The future of video is in the network

We live in a world where more and more video is shifting to IP and mobile. According to the Cisco Visual Networking Index™ (Cisco VNI™), IP traffic will triple by 2021, reaching 278 exabytes per month. Video will dominate IP traffic, representing 82 percent of all traffic by 2021. (See Figure 1.) And with the nearly 13 billion video-enabled devices, mobile video will increase 9 times as more and more video is consumed on mobile connected devices.
IP is permeating the video network from the capture of video through the glass at the camera to the consumption of video through the glass at the consumer device. Capabilities that were once the domain of the core of the network are increasingly pushed out to the IP edge. Content providers are moving forward with professional 4K production environments (studios, stadiums, and so on) to create engaging and immersive 4K content, all running over IP networks. Service providers are shifting the distribution of premium video over efficient IP networks to reach consumers at the time, format, and location of their choosing. Environments that were once simple and single purpose—for example, a broadcast studio or truck, video distribution network, or set-top-box—are being asked to more flexibly support a host of services: High Definition (HD) and 4K, linear and on-demand, managed and Over-The-Top (OTT) traffic.

This increase in IP traffic and services is becoming increasingly complex to operate. Our networks are required to handle the massive scale of services being provisioned and managed without compromise on quality and without leading to proliferation of costs. Application environments are evolving to cloud-native environments, and new IP and cloud-based capabilities are being added to the network. This is enabling applications and workflows to be more rapidly onboarded, turned up, managed, and turned down.

The risks are also greater. With the speed enabled by IP and cloud capabilities, there needs to be an equal focus on maintaining quality, resilience, and error reduction. More importantly, security vulnerabilities are increasingly uncovered and exploited in this emerging world that is more IP and cloud connected. Security vulnerabilities are exploited anywhere along the network chain. Cisco predicts an increasing frequency and size of Distributed-Denial-Of-Service (DDOS) attacks taking down networks. More concerning is the speed with which security hacks/online piracy can do damage without being detected, often for 100 days or more. And headline-grabbing hacks are too frequent and numerous to mention, inflicting financial, brand, and operational headaches on studios, networks, and service providers alike.

At Cisco, we believe that a new networking foundation is required to address the challenges we face and deliver the results we need.

Primary principles for this networking foundation include:

- Delivers differentiated end-user experiences
- Is scalable and simple to operate
- Automatically and dynamically adjusts in response to real-time information
- Provides security built into the network fabric
Introducing Cisco Video-Aware Networking

Cisco® Video-Aware Networking automates how networks and applications adjust to real-time data. By combining the synergies between the network and the video applications, Video-Aware Networking delivers a better experience for the consumer.

Video-Aware Networking opens up the communication lines between the network and the applications. It provides the intent-based networking foundation that is informed by video-aware context (real-time data captured across the network), including network telemetry, video quality, security threats, and user behavior. The network is made contextually aware of the applications and services it is running, and the applications will advertise to the network what it requires so that the network can supply it. With orchestration, this data is transformed into intent that informs how networks and applications behave, including automating operations, video Quality of Experience (QoE), dynamic security, and subscriber monetization. It is a programmatic way to operate networks and services, based on their needs, through APIs.

Figure 2. Video-Aware Networking

Informed by context

![Network telemetry
video quality
security threats
user behavior](image)

Powered by intent

![Automated operations
Quality of Experience
dynamic protection
subscriber monetization](image)

Video-Aware Networking is the combination of two industry approaches. It combines the benefits of programmable networking with content-aware networking. The first utilizes Network Function Virtualization (NFV) and Software-Defined Networking (SDN) principles to enable infrastructure to be more adaptive and responsive. The second utilizes more descriptive and metadata-aware principles to enable more declarative network traffic and services. As a result, you have a more programmable infrastructure that is responsive to the needs of the applications that drive traffic, while at the same time having applications behave with more awareness to the underlying network. The result is an intent-based IP-networking foundation with deep understanding of the video applications and their specific service requirements.

“The speed at which many customers want to deploy new video services exceeds their network abilities, and that’s where we come in,” said Conrad Clemson, senior vice president and general manager, Service Provider Platforms and Applications, Cisco. “Our customers can count on Cisco as a trusted partner for IP transformation, to help design the best cloud-scale, video-aware networking foundation that can get new services to market faster and simplify how to manage and deliver superior experiences to their subscribers.”
Enabling a new era with Video-Aware Networking

Video-Aware Networking involves collecting information from the network and the application in real time and translating it into specific, automated actions. The following are a few implementations of Video-Aware Networking:

- Delivering consistent video quality while saving bandwidth
- Automating network routing for better quality of service
- Reducing vulnerability with application visibility and control

Delivering consistent video quality over IP while saving bandwidth

One of the primary challenges with IP streaming is inconsistent video quality. This is the result of Adaptive Bit-Rate (ABR) streaming approaches in the industry, which adjust the bit rate for video streaming based on the available network as determined by the requesting ABR client device (a subscriber’s iPad or IP/set-top-box). Video-Aware Networking adds real-time data about the quality of the content to enable the ABR encoder to make more intelligent decisions about how to encode the content to meet specific quality targets alongside bandwidth consumption targets.

This real-time data comes from a Cisco patent on a video quality metric we call Stream Video Quality (SVQ). This SVQ metric provides a rating for video quality, which we have tested alongside industry standard approaches. We use the SVQ metric to make an informed decision about how much to compress specific video frames to make sure of a more consistent video quality stream from the encoder. Typically, up to 50 percent of bandwidth can be saved, resulting from a more variable application of bit-rate adaptation, by allowing easier scenes to utilize less bandwidth than allocated while reaching their quality target.

This smart rate control functionality is a feature in the Cisco Virtual DCM. It changes the way video applications behave by acknowledging expected video quality targets and network bandwidth and matching the bit rate needed, without wasting precious bandwidth. (See Figure 3.)

Figure 3. Cisco smart rate control
Automating network routing for better quality of service

Segment routing, with its capacity for centralized and distributed intelligence and enhanced packet forwarding behavior, helps to solve the scale and complexity challenges that come with digitization and traffic growth. With video driving most IP traffic, it is only logical to expand segment routing for video services and automate routing of video traffic from source to destination, enabling better scale and better utilization of the installed network infrastructure.

Segment routing is an important step to help video operators simplify how the network and applications adjust to real-time data. As the market leader in segment routing deployments, with more than 20+ global customers on this path, Cisco is sharing its expertise in IP networking and video to help service providers explore the possibilities for segment routing with IP video service deployments.

Segment routing is a flexible, scalable way of doing source routing, where applications, including video, can determine their own paths in the network in order to provide the superior experiences operators want to offer their customers. It’s an improvement over traditional link-based routing, where at each “hop” along a data journey, the next best step is established. Segment routing creates “awareness” so that the network can adapt how it behaves according to contextual information from the video applications that it transports. (See Figure 4.)

Figure 4. Segment routing innovations for video

Benefits of segment routing for video:

- Simplifies IP network configuration and management, reducing traffic engineering time and errors
- Scales the delivery of diverse services with automation that can programmatically apply application-level requirements to the network
- Delivers quality-assured video experiences that differentiate your service and impress your customers without having to expend additional bandwidth
Reducing vulnerability with application visibility and control

One of the primary challenges in security is that attackers are motivated by the financial incentive of security exploits combined with increasingly simplified ways to execute an attack. There are many more ways to breach a company’s data center and network, and more tools are readily available. Technical wizardry is no longer required. Attacks today are stealthy and multipronged, meaning there’s a greater chance of success for hackers, with breaches often going unnoticed for 100 to 200 days.

With Video-Aware Networking, the combination of Cisco Tetration Analytics™ and Cisco Stealthwatch® solutions offers a holistic, multilayered approach to effective security, enabling you to:

• See more: detect anomalous behavior across your data center and network or unauthorized access to your services
• Protect better: reduce the attack surface area with segmentation capabilities that prevent attackers from moving laterally east to west
• Respond faster: isolate risks and automate responses that can rapidly detect and respond to threats before hackers can steal data or disrupt operations

Cisco Tetration Analytics offers full visibility into application components, including workloads, processes, and application behavior in the data center. It enables rapid segmentation to blacklist/whitelist areas in your data center and provides anomaly detection.

Cisco Stealthwatch offers enterprise-wide network visibility across users, hosts, networks, and infrastructure. It collects network flow and other data to provide network visibility for understanding networkwide traffic and discover threats and incorporates real-time situational awareness of users, devices, and applications. (See Figure 5.)

Figure 5. Application visibility and control

Conclusion

As consumer demand grows for higher quality, more personalized video experiences, so too does the pressure on our networks to keep up. Configuration and operations can become complex, scalability and quality are often difficult to balance, and speed and security seem diametrically opposed. When it comes to quickly, securely, and efficiently moving video bits across the network, the future of video is the network. We call it “video-aware networking,” and it will shift the future of video networks.