The Network: Artery and Brain for Big Data - Part 1

Cisco IT Insights Series - Network Architecture for Internet of Everything

This five-part series describes a new network architecture for collecting and analyzing big data in the Internet of Everything era. You can read the parts in any order. Part 1 explains the role of the network in the Internet of Everything era. Part 2 summarizes how big data is different from other data (volume, variety, and velocity). Part 3 describes the seven types of network intelligence to act on big data. Part 4 presents use cases for analyzing network data with big-data techniques. Part 5 presents a four-layer architecture: resource, distributed repository, processing, and application.

What You Will Learn

The network plays multiple roles in harnessing big data to make better, faster decisions:

- The network *gathers* data from the billions of devices that connect to the Internet of Everything.
- The network *produces* a new type of big data because it sees every IT activity. Analyzing network data can help to improve security, the user experience, and operational excellence.
- Intelligent network devices can *analyze* big data closer to the endpoints that gather the data. This capability reduces latency and bandwidth compared to sending data to a data center for analysis.
- Network devices can *automate responses* to real-time big data. An example is temporarily increasing bandwidth for certain applications.

Network: It's Everywhere Big Data Is

If you say "big data," people tend to think about data center solutions such as analytics software, computing frameworks like Hadoop[1], and storage. The network, too, plays a central role. Its importance continues to grow as we enter the Internet of Everything era, for four reasons.

The Network *Collects* All Sources of Big Data

The network no longer simply connects servers, switches, and routers. In the Internet of Everything era, it also connects building sensors, video surveillance cameras, door controllers, digital signage, swimming-pool monitors, wearable electronics, actuators, and even swallowable electronics for healthcare monitoring. In 2012, 8.9 billion things connected to the Internet. The number of Internet-connected things will grow to 15 billion by 2015, and 50 billion by 2020 (source: Cisco IBSG).

The network is the one common element connecting these billions of things. Therefore, it is the only entity that can correlate an abundance of data from clients, network devices, and the cloud. A simple example is detecting and responding to security incidents. A future example might involve car sensors that detect deep puddles and wirelessly send alerts to cars behind them, helping to avoid accidents.

[1] For an introduction to Hadoop, visit: http://en.wikipedia.org/wiki/Apache_Hadoop

The Network *Produces* Big Data

The network is the only entity that can see every event in your IT infrastructure. This power makes network data a rich source of intelligence to improve security and the user experience.

Network data used to be limited to logs, traps, events, alerts, and notifications. This traditional network data remains useful for monitoring network health or introducing Layer 4-7 business models. Now you can also collect new kinds of network data to make Layers 1-3 healthy, secure, and high performing. This type of network data is big data that relates to application performance, network services, storage, compute, collaboration, video, and the user experience.

Network data is a new form of big data. Analyzing it and acting on network data in real time can help you find out about potential security events sooner. It can also help you improve the user experience, for example, by reallocating bandwidth if hundreds or thousands of users request a video at the same time.

The Network Can *Analyze* Big Data Closer to Where It's Produced

It's not economical to build intelligence into low-cost endpoints such as building sensors or home-security sensors. But the alternative, sending information from millions or billions of Internet-connected endpoints to a central facility multiplies bandwidth requirements. Sending information from the network edge to the core also adds latency. This added burden is not acceptable for time-sensitive decisions such as what ad to display on a web page or how to respond to a suspected network attack.

Network devices can analyze big data locally to generate statistics, notifications, and orchestration data. Analyzing big data closer to network endpoints also avoids the latency that occurs if data is sent to central servers for analysis.

The Network *Acts* on Big Data

The network responds to the data that it collects to control quality of experience and deliver new kinds of user services. Table 1 shows a sample of conditions or events that the network can detect and respond to. The value of analyzing and acting on network data includes improved security, cost reduction, operational excellence, and user services.

Table 1. Intelligent Switches Detect and Respond to Events in Real Time

Condition Detected by Switch	Action
Surge in traffic from videoconferencing	Allocate more bandwidth for video traffic for duration of surge
Unusual traffic patterns that look like botnet activity or other fraud	Notify affected users or shut down traffic, according to policy
Customer walks down particular aisle in retail store	Send coupons for products on that aisle to customer's mobile device

For More Information

To read Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**