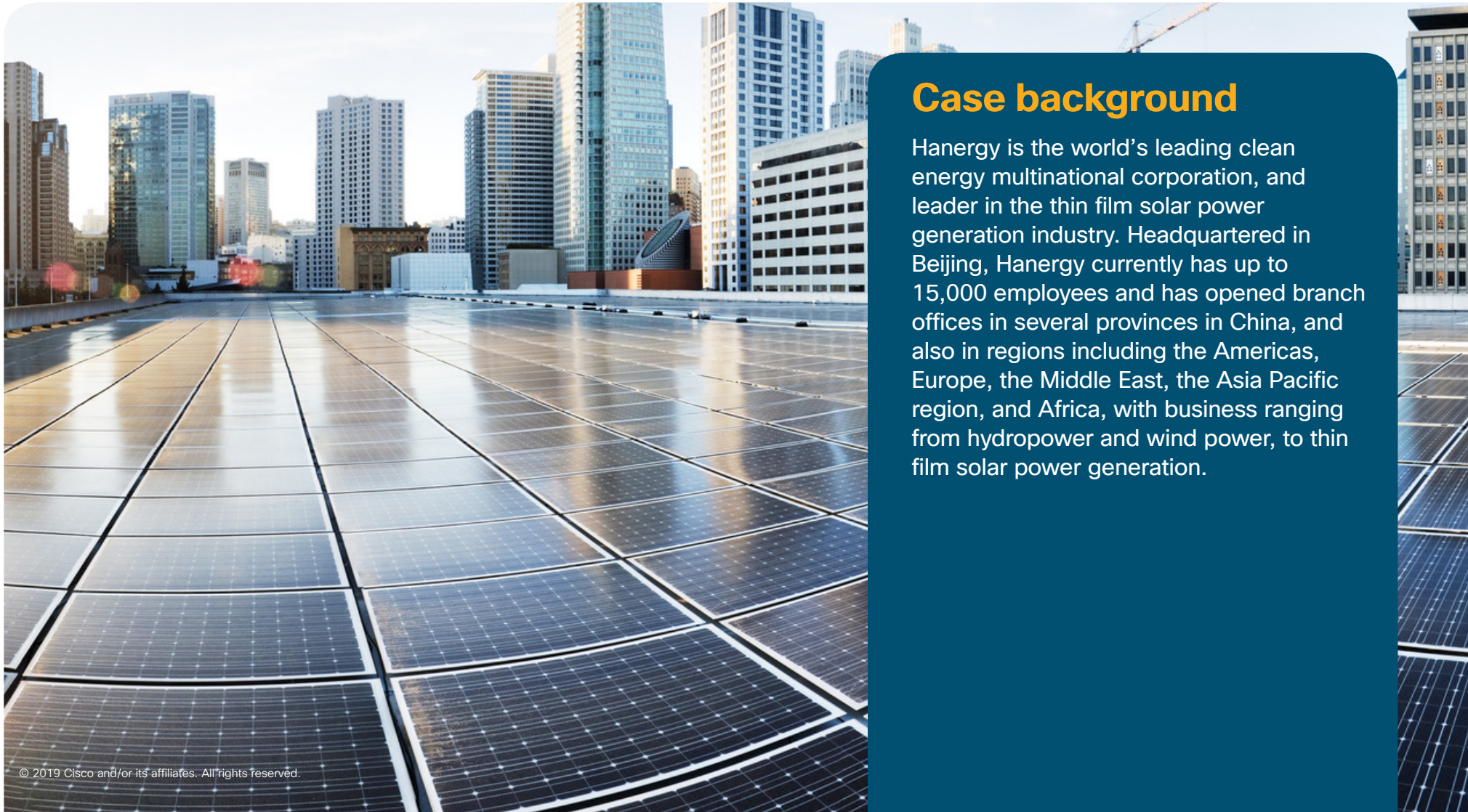
Case Analysis: Hanergy Group



Case background

Hanergy is the world's leading clean energy multinational corporation, and leader in the thin film solar power generation industry. Headquartered in Beijing, Hanergy currently has up to 15,000 employees and has opened branch offices in several provinces in China, and also in regions including the Americas, Europe, the Middle East, the Asia Pacific region, and Africa, with business ranging from hydropower and wind power, to thin film solar power generation.

Business and IT challenges

Hanergy's business is growing rapidly along with the world's increasing demand for clean energy, which creates higher requirements of the IT industry. Brisk demand for IT results in delivery of a multitude of business systems; business expansion gives rise to rapid increase in the number of employees; campus size also increasingly expands; and the shortage of basic network safety measures brings hidden dangers for information security. Conventional network architectures have a hard time responding, resulting in failure of rapid response.

Information architecture faces impending adjustments, and at the network level, various challenges:

- Architecture scalability (ensuring the business made available online rapidly in tandem with the exponential growth of personnel and business)
- Collaboration strategy (network and business expand securely and horizontally in tandem with massive collaboration of personnel)
- Effective and simplified operations and maintenance of the network (with a limited number of maintenance personnel)
- Many IoT terminals access (access control, automatic management of cameras, and flexible operations supporting the enterprise)
- Secure access and protection (unified access of key positions in R & D to Cisco Virtual Desktop Infrastructure [VDI])
- A unified cloud center and campus (unified strategy for users and applications)
- Efficient WAN connections (efficient interconnection between many branches and headquarters, and the cloud center)

Outcomes of the application

Deployment of Cisco Digital Network Architecture (Cisco DNA™) and Cisco Application Centric Infrastructure (ACI) solution enables Hanergy to rapidly expand its new campus, exponentially increase the number of employees, and make business available online without increasing the number of network administrators, as well as greatly simplifying network operations and maintenance, preparing strategic opportunities for rapid development of the group's businesses.

As the original network features a three-tier architecture, administrators need to manually adjust, configure, and test network equipment to increase staffing and expanding business. It takes about 4–5 days for the new campus to have them made available online, even in a best case scenario. With application of Cisco DNA, the network is simplified into a two-tier architecture. As a result, the network equipment in the new campus features access functionality only, and the center management console is used for configuration and adjustment. As the console is globally attuned, configuration is issued automatically without requiring configuration and adjustment of equipment individually after the network intent is configured by the administrator. Powered by Cisco DNA, the network features WYSIWYG configuration. As a result, it only takes 0.5–1 hour to deploy the network and make business available.

In tandem with horizontal expansion of the Hanergy facility, a many employees have had their offices changed. As a result, many coworkers in departments have to work in different buildings or campuses, and a large number of employees need to go back and forth between buildings, campuses, or both for collaboration, frequently working in one place in the morning and another place in the afternoon. This situation calls for prompt adjustment of network access/security policy accordingly. However, if the original architecture is deployed, such adjustments must be configured manually by administrators, requiring significant time expenditure. As a result, employees cannot quickly begin business tasks, impacting employees' mobile office and cross-zone collaboration. The collaboration strategy provided by Cisco DNA addresses this problem. Employees are classified into corresponding strategy groups when accessing the network for the first time, and no matter where they move in the company, that strategy will remain constant. This process occurs automatically with no operator intervention, which ideally supports more extensive collaboration among employees in tandem with rapid expansion of Hanergy.

Luo Cheng, Director of the Basic Architecture Department, the Information Management Center of Hanergy, is very satisfied with the Cisco DNA and ACI. He reports that new architecture kept problems resulting from rapid business expansion such as networking pressure, personnel changes, terminal migrations, and cloud center interconnections under control, safeguarding the success of Hanergy during the period of strategic opportunity for its business. He fully expects to meet the strategic objectives for the group's smart operations and intelligent manufacturing in the next stage to be supported by Cisco DNA and ACI in future.

Traditional solution and architecture reserves and configures the relevant terminal for Hanergy 's IoT terminals such as access control, camera, and sensor. When locations of terminals change, administrators are also needed to identify network equipment manually and migrate the configuration to the new terminal. If well-configured terminals are accessed maliciously by other equipment, the interception and sniffer equipment also cannot make detection or prohibition, which may cause greater hidden dangers. Using user groups, Cisco DNA addresses this problem. All IoT equipment is assigned to the relevant groups. The strategies are worked out according to the groups, and remain unchanged after the locations are migrated. Even if someone attempts to access other equipment, it cannot be added to the IOT terminal group, which controls access to the equipment fundamentally and ensures network security.

The cloud center supports the key business of Hanergy—how to open up the boundaries between the campus and cloud center, and develop end-to-end IT strategies by focusing on the key business of the corporation have always been challenges to IT managers. The traditional solution calls for configuration of a variety of equipment such as firewall, application delivery, and switch one by one, which is made possible in a complex way that is prone to errors and has poor instantaneity. Leveraging the integration of Cisco DNA and ACI, Hanergy unifies their strategies by connecting network between the campus and data center, which guarantees a single strategy for the whole process across the network.
The campus network and data center resource, which is physically close to employees, has been delivered automatically, enabling employees to complete self-service uniform application and dispatch of the resource, which is convenient and adequately secure. It gives the most prominent support to researchers. Hanergy's researchers started sharing resources using VDI. Specialized development of energy products requires invoking a large number of drawings and data, which are core assets of the corporation. Thus these assets are kept safe and secure, and developers can access to them in real-time and in an efficient way. Based on the employees and businesses, the new architecture can guarantee and reserve bandwidth for such key applications. More crucially, all functions mentioned above are configured and made available based on graphical interfaces. Following the configuration, all the adjustments are made automatically and in real time.

C36-742359-00 05/19