می‌شود که ابتدا باید فعال و یا غیر فعال بودن Feature مورد نظر را بررسی نمود و پس از آن دستورات که شامل تنظیم Peer Link، ایجاد دامنه vPC، تنظیم Keppalive Link، تنظیم Peer Link، عضو نمودن Member Port و فعال نمودن vPC در سمت تجهیزات پایین دستی

است. در هر قسمت از مراحل از صحت تنظیم و دستورات آن آشنا شده و در خروجی نمایش داده می‌شود.

توپولوژی به شرح تصویر زیر است.



۱. فعال نمودن Featureها

```
N9K-1# configure terminal
N9K-1(config)# feature lacp
N9K-1(config)# feature vpc
N9K-1# show feature
Feature Name        Instance  State
------------------- -------- --------
lacp                1         enabled
vpc                 1         enabled
```

۲. ایجاد دامنه vPC و تنظیم Keepalive

```
N9K-1# show ip interface brief
IP Interface Status for VRF "default"(1)
Interface         IP Address      Interface Status
Vlan10            10.10.10.1      protocol-up/link-up/admin-up
Vlan20            20.20.20.1      protocol-up/link-up/admin-up
Lo0               1.1.1.1         protocol-up/link-up/admin-up
N9K-1(config)# vpc domain 1
N9K-1(config-vpc-domain)# peer-keepalive destination 2.2.2.2 source 1.1.1.1 vrf
default
```

در سمت دیگر نیز از همین دستورات استفاده می‌شود.

```
N9K-2# show ip interface brief
IP Interface Status for VRF "default"(1)
Interface         IP Address     Interface Status
Vlan10            10.10.10.2     protocol-up/link-up/admin-up
Vlan20            20.20.20.2     protocol-up/link-up/admin-up
Lo0               2.2.2.2        protocol-up/link-up/admin-up
N9K-2(config)# vpc domain 1
N9K-2(config-vpc-domain)# peer-keepalive destination 1.1.1.1 source 2.2.2.2 vrf
default
N9K-2# show running-config vpc
vpc domain 1
  peer-keepalive destination 1.1.1.1 source 2.2.2.2 vrf default
N9K-2# show  vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer link not configured
vPC keep-alive status             : peer is alive
Configuration consistency status  : failed
Per-vlan consistency status       : failed
Configuration inconsistency reason : vPC peer-link does not exist
Type-2 consistency status         : failed
Type-2 inconsistency reason       : vPC peer-link does not exist
vPC role                          : none established
Number of vPCs configured         : 0
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Disabled (due to peer configuration)
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
```

همانطور که مشخص است Keepalive به درستی تنظیم شده است ولی Peer Link هنوز تنظیم نشده است.

۳. تنظیم Peer Link

```
N9K-1(config)# interface ethernet 1/1-2
N9K-1(config-if-range)# switchport mode trunk
N9K-1(config-if-range)# channel-group 12 mode active
N9K-1(config-if-range)# exit
```

```
N9K-1(config)# interface port-channel 12
N9K-1(config-if)# vpc peer-link
N9K-1# show running-config interface port-channel 12
interface port-channel12
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
N9K-1# show vpc
Legend:
        (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer link is down
vPC keep-alive status             : peer is alive
Configuration consistency status  : failed
Per-vlan consistency status       : success
Configuration inconsistency reason : Consistency Check Not Performed
Type-2 consistency status         : Consistency Check Not Performed
vPC role                          : none established
Number of vPCs configured         : 0
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Disabled (due to peer configuration)
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po12   down   -
```

به این دلیل هنوز غیر فعال است که باید در سمت دیگر فعال شود پس از تنظیمات در سمت دیگر می‌توان حالت زیر را مشاهده نمود.

```
N9K-2# show vpc
Legend:
        (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is not reachable through peer-keepalive
```

```
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : failed
Type-2 inconsistency reason       : QoSMgr Qos configuration incompatible
vPC role                          : secondary
Number of vPCs configured         : 0
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is on.(timeout = 30s, 24s left)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po12   up     1,10,20
```

۴. عضو نمودن Membor Port

```
N9K-1(config)# interface ethernet 1/3-4
N9K-1(config-if-range)# switchport mode trunk
N9K-1(config-if-range)# channel-group 99 mode active
N9K-1(config-if-range)#exit
N9K-1(config)# interface port-channel 99
N9K-1(config-if)# vpc 99
```

در سمت دیگر نیز باید این دستورات را تنظیم نمود.

```
N9K-2(config)# interface ethernet 1/5-6
N9K-2(config-if-range)# switchport mode trunk
N9K-2(config-if-range)# channel-group 99 mode active
N9K-2(config-if-range)# exit
N9K-2(config)# interface port-channel 99
N9K-2(config-if)# vpc 99
```

۵. فعال نمودن در سمت Switch پایین دستی

```
N9K-3(config)# interface ethernet 1/4-7
N9K-3(config-if-range)# switchport mode trunk
N9K-3(config-if-range)# channel-group 99 mode active
N9K-3(config-if-range)# exit
N9K-3(config)# interface port-channel 99
N9K-3(config-if)# no shutdown
```

```
N9K-3# show port-channel summary
--------------------------------------------------------------------------------
Group Port-      Type     Protocol  Member Ports
    Channel
--------------------------------------------------------------------------------
99   Po99(SU)   Eth      LACP      Eth1/4(P)   Eth1/5(P)   Eth1/6(P)
                                    Eth1/7(P)
N9K-1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 1
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po12   up     1,10,20
vPC status
----------------------------------------------------------------------------
Id   Port          Status Consistency Reason              Active vlans
--   ------------  ------ ----------- ------              ---------------
99   Po99          up     success     success             10,20
```

۶. تغییر نقش vPC

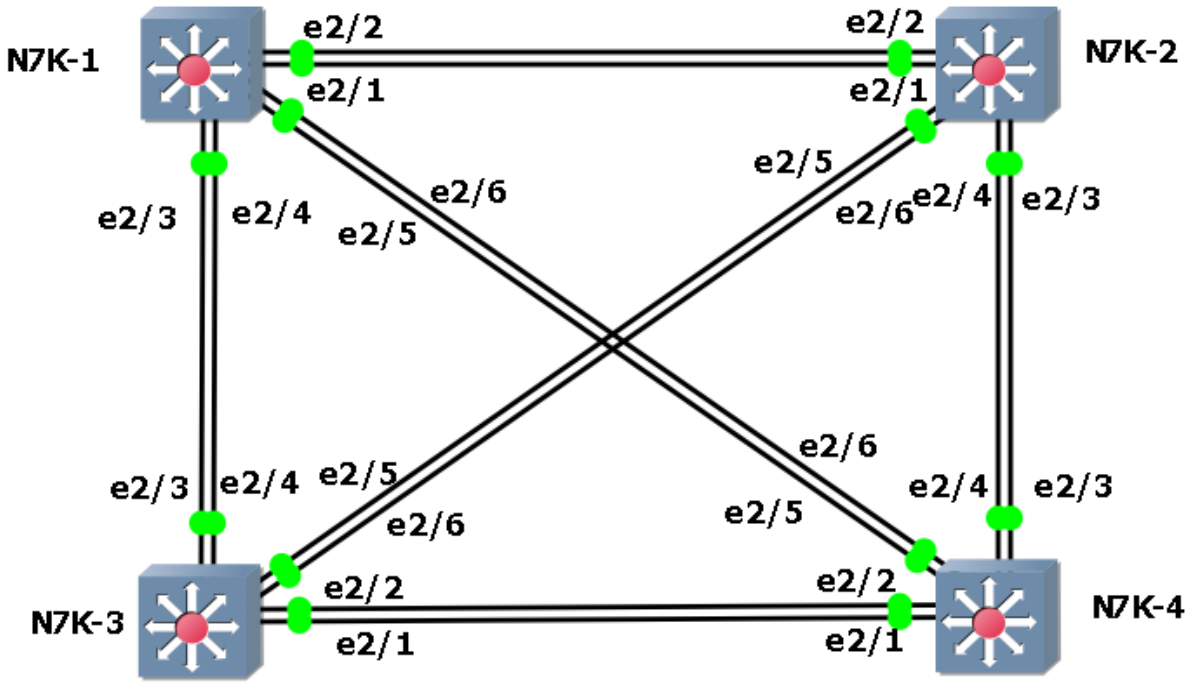
برای تغییر نقش می‌توان از دستورات زیر استفاده نمود.

```
N9K-1# configure terminal
N9K-1(config)# vpc domain 1
```

```
N9K-1(config-vpc-domain)# role priority ?
  <1-65535>  Specify priority value
```

FabricPath ۲-۱۱

دستورات مربوط به FP به این شکل است که ابتدا باید Feature مربوط به آن را فعال نمود. البته باید License مربوط به آن که ENHANCED_LAYER2_PKG است را در دستگاه وارد نمود. توپولوژی در تصویر زیر آمده است.




```
 N7K-1# show license usage
Feature                      Ins  Lic Count Status Expiry Date Comments
--------------------------------------------------------------------------------
MPLS_PKG                     No   -         Unused         -
STORAGE-ENT                  No   -         Unused         -
VDC_LICENSES                 No   0         Unused         -
ENTERPRISE_PKG               No   -         Unused         -
FCOE-N7K-F132XP              No   0         Unused         -
FCOE-N7K-F248XP              No   0         Unused         -
FCOE-N7K-F312FQ              No   0         Unused         -
FCOE-N7K-F348XP              No   0         Unused         -
ENHANCED_LAYER2_PKG          No   -         In use         Grace 119D 23H
SCALABLE_SERVICES_PKG        No   -         Unused         -
TRANSPORT_SERVICES_PKG       No   -         Unused         -
LAN_ADVANCED_SERVICES_PKG    No   -         Unused         -
LAN_ENTERPRISE_SERVICES_PKG  No   -         Unused         -
```

```
--------------------------------------------------------------------------------
N7K-1(config)# install feature-set ?
  fabric        FABRIC
  fabricpath    Fabricpath
  fex           FEX
  mpls          MPLS
N7K-1(config)# install feature-set fabricpath
N7K-1(config)# feature-set ?
  fabricpath    Installed feature-set
N7K-1(config)# feature-set fabricpath
2019 Sep  5 12:30:16 switch isis_l2mp[14736]: There is no active vlan on MT 0
```

پس از آن برروی هر VLAN حالت آن به FP تغییرداده می‌شود.

```
N7K-1(config)# vlan 100
N7K-1(config-vlan)# mode fabricpath
```

بعد از آن برروی هر اینترفیسی که بین دو دستگاه است حالت FP فعال می‌شود.

```
N7K-1(config-if)# interface ethernet 2/1-6
N7K-1(config-if-range)# switchport
N7K-1(config-if-range)# switchport mode fabricpath
N7K-1(config-if-range)# no shutdown
```

با دستور زیر می‌توان Switch-ID مربوط به تجهیز مورد نظر را تغییر داد.

```
N7K-1(config)# fabricpath switch-id 12
```

با استفاده از دستورات زیر می‌توان وضعیت FabricPath را مشاهده نمود.

```
N7K-1# show fabricpath switch-id
FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
      '[E]' - local Emulated Switch-id
      '[A]' - local Anycast Switch-id
Total Switch-ids: 1
================================================================
===============
   SWITCH-ID     SYSTEM-ID      FLAGS       STATE    STATIC  EMULATED/
                                                          ANYCAST
--------------+---------------+------------+-----------+--------------------
*  12         0cc8.fe05.282f    Primary     Confirmed Yes     No

N7K-1# show fabricpath isis interface brief
Fabricpath IS-IS domain: default
Interface    Type  Idx State      Circuit   MTU  Metric  Priority  Adjs/AdjsUp
```

```
--------------------------------------------------------------------------------
Ethernet2/1  P2P  1    Up/Ready   0x01/L1   1500 400    64       0/0
Ethernet2/2  P2P  2    Up/Ready   0x01/L1   1500 400    64       0/0
Ethernet2/3  P2P  3    Up/Ready   0x01/L1   1500 400    64       0/0
Ethernet2/4  P2P  4    Up/Ready   0x01/L1   1500 400    64       0/0
Ethernet2/5  P2P  5    Up/Ready   0x01/L1   1500 400    64       0/0
Ethernet2/6  P2P  6    Up/Ready   0x01/L1   1500 400    64       0/0
```

پس از تنظیم موارد بالا در همه Switchها می‌توان با دستور زیر همسای‌ها را مشاهده نمود.

```
N7K-1# show fabricpath isis adjacency
Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency database:
System ID      SNPA          Level  State  Hold Time  Interface
N7K-2          N/A           1      UP     00:00:29   Ethernet2/1
N7K-2          N/A           1      UP     00:00:29   Ethernet2/2
N7K-3          N/A           1      UP     00:00:31   Ethernet2/3
N7K-3          N/A           1      UP     00:00:26   Ethernet2/4
N7K-4          N/A           1      UP     00:00:30   Ethernet2/5
N7K-4          N/A           1      UP     00:00:28   Ethernet2/6
N7K-1# show fabricpath route
FabricPath Unicast Route Table
'a/b/c' denotes ftag/switch-id/subswitch-id
'[x/y]' denotes [admin distance/metric]
ftag 0 is local ftag
subswitch-id 0 is default subswitch-id



FabricPath Unicast Route Table for Topology-Default


0/12/0, number of next-hops: 0
      via ---- , [60/0], 0 day/s 00:13:15, local
1/265/0, number of next-hops: 2
      via Eth2/1, [115/400], 0 day/s 00:09:15, isis_fabricpath-default
      via Eth2/2, [115/400], 0 day/s 00:09:15, isis_fabricpath-default
1/1008/0, number of next-hops: 2
      via Eth2/3, [115/400], 0 day/s 00:05:30, isis_fabricpath-default
      via Eth2/4, [115/400], 0 day/s 00:05:30, isis_fabricpath-default
1/1065/0, number of next-hops: 2
      via Eth2/5, [115/400], 0 day/s 00:05:23, isis_fabricpath-default
```

```
    via Eth2/6, [115/400], 0 day/s 00:05:23, isis_fabricpath-default

N7K-1# show fabricpath isis database
Fabricpath IS-IS domain: default LSP database
 LSPID             Seq Number   Checksum  Lifetime   A/P/O/T
 N7K-1.00-00       * 0x00000009   0xC98D    752       0/0/0/1
 N7K-4.00-00         0x00000005   0xECD7    761       0/0/0/1
 N7K-2.00-00         0x00000008   0x6499    758       0/0/0/1
 N7K-3.00-00         0x00000006   0xAFF6    779       0/0/0/1

N7K-1# show fabricpath isis hostname
Fabricpath IS-IS domain: default dynamic hostname table
Legend: '*' - this system
 Level  System ID      Dynamic hostname
 1      0cc8.fe05.282f* N7K-1
 1      0cc8.fe26.ce2f  N7K-4
 1      0cc8.fe38.8d2f  N7K-2
 1      0cc8.fef7.dd2f  N7K-3


N7K-1# show fabricpath isis vlan-range
Fabricpath IS-IS domain: default
MT-0
Vlans configured:
100, 4040-4041
No VNI configured.

N7K-1# show fabricpath isis protocol


Fabricpath IS-IS domain : default
 System ID : 0cc8.fe05.282f  IS-Type : L1 Fabric-Control SVI: Unknown
 SAP : 432  Queue Handle : 15
 Maximum LSP MTU: 1492
 Graceful Restart enabled. State: Inactive
 Last graceful restart status : none
 Graceful Restart holding time:60
 Metric-style : advertise(wide), accept(wide)
 Start-Mode: Complete [Start-type configuration]
 Area address(es) :
  00
```

```
Process is up and running
CIB ID: 1
Interfaces supported by Fabricpath IS-IS :
  Ethernet2/1
  Ethernet2/2
  Ethernet2/3
  Ethernet2/4
  Ethernet2/5
  Ethernet2/6
Level 1
Authentication type and keychain not configured
Authentication check specified
LSP Lifetime: 1200
L1 LSP GEN interval- Max:8000 Initial:50     Second:50
L1 SPF Interval- Max:8000     Initial:50     Second:50
MT-0 Ref-Bw: 400000
    Max-Path: 16
Address family Swid unicast :
  Number of interface : 6
  Distance : 115
L1 Next SPF: Inactive
```

همانطور که قابل مشاهده است FabricPath یک پروتکل لایه سه بر روی لایه دو یا همان Layer 2 Routing است. اطلاعات adjacency، database، protocol، route و topology در بالا نشان داده شده است.

۱۲- Monitoring Nexus Switches

در این قسمت ابزارهای مدیریتی و مشاهده تجهیزات Nexus توضیح داده می‌شود. بعضی از این ابزارها ممکن است در تجهیزات دیگر سیسکو نیز استفاده شود و فقط منحصر به تجهیزات Nexus نمی‌شود.

۱۲-۱- Connectivity Management Processor (CMP)

Connectivity Management Processor (CMP) یکی از پورت‌هایی است که برای مشاهده و مدیریت تجهیزات Nexus که برروی ماژول Supervisor 1 قرار دارد استفاده می‌شود. باید توجه داشت که در ماژول‌های Supervisor 2 و یا Supervisor 2E این پورت وجود ندارد. پورت CMP یک پورت out-of-band(OOB) است. در مدیریت in-band و out-of-band هر دو بصورت ارتباط شبکه‌ای هستند، اما در مدیریت out-of-band می‌توان از یک اتصال دهنده شبکه فیزیکی جداگانه‌ای استفاده نمود. برروی این پورت یک پردازش CMP وجود دارد و زمانی که پردازش کنترلی اصلی یا Main Control Processor(CP) در دسترس نیست با استفاده از این اینترفیس می‌توان تنظیمات را برروی CP انجام داد. با استفاده از CMP می‌توان به CP Console دسترسی داشت و یا آن را راه‌اندازی مجدد نمود. هر CMP یک RAM، Boot flash و پورت

Ethernet مخصوص به خود دارد. همچنین از طریق CMP می‌توان به CP ارتباط SSH و یا Telnet برقرار و آن را مدیریت نمود. حتی در صورت خاموش و یا Standby بودن CP می‌توان به CMP متصل شد، زیرا برق جداگانه‌ای از دستگاه می‌گیرد و همانطور که گفته شد یک OOB است. عملکردهای CMP به شرح زیر است.

۱. CMP با ماژول‌های Sup 1 و I/O ارتباط برقرار می‌کند؛ حتی اگر Cisco Nexus-OS Switch برروی پورت MGMT0 پاسخگو نباشد.
۲. هنگام راه‌اندازی مجدد ماژول Supervisor همچنان اتصال CMP حفظ می‌شود.
۳. از طریق CMP می‌توان پورت کنسول ماژول Supervisor را مشاهده نمود.
۴. ماژول Supervisor و یا کل سیستم را می‌توان از طریق CMP راه‌اندازی مجدد نمود.
۵. Logها و پیام‌های Diagnostic هنگام Boot شدن را جمع‌آوری می‌کند.

۱۲-۲- Virtual Routing and Forwarding (VRF)

در لایه سه برای ارسال بسته‌های شبکه یک جدول مسیریابی وجود دارد تا بتوان بسته‌ها را با کمترین یا بهترین هزینه به سمت مقصد هدایت نمود. Virtual Routing and Forwarding (VRF) یک فن‌آوری است که در مسیریاب‌ها، تجهیزات Nexus و دیگر دستگاه‌ها قابل استفاده است و اجازه می‌دهد تا چندین نمونه از یک جدول مسیریابی وجود داشته باشد. این امر باعث می‌شود تا بدون استفاده از چندین دستگاه، مسیرهای شبکه از یکدیگر جدا شوند. به عبارت دیگر می‌توان چندین Data Plane و Control Plane جداگانه برای شبکه‌های مختلف داشت. بطور مثال می‌توان چندین جدول مسیریابی با IPهای یکسان از شبکه‌های مختلف و با پروتکل‌های مسیریابی مختلف ایجاد نمود. بصورت پیش‌فرض یک Default VRF یا یک جدول مسیریابی پیش‌فرض وجود دارد که همه مسیرها در آن قرار می‌گیرند. مدیر شبکه در صورت نیاز می‌تواند یک VRF دیگر ایجاد و از آن استفاده نماید. در تجهیزات Nexus یک Management VRF پیش‌فرض نیز وجود دارد که پورت مدیریتی MGMT0 OOB در ان قرار دارد. بطور کلی دو VRF پیش‌فرض Default و Management وجود دارد که قابل حذف نیستند.

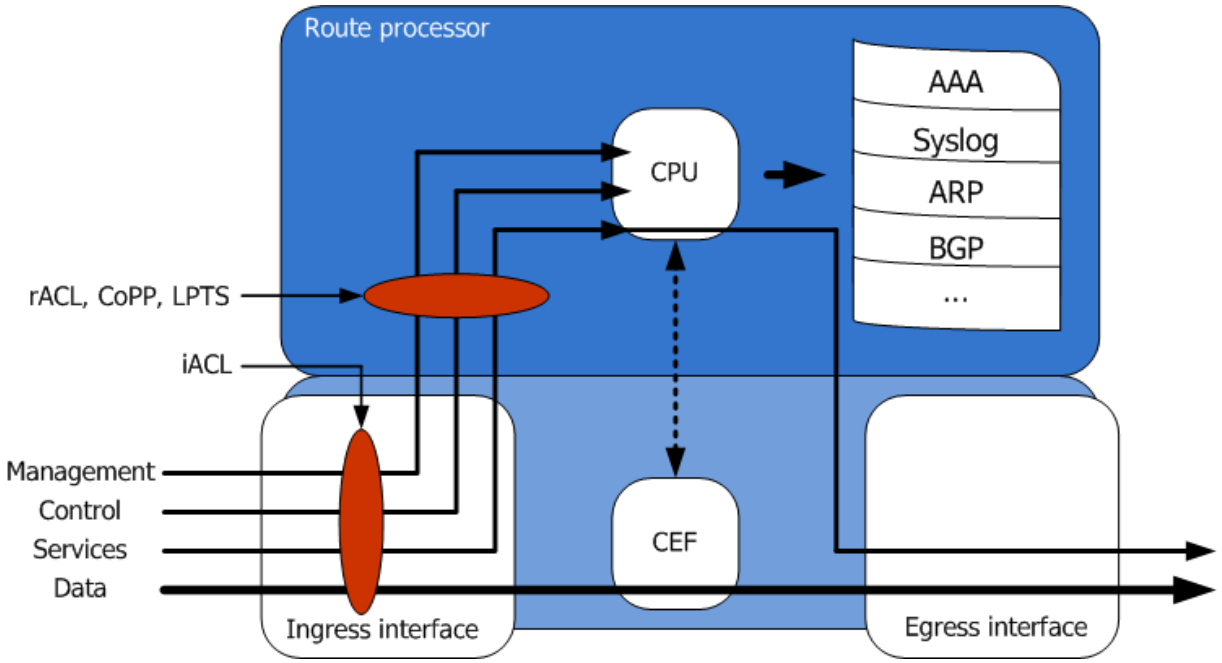
۱۲-۳- In-Service Software Upgrade (ISSU)

یک روش برای به‌روزرسانی یا Upgrade کردن تجهیزات سیسکو است. در این روش سیستم‌عامل سیسکو در حالی که به ارسال بسته‌ها ادامه می‌دهد، به‌روز می‌شود. در این روش دسترسی‌پذیری افزایش و زمان خاموشی یا Down Time کاهش می‌یابد. در تجهیزات سیسکو برای این که زمان خاموشی وجود نداشته باشد نیاز به دو Supervisor است و Switch باید از ISSU پشتیبانی نماید. هنگام به‌روزرسانی ابتدا ماژول Standby به‌روز می‌شود و بعد از آن در حالت Active قرار می‌گیرد که این امر با کمک HA انجام می‌شود. بعد از آن ماژول Active که الان در حالت Standby است به‌روز می‌شود. باید توجه نمود که نسخه سیستم‌عامل NX-OS باید 4.2.1 به بعد باشد. با استفاده از ISSU می‌توان Kickstart Image، SUP Bios، System Image، FEX

Image و I/O Moduleها را به‌روزرسانی نمود. زمانی که FEX Image برروی Nexus Switch به‌روزرسانی می‌شود، تجهیزاتی که به آن متصل هستند بصورت خودکار کدها را دریافت و به‌روز می‌شوند.

۱۲-٤- Control Plane Policing (CoPP)

CoPP قابلیتی است که از بخش Control Plane محافظت می‌کند و آن را از بخش Data Plane جدا نگه می‌دارد. همچنین به کاربران اجازه می‌دهد تا جریان ترافیک کنترل شده توسط پردازند مسیر را از دستگاه‌های شبکه خود مدیریت کنند. به عبارت دیگر CoPP از ورود مسیر به قسمت پردازشی مسیر یا Route Processor محافظت می‌کند. این امر باعث می‌شود تا از حملات DoS جلوگیری شود. بصورت پیش‌فرض سیاست‌های CoPP می‌تواند سخت‌گیرانه، در حت متوسط، ملایم و یا هیچکدام باشد. باید توجه داشت که CoPP فقط برروی Default VDC تنظیم می‌شود و می‌توان سیاست‌ها را برروی همه VDCها اعمل نمود.



۱۳- Overlay Transport Virtualization (OTV)

OTV ابزاری برای VPN و یا تونل زدن لایه دو برروی IPv4 است. علت اصلی طراحی این قابلیت برقراری ارتباط لایه دو بین مراکز داده یا Data Center Interconnect (DCI) است. بطور خاص می‌توان از آن برای VMware vMotion (انتقال ماشین‌های مجازی) بین مراکز داده استفاده نمود که نیاز به ارتباط لایه دو بین مراکز داده برای این قابلیت احساس می‌شود. OTV برروی تجهیزات Nexus 7K و همچنین پلتفورم‌های Aggregation Service Router (ASR) قابل اجرا است. در ادامه می‌توان به تفاوت OTV با دیگر تکنولوژی‌های ارتباطی لایه دو بین مراکز داده را مقایسه نمود.

۱. OTV برای مقیاس‌پذیری ارتباط لایه دو بین مراکز داده طراحی شده است.
۲. قابلیت‌های بسیاری که دیگر تکنولوژی‌ها مانند Dark Fiber (CWDM/DWDM)، VPLS و Bridging Over GRE دربردارند را در خود جا داده است.

۳. بهینه‌سازی کردن ARP Flood برروی ارتباط DCI به اینصورت انجام می‌گیرد که یک فضای Cache بعد از ARP Flood ایجاد می‌کند و از این فضا برای ARP استفاده می‌کند. این امر باعث می‌شود که دیگر ARP Flood رخ ندهد.
۴. STP در OTV متوقف می‌شود و بسته‌های BPDU ارسال نمی‌شوند. در واقع STP برروی هر سایت بطور جداگانه اجرا می‌شود.
۵. می‌توان از چندین Router که از VLANهای مختلف و Load Balancing پشتیبانی می‌کنند، استفاده نمود.
۶. از طوفان‌های همه پخشی یا Broadcast Storm جلوگیری می‌کند.
۷. با استفاده از Proxy ARP/ICMPv6 Neighbor Discovery Cache برروی AED، سیل اطلاعات غیر ضروری یا Unnecessary Flooding را کاهش می‌دهد.
۸. OTV یک VPN پوششی انعطاف‌پذیر در بالای شبکه بدون محدودیت در شبکه IP فراهم می‌کند. به عبارت دیگر می‌توان از هر نوع ارتباط شبکه‌ای IP استفاده نمود. در OTV هیچ پیش‌نیاز شبکه‌ای از جمله سرعت وجود ندارد و فقط باید دسترسی IP وجود داشته باشد.
۹. OTV از ارسال‌های تک‌پخشی، چندپخشی و همه‌پخشی پشتیبانی می‌کند. بطور مثال به راحتی می‌توان راه حل Point-to-Cloud را مدیریت و پیاده‌سازی نمود.

OTV Terminology -۱-۱۳

OTV Edge Device (OTV ED): Router یا مسیریابی است که برروی آن OTV پیاده‌سازی می‌شود. معمولاً در لبه شبکه و در Core قرار دارد.

Authoritative Edge Device (AED): یک Edge Device فعال برای یک VLAN خاص است. با استفاده از این قابلیت در OTV این امکان فراهم شده است که چندین Edge Router وجود داشته باشد و از حلقه جلوگیری می‌شود. در واقع در هر سایت می‌توان چندین Edge Device وجود داشته باشد، ولی در هر VLAN فقط یک دستگاه می‌تواند AED باشد.

Extend VLAN: در واقع VLANهایی هستند که برروی OTV اجازه عبور دارند.

Site VLAN: یک VLAN داخلی است که برای ارتباط بین AEDها استفاده می‌شود تا بتوانند AED را برای VLAN انتخاب کنند.

Site Identifier: یک عدد منحصر به فرد است که برای هر سایت استفاده می‌شود. این عدد بین AEDها به اشتراک گذاشته می‌شود. به عبارت دیگر EDها در هر سایت باید ID یکسانی داشته باشند.

Overlay Interface: یک اینترفیس مجازی است که تنظیمات مربوط به OTV در آن انجام می‌شود. بطور مثال شبیه GRE Tunnel است.

OTV Join Interface: یک لینک فیزیکی یا Port Channel است که بسته‌ها از طریق آن بین دو مرکز داده جابه‌جا می‌شوند.

Internal Interface: اینترفیس‌های لایه دو محلی EDها هستند که برروی آنها OTV تنظیم نشده است و با داخل سایت در ارتباط هستند.

OTV Control Group: آدرس چندپخشی است که Routerها از آن برای ارتباط Control Plane استفاده می‌کنند. به عبارت دیگر برای adjacency با Routerهای دیگر مورد استفاده قرار می‌گیرد.

OTV Data Group: آدرس چند پخشی است که برای ارسال ترافیک‌های لایه دو مراکز داده یا بخش Data Plane از آن استفاده می‌شود.

۱۳-۲- OTV Control Plane

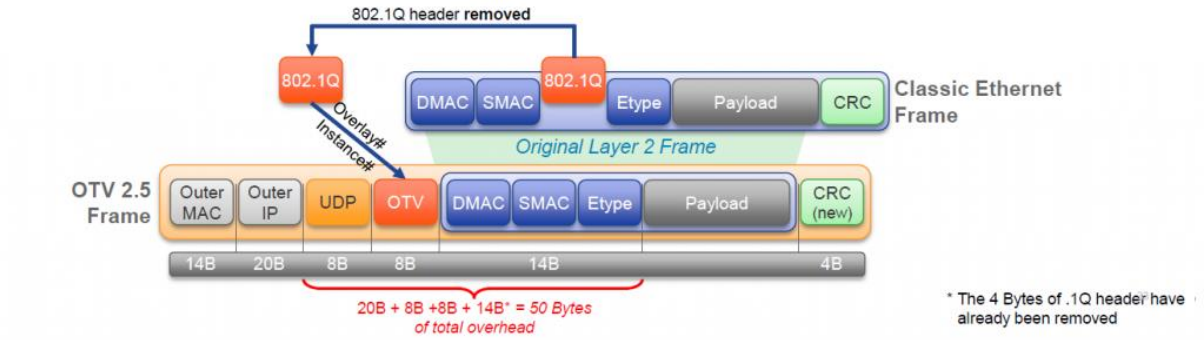
OTV از پروتکل IS-IS در لایه دو برای اعلام MAC Addressها بین AEDها استفاده می‌کند. OTV همانند پروتکل Fabricpath از IS-IS برای مسیریابی لایه دو یا MAC in IP Routing استفاده می‌کند. Routerها در بخش Control Plane با استفاده از Any Source Multicast (ASM) می‌توانند به گروه خاصی بپیوندند و همزمان نقش گیرنده و فرستنده را بازی نمایند. به عبارت دیگر با ارسال Multicast همدیگر را بیابند. همچنین می‌توانند از بسته‌بندی Unicast برای شناسایی OTV Server استفاده کنند. در این صورت با استفاده از OTV Server Adjacency مقیاس‌پذیری از بین می‌رود زیرا در صورت وجود داشتن چندین مرکز داده باید یکی‌یکی تنظیمات را انجام داد. البته دیگر پیچیدگی‌های مربوط به Multicast وجود ندارد.

۱۳-۲-۱- OTV Neighbor Discovery

۱. هر OTV Edge Device یک درخواست برای پیوستن به گروه ASM خاص برای انجام مبادلات کنترلی پروتکل ارسال می‌کند. EDها به عنوان یک میزبان به گروه می‌پیوندند. این عمل بدون فعال کردن PIM صورت می‌گیرد. تنها شرط مشخص شدن گروه ASM داشتن ارتباط از طریق Overlay Interface است. Protocol Independent Multicast (PIM) یک مجموعه‌ای از پروتکل‌های مسیریابی Multicast است که هرکدام برای محیط خاصی بهینه شده‌اند. در واقع PIM بین Routerها استفاده می‌شود تا آنها بتوانند بسته‌های Multicast را بین یکدیگر و شبکه‌هایی که به آنها متصل هستند، انتقال دهند.

۲. پروتکل برروی OTV ED اجرا شده و بسته‌های Hello را برای سایر OTV EDها ارسال می‌کند. این ارتباط برای برپایی Control Plane Adjacencies لازم است.

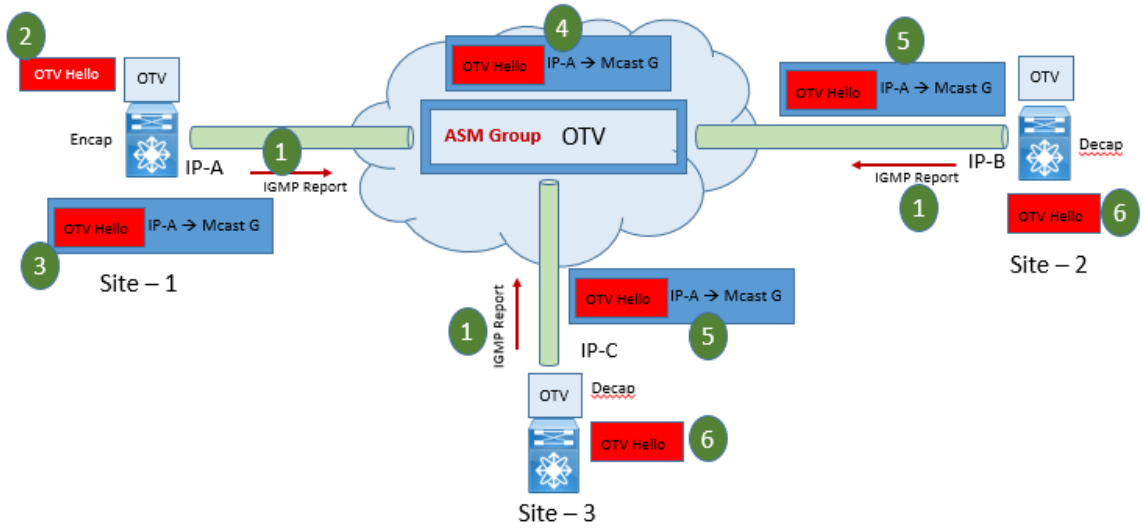
۳. پیام‌های OTV Hello باید برای تمامی دستگاه‌های OTV ارسال شود. برای اینکار باید Frame اصلی به OTV Encapsulate تبدیل شود.



۴. Multicast Frame برای رسیدن به همه OTV EDهایی که در گروه چندپخشی هستند تکثیر می‌شوند.

۵. OTV EDهایی که بسته را دریافت می‌کنند آن را Decapsulate می‌نمایند.

۶. بسته‌های Hello به قسمت OTV Control Protocol منتقل می‌شوند. اینگونه همسایه‌ها یکدیگر را پیدا می‌کنند. در نهایت EDها آدرس‌های MAC سایت‌ها را برای یکدیگر ارسال می‌کنند.



OTV Data Plane ۳-۱۳-

در قسمت Data Plane از هر دو ارسال Multicast و Unicast استفاده می‌شود. در ارسال Unicast بسته‌ها به حالت Unicast بین AEDها Encapsulate و ارسال می‌شوند. ترافیک Multicast لایه دو برای ارسال Data Plane باید از OTV Overlay عبور داده شود و از تکرار در زیرمجموعه‌ها جلوگیری نماید. همچنین مکانیزم خاصی برای اطمینان ارسال Multicast در سراسر زیرساخت لازم است. این مکانیز ارسال چندپخشی در گروه Source Specific Multicast (SSM) نام دارد. این گروه از گروه‌های ASM که در Data Plane ایجاد شد کاملاً مستقل است.

در صورت استفاده از OTV Adjacency Server تمامی پیش‌نیازهای Multicast از بین می‌رود و تکثیر ابتدا تا انتها زمانی که بیشتر از دو مرکز داده وجود دارد رخ می‌دهد.

۱۳-۳-۱- Receiver Joining the Multicast Group Gs

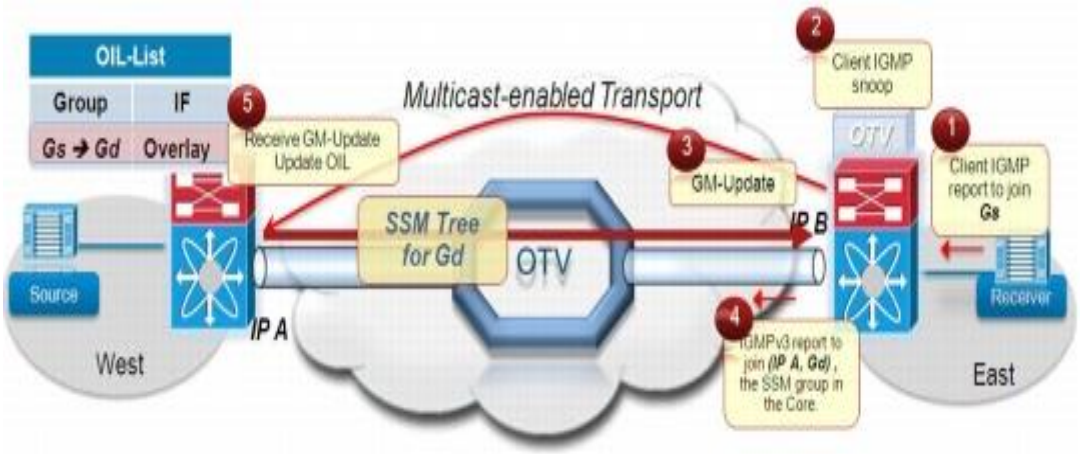
۱. کاربر درخواست IGMP Report را برای پیوستن به گروه ارسال می‌کند.

۲. OTV Edge Device پیام IGMP را شنود می‌کند و متوجه می‌شود که یک گیرنده فعال در سایت خودش وجود دارد که متعلق به گروه Gs و VLAN A است.

۳. OTV Edge Device یک پیام OTV Control Protocol به همه OTV Edge Deviceهای دیگر که شامل اطلاعات GM-Update است ارسال می‌کند.

۴. OTV Edge Device پس از دریافت GM-Update لیست اینترفیس خروجی یا Outgoing Interface List (OIL) را به‌روزرسانی می‌کند.

۵. در نهایت همه OTV Edge Deviceها با دریافت اطلاعات Mapping دستگاه‌های دیگر را با IP شناسایی و ذخیره می‌کنند. OTV Edge Device که از ا« پیام IGMP Report ارسال شده است، یک بسته IGMPv3 Report به قسمت Transport ارسال می‌کند تا به گروه SSM با IP A و گروه Gd بپیوندد. این عملیات کمک به ساختن درخت SMM یا Group Gd می‌کند که از طریق آن بسته‌های چندپخشی Gs ارسال می‌شوند.

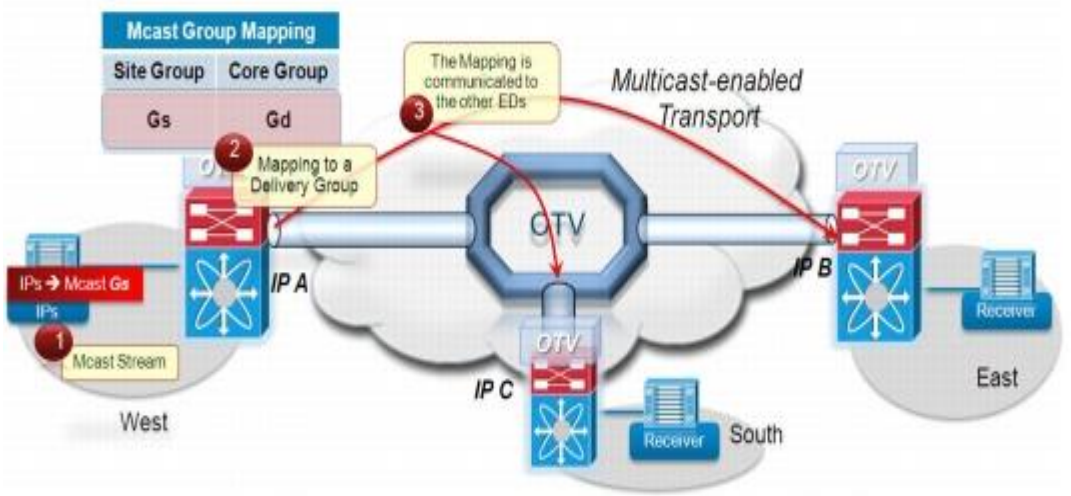


۱۳-۳-۲- Multicast Source Streaming to Group Gs

۱. دستگاه مبدأ Multicast فعال می‌شود و شروع به ارسال ترافیک برای گروه Gs می‌کند. بطور مثال شروع به ارسال یک Stream Video می‌کند.

۲. OTV Edge Device محلی به محض دریافت اولین Multicast Frame یک جدول Mapping بین گروهی که مبدأ به آن بسته ارسال می‌کند Gs و گروه SMM که در زیرساخت Transport در دسترس است Gd ایجاد می‌کند. از گروه SMM برای ارسال ترافیک لایه دو چندپخشی که هنگام تنظیم Overlay Interface تنظیم شده است استفاده می‌شود.

۳. از OTV Control Protocol برای ساخت جدول Mapping و ارتباط بین OTV Edge Deviceها استفاده می‌شود. اطلاعا Mapping شامل VLAN محلی A، گروه Multicast متعلق به مبدأ و IP Edge Device که جدول را ساخته است، می‌شود.



Delivery of the Multicast Stream Gs ۱۳-۳-۳-

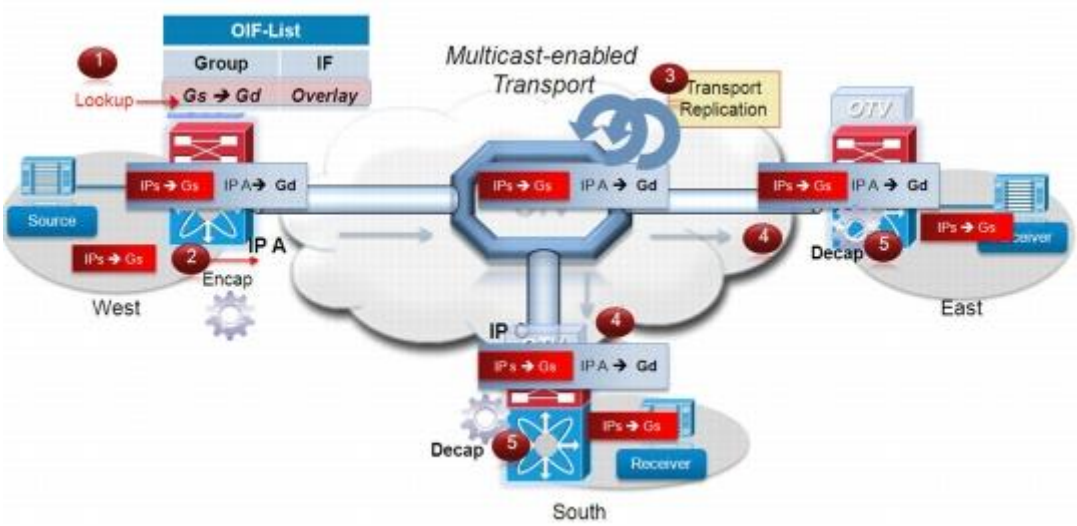
۱. OTV Edge Device ترافیک Gs را دریافت می‌کند و پس از نگاه به لیست OIL در صورت این که گیرنده‌ای از گروه Gs برروی Overlay داشته باشد. به مرحله بعد می‌رود.

۲. OTV Edge Device بسته اصلی Multicast Frame را Encapsulate می‌کند و IP مبدأ خود را IP خروجی یا Overlay Interface و آدرس مقصد را آدرس گروه Gd SSM قرار می‌دهد.

۳. ترافیک چندپخشی Gd از طریق درخت SSM که قبلاً شناخته شده است به تمامی سایت‌ها ارسال می‌شود.

۴. OTV Edge Deviceها ترافیک را دریافت می‌کنند.

۵. ترافیک Decapsulate شده و به گیرنده ارسال می‌شود.



Broadcast Users Traffic ۱۳-۳-٤-

رفتار OTV در ارسال ترافیک Broadcast به این گونه است که در زمان ارسال ترافیک‌های Broadcast مانند ARP، اگر بستر Multicast برای ارسال ترافیک بین Edge Deviceها برقرار باشد، ترافیک Broadcast به صورت Multicast به تمام Edge Deviceها ارسال می‌شود؛ در غیر اینصورت ترافیک به صورت unicast به تمام Edge Deviceها ارسال می‌شود. OTV به منظور کاهش ترافیک Broadcast ایجاد شده توسط ARP، راه‌کاری به نام ARP Optimization ارائه داده است.

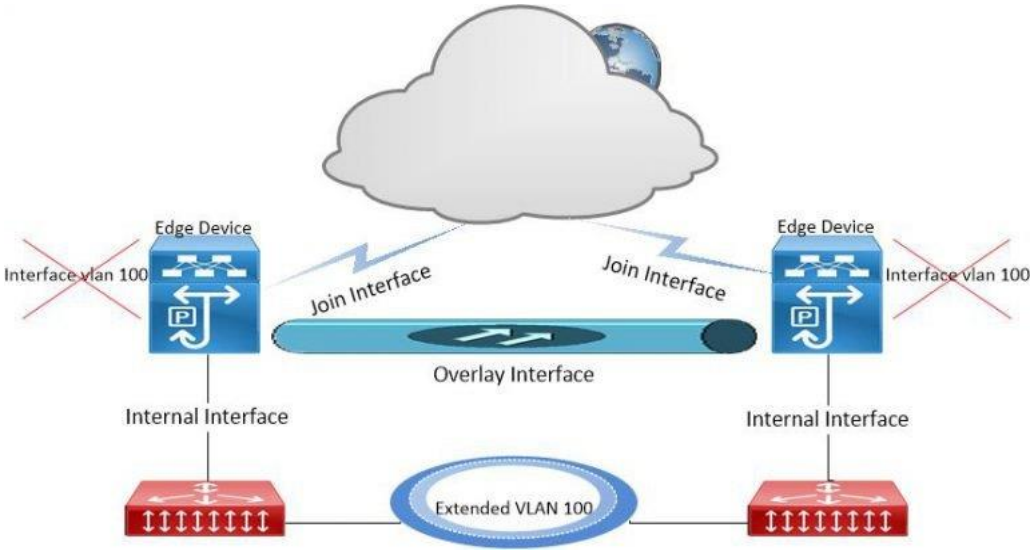
زمانی که دستگاهی در سایت سمت چپ یک ARP Request به آدرس IP A ارسال می‌کند این ARP request به صورت Broadcast به Edge Device رسیده و سپس به تمامی Edge Deviceها ارسال می‌شود. بعد از رسیدن پیام ARP به دستگاه مورد نظر و بازگشت ARP Reply به دستگاه مبدأ، OTV Edge Device سایت سمت چپ این ARP reply را Cash می‌کند تا در درخواست بعدی به همان ادرس IP، مجدداً ترافیکی به کل Edge Device ها ارسال نشود.

OTV ARP aging-timer برای کاهش unicast flooding یه صورت پیش‌فرض کمتر از MAC aging-timer است.

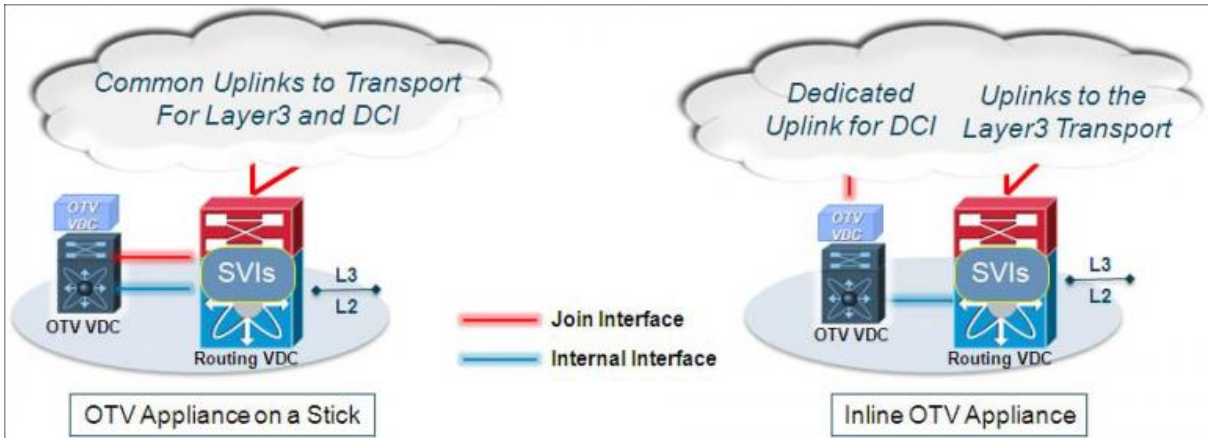
OTV ARP aging-timer: 480 seconds / 8 minute
MAC aging-timer: 1800 seconds / 30 minutes

OTV vs SVI ۱۳-۳-۵-

در پیاده سازی OTV دستگاهی که به عنوان Edge Device پیکربندی می‌شود و وظیفه حمل ترافیک لایه ۲ VLANها را برعهده دارد، نباید دارای اینترفیس SVI آن VLAN باشد. یعنی اگر بخواهید ترافیک VLAN 100 را با استفاده از OTV به مرکز داده دیگری ارسال کنید، Edge Device شما نباید SVI آن VLAN را داشته باشد.



برای حل این مسئله می‌توان از VDC به منظور ایجاد یک Switch مجازی یه عنوان یک Edge Device کمک گرفت.



به حالتی که از یک اینترفیس مشترک به عنوان Join interface استفاده شود OTV-ON-Stick می‌گویند.

به حالتی که از یک اینترفیس مستقل به عنوان Join interface استفاده شود inline می‌گویند.

بصورت پیش‌فرض OTV هیچگونه اطلاعاتی در مورد STP هر سایت بر روی Interface Overlay ارسال نمی‌کند و هر سایت می‌تواند دامنه STP مجزای خود را داشته باشد.

۱۳-٤- OTV Commands

دستورات برای تنظیم OTV برروی دو دستگاه N7K-A و N7K-B بصورت زیر است.

```
N7K-A(config)#feature pim
N7K-A(config)#feature eigrp
N7K-A(config)#feature otv
N7K-A(config)#ip pim rp-address 192.168.1.101 group-list 224.0.0.0/4
N7K-A(config)#ip pim ssm range 232.0.0.0/8
N7K-A(config)#vlan 1-10,100
N7K-B(config-vlan)#exit
N7K-A(config)#router eigrp 11
N7K-A(config-router)#exit
N7K-A(config)# interface Ethernet 2/2
 N7K-A(config-if)#no switchport
N7K-A(config-if)# ip address 192.168.1.1/24
N7K-A(config-if)# ip router eigrp 11
N7K-A(config-if)# ip pim sparse-mode
N7K-A(config-if)# ip igmp version 3
N7K-A(config-if)# no shutdown
N7K-A(config-if)#exit
N7K-A(config)#otv site-vlan 100
```

```
N7K-A(config)#otv site-identifier 0x1
N7K-A(config)# interface Overlay 0
N7K-A(config-if-overlay)# otv join-interface Ethernet 2/2
N7K-A(config-if-overlay)# otv control-group 239.1.1.1
N7K-A(config-if-overlay)# otv data-group 232.1.1.0/28
N7K-A(config-if-overlay)# otv extend-vlan 2-9
N7K-A(config-if-overlay)# no shutdown
N7K-A# show otv
OTV Overlay Information
Site Identifier 0000.0000.0001
Encapsulation-Format ip - gre
Overlay interface Overlay0
 VPN name              : Overlay0
 VPN state             : UP
 Extended vlans        : 2-9 (Total:8)
 Control group         : 239.1.1.1
 Data group range(s)   : 232.1.1.0/28
 Broadcast group       : 239.1.1.1
 Join interface(s)     : Eth2/2 (192.168.1.1)
 Site vlan             : 100 (up)
 AED-Capable           : Yes
 Capability            : Multicast-Reachable
```

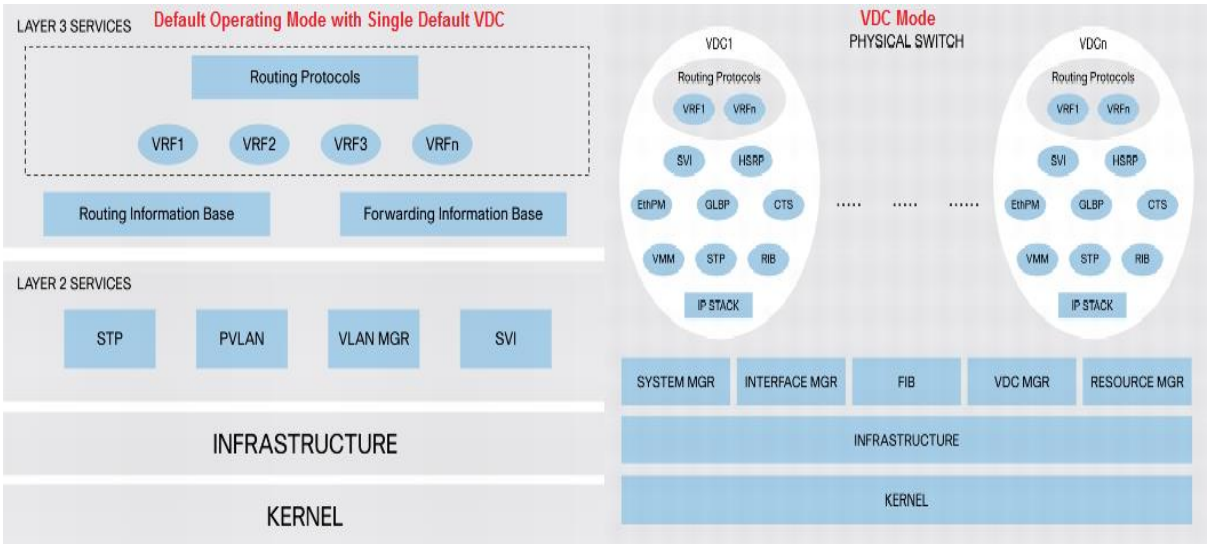
بعد از این مراحل باید اینترفیس‌های پایین دستی در حالت Trunk و اجازه عبور این VLANها را داشته باشند.

همین مراحل برای N7K-B نیز انجام می‌شود و پس از آن می‌توان ارتباط آن دو را مشاهده نمود.

```
N7K-A# show otv adjacency
Overlay Adjacency database
Overlay-Interface Overlay0 :
Hostname                  System-ID      Dest Addr       Up Time     State
N7K-B                     0c5a.ff54.7a2f 192.168.1.2     00:55:49    UP
```

۱۴- Virtual Device Context (VDC)

در تجهیزات Nexus 7000 به مجازی‌سازی کردن سخت‌افزار فیزیکی VDC گفته می‌شود. همچنین بخش کنترلی پروتکل‌ها یا Control Plane Protocols را مجازی‌سازی می‌کند. به عبارت ساده‌تر Switch فیزیکی به چندین Switch مجازی جدا از هم تقسیم می‌شود که هر VDC تنظیمات مربوط به خود را دارد و هیچ ارتباطی با دیگر VDCها ندارد. هر کدام از VDCها لایسنس، جدول مسیریابی، جدول MAC، VLAN و دیگر موارد مخصوص به خود را دارد. بطور مثال VLAN 10 و OSPF PID 1 در VDC 2 هیچ ارتباطی با VLAN 10 و OSPF PID 1 در VDC 3 ندارد. برای فعال نمودن VDC نیاز به Advanced Service License است.



به دو دلیل مهم از VDC می‌توان استفاده نمود. در ابتدا این که می‌توان برای هر شاسی فیزیکی چندین Role متفاوت مشخص نمود. بطور مثال می‌توان VDC 1 را در طراحی در لایه Core و VDC 2 را در لایه Aggregation قرار داد. دلیل دیگر این که می‌توان از یک Switch برای سرویس دادن به چند مشتری استفاده نمود. حداکثر تداد VDC برای هر شاسی در SUP 1 برابر ۴ و برای SUP 2 برابر ۸ است. باید توجه داشت که هیچ ارتباطی بین VDCها وجود ندارد و برای ارتباط بین آنها باید از کابل فیزیکی به عوان Loop بین دو پورت از دو VDC جدا استفاده نمود. برای هر VDC می‌توان منابع را تعریف و محدود نمود. این منابع می‌توان شامل VLAN، VRF، Port Channel، SPAN، ERSPAN، IPv4/v6 Unicast/Multicast Routing، Table، Module Type و دیگر موارد باشد. بعضی از قابلیت‌ها و سرویس‌ها را هم زمان برروی یک VDC نمی‌توان داشت. بطور مثال SVI و OTV هم زمان برروی یک VDC قابل اجرا نیست. مورد دیگر ماژول F1 و M1 نمی‌توانند هم زمان برروی یک VDC باشند ولی ماژول F2E این مشکل را برطرف نموده است. مورد دیگر قابلیت FCoE نیاز به نوع Storage VDC مخصوص به خودش دارد.

Default VDC ۱-۱۴-

بصورت پیش‌فرض VDC 1 یا Default VDC وجود دارد و نمی‌توان آن را حذف نمود. از طریق این VDC می‌توان VDCهای دیگر را ایجاد و مدیریت نمود. بطور مثال می‌توان تعدادی پورت را از VDC 1 جدا و به VDC دیگری اضافه نمود. همچنین از طریق VDC 1 می‌توان منابع دیگر VDCها را تعریف و محدود نمود. بصورت پیش‌فرض تمامی پورت‌ها عضو VDC 1 هستند. برای ایجاد VDC باید در قسمت Global Configuration و در Default VDC با دستور VDC <word> آنها را ایجاد نمود. برای جابه‌جایی بین VDCها باید از دستور switchto و برای برگشتن به Default VDC باید از دستور switchback برروی Default VDC استفاده نمود. از دستور switchto برای تنظیمات ابتدایی استفاده می‌شود و پس از آن می‌توان با دستوراتی مانند SSH آنها را مدیریت نمود.

VDC Resources -۲-۱٤

برای اختصاص دادن اینترفیس به VDCها باید از محدودیت‌های ASIC Port Group پیروی نمود. بطور مثال هر Line Card بر اساس طراحی ASIC محدودیت‌های مخصوص به خود دارد. ماژول N7K-M132XP-12 دارای دو Port Group پیوسته است که در هر گروه باید ۴ پورت باشد. در گروه اول پورت‌های فرد و در گروه دوم پورت‌های زوج قرار دارند. حال برای اختصاص دادن اینترفیس‌ها اگر در یک VDC پورت فردی از این ماژول اضافه شود، دیگر پورت‌های عضو همان گروه بصورت خودکار توسط NX-OS اضافه می‌شوند. Application-Specific Integrated Circuit (ASIC) یک مدار مجتمع است که وظیفه پردازشی خاصی را برعهده دارد. بطور مثال Port ASIC در داخل Switch وظیفه پردازش ترافیک برروی همان پورت را برعهده دارد. برای منابع دیگر نیز می‌توان از دستورات زیر استفاده نمود.

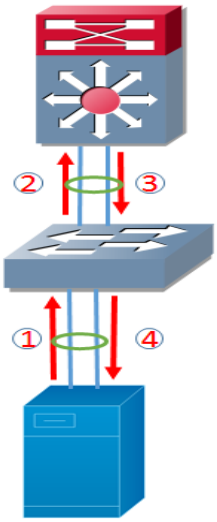
```
limit-resource vrf minimum 2 maximum 4096
limit-resource port-channel minimum 0 maximum 768
limit-resource vlan minimum 16 maximum 4094
```

VDC Users -۳-۱٤

کاربران بصورت پیش‌فرض به دو دسته تقسیم می‌شوند. vdc-admin که همه دسترسی‌های خواندنی و نوشتنی و network-operator که دسترسی‌های فقط خواندنی برروی VDC رادارند. همچنین بصورت پیش‌فرض VDCها دسترسی‌های خود را از Default VDC به ارث می‌برند. بطور مثال vdc-admin نقش network-admin و vdc-operator نقش network-operator را برعهده می‌گیرد. باید توجه داشت که کاربران vdc-admin و vdc-operator نمی‌توانند از دستور switchback برای برگشتن به Defaut VDC استفاده نمایند.

Fabric Extender (FEX) -۱۵

این تکنولوژی سیسکو گسترش دهنده شبکه در لایه Access شبکه مرکز داده است. با استفاده از این تکنولوژی به Switchها اجازه داده می‌شود تا در لایه Access شبکه را رشد و گسترش دهند. تجهیزات سری Nexus 2000 این قابلیت را فراهم کرده است تا همه سرورها در لایه پایین به آنها متصل شوند. برروی N2K هیچ تنظیماتی وجود ندارد و به وسیله Switch بالا دستی یا Parent Switch مدیریت می‌شوند. این تجهیزات پورت Console و VTY ندارند. سیستم‌عامل این تجهیزات از Switch بالا دستی بصورت خودکار دانلود و اجرا می‌شود. زمانی که FEX روشن می‌شود مدت زمانی برای دانلود NX-OS صرف می‌شود و بعد از آن مانند یک پورت معمولی به کار خود ادامه می‌دهد. این تجهیزات هیچ انتقال ترافیک محلی ندارند. به عبارت دیگر ترافیک هنگام دریافت به Switch بالا دستی ارسال می‌شود. پس از بررسی و اعمال سیاست‌ها به FEX اعلام می‌کند که این بسته را به کدام پورت ارسال نماید. در شکل زیر این روند به تصویر کشیده شده است.

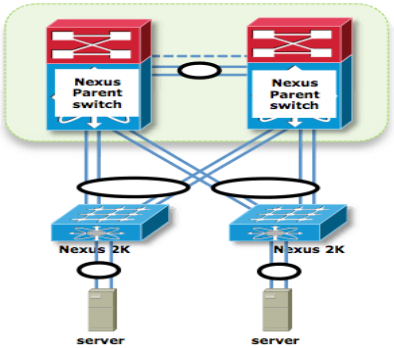


Parent Switch در FEX می‌تواند سری N5K، N6K، N7K و یا N9K باشد که البته بستگی به نوع و پلتفورم Switch دارد. ارتباط FEX با Parent به دو صورت Static Pinning و Dynamic Pinning انجام می‌شود. در حالت Static Pinning تعداد Uplink بصورت دستی مشخص می‌گردد. بطور مثال اگر یک Uplink تعریف شود در صورت از بین رفتن Uplink ارتباط قطع می‌گردد. در حالت Dynamic Pinning از vPC استفاده می‌شود که ضریب اطمینان بالا می‌رود.

اگر Parent از سری N5K باشد از حالت Static Pinning و Dynamic Pinning پشتیبانی می‌شود. همچنین پورت‌های FEX فقط لایه دو می‌توانند باشند.

اگر Parent از سری N7K باشد فقط از حالت Dynamic Pinning پشتیبانی می‌شود. همچنین پورت‌های FEX هم لایه دو و هم لایه سه می‌توانند باشند. البته در سری N7K همه Line Cardها از این قابلیت پشتیبانی نمی‌شود و سیستم‌عامل NX-OS نسخه 7.2 بخ بالا نیاز است. بستگی به نوع طراحی، vPC و نوع Switch پشتیبانی از FEX متفاوت است که چند نمونه در زیر نشان داده شده است.

Host Port Channel and Active-Active FEX Design



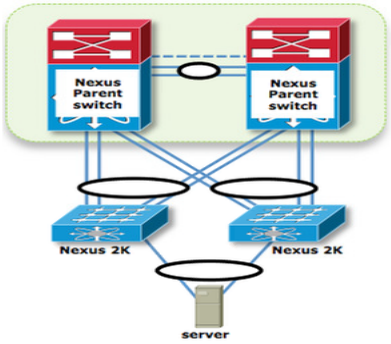
Platform	Code	comment
Nexus 5K	any	Supported
Nexus 6K	any	Supported
Nexus 7K	any	Supported*
Nexus 9K	any	Supported**

* Support introduced from 7.x release

** Supported in 7.0(3)I5(2) and later. Support is for N93XX models only as listed in the release notes.

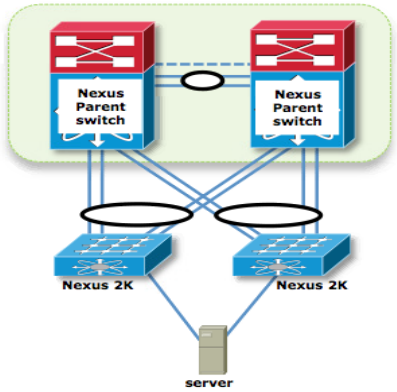
** FEX vPC is not supported between any model of FEX and the Cisco Nexus 9500 platform switches as the parent switches.

Host VPC (Single Link) and Active-Active FEX with FEX HIF VPC PO(Enhanced VPC) Design



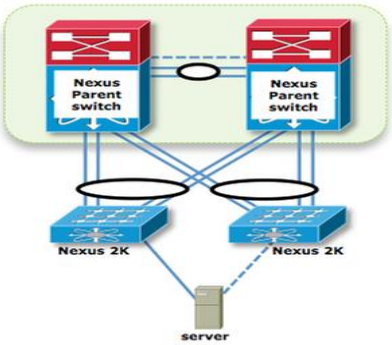
Platform	Code	comment
Nexus 5K	any	Supported
Nexus 6K	any	Supported
Nexus 7K	any	Not Supported
Nexus 9K	any	Not Supported

Dual Homed Host (Active/Active) and Active-Active FEX Design



Platform	Code	comment
Nexus 5K	any	Not Supported
Nexus 6K	any	Not Supported
Nexus 7K	any	Not Supported
Nexus 9K	any	Not Supported

Dual Homed Host (Active/Standby) and Active-Active FEX (VPC) Design



Platform	Code	comment
Nexus 5K	any	Supported
Nexus 6K	any	Supported
Nexus 7K	any	Supported*
Nexus 9K	any	Supported**

*Supported in 7.2 and later

** Supported in 7.0(3)I5(2) and later. Support is for N93XX models only as listed in the release notes.

** FEX vPC is not supported between any model of FEX and the Cisco Nexus 9500 platform switches as the parent switches.

در لایه دو FEX پورت‌ها به عنوان STP Edge Port شناخته می‌شوند و زمان Listening و Learning وجود ندارد. BPDU برروی این پورت‌ها ارسال نمی‌شود و در صورت دریافت BPDU پورت به حالت Disable می‌رود.

۱۶- Virtualization

در این قسمت با انواع مجازی‌سازی در سطح‌های مختلف Storage، Server و Network آشنا شده و توضیح مختصری ارائه می‌گردد. در واقع به جداسازی لایه‌های کامپیوتر از یکدیگر مجازی‌سازی گفته می‌شود.

۱۶-۱- Storage Virtualization

برای دسترسی به یک منبع ذخیره‌سازی اطلاعات سه روش معمول وجود دارد.

۱۶-۱-۱- Direct Attached storage (DAS)

Direct Attached Storage یا DAS به سیستمی گفته می‌شود که در آن ذخیره‌ساز بصورت مستقیم به سرور از طریق کابل متصل می‌شود. با این تعریف یک دیسک که به تنهایی از طریق یکی از اینترفیس‌های مشهور مانند SATA، IDE و SCSI به سیستم متصل شده است، می‌تواند یک DAS باشد. همچنین مجموعه‌ای از دیسک‌ها که توسط یک Controller داخلی یا خارجی به کامپیوتر متصل می‌شوند شکل مشخص‌تری از یک DAS هستند. نکته قابل توجه این است که ذخیره ساز فقط در اختیار یک سیستم است و منابع را با دیگر میزبان‌ها به اشتراک نمی‌گذارد. با استفاده از DAS می‌توان اکثر کارهای معمول از قبیل فایل سرور، وب سرور ، ایمیل سرور و دیتابیس سرور را انجام داد. چنانچه موارد استفاده از حد معمول فراتر رود و حجم اطلاعات افزایش یابد می‌بایست به روش‌های دیگری مانند SAN و NAS مراجعه نمود. در سیستم‌های فعلی سازمانی از DAS بیشتر برای موارد فایل سروری استفاده می‌شود.

۱۶-۱-۲- Network Attached Storage (NAS)

سیستم ذخیره‌سازی متصل به شبکه (Network Attached Storage) یا به اختصار NAS دستگاهی است که به صورت اشتراکی در شبکه مورد استفاده قرار می‌گیرد. این نوع سیستم‌های ذخیره‌سازی تحت سیستم‌عامل‌های مختلف، با استفاده از Network File System (NFS) در محیط‌های Linux و Common Internet File System (CIFS) در محیط‌های Windows با اجزای شبکه ارتباط برقرار می‌کنند. NAS برخلاف SAN از سطح File-Level در عملیات استفاده می کند. وجود NAS در یک شبکه برای کاربران آن شبکه افزایش کارایی و استقلال را به وجود می‌آورد. خود دستگاه NAS یک وسیله پرسرعت، کارآمد، تک‌منظوره و اختصاصی است که در قالب یک ماشین یا جعبه عرضه می‌شود. این دستگاه طوری طراحی شده که به تنهایی کار کند و نیازهای خاص ذخیره‌سازی سازمان را با استفاده از سیستم‌عامل، سخت‌افزار و نرم‌افزار خود در بهترین حالت برآورده سازد. NAS را می‌توان مثل یک دستگاه plug-and-play در نظر گرفت که وظیفه آن تأمین نیازمندی‌های ذخیره‌سازی است. یک واحد NAS در حقیقت سیستمی خاص برای به اشتراک گذاری فایل‌ها در

شبکه است. این نوع سیستم‌های ذخیره‌سازی، بسیار شبیه به File Sharing است که فایل‌ها را در شبکه توسط File Server و با آدرس IP مشخص به اشتراک می‌گذارند. سیستم‌های ذخیره‌سازی NFS ساختار Client/Server دارند. NFS توسط SUN Microsystem طراحی شده است و حدود ده درصد سریع‌تر از CIFS است. سه نسخه متفاوت در NFS وجود دارد که در NFSv2 از پروتکل UDP با اندازه فایل 32 Bit، در نسخه NFSv3 از پروتکل TCP و با اندازه فایل 64 Bit و در نسخه NFSv4 از پروتکل Stateful و عملکرد و امنیت بالا استفاده می‌شود. کاربران NFS با استفاده از دستور mount می‌توانند فایل سیستم از راه دور را برروی سیستم خود سوار (mount) نمایند. بعد از آن باید با استفاده از Remote Procedure Call (RPC) به پورت TCP/UDP 111 که برروی سرور درحال اجرا است متصل شوند. Mount و RPC هر دو باهم دسترسی به فایل‌های برروی File Server را فراهم و دستوراتی مانند خواندن، نوشتن و ... را اجرا می‌کنند.

۱۶-۱-۳- Storage Area Network (SAN)

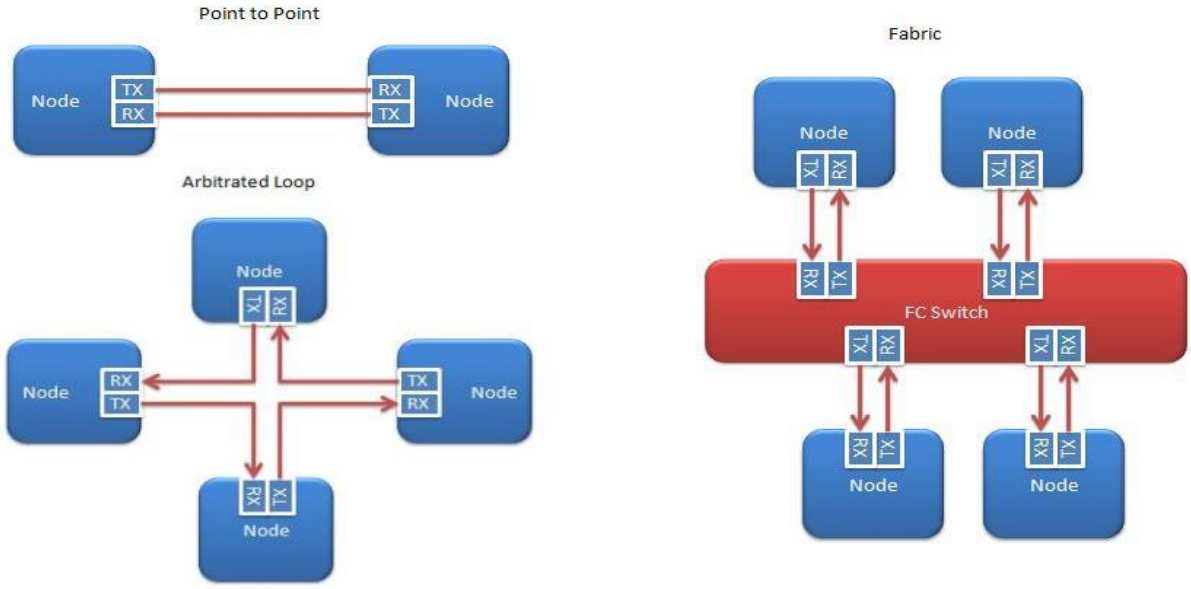
Storage Area Network یا SAN شبکه‌ای است که برای ذخیره‌سازی داده‌ها اختصاص داده شده و بصورت Block Based است. بطور معمول SANها از شبکه داخلی برای میزبان‌های ذخیره‌سازی خود بهره می‌برند. SAN می‌تواند از ایجاد ترافیک در شبکه، به عنوان یک عامل بازدارنده سرعت جلوگیری نماید. در این نوع از Data Block یا بلوک داده سیستم‌های ذخیره‌سازی برای خواندن، نوشتن و ... استفاده می‌شود. پروتکلی که برای انتقال Data Block در این سیستم‌های ذخیره‌سازری استفاده می‌شود Small Computer System Interface (SCSI) نام دارد که از طریق کابل SCSI به Disk متصل می‌شود. در شبکه‌های SAN از پروتکل SCSI برای ارتباط بین Server (Initiator) و Disk Array (Target) استفاده می‌شود. پروتکل SCSI دستورات SCSI و Data Block را برروی یک کانال SCSI عبور می‌دهد. دستورات SCSI می‌تواند خواندن، نوشتن و ... باشد. کانال SCSI می‌تواند در حالت پایه‌ای یک Parallel Shared Bus در داخل و یا خارج از سرور باشد. از این پروتکل بیشتر داخل سرور استفاده می‌شود. پروتکل‌های دیگری وجود دارد که می‌توانند جایگزین SCSI شوند تا بتوان از راه دور Data Block را انتقال داد. پروتکل iSCSI انتقال SCSI برروی IP یا TCP/IP را تأمین می‌کند. پروتکل Fiber Channel (FC) دستورات SCSI را برروی بستر Fiber Optic یا فیبر نوری انتقال می‌دهد که تأخیر کمتر و پهنای‌باند بیشتری را فراهم می‌کند. پروتکل Fiber Channel Over Ethernet (FCoE)، پروتکل FC را برروی بستر Ethernet بسته‌بندی و ارسال می‌کند. FCoE یک I/O یکپارچه را فراهم می‌کند. به عبارت دیگر شبکه LAN و SAN برروی یک کابل انتقال داده می‌شوند. به همین جهت، ایجاد یک شبکه ذخیره‌سازی از راه دور با SAN امکان‌پذیر است. SAN غالباً بهترین انتخاب برای بررسی مسائل پهنای‌باند، دسترسی به داده‌ها و یکپارچه‌سازی است. با توجه به تفاوت‌های بنیادینی که بین تکنولوژی و اهداف SAN و NAS وجود دارد، برای انتخاب هر یک باید تصمیم اساسی گرفته شود. هر یک از این دو را می‌توان برای رفع نیازهای ذخیره‌سازی مورد استفاده قرار داد. از سیستم‌های ذخیره‌سازی Block Level برای

DB APP، مواردی که نیاز به پهنای‌باند و عملکرد بالا یی است مورد استفاده قرار می‌گیرد. همچنین این سیستم‌ها قابلیت Boot شدن از روی SAN را فراهم می‌کنند.

۱۶-۱-٤- Fiber Channel (FC)

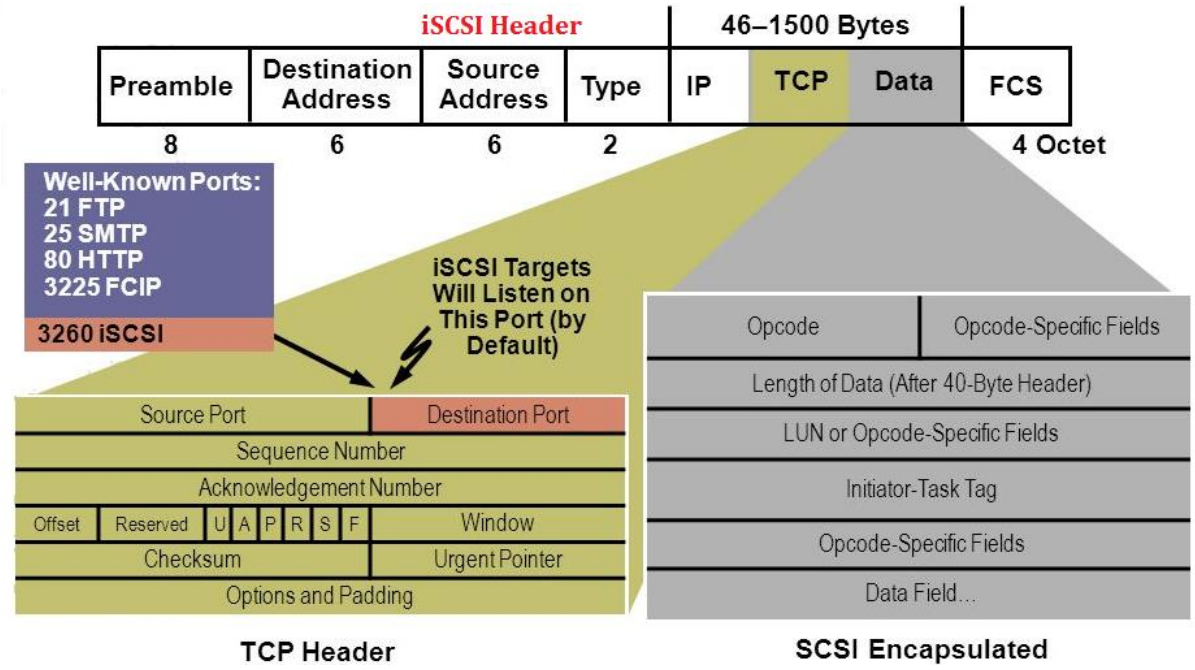
پروتکل FC محیط SCSI را با استفاده از شبکه گسترش می‌دهد. پروتکل FC تعداد 2^{24} دستگاه و تا فاصله ده کیلومتر و در بعضی موارد تا پنجاه کیلومتر و از سرعت 1/4/.../128 Gbit/s پشتیبانی می‌کند. در FC سه نوع توپولوژی Pint-to-Point، Arbitrated Loop و Switch Fabric وجود دارد که مشخص می‌کند چگونه Nodeها و یا دستگاه‌ها با یکدیگر ارتباط برقرار نمایند. FC Initiator و FC Target از طریق FC Frame Sequence با یکدیگر ارتباط برقرار می‌کنند. کوچک‌ترین واحد داده در FC Frame برابر 4 Byte است که داخل صف فرستاده می‌شود. هر صف بصورت یکطرفه است و این صف بین FC Nodeها جابه‌جا می‌شود. Host Bus Adapter (HBA) در واقع همان کارت شبکه در شبکه‌های SAN است. از طریق HBA سرورها و سیستم‌های ذخیره‌سازی با SAN Switch ارتباط برقرار می‌کنند. HBA فقط وظیفه انتقال ترافیک شبکه SAN را برعهده دارد. سرعت HBAها از 1/.../32 Gbit/s است. همچنین HBAها عملیات پردازشی پروتکل FC را برروی سخت‌افزار فراهم می‌کنند.

Fiber Channel Frame
Start of Frame (SOF) (4 Bytes)
Frame Header (24 Bytes)
Optional Header (ESP(8), network(16), association(32), device) (0-64 Bytes)
Optional Association Header (32 Bytes)
Data Payload (0-2048 Bytes)
Necessary Fill Bytes, Optional ESP Checksum Trailer (0-36 Bytes)
Cyclic Redundancy Checksum (CRC) (4 Bytes)
End of Frame (EOF) (4 Bytes)



Internet Small Computer System Interface (iSCSI) ۱۶-۱-۵-

این پروتکل دستورات SCSI را برروی بستر TCP و برروی IP ارسال می‌کند. ساختار Protocol Stack آن با FC کاملاً متفاوت است. پروتکل iSCSI معمولاً در شبکه‌های کوچک و متوسط استفاده می‌شود و نیاز به SAN Switch مجزا ندارد و از سرعت 1/.../100 Gbit/s پشتیبانی می‌کند. برای استفاده از این پروتکل می‌توان از نرم‌افزارهای iSCSI یا همان Software Driver به جای سخت‌افزار iSCSI استفاده نمود. البته همانطور که واضح است عملکرد خوبی ارائه نمی‌شود. سخت‌افزارهای iSCSI به دو دسته تقسیم می‌شوند. Full Offload که تمام پردازش‌های iSCSI و TCP برروی کارت شبکه انجام می‌دهد. در Partial Offload کارت شبکه فقط وظیفه ایجاد و مدیریت پردازش‌های TCP و ارتباطات را برعهده دارد که TCP Offload Engine (TOE) نام دارد. iSCSI Initiator همان Server و iSCSI Target همان Disk Array هستند. iSCSI Qualified Name (IQN) شبیه DNS است و یک نام برای iSCSI Node است. کارت دیگری نیز به نام Converged Network Adapter (CAN) نیز وجود دارد که ترکیبی از HBA و NIC است.



Logical Unit Number (LUN) ۱۶-۱-۶-

زمانی که از مجازی‌سازی ذخیره‌ساز استفاده می‌شود برای بدست آوردن محلی برای ذخیره‌سازی برروی دیسک داخل یک آرایه از دیسک‌ها از LUN استفاده می‌شود. به عبارت دیگر از LUN برای ارائه‌کردن (Present) دیسک به میزبان (Host) استفاده می‌شود. در واقع از LUN برای شماره‌گذاری یک واحد منطقی برروی دیسک در جایی که پروتکل SCSI یا پروتکل‌های شبکه ذخیره‌سازی دیگری که SCSI را بسته‌بندی می‌کنند مانند iSCSI یا Fiber Channel کاربرد دارند، استفاده می‌شود. در سیستم‌های ذخیره‌سازی Block Based یک Block از اطلاعات توسط LUN آدرس‌گذاری می‌شود. در آرایه‌های ذخیره‌سازی (Storage Arrays)، LUNها با اندازه‌های مختلف MB، GB و TB به میزبان‌ها ارائه می‌شوند. در آرایه‌های ذخیره‌سازی مدیر سیستم ذخیره‌ساز

تعدادی LUN ایجاد می‌کند و آنها را به میزبان‌ها ارائه می‌نماید. آرایه‌های ذخیره‌سازی، دیسک‌ها را مجازی‌سازی و آنها را به میزبان‌ها ارائه می‌کنند تا میزبان‌ها از آنها استفاده نمایند. در واقع میزبان‌ها می‌توانند به LUNهای متفاوتی دسترسی داشته و یا از یک LUN بصورت اشتراکی استفاده نمایند. در آرایه‌های ذخیره‌سازی می‌توان بنابر نیاز و دسترسی‌پذیری از RAIDهای مختلف استفاده نمود. همچنین می‌توان از تکثیر داده‌ها (Replication) بین آرایه‌های ذخیره‌سازی استفاده نمود. به عبارت دیگر یک کپی از داده‌ها برروی آرایه دیگر داشت.

۱۶-۱-۷- LUN Management

اصطلاحاتی که در این قسمت وجود دارد به اختصار توضیح داده شده است.

۱. LUN Masking: روشی برای کنترل دسترسی ارائه یک LUN به میزبان برروی آرایه ذخیره‌سازی است. بطور مثال می‌توان تعریف نمود که کدام LUN در دسترس کدام میزبان قرار گیرد.
۲. LUN Mapping: در واقع پردازشی است که LUN را تعریف می‌کند و LUN را برروی FC HBA قرار می‌دهد. بطور مثال برروی یک FC HBA یک میزبان تعدادی LUN در دسترس قرار می‌گیرد.
۳. LUN Zoning: یک قابلیتی است که ارتباط میزبان با دستگاه ذخیره‌سازی را محدود می‌کند.

بطور کلی ابتدا یک LUN توسط LUN Mapping تعریف و برروی FC HBA قرار می‌گیرد. پس از آن ارتباط میزبان توسط LUN Zoning برقرار می‌شود. برای امنیت بیشتر می‌توان با استفاده از LUN Masking دسترسی میزبان‌ها به LUNها را محدود نمود.

۱۶-۱-۸- Type Of Storage Virtualization

مجازی‌سازی در سیستم‌های ذخیره‌سازی انواع مختلفی دارد که در ادامه توضیح مختصری داده می‌شود.

۱. Host-Based Storage Virtualization: یک راه حل نرم‌افزار ذخیره‌سازی بروی Host است. در واقع همه مجازی‌سازی و مدیریت در سطح Host قرار دارد و از طریق نرم‌افزار انجام می‌شود. این راه حل به شرکت‌های ذخیره‌سازی و تکنولوژی‌هایی مانند FC یا iSCSI وابسته است. در این راه حل میزبان از CPU زیادی استفاده می‌کند، به Driverهای نرم‌افزاری نیاز دارد و مدیریت آن بصورت جداگانه است.
۲. Array-Based Storage Virtualization: در این راه حل نیاز به سخت‌افزار آرایه ذخیره‌سازی است. در این روش تعریف می‌شود که آرایه ذخیره‌سازی از کدام نوع از دیسک فیزیکی برای لایه‌بندی ذخیره‌سازی استفاده نماید. بطور مثال آرایه ذخیره‌ساز از کدام HDD و یا SSD استفاده نماید و آن را به میزبان ارائه کند. معمولاً به آرایه ذخیره‌ساز در این مدل Shared Storage گفته می‌شود. تمامی تنظیمات مجازی‌سازی در این مدل برروی آرایه ذخیره‌ساز یا Controller صورت می‌گیرد که Controller نزدیک به دیسک‌ها است. وابستگی این مدل به سیستم‌عامل یا میزبان است. شرکت‌های

متعددی در این زمینه تجهیزاتی ساخته‌اند که برای مدیریت آنها نیاز به دانش خاصی احساس می‌شود و مدیریت و هزینه بالایی دارند.

۳. Network-Based Storage Virtualization: در این راه حل از Virtual Appliance و یا FC Switch برای ساخت یک شبکه ذخیره‌سازی استفاده می‌شود. در این راه حل همه سیستم‌های ذخیره‌سازی و میزبان‌ها از طریق Switch به یک شبکه SAN متصل می‌شوند. این راه حل به روزترین و کارآمدترین راه حل است و به میزبان و یا سیستم عامل وابسته است. در هنگام طراحی باید به Bottleneck، Single Point Of Failure و Scalability توجه نمود.

۲-۱۶- Server Virtualization

به چکیده و جداسازی سیستم‌عامل و برنامه کاربردی از لایه سخت‌افزار مجازی‌سازی سرور گفته می‌شود. در واقع یک لایه نرم‌افزاری بین لایه سخت‌افزار و سیستم عامل قرار می‌گیرد که می‌توان چندین سیستم‌عامل را بطور هم‌زمان اجرا نمود. به سیستم‌عامل اجرا شده برروی این لایه Virtual Machine (VM) یا ماشین‌مجازی گفته می‌شود. به لایه نرم‌افزاری که ماشین‌های مجازی برروی آن اجرا می‌شوند سیستم عامل مجازی‌ساز یا Hypervisor گفته می‌شود. وظیفه Hypervisor مدیریت منابع سخت‌افزاری و به اشتراک گذاشتن آنها است. نتیجه مجازی‌سازی سرور استفاده بیشتر از منابع، اجرای هم‌زمان چندین سیستم‌عامل برروی یک سخت‌افزار فیزیکی، کاهش تعداد سرور فیزیکی و کاهش هزینه‌ها است. Hypervisor یک سیستم‌عامل بسسار سبک است که برروی میزبان فیزیکی بین سخت‌افزار و VM نصب می‌گردد. وظیفه اصلی Hypervisor کنترل و مدیریت منابع سخت‌افزاری، ایجاد و یا حذف ماشین‌مجازی و همچنین مجازی‌سازی کردن سخت‌افزار و ارائه آن به ماشین‌های مجازی است. به عبارت دیگر CPU، Memory، Network و Disk را بصورت اشتراکی در اختیار ماشین‌های مجازی قرار می‌دهد. ماشین‌مجازی شامل سیستم عامل و برنامه کاربردی است. به سیستم‌عامل ماشین‌مجازی Guest OS یا سیستم‌عامل مهمان گفته می‌شود. هر ماشین‌مجازی آدرس MAC مجازی شبیه به آدرس MAC فیزیکی و آدرس IP برای تنظیمات شبکه خود دارد. همچنین هر ماشین‌مجازی دارای vCPU، vMemory و دسترسی منابع ذخیره‌سازی محلی و یا از راه دور دارد. فوایدی که ماشین‌مجازی ایجاد می‌کند شامل موارد زیر است:

۱. از حداکثر منابع سخت‌افزاری استفاده می‌شود. می‌توان چندین ماشین‌مجازی برروی یک سرور فیزیکی راه‌اندازی نمود.
۲. ماشین‌های مجازی که برروی یک سرور فیزیکی قرار دارند کاملاً از هم جدا هستند و تدابیر امنیتی برروی آنها اعمال می‌گردد.
۳. فایل‌های ماشین‌مجازی به راحتی قابل کپی و پشتیبان‌گیری هستند.

۴. ماشین‌های مجازی می‌توانند بین سرورهای فیزیکی جابه‌جا شوند. به جابه‌جایی ماشین‌های مجازی بین سرورهای فیزیکی vMotion گفته می‌شود. البته این قابلیت پیش‌نیازهایی اعم از Shared Storage، پیش‌نیازهای شبکه و ... دارد.

۱۶-۲-۱- Type Of Server Virtualization

مجازی‌سازی در لایه سرور به دو دسته تقسیم می‌شود.

۱. Hosted Hypervisor: در واقع به اجرا کردن یک سیستم‌عامل داخل سیستم‌عامل دیگر گفته می‌شود. بطور مثال برروی یک سیستم‌عامل یک نرم‌افزار مجازی‌سازی نصب می‌شود که داخل آن می‌توان سیستم‌عامل دیگری راه‌اندازی نمود. نمونه‌ای از این نرم‌افزار VMware Workstation است.

۲. Bare-Metal Hypervisor: در واقع همان سیستم‌عامل مجازی‌ساز است که بدون واسطه برروی سرور فیزیکی نصب می‌گردد. نمونه‌ای از این سیستم‌عامل VMware ESXi است. در واقع این محصول لایه‌ای فراهم می‌کند تا ماشین‌های مجازی بروی آن نصب شوند. این سیستم‌عامل بسیار سبک است و قابلیت Bootable شدن برروی USB Drive را دارد. ESXi می‌تواند منابع سخت‌افزاری را برای ماشین‌های مجازی به اشتراک گذارد.

۱۶-۲-۲- ESXi Feature

در زیر نمونه‌ای از قابلیت‌های ESXi به اختصار توضیح داده شده است.

۱. در زمینه شبکه از مجازی‌سازی شبکه پشتیبانی می‌کند. این سیستم‌عامل قابلیتی را فراهم می‌کند تا یک Switch مجازی به نام Standard vSwitch بصورت جداگانه برروی هر ESXi نصب و مدیریت شود. همچنین یک Switch مجازی دیگر به نام Distributed vSwitch را فراهم می‌کند تا بصورت توزیع شده برروی همه ESXiها پیاده‌سازی و بصورت یکپارچه مدیریت و تنظیم شود. همچنین از محصول Cisco 1000v پشتیبانی می‌کند.

۲. در زمینه منبع ذخیره‌سازی یک فایل سیستم به نام Virtual Machine File System (VMFS) برای ماشین‌مجازی فراهم می‌کند تا بتواند دیسک‌های مجازی، فایل تنظیمات و ... خود را برروی آن قرار دهد.

۳. این سیستم‌عامل مجازی‌ساز می‌توان توسط یک نرم‌افزار مدیریتی یکپارچه به نام VMware vCenter مدیریت شود.

۴. ESXi از قابلیت vMotion (Live & Cold) برای جابه‌جایی ماشین‌های مجازی پشتیبانی می‌کند.

VMware vCenter یک نرم‌افزار مدیریتی یکپارچه و مرکزی است که می‌تواند ESXiها را مدیریت نماید. همچنین قابلیت‌های بیشتر و پیشرفته‌ای مانند Virtual Distributed vSwitch، Fault Tolerance،

vMotion و ... را فراهم می‌کند. در نسخه‌های قدیمی برای اتصال به vCenter یا ESXi نیاز به یک نرم‌افزار به نام vSphere Client بود که در نسخه‌های جدید کاملاً تحت وب هستند.

Microsoft Hyper-V نیز یک سیستم‌عامل مجازی‌ساز برروی Windows Server 2008 R2 به بعد است که از قابلیت‌هایی همچون Live Migration یا vMotion پشتیبانی می‌کند. همچنین قابلیت نصب چندین VM بروی یک سرور فیزیکی را دارد. این نرم‌افزار توسط شرکت Microsoft ارائه شده است و جایگزینی بعد از VMware است.

۱۶-۳- Network Virtualization

در قسمت مجازی‌سازی شبکه به توضیح مختصری در رابطه با محصولات VMware و Cisco پرداخته می‌شود. در لایه سخت‌افزار کارت شبکه سرور از طریق کابل به Switch فیزیکی متصل می‌شود. زمانی که Hypervisor برروی یک سرور فیزیکی نصب می‌شود و ماشین‌های مجازی متعددی برروی Hypervisor نصب می‌گردد. برای برقراری ارتباط ماشین‌های مجازی با یکدیگر، ارتباط ماشین‌های مجازی با کارت شبکه فیزیکی سرور و ارتباط ماشین‌های مجازی با خارج از سرور فیزیکی نیاز به یک لایه شبکه مجازی است. این لایه شبکه مجازی می‌تواند Standard Switch، Distributed Switch و یا Nexus 1000v باشد.

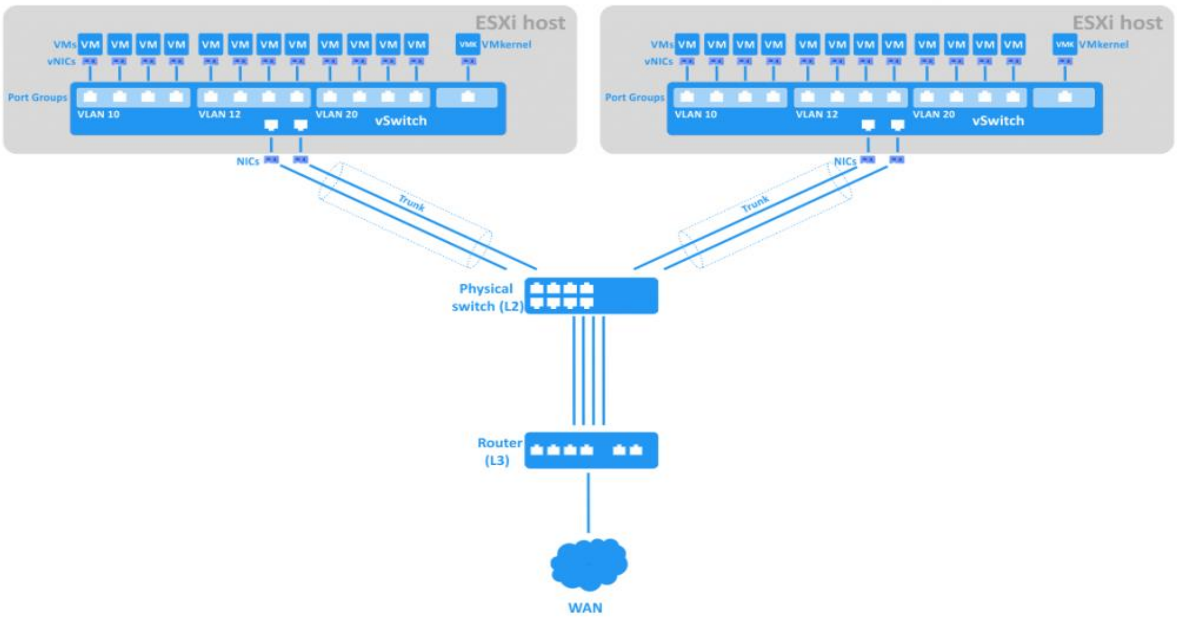
قسمت‌های مختلف شبکه مجازی شامل موارد زیر است:

۱. ماشین‌مجازی یا VM که برروی آن IPv4 تنظیم شده است.
۲. کارت شبکه مجازی یا vNIC که برروی ماشین‌مجازی قرار دارد.
۳. Virtual Switch که برروی Hypervisor نصب شده و ماشین‌های مجازی به آن متصل می‌شوند.
۴. ارتباط بین Virtual Switch و کارت شبکه فیزیکی است که در واقع ارتباط با Switch فیزیکی را برقرار می‌کند.

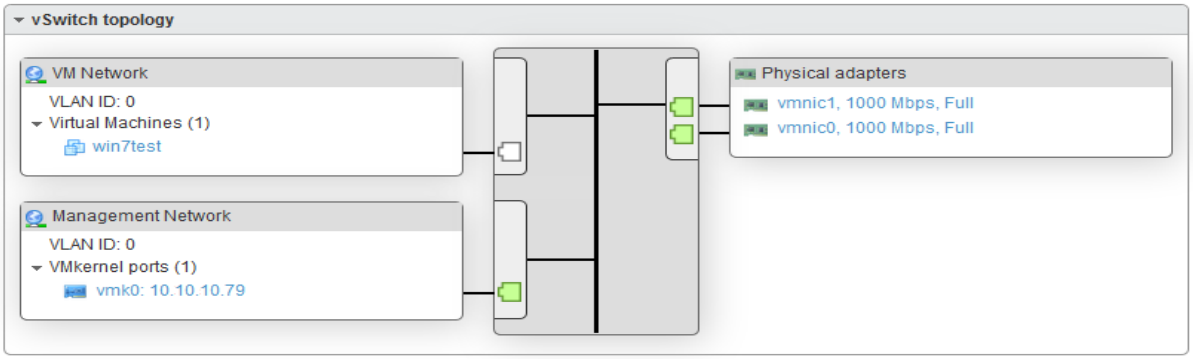
۱۶-۳-۱- Standard vSwitch (vSwitch)

این Switch مجازی داخل هر Hypervisor بصورت جداگانه ایجاد و مدیریت می‌شود. با استفاده از این Switch مجازی ارتباط بین VMهای داخل یک Hypervisor و ارتباط آنها با کارت شبکه فیزیکی برقرار می‌شود. چندین نوع پورت در این Switch وجود دارد. نوع اول VM Port Group که همان Access Port است و به VMها یک VLAN اختصاص داده می‌شود. نوع دوم Uplink Port Group که ارتباط VMها با کارت شبکه فیزیکی را برقرار می‌کند. نوع سوم VMKernel Port که برای ترافیک مدیریتی، vMotion و دیگر موارد استفاده می‌شود. در نوع سوم این پورت به خود یک آدرس IP برای مدیریت اختصاص می‌دهد. در واقع به سرور فیزیکی یک پورت از نوع VMKernel اختصاص داده می‌شود تا از طریق آن بتوان سرور مذکور را مدیریت نمود.

برروی هر ESXi می‌توان چندین Standard vSwitch ایجاد نمود که هر ESXi می‌تواند حداکثر ۱۰۱۶ پورت فعال و ۳۲ پورت Uplink داشته باشد. عملیات‌هایی که می‌توان برروی لایه دو این Switch انجام داد شامل ارسال Frame با استفاده از آدرس MAC، نگهداری جدول MAC و جابه‌جایی ترافیک بین VMهای داخلی می‌شود. Uplinkها پورت‌های Trunk با استاندارد 802.1q هستند و از Port Channel پشتیبانی می‌کنند.



vSphere	5.0	5.1	5.5	6.0	6.5	6.7
Total virtual network switch ports per host	4096	4096	4096	4096	4096	4096
Maximum active ports per host	1050	1050	1016	1016	1016	1016
Virtual network switch creation ports	4088	4088	4088	4088	4088	4088
Port groups	512	512	512	512	512	512
Distributed virtual network switch ports per vCenter	60000	60000	60000	60000	60000	60000
Static port groups per vCenter	10000	10000	10000	10000	10000	10000
Ephemeral port groups per vCenter	1016	1016	1016	1016	1016	1016
Hosts per distributed switch	350	500	500	1000	2000	2000
Distributed switches per vCenter	32	128	128	128	128	128



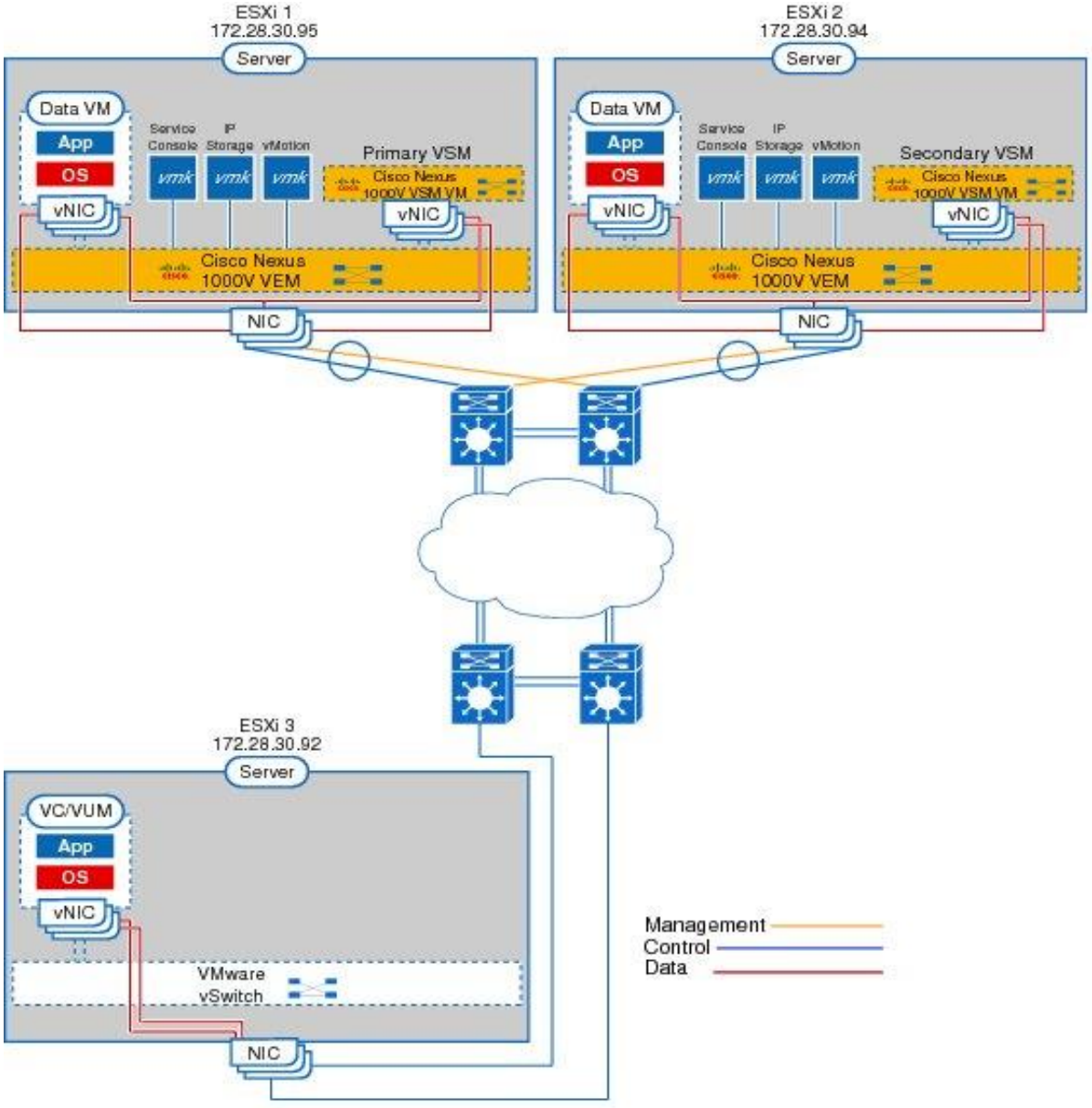
Virtual Distributed Switch (vDS) ۱۶-۳-۲-

این نوع Switch مجازی قابلیت پشتیبانی از چندین ESXi را دارد که می‌توانند بصورت اشتراکی از آن استفاده نمایند. vDS توسط یک نرم‌افزار مدیریتی یکپارچه به نام VMware vCenter ایجاد و مدیریت می‌شود. vDS

مدیریت شبکه را از Host Level به سمت Cluster Level انتقال می‌دهد. مدیریت مرکزی یکپارچه، اجرای سیاست‌های شبکه بین ESXiها، پشتیبانی از Private VLAN و اعمال محدودیت‌های شبکه ار فواید vDS است.

۱۶-۳-۳- Nexus 1000v (N1Kv)

این نرم‌افزار توسط شرکت سیسکو برای محیط مجازی به ویژه VMware طراحی شده است. 1000v یک Switch مجازی با سیستم‌عامل NX-OS است که شبیه به یک Cisco Modular Chassis Switch عمل می‌کند. این Switch همانند vDS بصورت توزیع شده برروی ESXiها قرار می‌گیرد و قابلیت اعمال سیاست بین ماشین‌های مجازی را دارد. همچنین یک محیط CLI در اختیار مدیر قرار می‌دهد تا به راحتی بتواند شبکه مجازی را مدیریت و مشکلات آن را برطرف نماید. N1Kv از Hypervisorهای متفاوتی مانند ESXi، Hyper-V، KVM، XEN و ... پشتیبانی می‌کند. این Switch مجازی از قسمت‌های مختلفی تشکیل شده است که به اختصار توضیح داده می‌شود.



۱. Virtual Supervisor Module (VSM): این قسمت بخش Control Plane را برعهده می‌گیرد. در واقع بخش کنترلی و مدیریت شبکه VMهایی که برروی NX-OS هستند را برعهده می‌گیرد.
۲. Virtual Ethernet Module (VEM): در واقع یک Line Card مجازی است که برروی هر ESXi جانمایی شده است. VEM یک بخش داخلی از Kernel سیستم‌عامل مجازی‌ساز یا Hypervisor است که VEM Agent نام گذاری می‌شود.
۳. Cisco vPath: این بخش اختیاری است و در واقع زنجیره‌ای از سرویس‌ها است که به عنوان یک هوش داخلی برروی ماژول VEM جانمایی شده است. این مدل بصورت پویا چندین سرویس را برروی ترافیک ماشین‌مجازی اعمال می‌کند. این مدل برای محیط‌های مجازی ابری پیشنهاد می‌گردد. ساختار vPath یک Forwarding-Plane و یک چهارچوب قابل برنامه‌نویسی برای ایجاد و یا حذف سرویس‌های شبکه مانند Firewall، Load Balancer و ... در لایه Hypervisor فراهم می‌کند.

۱۶-۳-٤- Nexus 1000v Installation

برای نصب این Switch نیاز به VMware vCenter است. VSM یک Appliance مجازی یا ماشین‌مجازی است که برروی vCenter، Deploy می‌گردد و Distributed Virtual Switch (DVS) را فراهم می‌کند. برای ارتباط VSM و vCenter باید از دستور svs connection در محیط Global استفاده نمود. svs کوتاه شده عبارت Server Virtualization Switch است. VEM نیز یک Agent است که برروی ESXi نصب می‌شود. باید توجه داشت که نسخه‌های VSM و VEM باید یکسان باشند.

پس از Deploy شدن VSM باید VEM را برروی هر ESXi نصب و تنظیم نمود. VSM یک محیط وب در اختیار مدیر می‌گذارد تا VEM را دانلود نماید. زمانی که یک ESXi به یک N1Kv-DVS متصل می‌شود vCenter اطلاعاتی را به ESXi انتقال می‌دهد تا VEM از آن برای اتصال به VSM استفاده نماید. ماشین‌مجازی VSM نیاز به سه کارت شبکه مجازی برای Control، Packet و Data دارد. System Port Profile برای برپا نگهداشتن و حفاظت از پورت‌ها و VLANها قبل از اینکه VEM به VSM متصل شود، طراحی شده است. زمانی که مدیر یک ESXi را به DVS اضافه می‌نماید، ماژول VEM باید با VSM ارتباط برقرار نماید. این روند

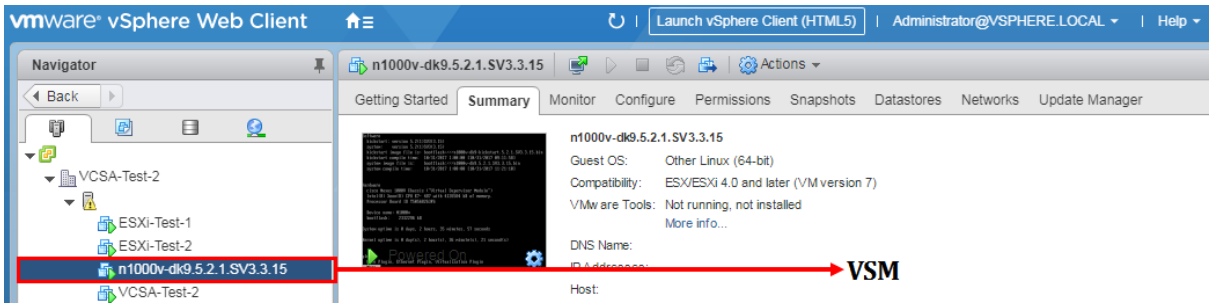
Cisco Nexus 1000V

Following files are available for download :

- Cisco Nexus 1000V Installer Application
  - Launch Installer Application (deprecated)
- Cisco Nexus 1000V Extension
  - cisco_nexus_1000v_extension.xml
- VEM Software

Description	File
ESXi 6.5 or later	cisco-vem-v470-5.2.1.3.3.15.0-6.5.1.zip
ESXi 6.0 or later	cisco-vem-v470-5.2.1.3.3.15.0-6.0.1.zip
ESXi 5.5 or later	cisco-vem-v470-5.2.1.3.3.15.0-3.2.1.zip
ESXi 6.5 or later	cross_cisco-vem-v470-5.2.1.3.3.15.0-6.5.1.vib
ESXi 6.0 or later	cross_cisco-vem-v470-5.2.1.3.3.15.0-6.0.1.vib
ESXi 5.5 or later	cross_cisco-vem-v470-5.2.1.3.3.15.0-3.2.1.vib

در حالی است که پورت‌ها و VLANها برای این ارتباط هنوز وجود ندارد. بنابراین VSM یک سری از تنظیمات حداقلی شامل System Port Profile و System VLANs به vCenter ارسال می‌نماید تا این تنظیمات را به VEM اعلام نماید. این امر باعث می‌شود حتی زمانی که VEM با VSM ارتباط برقرار نکرده است، ترافیک ماشین‌های مجازی ارسال شوند. زمانی که System Port Profile تنظیم می‌شود، باید مدیر VLANها را مشخص و آنها را به عنوان System VLANs معین نماید. System VLANs باید هم برروی ETH و vETH تعریف شود تا ترافیک ماشین‌های مجازی بتوانند از طریق کارت شبکه فیزیکی خارج شوند. به عبارت دیگر باید VLANهای مربوط به بخش Control و Packet، Management و Storage به عنوان System VLANs تعریف شوند تا در ارتباط مدیریتی اختلال به وجود نیاید. پس از نصب N1Kv برای SVS دو حالت Layer 2 و Layer 3 وجود دارد. در حالت L2 شبکه VEM و VSM Control VLAN در یک VLAN هستند. معمولاً از L2 استفاده نمی‌شود زیرا معمولاً سرویس‌ها در VLANهای متفاوتی هستند. در L3 ترافیک VEM در VLAN متفاوتی قرار دارد که در قالب UDP 4785 بسته‌بندی می‌شود و باید آن را به VSM مسیریابی نمود. دستور capability l3control باید برروی vETH Profile قبل از انتقال ESXi VMKernel از vSwitch0 به VSM وارد شود. باید توجه داشت VLANهایی که برروی Port Profile برای Data Plane استفاده می‌شود، نباید با VLANهایی که برروی Port Profile برای Control-Plane و Packet-Plane استفاده می‌شوند، یکی باشند. در غیر اینصورت این امر باعث جداسازی VEM از VSM می‌شود. باید توجه داشت که دو نوع پورت در VEM Port Profile وجود دارد. یکی پورت ETH که در واقع Uplink به پورت فیزیکی است و دیگری



vETH که یک پورت مجازی برای ماشین‌های مجازی و یا ESXi VMKernel است.

Feature	VEM	DVS
Hosts/DVS	-	250 (includes gateways)
Total vEth ports	1000	10240
Ports per port profile	1024	2048
Port profiles	6144	6144
Physical NICs	32	2000
Physical trunks	32	2000
vEthernet trunks	32	1024
Port channels	8	1024
Active VLANs	4096	4096
MAC addresses	32000	-
MAC address per VLAN	4096	4096
ACLs	128	128

PVLANs	512	512

۱۶-٤- Nexus 1000v Command

پس از نصب نوبت به تنظیمات ابتدایی می‌رسد. تنظیمات ابتدایی مانند دیگر Switchهای Nexus است که در قسمت‌های قبل توضیح داده شده است. به اینترفیس MGMT0 آدرس IP داده می‌شود و از طریق آن این Switch مدیریت می‌شود. پس از نصب باید ارتباط VSM را با vCenter برقرار نمود که از دستورات زیر استفاده می‌شود.

```
N1000v# configure terminal
N1000v(config)# svs connection VCSA-Test
N1000v(config-svs-conn)# protocol vmware-vim
N1000v(config-svs-conn)# remote ip address <vcenter-ip> port 80
N1000v(config-svs-conn)# vmware dvs <datacenter-name> VCSA-Test-2
N1000v(config-svs-conn)# register-plugin remote username <user> password
<pass>
N1000v(config-svs-conn)# connect
N1000v(config-svs-conn)# exit
```

بعد از آن نوبت به ساخت Port Profile یا Port Group است.

```
N1000v(config)# port-profile type vethernet vlan-20
N1000v(config-port-prof)# vmware port-group
N1000v(config-port-prof)# switchport mode access
N1000v(config-port-prof)# switchport access vlan 20
N1000v(config-port-prof)# no shutdown
N1000v(config-port-prof)# state enabled
N1000v(config-port-prof)# exit
```

بعد از آن نوبت به ساخت Uplink است.

```
N1000v(config)# port-profile type ethernet Uplink
N1000v(config-port-prof)# vmware port-group Uplink
N1000v(config-port-prof)# switchport mode trunk
N1000v(config-port-prof)# switchport trunk allowed vlan 10-20
N1000v(config-port-prof)# no shutdown
N1000v(config-port-prof)# system vlan 1,115
N1000v(config-port-prof)# state enabled
N1000v(config-port-prof)# exit
```

پس از آن نوبت به نصب ماژول VEM است.

```
[root@localhost:/vmfs/volumes/mpx.vmhba64:C0:T0:L0] esxcli software vib
install -v /vmfs/volumes/mpx.vmhba64\:C0\:T0\:L0/VEM.VIB
Installation Result
  Message: Operation finished successfully.
```

Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v470-esx_5.2.1.3.3.15.0-6.5.1
VIBs Removed:
VIBs Skipped:

بعد از آن باید Hostها را از طذیق vCenter به Switch N1000v اضافه نمود.

۱۷- Fiber Channel Storage

Fiber Channel دارای استادارد T11 مربوط به سازمان International Committee for Information Technology Standards (INCITS) است. همچنین Fiber Channel Over Ethernet (FCoE) دارای استاندارد Fiber Channel Backbone 5 (FC-BB-5) زیر مجموعه T11 است. همانطور که گفته شد توپولوژی FC به سه دسته تقسیم می‌شود. FC-Point-to-Point که سرور و سیستم ذخیره‌ساز بصورت مستقیم با یکدیگر متصل می‌شوند. FC-Arbitrated-Loop که بصورت توپولوژی حلقه است و مانند Token Ring عمل می کند که برای استفاده از لینک مشاجره صورت می گیرد. FC-Switch شبیه به شبکه Ethernet است که در آن LAN Switch وجود دارد و مشاجره رخ نمی‌دهد. در FC-SW ارتباطات توسط Switch مدیریت می‌شود و از 2^{24} آدرس پشتیبانی می‌شود.

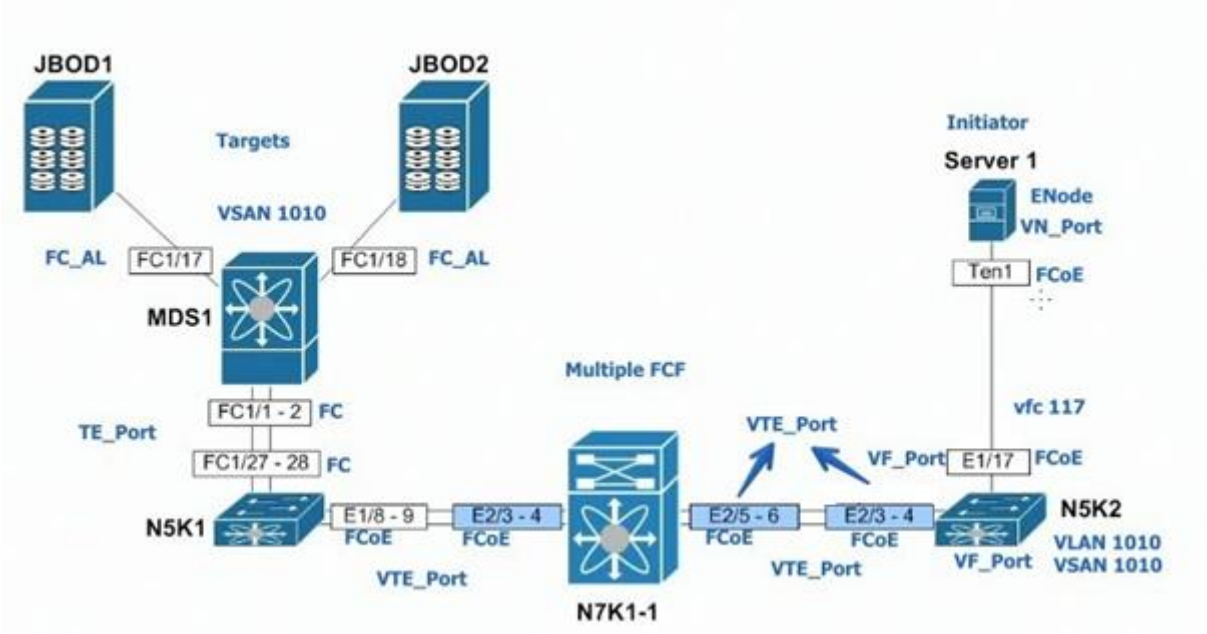
۱۷-۱- Type Of Fiber Channel Port

در FC پورت‌های متفاوت با عملکردهای متفاوتی وجود دارد که تعدادی از آنها در ادامه توضیح داده می‌شود.

۱. Node Port (N_Port): این پورت مربوط به End Host در FC-P2P یا FC-SW است که Initiator یا Target می تواند باشد.
۲. Fabric Port (F_Port): به پورتی از Switch گفته می‌شود که به یک N_Port متصل می‌شود.
۳. Node Loop Port (NL_Port): در توپولوژی FC-AL به پورت مربوط به Host، Storage Array، JBOD و ... یا در کل به End Host گفته می‌شود.
۴. Fabric Loop Port (FL_Port): به پورتی از Switch گفته می‌شود که به یک NL_Port متصل شده است.
۵. Expansion Port (E_Port): به پورتی از Switch گفته می‌شود که با Switch دیگر در ارتباط است. به عبارت دیگر پورت لینک ارتباطی بین دو Switch یا Inter Switch Link (ISL) است.
۶. Trunking Expansion Port (TE_Port): همانند پورت E_Port است با این تفاوت که از 802.1q Trunk بین دو Switch استفاده می‌شود. به عبارت دیگر Expansion ISL است و vSANها را از خود عبور می‌دهد.
۷. Virtual Node Port (VN_Port): در واقع زمانی که یک پورت N_Port برروی یک سرور اجازه عبور Ethernet و FCoE داشته باشد به آن VN_Port گفته می‌شود.

۸. Virtual Expansion Port (VE_Port): به پورتی از FCoE Switch گفته می‌شود که ارتباط مبتنی بر FCoE را با یک FCoE Switch دیگر برقرار می‌کند.

۹. Virtual Fabric Port (VF_Port): به پورتی از FCoE Switch گفته می‌شود که با یک دستگاه دیگر با VN_Port متصل می‌شود. یک VF_Port فقط به یک VN_Port متصل می‌شود.



FC Addressing -۲-۱۷

آدرس‌دهی در FC مشابه آدرس مشابه IP است. در آدرس‌دهی شبکه‌های Ethernet، آدرس IP یک آدرس منطقی و اختصاص داده شده دستی و یا خودکار است. همچنین آدرس MAC یک آدرس فیزیکی برروی سخت‌افزار کارت شبکه است. در FC نیز World Wide Name (WWN) یک آدرس فیزیکی به اندازه 8 Byte است و Fiber Channel Identifier (FCID) یک آدرس منطقی به اندازه 3 Byte است که توسط Fabric Switch اختصاص داده می‌شود. WWN به دو دسته تقسیم می‌شود. World Wide Node Name (WWNN or nWWN) یک آدرس فیزیکی در داخل میزبان است که میزبان می‌تواند Swirtch، Server و Disk باشد. World Wide Port Name (WWPN or pWWN) آدرس مربوط به یک پورت میزبان است. بطور مثال یک Switch دارای یک WWNN و چندین WWPN است. از WWNN در قسمت Data Plane Switching استفاده نمی‌شود، بلکه برای Security، Zoning و ... استفاده می‌شود. آدرس FCID شامل سه قسمت Domain ID، Area ID و Port ID است. بطور مثال 0x010423.

Domain ID	Area ID	Port ID
8 Bit	8 Bit	8 Bit
239 Addresses	256 Addresses	256 Addresses

۱. Domain ID: این قسمت توسط Switch تعریف می‌شودو شبیه Switch ID در FabricPath است. Domain ID به عنوان شناسه Switch در FC استفاده می‌شود. این آدرس هم بصورت دستی و هم

خودکار قابل اختصاص است. در حالت خودکار مشابه انتخاب Root Bridge STP است که دد FC به آن Principle Switch (PS) گفته می‌شود.

۲. Area ID: از این قسمت معمولاً استفاده نمی‌شود ولی گاهی اوقات باید Area ID بین Initiator و Target متفاوت باشد. از Area ID برای مشخص کردن گروهی از پورت‌های یک Switch استفاده می‌شود. همچنین هر شبکه Arbitrated Loop باید یک Area ID یکتا داشته باشد.

۳. Port ID: به هر پورت از Switch یک Port ID اختصاص داده می‌شود که برای شناسایی پورت است.

از FCID برای ترافیک Data Plane Switching استفاده می‌شود.

FC Routing -۳-۱۷

مسیریابی در FC بصورت Flooding یا ارسال سیل اطلاعات نیست. با استفاده از Fabric Shortes Path First (FSPF) ترافیک بین Switchها مسیریابی می‌شود. FSPF بسیار مشابه OSPF است و از الگوریتم Dijkstra برای ساخت Shortest Path Tree (SPT) استفاده می‌کند. Node ID در درخت SPT همان Domain ID مربوط به Switch است. ترافیک بین Domainها با کمترین هزینه مسیریابی می‌شوند. پروتکل FSPF از Equal-Cost Multi-Path (ECMP) یا استفاده از چند مسیر با هزینه یکسان پشتیبانی می‌کند. FSPF بصورت خودکار به عنوان Fabric Service اجرا می‌شود و نیازی به تنظیمات ندارد.

Fiber Channel Name Service (FCNS) مانند جدول ARP است که WWN را به FCID و برعکس ترجمه می‌کند. FCNS نیز نیازی به تنظیمات برروی Switch ندارد.

FC Login Process -٤-۱۷

دستگاه‌های که در شبکه FC با یکدیگر ارتباط برقرار می‌کنند با شبکه Ethernet متفاوت است. شبکه‌های Ethernet بصورت Connectionless هستند. این بدین معنی است که ترافیک Data Plane نتیجه‌ای از یادگیری توپولوژی در Control Plane است. شبکه‌های FC بصورت Connection Oriented است و در آن مفهومی به نام Fiber Channel Login وجود دارد. این بدین معنی است که همه دستگاه‌ها ابتدا باید توسط Control Plane ثبت شوند و سپس شروع به ارسال ترافیک نمایند. به عبارت دیگر دستگاه‌ها ابتدا باید FCID به خود اختصاص دهند و سپس شروع به خواندن و نوشتن برروی دیسک نمایند. Fabric Registration شامل سه مرحله می‌شود.

۱. Fabric Login (FLOGI): ابتدا یک Node Port (N_Port) به Fabric Port (F_Port) یک Switch درخواست Registration می‌دهد. در این هنگام Switch آدرس‌های WWNN و WWPN مربوط به Node را یاد می‌گیرد و در FCNS DB خود ذخیره می‌کند. سپس Switch به Node مربوطه یک آدرس FCID اختصاص می‌دهد.

۲. Port Login (PLOGI): در این مرحله ارتباط End-to-End بین Nodeها برقرار می‌شود. در واقع Initiator به Target درخواست صحبت ارسال می‌کند. در این مرحله از برنامه‌های کاربردی برای کنترل جریان استفاده می‌شود.
۳. Process Login (PRLI): در مرحله آخر دستورات مربوط به SCSI برروی FC بین دو دستگاه ارسال می‌شود.

۱۷-۵- Virtual SAN (vSAN)

همانند VLAN برای جداسازی شبکه‌های Ethernet بصورت منطقی از یکدیگر، در شبکه‌های SAN نیز مفهومی به نام vSAN وجود دارد تا بتوان شبکه‌های SAN را بصورت منطقی از یکدیگر جدا نمود. در صورت عدم استفاده از vSAN و جدا کردن SAN بصورت فیزیکی نیاز به هزینه‌های زیادی مانند سیستم برق و خنک کننده جدا، مدیریت مجزا و ... است. با استفاده از vSAN مشکل جدا کردن Broadcast Domain نیز حل می‌شود. همچنین vSAN یک دامنه مدیریتی جدا ارائه می‌کند. در vSAN می‌توان FLOGI، FCNS، Zoning، Alias و ... جدا داشت. در vSAN برای ارتباط بین دو Switch باید E_Port به TE_Port تبدیل شود تا بتوان ترافیک 802.1q Trunk را از آن عبور داد.

۱۷-۶- Zoning

بصورت پیش‌فرض تمام Initiatorها از تمام Targetها در طول Login اطلاعات بدست می‌آورند. FCNS اطلاعات همه WWPNها به FCIDها را ذخیره می‌کند. این امر باعث می‌شود که در صورت mount کردن یک volume در یک سرور اشتباهی باعث خرابی اطلاعات شود. بطور مثال Windows NTFS & MBR با Linux GPT مطابقت ندارد. Zoning مانند ACL در شبکه‌های Ethernet باعث محدود کردن ارتباط بین Initiator و Target می‌شود. برای تعریف Zoning می‌توان از WWN، FCID، Alias و ... استفاده نمود. Alias برای نام‌گذاری راحت‌تر یک WWN استفاده می‌شود. Zoning نیز مانند Fabric Service بصورت توزیع شده است. در سیسکو بصورت پیش‌فرض Nodeها با یکدیگر در ارتباط نیستند.

۱۸- Fiber Channel Over Ethernet (FCoE)

در مراکز داده سنتی شبکه‌های LAN و SAN از یکدیگر کاملاً جدا هستند. هر سرور از یک کارت NIC برای ارتباط با LAN و از یک کارت HBA برای ارتباط با SAN استفاده می‌کند. در مراکز داده یکپارچه (Unified Fabric) سرورها فقط از یک کارت Converged Network Adapter (CNA) که ترکیبی از HBA و NIC است، استفاده می‌کنند. در حال حاضر در محصولات CNA Intel حداکثر از سرعت 40 Gb/s پشتیبانی می‌شود. در واقع ترافیک LAN و SAN بصورت یکپارچه برروی یک کابل عبور داده می‌شود و یک I/O ادغم شده را فراهم می‌کند.

FCoE یک پروتکل برای انتقال FC Frameها برروی لینک Ethernet است. یک قالب مربوط به FC Frame باید به یک Jumbo Ethernet Frame بسته‌بندی (Encapsulate) شود. Jumbo Frame در واقع بسته‌هایی هستند که اندازه Maximum Transmission Unit (MTU) آنها بیشتر از حالت استاندارد یعنی 1500 Byte باشد. Jumbo Frame حداکثر 9000 Byte را در یک Frame انتقال می‌دهد. FCoE نیاز به یک شبکه انتقال Lossless و یک VLAN جدا از VLANهای ترافیک عادی دارد.

۱۸-۱- FCoE Terminology

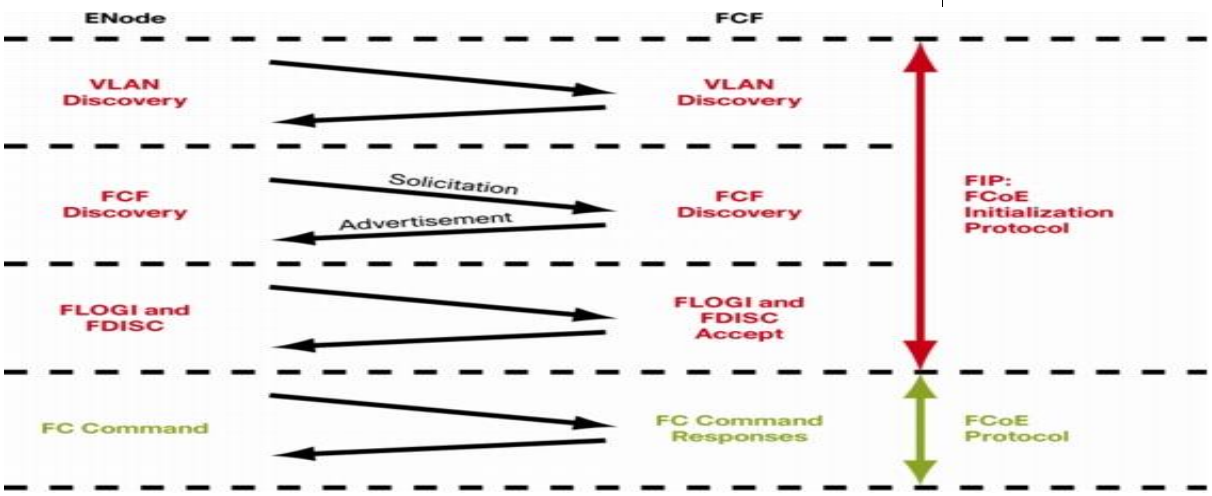
اصطلاحات فنی که در FCoE استفاده می‌شود بصورت مختصر توضیح داده می‌شود.

۱. FCoE Initialization Protocol (FIP): یک پروتکل کنترلی برروی FCoE است که وظیفه ایجاد و نگهداری لینک مجازی بین دو دستگاه FCoE را بر عهده دارد.
۲. FCoE Forwarder (FCF): یک Switch یا یک انتقال دهنده بسته‌های FCoE است. به عبارت دیگر یک Switch است که ترکیبی از Switchهای FC و Ethernet است.
۳. ENode: یک کارت CNA است که برروی آن FCoE اجرا شده باشد.
۴. Virtual Fiber Channel (VFC): در سیستم‌های سیسکو به اینترفیسی گفته می‌شود که برروی یک پورت فیزیکی Ethernet اجازه عبور FCoE داشته باشد. به عبارت دیگر هم پروتکل FC و هم Ethernet بین Switch و Server اجرا شده باشد. VFC در جایی که Hypervisor استفاده شود نیز کاربرد دارد و قابلیتی است که یک ماشین‌مجازی به یک سیستم ذخیره‌سازی مبتنی بر FC بصورت مستقیم متصل شود و این ماشین‌مجازی از یک WWN استاندارد استفاده کند.
۵. Virtual Port Type: همه پروت‌های توضیح داده شده در قسمت FC بصورت VN_Port، VF_Port و VE_Port هستند.

۱۸-۲- How FCoE Works

پروتکل FCoE لایه‌های یک و دو مربوط به پروتکل FC را تغییر می‌دهد و لایه‌های بالایی را بدون هیچ تغییری به همان شکل قبلی خود هستند. در واقع از مفاهیم Domain ID، FSPT، FCNS، Zoning و ... استفاده می‌شود و به کار خود ادامه می‌دهند. پروتکل FIP برای ارتباط بین Node و Fabric استفاده می‌شود. Fabric در اینجا یک FCF و Node یک Enode است. FIP در واقع مربوط به بخش Control Plane پروتکل FCoE است و خود پروتکل FCoE مربوط به بخش Data Plane است. FIP و FCoE دارای دو EtherType متفاوت هستند. EtherType همان فیلدی است که مشخص می‌کند بسته Ethernet توسط چه پروتکلی بسته‌بندی (Encapsulate) شده است. FIP از EtherType 0x8914 استفاده می‌کند. وظیفه FIP برقراری ارتباط FLOGI بین FCF و ENode است. FCoE از EtherType 0x8906 استفاده می‌کند. بعد از برقراری ارتباط،

FCoE بسته‌های خود را که حداکثر 2240 Byte است ارسال می‌کند. باید توجه داشت که حتماً Jumbo Frame اجرا شده باشد.



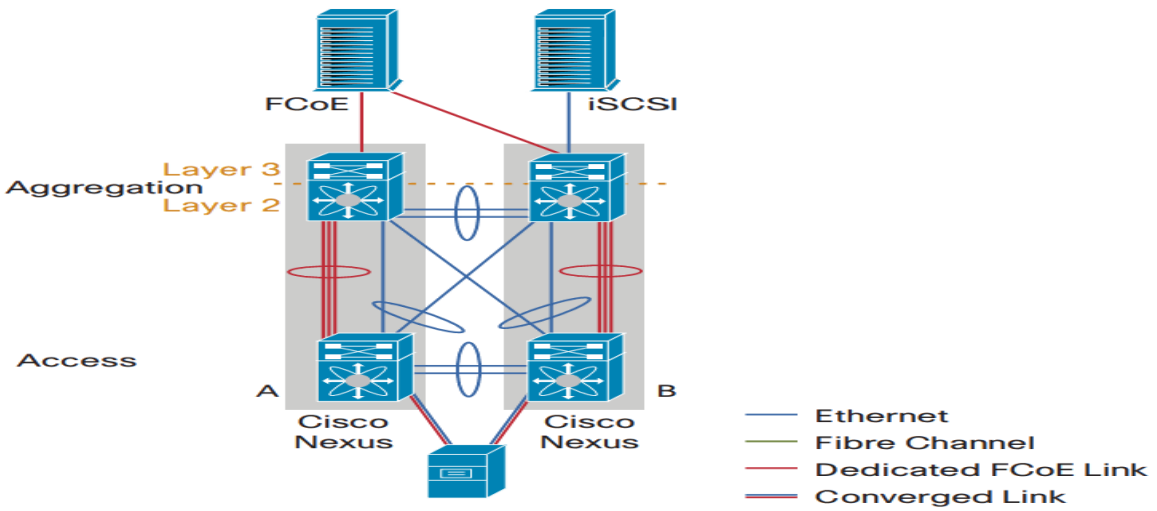
Fabric Provided MAC Address (FPMA) ۱۸-۳-

در طول انجام برقراری ارتباط FLOGI توسط FIP به ENodeها آدرس FCID 3 Byte اختصاص داده می‌شود. FCF نیز در تنظیمات مربوط به خود آدرسی به نام FCoE MAC Adress Prefix (FC-MAP) دارد که این آدرس نیز 3 Byte است. آدرس FC-MAP بین 0xefc00 و 0xefcff است که پیش‌فرض آن 0xefc00 است. حال ENode برای برقراری ارتباط نیاز به یک آدرس MAC دارد مه توسط FPMA محاسبه و اختصاص داده می‌شود. 3 Byte ابتدایی این آدرس MAC از FC-MAP و 3 Byte انتهایی از FCID بدست می‌آید.

FC-MAP (3 Byte) + FCID (3 Byte) = FPMA (6 Byte)

Multihop FCoE ۱۸-۴-

VE_Port برروی یک FCF تعریف می‌شود تا بتواند با یک FCF دیگر ارتباط برقرار نماید. در واقع یک لینک ISL بین دو FCF وجود دارد و پورت‌های E_Port و TE_Port در پروتکل FC را تقلید می‌کنند. در FCoE



نیز می‌توان با استفاده از VE_Port چندین FCF را به یکدیگر متصل نمود. همچنین VE_Port Trunking بین FCoE VLAN پشتیبانی می‌شود.

۱۸-۵- Data Center Bridging (DCB)

DCB مجموعه‌ای از استانداردها است که یک ارتباط Ethernet و یا Fabric یکپارچه برای شبکه‌های LAN و SAN در مراکز داده را تعریف می‌کند. مؤسسه Institute of Electrical and Electronics Engineers (IEEE) این استانداردها را در خانواده 802.1 تعریف می‌کند. سه نمونه از استانداردهای Unifide Fabric در ادامه به اختصار توضیح داده می‌شود.

۱۸-۵-۱- Priority-based Flow Control (PFC) (802.1Qbb)

استاندارد 802.1Qbb اجازه انتقال Lossless برای کلاس‌های مختلف سرویس یا Class Of Service (CoS) را فراهم می‌کند. PFC یا کنترل جریان بر مبنای اولویت، یک قالب توقف Ethernet برای کلاس خاصی از ترافیک ارائه می‌دهد. PFC با استفاده از استاندارد IEEE 802.1p هشت کلاس مختلف سرویس را فراهم می‌کند. به عبارت دیگر هر کلاس بنا بر اولویتی که دارد برروی آن کنترل جریان صورت می‌گیرد. FC و FCoE کلاس مربوط به خود را دارند. این مکانیزم به این ترتیب است که در صورت پر شدن Buffer و جلوگیری از حذف بسته‌ها، دریافت کننده پیام Pause برای ارسال کننده ارسال می‌کند تا ارسال بسته‌ها را متوقف نماید.

Traffic types	Acronym	Priority	PCP value
Background	BK	0 (lowest)	1
Best effort	BE	1 (default)	0
Excellent effort	EE	2	2
Critical applications	CA	3	3
Video, < 100 ms latency and jitter	VI	4	4
Voice, < 10 ms latency and jitter	VO	5	5
Internetwork control	IC	6	6
Network control	NC	7 (highest)	7

۱۸-۵-۲- Enhanced Transmission Selection (ETS) (802.1Qaz)

استاندارد 802.1Qaz مدیریت پهنای‌باند ترافیک را برای کلاس‌های مختلف فراهم می‌کند. ETS این اجازه را می‌دهد تا پهنای‌باند مختلفی برای هر کلاس تأمین شود. بطور مثال شبکه SAN از 8GB/s و شبکه LAN از 2Gb/s استفاده نماید.

۱۸-۵-۳- Data Center Bridging eXchange (DCBX) (802.1Qab)

در این استاندارد نحوه جابه‌جایی پروتکل‌ها بین دستگاه‌های مختلف و DCB تعریف می‌شود. DCBX برای فهمیدن قابلیت‌های دستگاه‌های مختلف از پروتکل Link Layer Discovery Protocol (LLDP) استفاده می‌کند. با استفاده از پیام‌های LLDP می‌توان از قابلیت‌های PFC، ETS، FCoE، Link Down و ... دیگر

دستگاه‌ها مطلع شد. دستگاه‌های سیسکو از Cisco Discovery Protocol برای ارتباط با یکدیگر استفاده می‌کنند. در صورت اینکه دستگاهی غیر از سیسکو در شبکه باشد باید LLDP را فعال نمود.

۱۹- Unified Computing System (UCS)

UCSها سیستم‌های کامپیوتری سرور در مراکز داده هستند که خط تولید آنها شامل سخت‌افزارهای محاسباتی که از مجازی‌سازی پشتیبانی می‌کنند (Computing Hardware)، Fabric Switch و نرم‌افزار مدیریتی هستند. ساختار فیزیکی UCS شامل موارد زیر است.

۱۹-۱- Fabric Interconnect (FI)

هوش اصلی UCSهای سرورهای Blade یا تیغه است. این بخش اجازه می‌دهد که هر ارتباطی با UCS، Chassis و Rack Server برقرار شود، چه این ارتباط از نوع LAN و چه از نوع SAN باشد. برروی FI یک نرم‌افزار مدیریتی اجرا می‌شود. FI از Nexus 5000 Switch نشأت گرفته است و برروی آن NX-OS اجرا می‌شود. این Switchها مدل‌های مختلفی دارند که شامل سری 6100، 6200، 6300 و 6400 می‌شوند. در حال حاضر فقط سری‌های 6300 و 6400 فروش و پشتیبانی می‌شوند. در مدل‌های 6100 حداکثر سرعت 1/10Gb/s و فقط از Ethernet و در سری‌های 6200 حداکثر از سرعت 1/10Gb/s Ethernet و 1/2/4/8Gb/s FC پشتیبانی می‌شد. در سری 6300 از 10/40Gb/s Ethernet و 4/8/16Gb/s FC در سری 6400 از 40/100Gb/s Ethernet و 8/16/32Gb/s FCپشتیبانی می‌شود. از مدل‌های پایین به بالا تأخیر کمتر و در صفر است. این Switchها معمولاً در بالای رک نصب (Top Of Rack) می‌شوند و معمولاً برای Redundancy از دو Switch استفاده می‌شود.

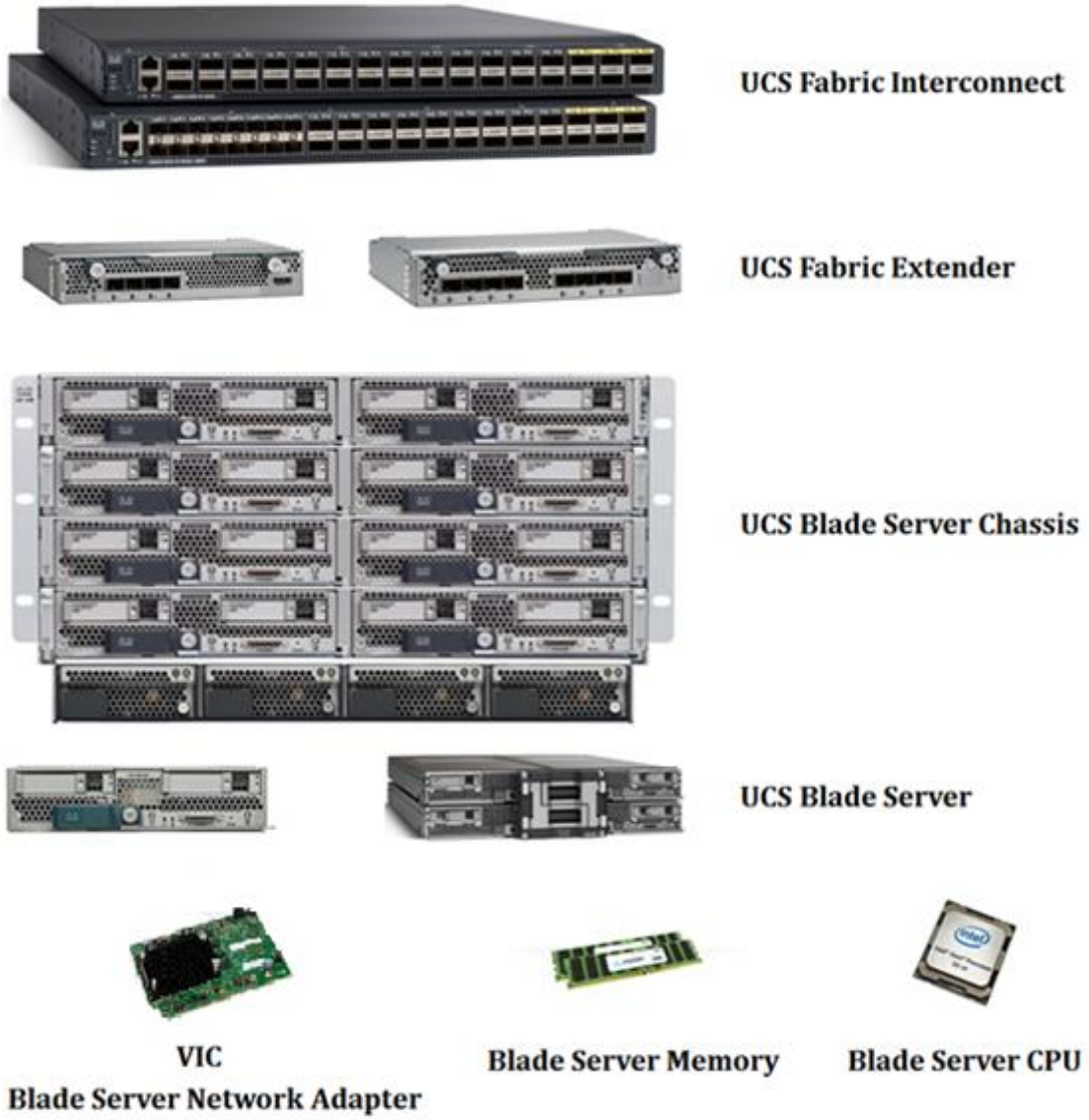
۱۹-۲- Chassis

این بخش به خودی خود هیچ هوش و نرم‌افزاری ندارد و فقط شامل بدنه ارتباطات است. یک شاسی خام است که در آن می‌توان تیغه و یا Blade قرار داد. هر Blade شامل CPU، RAM، CNA و ... است. Chassis فقط مدل 5100 دارد که درون آن تیغه‌های B-Series و C-Series و ماژول‌های IOM/FEX قرار می‌گیرند. شاسی‌ها معمولاً در پایین FI در رک‌ها نصب می‌شوند.

۱۹-۳- I/O Module (IOM) (FEX)

ماژول‌های IOM به عنوان FEX نیز شناخته می‌شوند. در واقع این ماژول‌ها مانند Line Card FEX در Nexus Switchها هستند. این ماژول‌ها یک اینترفیس ارتباطی برای Blade Serverها به FI فراهم می‌کنند. ماژول‌های FEX شامل دو بخش هستند. بخش اول Chassis Management Switch (CMS) که ترافیک مدیریتی را بین Cisco Integrated Management Controller (CIMC) برروی Blade Server و FI جابه‌جا می‌کند. بخش دوم Chassis Management Controller (CMC) که تمامی سنسورها و قسمت‌های شاسی مانند Fan، Power Supply و ... را مانیتور می‌کند و تشخیص می‌دهد که چه جزئی از شاسی مانند Blade و

یا FEX اضافه و یا خارج شده است. این ماژول‌ها پشت شاسی نصب می‌گردند. اولین سری IOM مدل 2104XP تولید شد که این مدل تأخیری برابر 0.8 microsecond داشت و از 4×10Gb/s پورت Northbound به FI و 8×10Gb/s پورت Southbound به Blade Server پشتیبانی می‌شد. در آخرین سری تا به امروز مدل



2408 است که از 8×25Gb/s پورت به FI و 32×10Gb/s به Blade Server پشتیبانی می‌کند. هر IOM می‌تواند تنها به یک FI متصل شود و بعد از اتصال قسمتی از FI می‌شود. IOMها از طریق MUX یا Multiplexer سرورهای Blade را به لینک‌های خروجی I/O متصل می‌کند.

UCS Products -٤-١٩

در مجموعه UCS، Chassis، B-Series (Blade Servers)، C-Series (Rack Servers)، S-Series (Storage Servers)، E-Series (Blade Servers for ISR routers)، UCS Management Software، Fabric Interconnects and Extenders و Adapters قابل مشاهده است. حرف M در انتهای محصولات نشان دهنده Generation محصول است. اکثر سرورهای B-Series از RAID صفر و یک

پشتیبانی می‌کند. سرورهای C-Series هم قابلیت استفاده به تنهایی(Standalone) و هم قابلیت جانمایی در Chassis (Blade) دارند و از RAIDهای بیشتری پشتیبانی می‌کنند. در صورت استفاده از SAN Storage نیازی به پشتیبانی بیشتر RAID برروی سرورها نیست.

در زیر مقایسه‌ای به اختصار صورت گرفته است.

UCS B-Series	B480 M5	B200 M5
Processors	4	2
Processor supported	2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processors	2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processors
Maximum memory	18 TB with Intel Optane™ DC Persistent Memory	9 TB with Intel Optane™ DC Persistent Memory
Form factor	Full-width blade	Half-width blade
Built-in RAID	0, 1	0, 1
Mezzanine I/O adapter slots	Up to 5	Up to 3
GPUs	Up to 4	Up to 2
Max I/O throughput per blade	160 Gbps (4 x 40 Gbps)	80 Gbps (2 x 40 Gbps)
Maximum servers per chassis	4	8
Internal storage	Up to four SAS/SATA/SSD/NVMe	Up to two SAS/SATA/SSD/NVMe
Maximum internal storage	39 TB	20.5 TB

UCS C-Series	C480 ML M5	C480 M5	C240 M5	C220 M5	C125 M5
Processors	2	2 or 4	2	2	
Processor supported	Intel® Xeon® Scalable processors	2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processor	2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processors	2nd Gen Intel® Xeon® Scalable and Intel Xeon Scalable processors	AMD® EPYC™ 7000 series processors
Maximum Memory	3 TB, 24 x DDR4 DIMMs	18 TB with Intel Optane™ DC Persistent Memory	9 TB with Intel Optane™ DC Persistent Memory	9 TB with Intel Optane™ DC Persistent Memory	2 TB, 16 x DDR4 DIMMs
Form factor	4 RU	4 RU	2 RU	1 RU	.5 RU
Optional RAID	0, 1, 5, 6, 10, 50, 60	0, 1, 5, 6, 10, 50, 60	0, 1, 5, 6, 10, 50, 60	0, 1, 5, 6, 10, 50, 60	0, 1, 5, 6, 10, 50, 60
Integrated networking (I/O) - LOM	2 x 10 Gb ports Dedicated OOB management port	2 x 10 Gb ports Dedicated OOB management port	2 x 10 Gb ports plus 1 x Modular LOM (mLOM) Dedicated OOB	2 x 10 Gb ports plus 1 x Modular LOM (mLOM) Dedicated	Dedicated OOB management port

			management port	OOB management port	
Maximum Internal Storage	182.4 TB	246.4 TB	SFF - 197.6 TB SSD + 2x M.2 960 GB + 46.2 TB PCIe NVMe LFF - 120 TB HDD + 2x M.2 960 GB + 46.2 TB PCIe NVMe	SFF - 76 TB SSD + 2x M.2 960 GB + 15.5 PCIe NVMe LFF - 80 TB HDD + 2x M.2 960 GB + 15.5 PCIe NVMe	47.5 TB SSD + 2x M.2 960 GB per node

Item	Cisco UCS 6324 Fabric Interconnect
Description	Fabric interconnect with 4 unified ports and 1 scalability port
Form factor	I/O module for Cisco UCS 5108 chassis
Number of 1 and 10 Gigabit Ethernet, FCoE, or Fibre Channel Enhanced Small Form-Factor Pluggable (SFP+) external ports	4
Number of 40 Gigabit Ethernet or FCoE Enhanced Quad SFP (QSFP) ports	1
Server ports	16 x 10GBASE-KR lanes
Number of rack servers supported	Single Cisco UCS 5108 Blade Server Chassis: 7 With second Cisco UCS 5108 Blade Server Chassis: 4
Throughput	500 Gbps
Latency	Less than a microsecond
Quality-of-service (QoS) hardware queues	16 (8 each for unicast and multicast)

Item	Cisco UCS 6454 Fabric Interconnect
Description	54 port fabric interconnect
Form factor	1 RU
Number of fixed 10/25/40/100-Gbps and FCoE ports with optional unified ports	54 fixed ports
Maximum number of unified ports	4 ports (45-48)
Maximum number of 1-Gbps Ethernet ports	6 ports (49-54)
Maximum number of 40/100-Gbps Ethernet ports	Single Cisco UCS 5108 Blade Server Chassis: 7 With second Cisco UCS 5108 Blade Server Chassis: 4
Throughput	3.82 Tbps
Fan modules	3+1

۱۹-۵- Redundant Array of Independent Disks (RAID)

RAID یک تکنولوژی مجازی‌سازی ذخیره داده است که چند دیسک فیزیکی را به یک یا چند دیسک منطقی برای رسیدن به هدف Data Redundancy یا افزونگی داده تبدیل می‌کند.

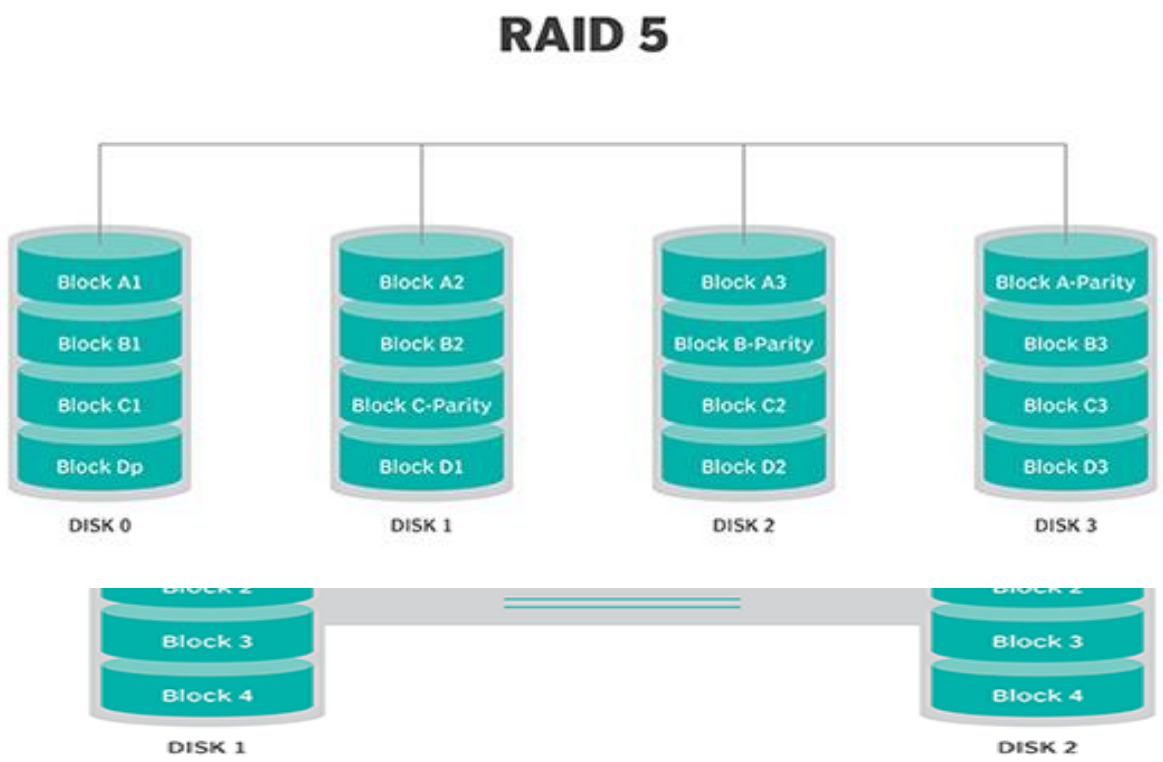
Data Striping تکنیکی برای ذخیره اطلاعات برروی دیسک فیزیکی است. به عبارتی یک فایل را برروی دیسک‌های مختلف ذخیره می‌کند تا در صورت خرابی دیسک فقط قسمتی از اطلاعات از بین برود.

Parity مکانیزم حفاظت از خطا رد داده‌ها است تا تحمل‌پذیری در برابر خطا را افزایش دهد. Parity Bit یا Check Bot یک بیت است که در یک آرایه‌ای از صفر و یک‌ها در صورت زوج بودن تعداد یک‌ها برابر صفر و در صورت فرد بودن یک‌ها برابر یک است.

۱. RAID 0 (Data Striping): در این روش حداقل نیاز به دو دیسک است و داده برروی دیسک‌ها پخش می‌شود. در صورت از بین رفتن دیسک داده از بین می‌رود و تحمل‌پذیری در برابر خطا را ندارد ولی عملکرد خوبی دارد.

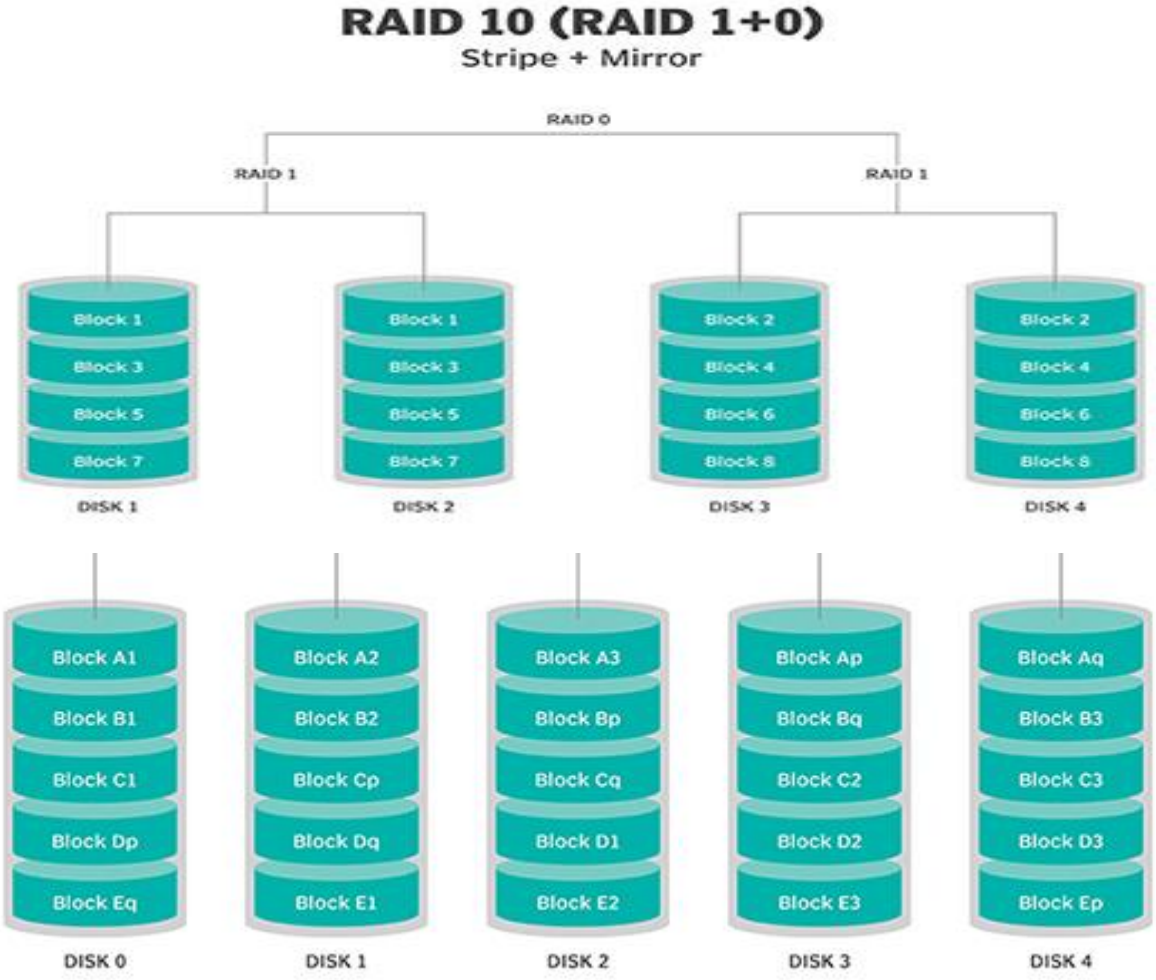
۲. RAID 1 (Disk Mirroring): در این روش نیز حداقل نیاز به دو دیسک است و داده برروی هر گروه از دیسک‌ها کپی می‌شود. تحمل در برابر خطا را دارد، استفاده از آن آسان است ولی بار زیادی برروی دیسک قرار می‌گیرد.

۳. RAID 5 (Striping With Parity): در این روش حداقل نیاز به سه دیسک است و هم داده و هم Parity برروی دیسک پخش می‌شوند. برای خواندن عملکرد بالا ولی برای نوشتن عملکرد متوسطی دارد.



۴. RAID 6 (Striping With Double Parity): در این روش حداقل نیاز به سه دیسک است و هم داده و هم Parity برروی دیسک پخش می‌شوند ولی در این روش از دو Parity برروی دیسک‌های مختلف استفاده می‌شود. برای خواندن عملکرد بالا ولی برای نوشتن عملکرد پایینی دارد.

۵. RAID 1+0 (10) (Mirrored Array of Striped Disks): در این روش حداقل نیاز به چهار دیسک است. بعد از RAID 0 بهترین عملکرد خواندن را دارد. در برابر از بین رفتن چند دیسک تحمل‌پذیری بالایی دارد.



۶. RAID 0+1 (01) (Striped Array of Mirrored Disks): مشابه RAID 10 است ولی فقط نحوه ذخیره‌سازی داده برروی دیسک متفاوت است. تحمل‌پذیری این روش در برابر خطا خوب است و عملکرد I/O بالایی دارد.

۱۹-۶- UCS Overview

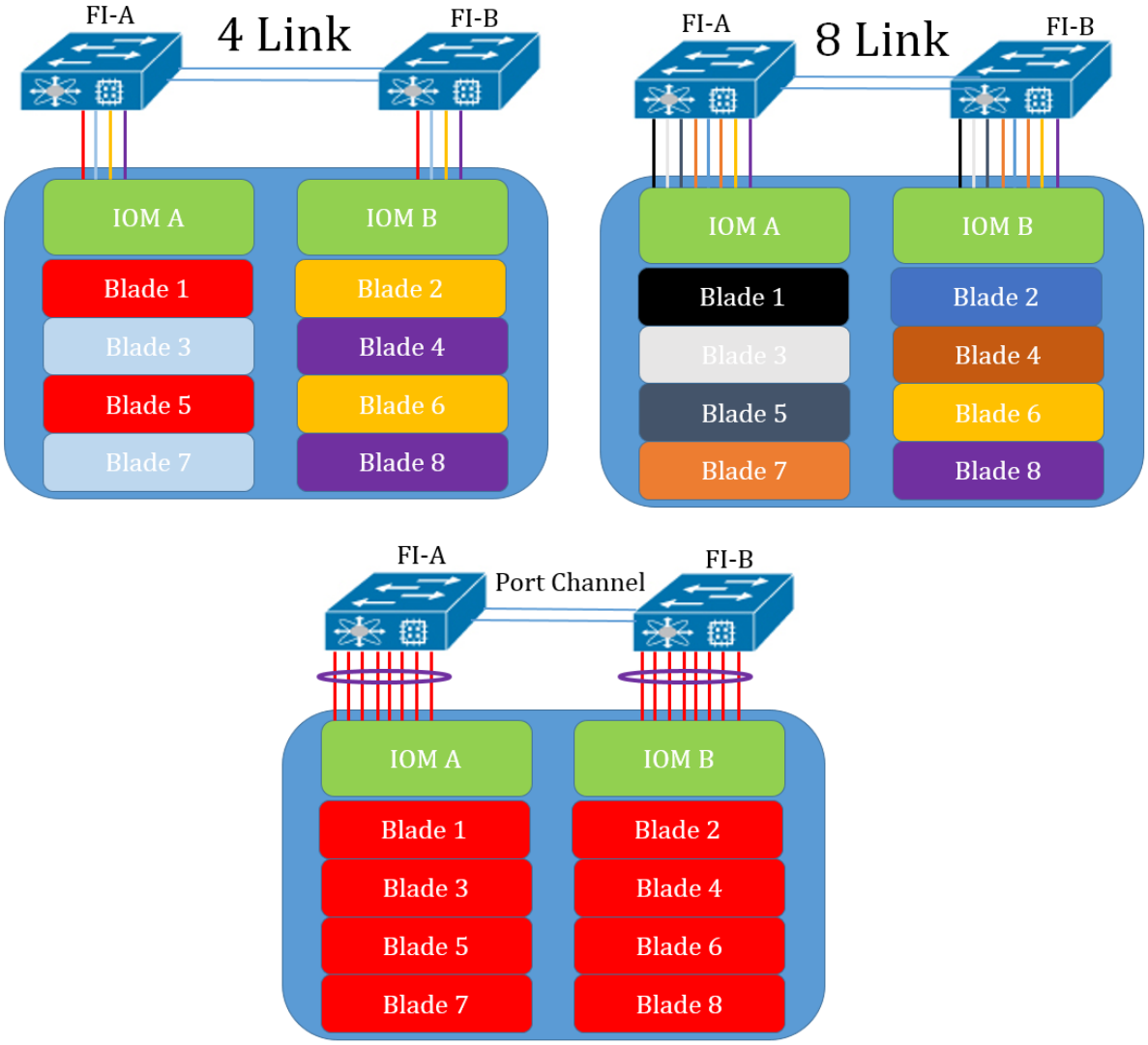
در ساختار سرورهای Blade نرم‌افزار مدیریتی UCS بالاترین جایگاه را دارد تا بتواند Fabric Interconnect، Chassis، Blade و Rack را مدیریت نماید. برای برقراری ارتباط Redundant باید از دو Fabric Interconnect استفاده نمود که یکی از آنها Active و دیگر Standby می‌شود. هر دو FI با همدیگر در

ارتباط هستند و بخش مدیریتی یا Control Plane را با یکدیگر به اشتراک و همگام‌سازی می‌کنند. باید توجه داشت که در قسمت مدیریتی یکی فعال و دیگری در حالت آماده‌باش است ولی در بخش Data Plane هر دو پردازش را انجام می‌دهند و هر دو Active/Active هستند. زمانی که از دو FI استفاده می‌شود به اصطلاح به آنها Cluster گفته می‌شود. بین ای دو Switch برای برقراری HA از دو لینک استفاده می‌شود که به این لینک‌ها Cluster Link گویند. از طریق این دو لینک بخش Control Plane با یکدیگر Sync می‌شوند. برای برقراری این لینک‌ها می‌توان از کابل Cat5 نیز استفاده نمود.

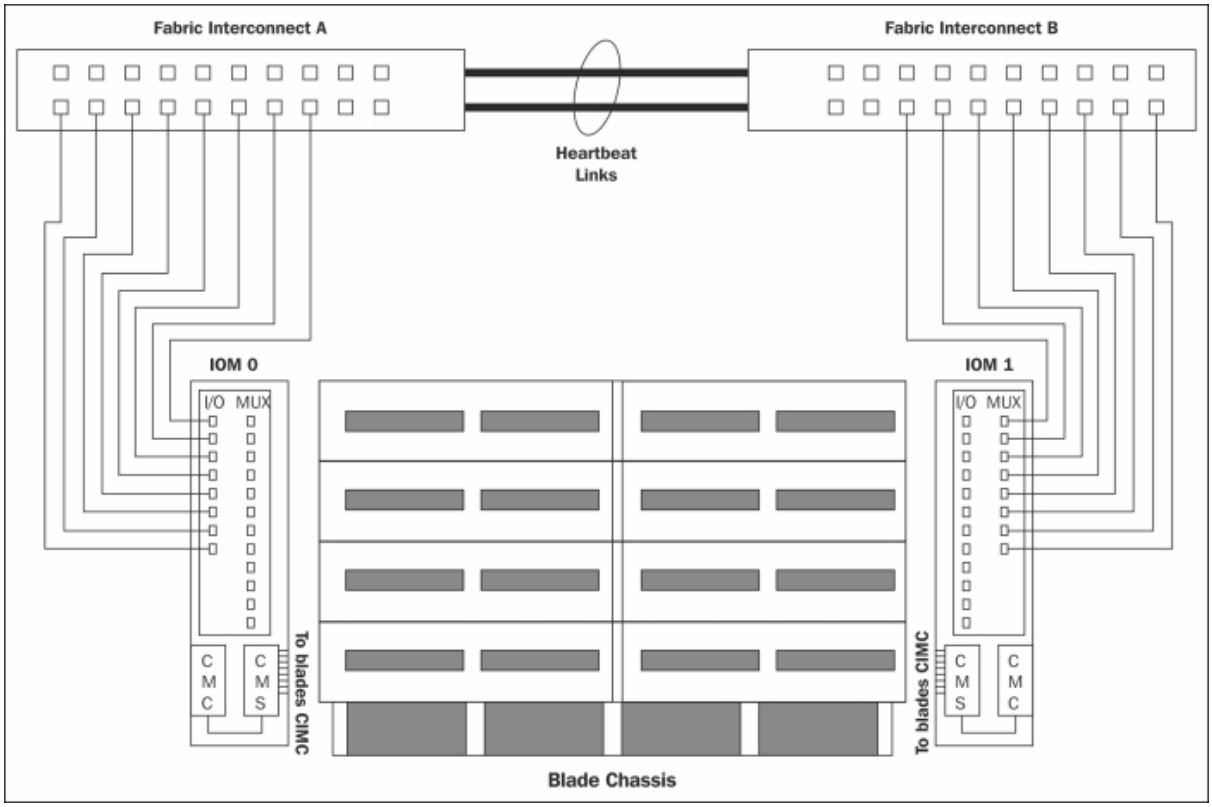
زبان اصلی UCS Manager به فرمت XML است ولی با GUI، CLI و نرم‌افزارهای 3rd Party نیز می‌توان با آن ارتباط برقرار نمود. UCS Manager از یک پایگاه داده برای ذخیره اطلاعات مدیریتی استفاده می‌کند که به فرمت XML است. این نرم‌افزار مدیریتی از پروتکل‌های مختلفی مانند SNMP، IPMI، CIM XML و ... پشتیبانی می‌کند.

زمانی که Blade درون شاسی قرار می‌گیرد، نیاز دارد تا از طریق ماژولی به FI متصل شود. این اتصال از طریق ماژول IOM/FEX صورت می‌گیرد. برای برقراری ارتباط نیاز به هیچ تنظیماتی مانند STP نیست و بصورت خودکار Bladeها به IOMها متصل می‌شوند. می‌توان برای هر Blade مشخص نمود که از کدام Uplink

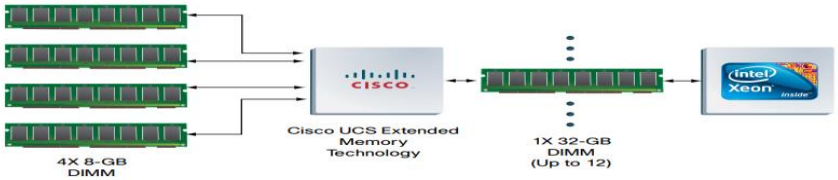
استفاده نماید و یا اینکه از Port Channel استفاده نمود. بهترین راه حل پیشنهادی استفاده از Port Channel است. در تصویر زیر نمونه‌ای از ارتباطات ترسیم شده است.



همانطور که گفته شد IOM/FEX شامل CMC، CMS و MUX است. Cisco Integrated Management Controller (CIMC) به عنوان یک Baseboard Management Controller (BMC) شناخته می‌شود که برروی C-Series و S-Series یک سیستم مدیریت سرور تعبیه شده را در مرکز داده و شعبه‌های دیگر فراهم می‌کند که یکی از قسمت‌های UCS Manager است. CIMC قابلیت‌های KVM، Serial over LAN و پشتیبانی از پروتکل‌هایی مانند IPMI را فراهم می‌کند. در تصویر زیر ساختار UCS بطور منطقی آورده شده است. Blade درون شاسی نصب می‌شود و بعد از آن از طریق قسمت MUX به IOM/FEX متصل می‌شود. ارتباط IOM/FEX از طریق پورت‌های I/O به Fabric Interconnect برقرار می‌شود. FI نیز در بالای Rack قرار دارد که از طریق پورت‌های Uplink به Switchهای بالادستی متصل می‌شود.



سرورهای B-Series دو مدل Full Width و Half Width دارند. در سری‌های Half Width در صورت نصب نیمی از CPUها، مقدار RAM نیز نصف می‌شود. بطور مثال در مدل UCS B200 M1 کل ظرفیت RAM برابر 96G که دوازده تا هشت گیگ است و کل تعداد سوکت CPU برابر 2 است. حال اگر از یک CPU استفاده شود فقط مقدار 48G RAM می‌توان استفاده نمود. در سری Half Width تنها یک Mezzanine Card برای همه I/Oها می‌توان استفاده نمود. Mezzanine Card می‌توان شامل کارت شبکه، کارت گرافیک و ... باشد که برروی سرور تیغه نصب می‌شود. در سری‌های Full Width با استفاده از Cisco Extended Memory Technology مشکل تعداد پشتیبانی کردن RAM در یک CPU برطرف شده است و با استفاده از یک CPU می‌توان از همه ظرفیت RAM استفاده نمود. این تکنولوژی به این صورت است که بین RAMها و CPU یک واسطی قرار می‌گیرد و چهار کانال RAM را به یک کانال RAM تبدیل می‌نماید. در سری Full Width از دو Mezzanine Card پشتیبانی می‌شود. در سرورهای Blade کارت‌های شبکه به PCI Slot یا همان Mezzanine Slot متصل می‌شوند. کارت‌های شبکه می‌توانند Ethernet Adapter (EA)، Converged Network Adapter (CNA) و Virtual Interface Card (VIC) باشند. کارت‌های VIC



از VN_Port پشتیبانی می‌کنند و به Virtual Interfaceهای زیادی تبدیل می‌شوند. مدیریت آن توسط UCS Manager صورت می‌گیرد که Hypervisor آن را به عنوان چندین Physical NIC مشاهده می‌کند.

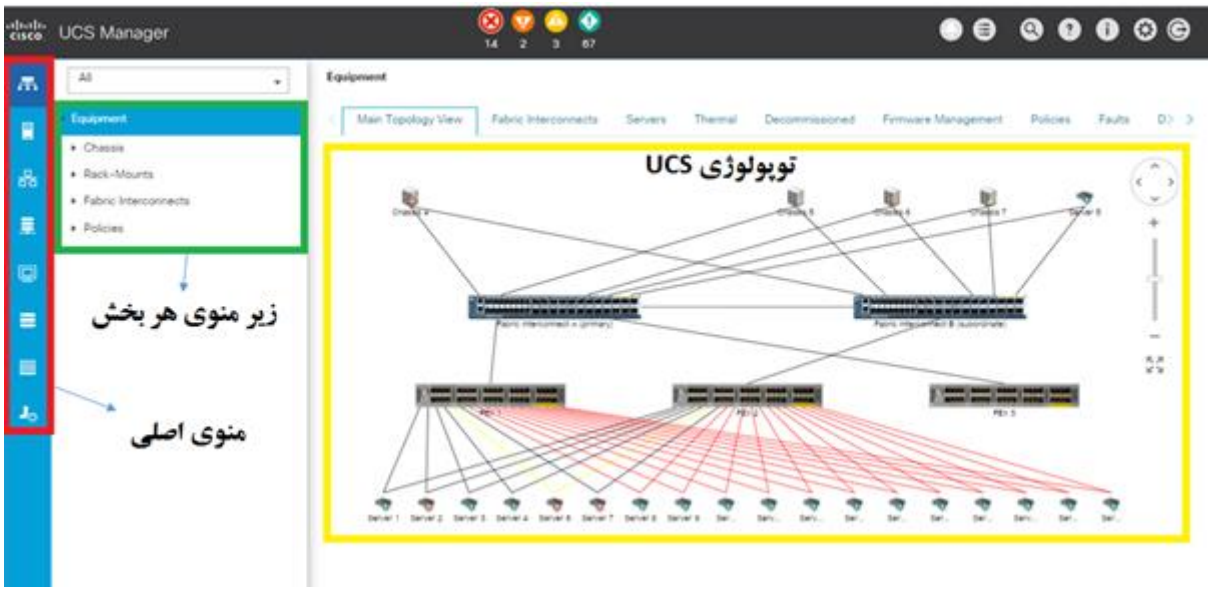
UCS Manager -۷-۱۹

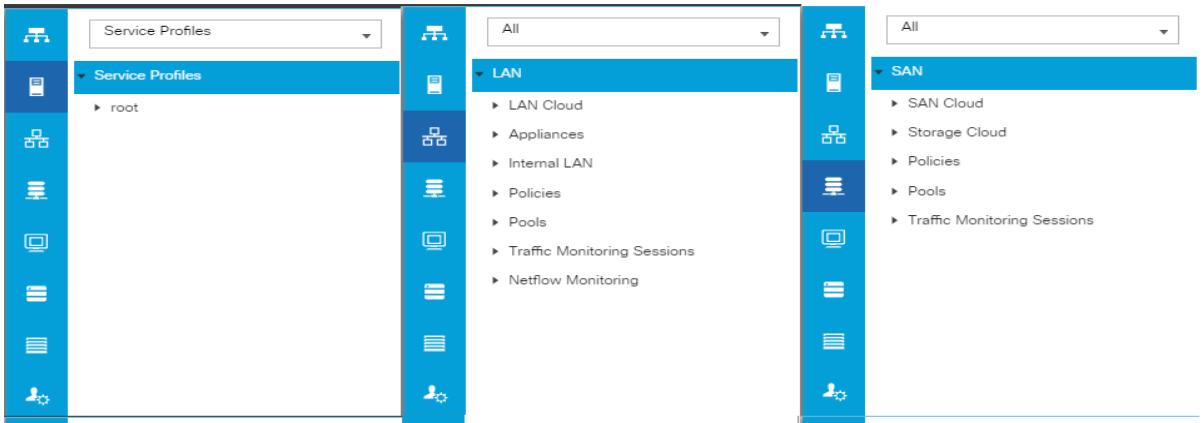
نرم‌افزار مدیریتی UCS قابلیت‌های بسیاری جهت مشاهده و مدیریت سیستم‌ها دارد. در این قسمت توضیح مختصری در مورد Service Profile (SP) ارائه می‌شود. Service Profile یک ساختار نرم‌افزاری شامل چکیده‌ای از ویژگی‌ها و مشخصات یک سرور فیزیکی است. به عبارت دیگر تنظیماتی که برروی یک سرور UCS انجام می‌شود را در قالب یک فایل نرم‌افزاری به نام Service Profile ذخیره کرده تا بتوان برروی سرورهای دیگر اعما نمود. در Stateless Computing از Service Profile برای فراهم کردن جابه‌جایی بین سخت‌افزار بدون تغییر دادن هیچ تنظیماتی استفاده می‌شود. یک Service Profile می‌تواند شامل UUID منحصر به فرد برای سرور، آدرس MAC برای اتصال به شبکه LAN، آدرس WWNN و WWPN برای اتصال به شبکه SAN، تعریف سیاست‌های BIOS، BOOT و ...، تنظیمات vNIC، HBA و دیگر تنظیمات باشد. در واقع Service Profile کمک می‌کند تا همه تنظیمات مربوط به Compute، Network، Storage و دیگر موارد در یک مکان قرار گیرد. همچنین می‌توان با گرفتن Clone یا Template از یک سخت‌افزار، Deploy یا گسترش دادن را سریع‌تر و Maintenance یا تعمیر و نگهداری را آسان‌تر انجام داد.

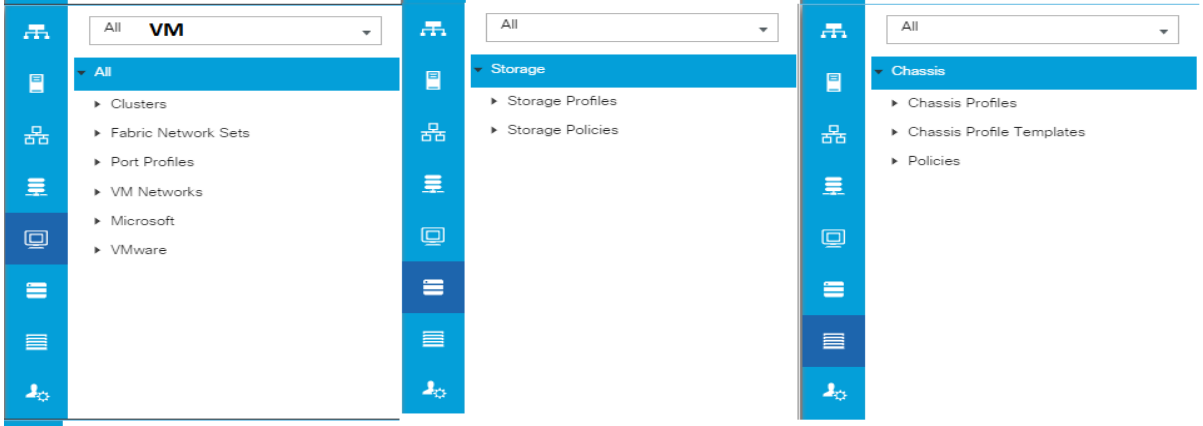
اصطلاح Pool به معنای استخری از هر چیزی است. در سیستم‌های UCS به معنای استخری از منابع یا Resource Pool است. این منابع می‌توان شامل استخری از آدرس‌های IP مدیریتی، UUID، MAC، WWNN، WWPN و ... باشد. تنظیمات مربوط به Pool در نرم‌افزار UCS Manager در قسمت Server، LAN و SAN انجام می‌شود که بستگی به نوع منابع دارد.

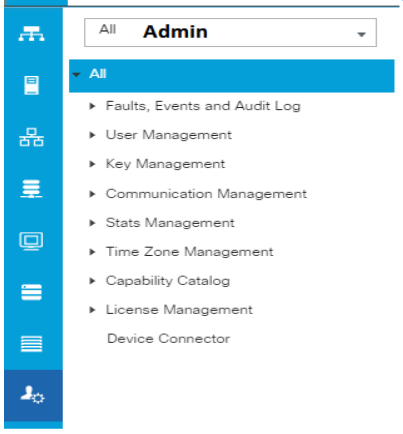
Service Profile Template راهی برای Deploy یا گسترش دادن خودکار Service Profile است. بطور مثال تعریف می‌شود که تعدادی از Service Profile ایجاد شود و از آنها برای نرم‌افزارهای مختلف مانند Web، Database و ... استفاده شود. Template شامل همان مقادیر Pool، UUID، IP و ... است که در Service Profile تعریف شده است. در UCS دو نوع Tempalte وجود دارد. در Initial Template زمانی که یک Template از یک Service Profile گرفته می‌شود، اگر تغییری برروی Template صورت گیرد، این تغییرات برروی سرورهای قبلی که از این Template استفاده شده‌اند اعمال نمی‌گردد ولی برروی سرورهای جدید اعمال می‌شود. در Updating Template تغییرات اعمال شده برروی Template برروی سرورهای قبلی و بعدی که از این Template استفاده می‌کنند، اعمال می‌شود. در واقع لینکی بین Template و سروری که از آن ساخته می‌شود وجود دارد.

در تصویر زیر ساختار نرم‌افزار UCS Manager نمایش داده شده است.


UCS Manager
Equipment
Chassis
Rack-Mounts
Fabric Interconnects
Policies
زیر منوی هر بخش
منوی اصلی
توپولوژی UCS


Service Profiles
root
All
LAN
LAN Cloud
Appliances
Internal LAN
Policies
Pools
Traffic Monitoring Sessions
Netflow Monitoring
All
SAN
SAN Cloud
Storage Cloud
Policies
Pools
Traffic Monitoring Sessions


All VM
All
Clusters
Fabric Network Sets
Port Profiles
VM Networks
Microsoft
VMware
All
Storage
Storage Profiles
Storage Policies
All
Chassis
Chassis Profiles
Chassis Profile Templates
Policies


All Admin
All
Faults, Events and Audit Log
User Management
Key Management
Communication Management
Stats Management
Time Zone Management
Capability Catalog
License Management
Device Connector

All Menu