

سوال 1: SDN چیست؟

جواب: SDN یا Software Defined Networking به معنی «شبکه نرم افزارمحور» یک معماری جدید در طراحی شبکه است که هدف آن جدا کردن بخش کنترل (Control Plane) از بخش داده (Data Plane) در تجهیزات شبکه مثل سویچ ها و روترها است.

SDN به جای اینکه تصمیمات مربوط به مسيردهی و کنترل ترافیک در خودِ سویچ ها و روترها گرفته شود، این تصمیمات را به یک کنترل کننده مرکزی نرم افزاری (SDN Controller) منتقل می کند.

سوال 2: تفاوت مسیریابی سنتی (توزیع شده) و مسیریابی متمرکز در چیست؟

جواب: در روش مسیریابی سنتی (توزیع شده)، هر مسیریاب (روتر) به صورت مستقل عمل می کند و با استفاده از الگوریتم ها و پروتکل های خاصی مانند RIP ، OSPF یا BGP ، جدول مسیریابی خود را به روز می نماید. این روترها اطلاعات مربوط به توپولوژی شبکه را از همسایگان خود دریافت کرده و بر اساس آن تصمیم می گیرند که بسته ها را از کدام مسیر هدایت کنند.

اما در روش مسیریابی متمرکز که در معماری های نظیر SDN (Software Defined Networking) استفاده می شود، تصمیمات مربوط به مسيردهی توسط یک کنترل کننده مرکزی گرفته می شود. این کنترل کننده با داشتن دید کامل از وضعیت شبکه، مسیر مناسب را انتخاب کرده و قوانین مورد نظر را به تجهیزات شبکه (مانند سویچ ها) ارسال می کند.

سوال 3: مزایا و معایب شبکه های نرم افزار محور را شرح دهید؟

جواب: مزایای شبکه های نرم افزار محور (SDN)

۱. مدیریت متمرکز و ساده تر: در SDN ، کنترل متمرکز باعث می شود مدیر شبکه بتواند از یک نقطه مرکزی کل شبکه را پیکربندی و نظارت کند. این ویژگی به خصوص در شبکه های بزرگ، پیچیدگی عملیاتی را کاهش می دهد.
۲. انعطاف پذیری و پویایی بالا: SDN امکان تغییر قوانین مسیریابی و سیاست های شبکه را در زمان واقعی (real-time) فراهم می سازد. به راحتی می توان سیاست های امنیتی، QoS ، یا مسيردهی را بدون دخالت فیزیکی در تجهیزات، تغییر داد.
۳. قابلیت خودکارسازی (Automation): با بهره گیری از اسکریپت ها و API ، بسیاری از وظایف مدیریتی مانند پیکربندی، مانیتورینگ و عیب یابی قابل خودکارسازی هستند.
۴. بهینه سازی مصرف منابع: کنترل کننده با داشتن دید سراسری از توپولوژی شبکه، می تواند تصمیماتی بهینه برای مسيردهی، بالانس بار و تخصیص منابع اتخاذ کند.

معایب شبکه های نرم افزار محور (SDN)

۱. وابستگی به کنترلر مرکزی: اگر کنترلر مرکزی دچار اختلال شود و راهکار پشتیبان (Redundancy) در نظر گرفته نشده باشد، کل شبکه ممکن است مختل شود. این یک نقطه ضعف بحرانی (Single Point of Failure) محسوب می شود.
۲. پیچیدگی در طراحی و پیاده سازی اولیه: راه اندازی اولیه SDN نیازمند دانش فنی عمیق در زمینه شبکه و برنامه نویسی است. هماهنگی بین تجهیزات قدیمی و فناوری های SDN ممکن است نیازمند مهاجرت تدریجی و هزینه بر باشد.
۳. مسائل امنیتی جدید: با متمرکز شدن کنترل شبکه، در صورت نفوذ به کنترلر، مهاجم می تواند به کل شبکه دسترسی پیدا کند. نیاز به سیاست های امنیتی دقیق تری در سطح کنترل کننده و ارتباط آن با تجهیزات وجود دارد.
۴. نیاز به تجهیزات و نرم افزارهای سازگار: تجهیزات شبکه باید از پروتکل هایی مانند OpenFlow یا API های استاندارد برای ارتباط با کنترلر پشتیبانی کنند. در برخی موارد، هزینه به روز رسانی تجهیزات موجود بالا است.