Network Administration:

Network administration involves a wide array of operational tasks that help a network to run smoothly and efficiently. Without network administration, it would be difficult for all but the smallest networks to maintain network operations.

The main tasks associated with network administration include:

- Design, installation and evaluation of the network
- Execution and administration of regular backups
- Creation of precise technical documentation, such as network diagrams, network cabling documents, etc.
- Provision for precise authentication to access network resources
- Provision for troubleshooting assistance
- Administration of network security, including intrusion detection

Network Administrator (definition & functions):

A **network administrator** maintains computer infrastructures with emphasis on networking. Responsibilities may vary between organizations, but on-site servers, software-network interactions as well as network integrity/resilience are the key areas of focus.

A network administrator is an IT expert who manages an organization's network.

The network administrator must possess a high level of technological knowledge and is most commonly the highest level of technical staff within a given organization. Network administrators keep networks operational and monitor functions and operations within the network.

VIPUL RAJPUT

A network administrator is responsible for installing, maintaining and upgrading any software or hardware required to efficiently run a computer network. The IT or computer network may extend to a local area network, wide area network, the Internet and intranets.

The network administrator usually has a higher degree associated with computer science and IT. Administrators typically also acquire certificates related to networking or undergo high-level training related to specific software or hardware included in the network. This enables the network administrator to rapidly take control of new network additions or even create a new network completely from scratch. Certificates related to network administration are offered by well-known organizations like Microsoft, Cisco, Redhat and Juniper. Network administrators are rarely involved in direct user support like help desk duties. Instead, they engage in high-level technological support, such as maintaining network hardware and software equipment, and monitoring equipment to ensure overall network operations. Network addresses are often assigned through the network administrator. In addition, network administrators configure the authorization and authentication of individuals or groups who access network resources.

The exact definition of "network administration" is hard to pin down. In a larger enterprise, it would more often be strictly related to the actual network.

Specifically, this would include the management and maintenance of switches, routers, firewalls, VPN gateways, etc. In smaller companies, the network admin is often a jack-of-all trades and involved in the configuration of databases, installation, maintenance and upgrading of software, management of user accounts and security groups, desktop support, and sometimes even basic software development.

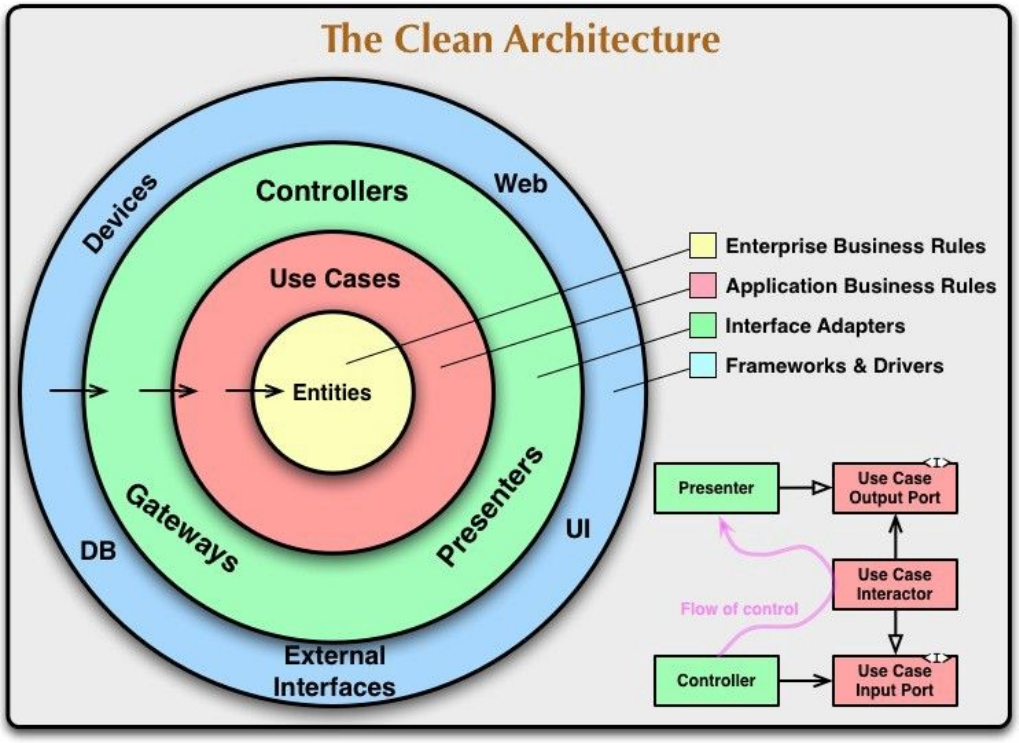
Network administrators are often involved in proactive work. This type of work will often include

VIPUL RAJPUT

- Network monitoring
- Testing the network for weakness
- Keeping an eye out for needed updates
- Installing and implementing security programs
- In many cases, E-mail and Internet filters
- Evaluating implementing network

CLEAN ARCHIETECTURE

The Clean Architecture is proposed by Robert C. Martin, also known as Uncle Bob. This architecture is similar to the Onion, Hexagonal, Screaming, and DCI architectures. Though these architectures all vary somewhat in their details, they are very similar. They all have the same objective, which is the separation of concerns. They all achieve this separation by dividing the software into layers.



The value it can provide

- An effective testing strategy that follows the testing pyramid

VIPUL RAJPUT

- Frameworks are isolated in individual modules. When (not if) we change our mind, we only have to make a change in one place. The app has use cases rather than being tied to a CRUD system
- Screaming architecture a.k.a. it screams its intended usage. When you look at the package structure, you get a feel for what the application does rather than seeing technical details
- All business logic is in a use case, so it's easy to find and not duplicated anywhere else
- Hard to do the wrong thing because modules enforce compilation dependencies.
- If you try to use something that you're not meant to, the app doesn't compile
- It is always ready to deploy by leaving the wiring up of the object for last. Or by using feature flags, so we get all the benefits of continuous integration

he rules are driven by The Dependency Rule, which states that:

...source code dependencies can only point inwards. Nothing in an inner circle can know anything at all about something in an outer circle. In particular, the name of something declared in an outer circle must not be mentioned by the code in the an inner circle. That includes, functions, classes. variables, or any other named software entity.

Finally, when obeying this rule and using this architecture it is proposed that:

By separating the software into layers, and conforming to The Dependency Rule, you will create a system that is intrinsically testable, with all the benefits that implies.

Layers and Organization
The common depiction of clean architecture is a diagram consisting of concentric circular layers, very reminiscent of the onion architecture, which is not a surprise. The idea here is that the inner layers are high-level, abstract policies; the outer layers are technical implementation details.

The proposed layers are

- Entities. Here should live the business objects of your application, generally called "entities," in DDD lingo.

VIPUL RAJPUT

- Use cases. In this layer reside the use cases; in short, we could say that these are objects that represent an action a user can perform in the application.
- Interface adapters. This layer contains code whose goal is basically to provide a bridge between the outside world and the immaculate world inhabited by the use cases and entities. Models, views, presenters, and repository implementations all should go here.
- Frameworks and drivers. Finally, we have the layer that basically represents external agents: the web, the database, etc.

ROUTING AND SWITCHING

The way a network operates is to connect computers and peripherals using two pieces of equipment - switches and routers. These two let the devices connected to your network talk with each other as well as talk to other networks.

Though they look quite similar, routers and switches perform very different functions in a network:

Switches are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers and servers, creating a network of shared resources. The switch would serve as a controller, allowing the various devices to share information and talk to each other. Through information sharing and resource allocation, switches save you money and increase productivity.
There are two basic types of switches: managed and unmanaged.

- An unmanaged switch works out of the box and does not allow you to make changes. Home-networking equipment often will have unmanaged switches.
- A managed switch allows you access to program it. This provides greater flexibility because the switch can be monitored and adjusted locally or remotely to give you control on how traffic travels over the network and who has access to your network.

Routers are used to tie multiple networks together. For example, you would use a router to connect your networked computers to the Internet and thereby share an Internet connection among many users. The router will act as a dispatcher, choosing the best route for your information to travel so that you receive it quickly.

VIPUL RAJPUT

Routers analyze the data being sent over a network, change how it is packaged and send it to another network or over a different type of network. They connect your business to the outside world, protect your information from security threats, and can even decide which computers get priority over others.

LAYER-2 AND LAYER-3 SWITCHING

Layer 2 switches are frequently installed in the enterprise for high-speed connectivity between end stations at the data link layer. Layer 3 switches are a relatively new phenomenon, made popular by (among others) the trade press. This article details some of the issues in the evolution of Layer 2 and Layer 3 switches. We hypothesize that that the technology is evolutionary and has its origins in earlier products.

A **Layer 2** switch does switching only. This means that it uses MAC addresses to switch the packets from a port to the destination port (and only the destination port). It therefore maintains a MAC address table so that it can remember which ports have which MAC address associated. Bridging technology has been around since the 1980s (and maybe even earlier). Bridging involves segmentation of local-area networks (LANs) at the Layer 2 level. A multiport bridge typically learns about the Media Access Control (MAC) addresses on each of its ports and transparently passes MAC frames destined to those ports. These bridges also ensure that frames destined for MAC addresses that lie on the same port as the originating station are not forwarded to the other ports. For the sake of this discussion, we consider only Ethernet LANs. Layer 2 switches effectively provide the same functionality.

VIPUL RAJPUT

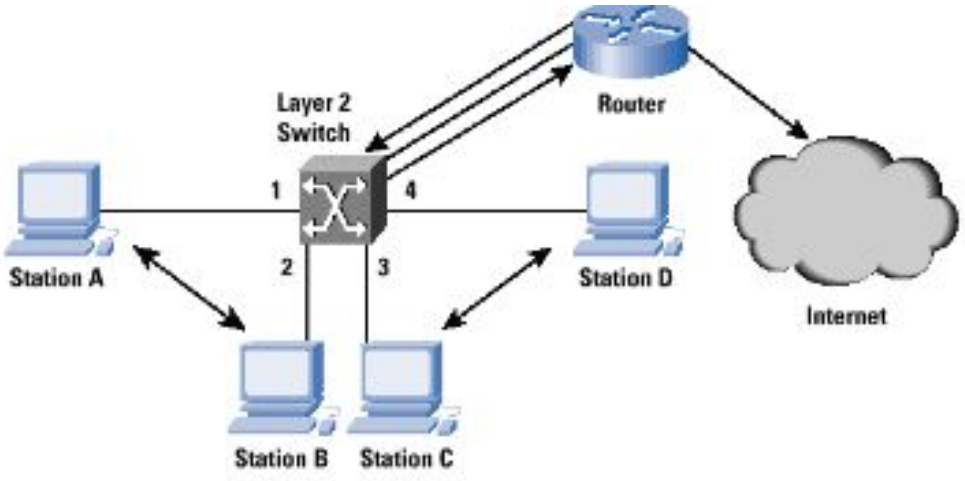


Figure 1: Layer 2 switch with External Router for Inter-VLAN traffic and connecting to the Internet

A **Layer 3** switch also does switching exactly like a L2 switch. The L3 means that it has an identity from the L3 layer. Practically this means that a L3 switch is capable of having IP addresses and doing routing. For intra-VLAN communication, it uses the MAC address table. Layer 3 switching is a relatively new term, which has been extended by a numerous vendors to describe their products. For example, one school uses this term to describe fast IP routing via hardware, while another school uses it to describe Multi Protocol Over ATM (MPOA). For the purpose of this discussion, Layer 3 switches are superfast rout-ers that do Layer 3 forwarding in hardware. In this article, we will mainly discuss Layer 3 switching in the context of fast IP routing, with a brief discussion of the other areas of application. To summarize, Layer 3 switches are routers with fast forwarding done via hardware. IP forwarding typically involves a route lookup, decrementing the Time To Live (TTL) count and recalculating the checksum, and forwarding the frame with the appropriate MAC header to the correct output port. Lookups can be done in hardware, as can the decrementing of the TTL and the recalculation of the checksum. The routers run routing protocols such as Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) to communicate with other Layer 3 switches or routers and build their routing tables. These routing tables are looked up to determine the route for an incoming packet.

VIPUL RAJPUT

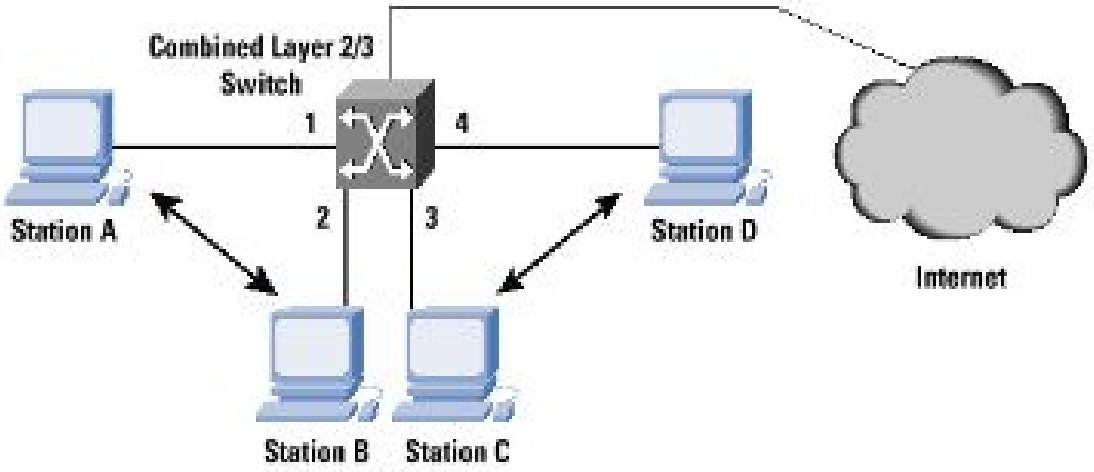


Figure 2: Combined Layer2/Layer3 Switch connecting directly to the Internet

Layer 2 Switch	Layer 3 Switch
Switching operates at the Layer 2 of the OSI Reference Model.	Layer 3 switches do both switching as well as routing.
It uses MAC addresses to facilitate communication within devices from the same network.	It uses IP addresses to link different subnets together using dynamic routing protocols.
It is a single broadcast domain.	It is a multiple broadcast domain.
Devices can only communicate within the same network.	Devices can communicate within or outside the networks.
Switching at Layer 2 is quite fast as they do not look at the Layer 3 portion of the data packets.	It takes time to examine data packets before sending them to their destination.

ROUTING

To summarize, Layer 3 switches are routers with fast forwarding done via hardware. IP forwarding typically involves a route lookup, decrementing the Time To Live (TTL) count and recalculating the checksum, and forwarding the frame with the appropriate MAC header to the correct output port. Lookups can be done in hardware, as can the decrementing of the TTL and the recalculation of the checksum. The routers run routing protocols such as Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) to communicate with other

VIPUL RAJPUT

Layer 3 switches or routers and build their routing tables. These routing tables are looked up to determine the route for an incoming packet.

In general, routing involves the network topology, or the setup of hardware, that can effectively relay data. Standard protocols help to identify the best routes for data and to ensure quality transmission. Individual pieces of hardware such as routers are referred to as "nodes" in the network. Different algorithms and protocols can be used to figure out how to best route data packets, and which nodes should be used. For example, some data packets travel according to a distance vector model that primarily uses distance as a factor, whereas others use Link-State Protocol, which involves other aspects of a "best path" for data.
Data packets are also made to give networks information. Headers on packets provide details about origin and destination. Standards for data packets allow for conventional design, which can help with future routing methodologies. As the world of digital technology evolves, routing will also evolve according to the needs and utility of a particular network.

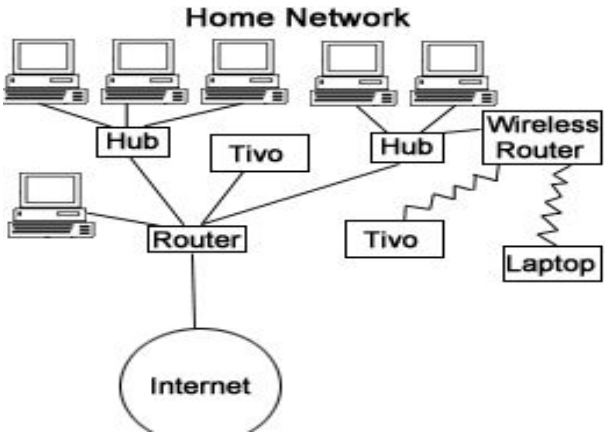


Figure 3: Routing

DHCP

The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default gateway, and other IP parameters. [1]

When a DHCP-configured client (be it a computer or any other network aware device) connects to a network, the DHCP client

VIPUL RAJPUT

sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other TCP/IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.

DHCP provides three modes for allocating IP addresses. The best-known mode is dynamic, in which the client is provided a "lease" on an IP address for a period of time. Depending on the stability of the network, this could range from hours (a wireless network at an airport) to months (for desktops in a wired lab). At any time before the lease expires, the DHCP client can request renewal of the lease on the current IP address. A properly-functioning client will use the renewal mechanism to maintain the same IP address throughout its connection to a single network, otherwise it may risk losing its lease while still connected, thus disrupting network connectivity while it renegotiates with the server for its original or a new IP address.

The two other modes for allocation of IP addresses are automatic (also known as DHCP Reservation), in which the address is permanently assigned to a client, and manual, in which the address is selected by the client (manually by the user or any other means) and the DHCP protocol messages are used to inform the server that the address has been allocated.

What is Access Point?

VIPUL RAJPUT

In a wireless local area network (WLAN), an access point is a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each access point can serve multiple users within a defined network area; as people move beyond the range of one access point, they are automatically handed over to the next one. A small WLAN may only require a single access point; the number required increases as a function of the number of network users and the physical size of the network.

An access point is a wireless network device that acts as a portal for devices to connect to a local area network. Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it.

A high-speed Ethernet cable runs from a router to an access point, which transforms the wired signal into a wireless one. Wireless connectivity is typically the only available option for access points, establishing links with end-devices using Wi-Fi.

What is wireless router?

A wireless router connects a group of wireless stations to an adjacent wired network. Conceptually, a wireless router is a wireless AP combined with an Ethernet router. A wireless router forwards IP packets between your wireless subnet and any other subnet.

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network . It can function in a wired LAN (local area network), in a wireless-only LAN (WLAN), or in a mixed wired/wireless network, depending on the manufacturer and model.

A router is a network device that serves two primary functions: (1) it connects multiple computers, phones, tablets, or other devices to form a managed local area network, and (2) it provides Internet access to all of the compatible devices that are connected to the router. A local area network (LAN) can be set up by simply deploying a router and connecting one or several devices to it. Modern routers allow users to connect devices both via Ethernet cables or wirelessly (using Wi-Fi).

Why and how to configure wireless router?

VIPUL RAJPUT

Configure your router to make your network complete. You need to configure the router so that it can communicate with your network components. Fortunately, the configuration steps are rather straightforward.

After you connect the router to the network, or simply turn on a wireless router, you connect to the router by using your PC's Web browser, such as Internet Explorer. The documentation that came with the router gives you the router's Web page address. Usually, it's numerical, such as http://192.168.0.1/

After accessing the router, and (optionally) entering its password, you see a Web page displayed. The Web page is really the router's configuration program. Follow the directions that came with the device for the basic configuration of the router. In addition to those directions, consider the following points:

- Enable the router's firewall. You don't need to adjust the firewall; most routers set things up just as you need them.
- Set a Service Set Identifier, or SSID, for your wireless network. This is the name by which the wireless network is known.
- Set the encryption for the network, known as the WEP, or Wired Equivalent Privacy. Make sure that you note the password! It's a long string of numbers and letters, and you must enter it exactly to access the network.
- You may hear or read that the password is optional, but generally, it's not. Don't compromise your network by omitting the password. In fact, Windows may not even connect to a wireless network that lacks a password.
- (Optional) Configure the base station to allow connections only from known computers. You specify this setting by listing the MAC address of the wireless Ethernet adapter in each PC.
- Tell the wireless router to provide IP addresses dynamically for all computers on the network. This is also known as Dynamic Host Configuration Protocol (DHCP).

VIPUL RAJPUT