Almadar Aljadid Enterprise Network

Agenda

▶ Introduction

▶ Logical topology

▶ Network Endpoints

▶ Access to the network

▶ MAN & WAN

▶ Collaboration

▶ Security

▶ Management & Monitoring

Introduction

- ▶ Network equipment are the bridge that connects systems & services runs and its intended users, whether these users are local, remote, or mobile.

- ▶ Reliability, availability, and continuity are mandatory in today's networks, specially for sensitive real-time applications such voice & video, and e-Commerce.

- ▶ State of the art collaboration tools allows fast & ease meetings, conferences, and increase employee availability.

- ▶ Also, securing network resources is a major factor on all levels, whether secure access for local or mobile users to company's systems and resources, users accessing or receiving malicious content, or protecting against attacks.

Logical Topology

- Our network consist of four parts:

  - **Core-Network / Datacenters:**

  This part contains network equipment with high redundancy and throughput capabilities that can handle the demand for current and future services hosted in DC including security enforcement.

  - **Main-Buildings:**

  Main buildings has multiple offices and they have 2-teir switching structure, and they have MAN/LAN connectivity core network.

  Almadar has 4 sites with such structure (including HQ).

  - **Remote-Sites/Offices:**

  Remote offices have small number of users and they have WAN (E1) connectivity to the routers in the core network.

  - **Edge:**

  Contains the appliances that handle access by devices out of enterprise network including internet & wireless to the systems in house, where it provides secure-access for remote users by VPNs or Web-APP publishing, and inspection for company partners & customers.
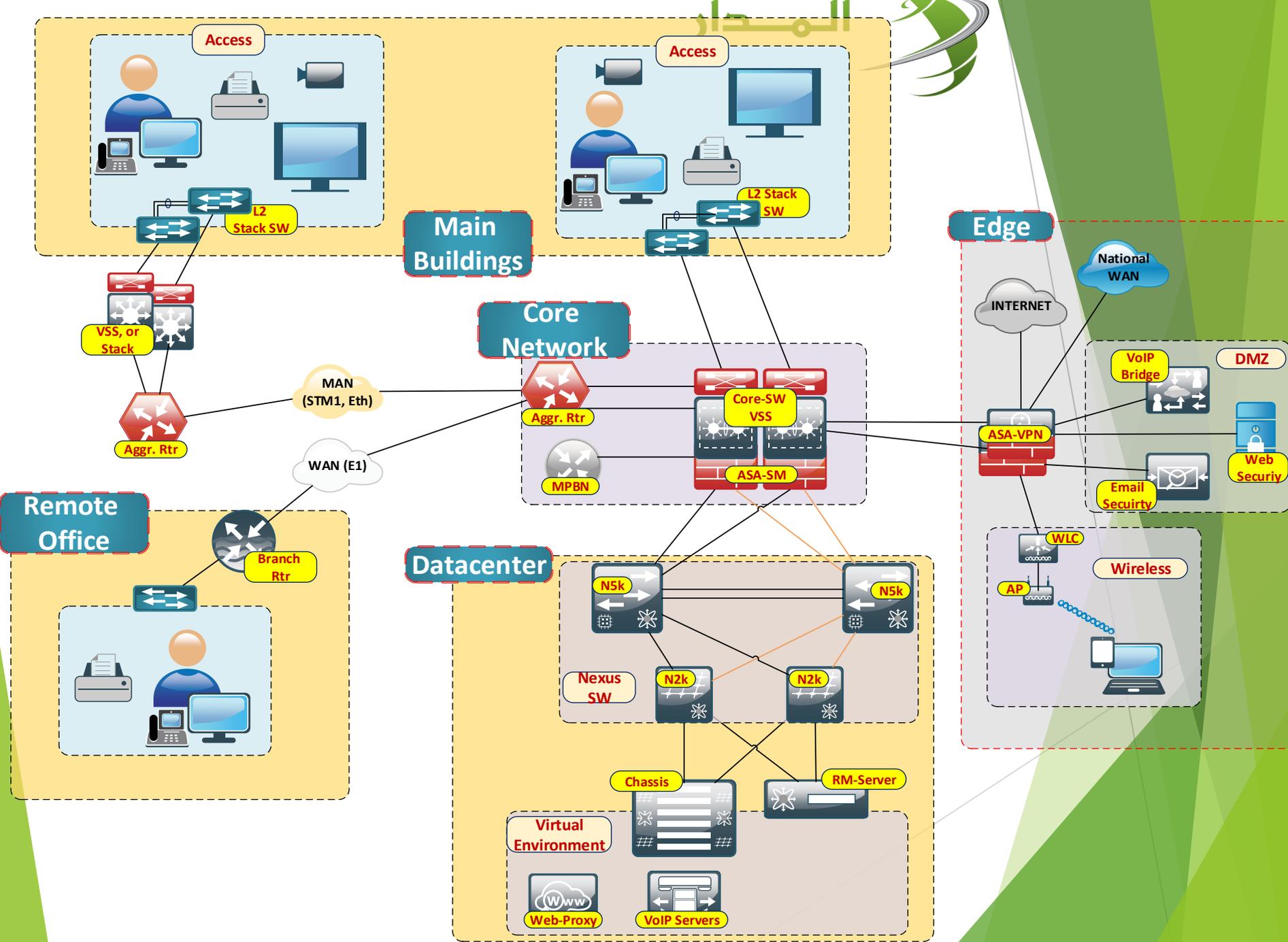
Network Endpoints

▶ Almadar enterprise network provide wired & wireless connectivity to the following nodes:

❖ Servers (Rack-mounted, or Chassis)

❖ Security Appliances.

❖ Telecom systems

❖ Office devices:

- Desktops
- Printers
- Document Scanner
- Smart-Board
- Finger-Print reader
- Smart-Screen

❖ Real-time devices:

- IP-Phone
- Video Conference station
- IP-Camera

❖ Wireless devices:

- Laptop
- Smartphone
- Tablet

Access to the network

▶ Switches are used to provide the access function to our network, and they are

▶ Datacenter Servers & Appliances:

❑ Communications between systems require high bandwidth with low latency, Cisco Nexus 5500 and 2200 switches delivers them in a Spine (Nexus 5500) & Leaf (Nexus 2200) architecture.

❑ The uplinks from spine switches are grouped in one LAG towards core-networks in

▶ Endpoint Devices & End-User:

❑ Multiple switches are implemented in each floor to deliver the needed amount of access ports

❑ The switches in each floor are stacked together to form one big switch

❑ Uplinks towards the core-network are puddled in one LAG to provide higher throughput and availability in an Access to Aggr./Core architecture

MAN & WAN

- ▶ Almadar has a MAN & WAN routers to connect its multiple office across the country.

- ▶ The Aggregation routers has interfaces for different carrier protocols such SDH/STM1, PDH/E1, and Giga & Fast-Ethernet to connect with either other aggr. Routers or remote office routers.

- ▶ Dynamic routing protocol are used to provide IP connectivity between endpoint devices at the sites.

- ▶ Also, Quality of service are implemented whenever application requires it.

Collaboration

▶ With the evolution of technologies, new solutions require employees with different specialties to work together;

Therefore, Collaboration became a major factor for faster decisions and reducing time to market.

▶ Collaboration systems involves voice & video calls using IP-Phones and Soft-Phones (Cisco Jabber) which facilitates the voice communications, also instant messaging and presenting contents

▶ Conference rooms are equipped with Telepresence stations that provides voice (sometimes with video) between team members across locations.

▶ Also Collaboration edge node (Expressway) allows mobile users to communicate and collaborate with other members in the offices

Security

▶ Security are implemented on multiple levels providing isolation, access-control & filtration, and inspection.

▶ VLANs are implement in as Layer-2 segregation techniques that isolate broadcast domains and enforce traffic to go through L3 interfaces.

▶ Access Control Lists (ACLs) are used in network switches routers to filter users traffic.

▶ Firewalls provides ACL & inspection on the infrastructure traffic payloads such FTP & DNS;

▶ Also, Firewalls provide encrypted tunnels to partners and remote users over untrusted networks (such the internet).

Management & Monitoring

▶ Network performance is measured by collecting network devices counters over period of time;

▶ The counters varies between device health, interface statistics, and application visibility.

▶ Also, Failure in network is discovered and alerted through monitoring system that tracks the states of each listed device, or by a threshold/fault traps .

▶ Network management systems are used to collect, store and present these data; SNMP protocol is used to collect data and receive traps from network equipment.

▶ Cisco's net-flow is used on core devices for application visibility on MAN & WAN links.