Network Classification for an Enterprise

Anshuman Awasthi

Director – Engineering, Restoration Hardware

Abstract: ***Infrastructure Network lays the foundation for an organization to perform its critical business functions. Most of the time we refer network as just simple connectivity to other resources but actually it can be classified into different categories based on the function. Let us try to understand what are the different types of network that function in an enterprise and the types of devices that function in different layers in an OSI model.***

Keywords: Network Engineering, OSI Model, Types of Network, Infrastructure Network

1. Article

The enterprise network is the foundation of connecting your local office to the whole world. It is not possible to collaborate without an excellent infrastructure of IT systems working in an efficient network. We can classify network in three different types:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Wireless Network

1.1 Local Area Network (LAN)

A local area network is a backbone for the enterprise information technology infrastructure. A local area network (LAN) is a network of interconnected servers, printers, desktop, laptops, and other appliances within a small area like for an office building, a school, or a campus. In today's changing world, the basic requirements for features and abilities required from an application or a server are changing and the network needs to evolve rapidly. Due to high bandwidth requirements for applications that are rich in contents like multimedia presentations, video conferencing, a network administrator, has to come up with a design that is not only reliable but should be scalable.

In a typical LAN design, the network is broken into small segments; this is called network segmentation or VLAN (Virtual Local Area Network). VLANs are created as we logically break broadcast domains in layer 2, switched network. Network segmentation helps in better traffic management by avoiding collisions. We can use network switches like Cisco 9300 48 port POE (Power over Ethernet) switches. The primary purpose of these switches is to simplify local area networks by breaking a much bigger chunk into smaller segments—to optimize its performance—provide more bandwidth and avoid internal collisions for the LAN's users. Layer 2 switches just perform the task of switching frames from one network port to a different one within the same switched network. Switches do not forward packets to other networks as routers do. POE enabled switches are capable of providing enough bandwidth and power to the attached wireless access points. Cisco 9300 switches can be connected to the core infrastructure using 10G uplinks, which improves LAN network performance significantly. Cisco core 9500 -40X switches can be installed in a virtual stack configuration, which means they provide complete hardware redundancy. In case one of the switches goes down, the other switch in the virtual automatically takes control of the traffic. All the network switches and routers are equipped with dual power supplies, and each power supply is connected to a separate power source to provide redundancy.

1.2 Wide Area Network (WAN)

Network devices that are used to connect to the outside world are classified as Wide Area Network (WAN). A significant distinction between a WAN and a LAN is that while an organization generally own a LAN infrastructure, but they usually lease a WAN infrastructure from an internet service provider. Routers that are called as gateways when operated on Layer 3 and Internet Edge switches are the most common devices used in most of the organization to connect to Wide Area Network.

According to Lammle, T (n.d.), routers provide connections to Wide Area Network (WAN). Here are some of the characteristics of the router.

- Routers, by default, will not forward any broadcast or multicast packets.
- Routers use the logical address in a Network layer header to determine the next-hop router to forward the packet.
- Routers can use access lists, created by an administrator, to control security based on the types of packets allowed to enter or exit an interface.
- Routers can provide layer two bridging function if needed and can simultaneously route through the same interface.
- Layer 3 devices—in this case, routers—provide connections between virtual (VLANs).
- Routers can provide quality of service (QoS) for specific types of network traffic.

The router can perform below functions in an enterprise network:

- Packet switching
- Packet filtering
- Internetwork communication
- Path selection

Routers are used to filter packets by using inbuilt access lists and is connecting two different networks using logical addressing (IPv4); this is called an internetwork. A router can use a static or a dynamic routing table, which is usually a map of the interconnected devices, these routing tables are used to make decisions regarding best path for moving a packet from a source to the desired destination

1.3 Wireless Network

The use of wireless devices in our daily life has grown exponentially in the past few years. Many enterprises are installing a large number of wireless devices to perform the business transaction, and the use of wired internet connections are slowly becoming obsolete. Wireless devices provide a different level of freedom in terms of usage and experience, but it also increases security risks. In addition to the security aspect, a wireless network needs serious design considerations as the improper design will affect the performance and user experience.

It is essential to segregate wireless networks based on the type of users like for Guest, Corporate users, or for Point of Sale (POS) devices. The wireless user or a device has to go through an authentication and authorization process before granting access to the wireless network.

1.4 Guest WIFI

Providing wireless connections to the visitors or customers in a retail location is becoming common practice for different organizations. The guest network usually has a simple authentication process. The user may need to accept the terms and conditions on a splash page or authenticate using a WIFI password. We can also request the user to provide his social media account credentials for authentication. As this network is simple to gain access, it is the more vulnerable to security attacks. To avoid these threats getting into your other systems, it is not only essential to segregate network traffic but also restrict the usage. If we have deployed SDWAN (Software-Defined Wide Area Network) appliance, we can send the guest traffic directly to the internet using application-based routing policies. We can restrict internet usage by blocking specific categories of the website like gaming depending on the organization's information security policies.

1.5 Corporate WIFI

Corporate WIFI is usually the most heavily used wireless network in an enterprise. It is essential to make it secure but at the same time, easily accessible. The authentication and authorization process needs to be clearly defined. The simple active directory-based authentication process has now been transformed into identity services. One of the widely used applications for this purpose is the Cisco Identity Services Engine popularly referred to as "Cisco ISE." The identity services engine allows for different authentication protocols. A few are listed below.

- Password **Authentication** Protocol (PAP)
- Protected Extensible **Authentication** Protocol (PEAP)
- Microsoft Challenge Handshake **Authentication** Protocol Version 2 (MS-CHAPv2)
- Extensible **Authentication** Protocol-Message Digest 5 (EAP-MD5)
- **EAP** Transport Layer Security (**EAP-TLS**)

One of the popular authentication methods for enterprise WIFI users is EAP-TLS. (**EAP-TLS**), defined in RFC 5216, is an IETF (The Internet Engineering Task Force) open standard that uses the Transport Layer Security (**TLS**) protocol, and is well-supported among wireless vendors. **EAP-TLS** is the original, standard wireless LAN **EAP authentication** protocol. The EAP-TLS certificate-based authentication provides a convenient and secure mode of authentication. In this process, each user is issued a certificate that is installed on their laptops, MacBook's, iPad, or any mobile device. Depending on the type of policy check configured in the identity application, it will first validate the certificate. It will also check the account's validity in the active directory before granting access as per authorization policy.

You can use the identity service application for profiling the devices. This option can be used if we want to take a different action based on the type of devices. To design the wireless network for a warehouse, we can have EAP-TLS authorization for standard corporate devices, but for handhelds, we can allow a different authentication method. The device profiling can be helpful if we want to take various actions in the authorization stage. In a retail location, if we're going to separate the VLAN (Virtual Local Area Network) for POS devices from regular corporate devices, we can do that easily.

2. Discussion

This article explains how to design a network for a medium scale enterprise and what kind of different devices are involved.

3. Methods

Network Engineering using OSI model

4. Results/Conclusion

To design a network for an enterprise different kind of devices are involved in various stages. It is essential to understand the features and capabilities of each device so that they can provide optimal performance and security.

The layer 3 devices are routers and layer 2 devices are network switches. Routers can also be used as gateways to communicate between two different networks. Wireless security needs to be planned as per the organization’s info security policy and latest industry standards.

5. Challenges

The wireless deployment can be challenging and complicated at times as there are various variables involved at different levels. Few common issues that we may face are listed below:

- Authentication failures
- Not able to obtain a correct IP (Internet Protocol) address
- Devices cannot see the advertised wireless SSID (**Service Set Identifier)**

It is better to test the authentication and authorization process in real-time in the test or a restricted environment to ensure our policies are working the way we want.

References

[1] (n.d.). Article –CMS distribution. Retrieved from http://www.cmsdistribution.com/nl/product/solarwinds-network-performance-monitor-npm/

[2] T (n.d.).*CCNA Routing and Switching guide.* ISBN: 978-1-118-74973-9

[3] (n.d.). Report- Planning a network upgrade. Retrieved from http://catalogue.pearsoned.co.uk/samplechapter/1587132109.pdfdensity (n.d.).Blog- Windows Monitoring Tools. Retrieved from https://blog.serverdensity.com/windows-monitoring-tools/

Author Profile

Anshuman Awasthi, Director, Infrastructure Engineering at Restoration Hardware, responsible for IT infrastructure management and new implementations. Member of Forbes Technology Council.