Seven Essential Network Capabilities for the Internet of Everything - Part 3

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

Taking advantage of the network to collect, analyze, and act on big data requires:

- New kinds of network intelligence: This intelligence includes content-awareness, policy-based decision-making, and network programmability.
- Flatter network architecture: Traditional architectures add too much latency for the network to analyze and act on big data in real time. A new architecture for the Internet of Everything age needs to consolidate different places in the network (PINs), support east-west traffic, connect source to destination in one hop, and provide unified access.

New Kinds of Network Intelligence

Big data and the Internet of Everything demand the following types of network intelligence.

1 - Content-Awareness: Know How to Treat Different Kinds of Traffic

Content-aware networks can recognize different flows, services, and applications. Then they can adjust their own configuration to optimize performance. For example, data replication traffic needs low latency, while video and images need high bandwidth and better quality of service. Providing capacity on demand makes overprovisioning unnecessary, reducing costs. On-demand capacity also avoids oversubscription, which can degrade performance or cause failures.

Techniques that create content-aware networks include:

- Security Group Access (SGA) policies and Security Group Tags (SGT).
- Cisco® Identity Services Engine (ISE).
- NetFlow logs.
- Media Services Interface (MSI), a medianet API: MSI links endpoints (such as telepresence endpoints) to service-level agreement (SLA) information, service flows (RTP and TCP), and metadata. The metadata comes from medianet tools such as Performance Monitoring and mediatrace.
- Application Visibility and Control (AVC) flows: These flows link network data to application data, IP SLAs, management information bases (MIBs), and data about events, notifications, alerts, and incidents.

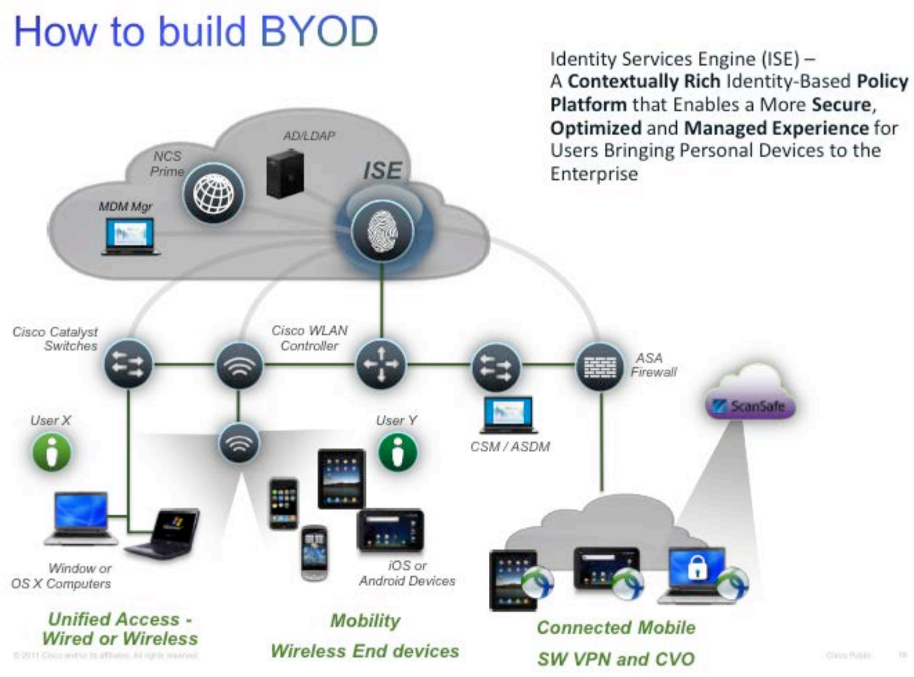
- Cisco onePK or other software-defined networking (SDN) APIs: These APIs can monitor and control network elements. Based on the information they gather, the APIs can initiate actions such as configuring a new bandwidth QoS, traffic route, or security response.

2 – Policy-Based Decision Making

To mine the insights hidden in network data, you need to harvest information from users, groups, and devices. With this information, the network can apply security policies that depend on *who* is making the request, and *how* and *what* content or service they are requesting. But traditional networks are aware only of infrastructure devices, not users and groups.

To provide the context of requests so that the network can make decisions, you can use the Cisco Identity Services Engine (ISE). Cisco ISE is a security policy management and control platform. It consistently applies policy for wired, wireless, and VPN connectivity, as shown in Figure 1. It meets the velocity requirements of big data by logging, reporting, classifying, encrypting, and routing traffic in real time. It can even apply policies concerning digital rights management. For example, Cisco ISE can analyze content leaving the network for predefined patterns that indicate sensitive information. Then it can block the content from leaving the network.

Figure 1. Policy-Based Decision Making Using Cisco ISE



How to build BYOD

Identity Services Engine (ISE) – A **Contextually Rich** Identity-Based **Policy Platform** that Enables a More **Secure**, **Optimized** and **Managed Experience** for Users Bringing Personal Devices to the Enterprise

3 – Network Programmability, or Software-Defined Networking (SDN)

SDN shifts network intelligence from individual routers and switches to a central controller. As you connect more people, process, data, and things to the network, SDN provides two important benefits:

- Simplifies network management by letting you centrally control policy for all devices on the network. You can manage one or a few control planes instead of one in every network element.
- Enables individual applications to directly program the network to acquire the resources they need. This helps to optimize performance under different network conditions. Some of these conditions might require an immediate response to vast amounts of information.

Cisco Open Network Environment (ONE) provides three approaches to network programmability:

- The traditional SDN approach, using a controller, northbound API, agents, and OpenFlow.
- A set of APIs called onePK (for One Platform Kit): Application developers can use onePK APIs to enable their applications to gather network statistics, program the network, or both.
- Virtual overlay: If you add a logical overlay to your physical network fabric, different people in your organization can create, modify, or tear down their own virtual networks. You don’t have to make any changes to the physical network. Virtual overlay technologies include Cisco Nexus® 1000V virtual switches and Quantum APIs, an OpenStack technology that Cisco helped develop.[1]

New Architecture for Internet of Everything

The network architecture for big data and the Internet of Everything requires a fresh approach. For example, maintaining different architectures for different places in the network (PINs) no longer makes sense. And WAN performance improves when the architecture supports east-west traffic flows, one hop from source to destination, and unified access.

4 – An End to Segmentation

Many campuses have one network architecture for the LAN, another for the WAN, and yet another for the data center. Segmentation based on “places in the network” (PINs) complicates monitoring, managing, and securing your network from end to end. It also makes it more difficult to mine network data for insights, enforce security policy, and program network behavior based on the type of workload.

Another problem with segmentation is that some software services, such as mobility, might be available only for a particular hardware platform and operating system. Abstracting common services from the hardware is more efficient. These services include security, mobility, management, and content awareness. Abstracting

[1] For a white paper on network programmability and virtual network overlays, visit: http://www.cisco.com/en/US/prod/collateral/iosswrel/content/white_paper_c11-707978.pdf

these services allows faster development of new business models and applications based on big-data analytics.

A network architecture that supports big data and the Internet of Everything isn’t based on PINs. Instead, a unified network fabric extends from the data center through the access edge. Partitions are formed by SDN network overlays. All network devices in a common overlay share a control plane and borderless services. And all overlays share a set of common network services, shown in the table. This same architecture supports BYOD, pervasive security, pervasive video, desktop virtualization, telework, and extranet services.

Table 1. Architecture for Internet of Everything and BYOD

Functions	Examples
Control Plane	Identity, presence, location, signaling, clocking, AAA, Quality of Service, and Quality of Experience
Borderless Services	Network service virtualization, cloud resource mapping, Medianet, Cisco TrustSec, application acceleration, directory services, power management, and mobility
Common Services for All Domains	Policy, security, any-to-any connectivity, network management, network awareness, and zero-touch deployment

5 – Designed for East-West Traffic, Not Just North-South Traffic

In traditional client-server networks, traffic flows from the endpoints up to the network backbone (south to north) and back down to another end device or data center server (north to south). That is, if you’re working on a laptop in your office, an application request flows north through each tier to the core network in the data center, where the application server sits. Then the application data flows south back along the same path to your laptop.

The north-south architecture adds latency, and is no longer practical in a world of mobile endpoints and cloud-based applications. Now virtual machines need to move between data centers, both on-premises and in the cloud. And mobile users connect from anywhere, with any device.

Big data and the Internet of Everything require a network architecture that also supports “east-west” traffic between different data centers. The idea is to allow virtual machines to migrate from one server to another, in any data center, without detouring through the core. With this architecture, any device (including mobile devices) can connect to enterprise or cloud services in any location, with the lowest possible latency.

Entrepreneurs are starting to introduce big-data analytics services, from analyzing sales to predicting the effect of weather forecasts on business. The service providers that provide big data analytics “as a service” in their data centers will need network architectures that can support south-north as well as east-west traffic. Uploading big data for analysis is a south-north activity. Analyzing the data across multiple servers is an east-west activity.

6 – Everything Is Just One Hop Away

Hierarchical data center network architectures add too much latency to support real-time or big data workloads. That's because all traffic between servers, or between a client and server, traverses each network tier. It flows to the core and then back through each tier to the destination. Each network hop adds latency. This can lead to an unacceptable user experience and prevent real-time decision-making based on current network conditions.

To gather and act on big data, the network destination should never be more than one hop away from the source. This architecture is sometimes called a connectivity fabric or application-centric infrastructure.

7 – Unified Access

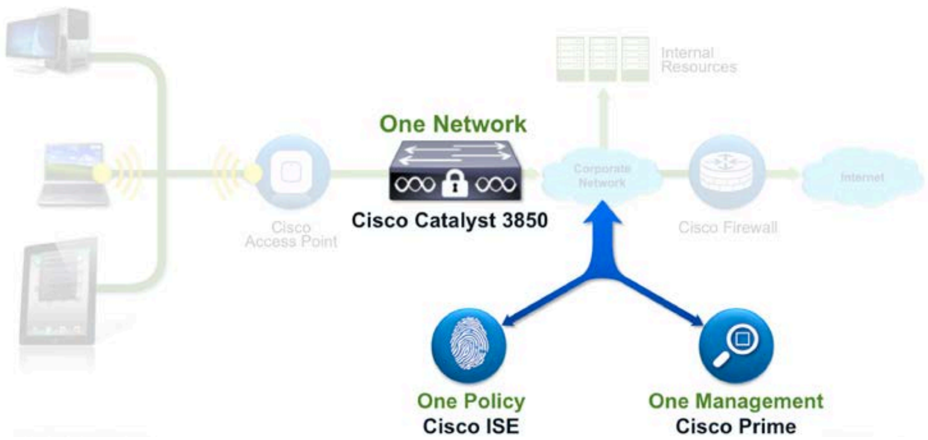
Today, many campuses have separate networks for wireless, wired, and VPN access. One problem is high support costs, which will increase as the number of endpoints grows. Another problem is the difficulty of consistently enforcing access policies across different networks. For example, your organization's security policy might prevent you from connecting wirelessly while in a conference room. But you might be able to go around the controls by plugging a cable into a wired RJ-45 jack. Another problem with separate access networks is the high management overhead.

Cisco Unified Access solves these problems by unifying all network, management, and policy domains. This unification helps to simplify operations, accelerate new service introductions, enforce security policies, and enable SDN. Unified Access serves as the foundation for the Internet of Everything as well as BYOD by providing:

- One Policy: Cisco ISE shows who and what is on the network, regardless of whether they are using a wired, wireless, or VPN connection.
- One Management: You can use a single interface for comprehensive lifecycle management, performance assurance, and compliance monitoring for wired and wireless networks.
- One Network: Wired and wireless networks share one infrastructure.

Cisco IT now has a Unified Access network, shown here. To read our case study, visit: http://www.cisco.com/en/US/solutions/collateral/ns340/ns1176/borderless-networks/CoC_UA-Converged_Access.pdf .

Figure 2. Cisco IT Has a Unified Access for Wired and Wireless



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.**