2. Network Installation and Configuration

2.1 Given a scenario, install and configure routers and switches.

The most common configuration problems arise out of switching loops, bad cables, wrong switch/router port configuration, LAN segmentation, wrong IP subnetting, etc. In addition to the physical connections, it is important to configure your network properly. Protocols such as NAT, PAT, VLAN, PoE , QoS are widely used in configuring a network. Hence. it is important to know the types of problems that might occur due to misconfiguration.
and QoS will give you options within your net work

Some of these protocols have been explained in the following sections:

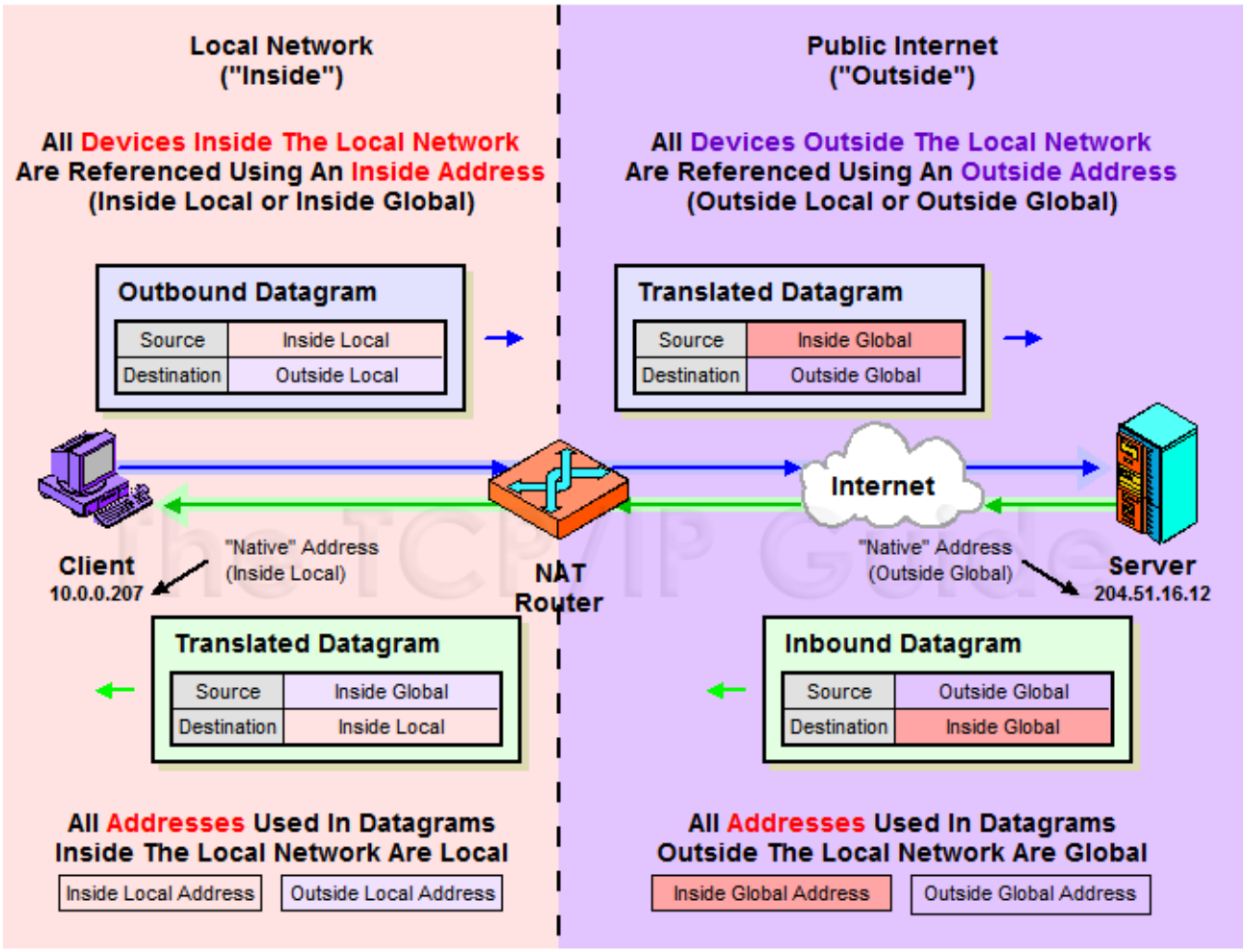
NAT – Network Address Translation.

NAT is very widely used in computer networking. The NAT router has the job of translating the inside network IP addresses to the outside global IP address network (the Internet) enabling inside devices to talk to outside devices and vice-verse, but inside devices can only use addressing consistent with the local network addressing scheme. Similarly, outside devices cannot use local addressing. Thus, both inside and outside devices can be referred to with local or global address versions.

- Address Classification – Initially, it would be a little confusing to understand the terminology like Inside, Outside, Local, and Global. The figure attempts to clear the concepts associated with NAT terminology.

    - Inside Global : An inside address seen from the outside. This is a global, publicly-routable IP address used to represent an inside device to the outside world. In a NAT configuration, inside global addresses are those “real” IP addresses assigned to an organization for use by the NAT router.
    - Inside Local - An address of a device on the local network, expressed using its normal local device representation. So for example, if we had a client on a network using the 10.0.0.0 private address block, and assigned it address 10.0.0.207, this would be its inside local address.
    - Outside Global : An address of an external (public Internet) device as it is referred to on the global Internet. This is basically a regular, publicly-registered address of a device on the Internet. In the example above, 204.51.16.12 is an outside global address of a public server.
    - Outside Local : An address of an external device as it is referred to by devices on the local network.
    - NAT Pool : A pool of IP addresses to be used as inside global or outside local addresses in translations.

    The figure provides a conceptual understanding of the Inside and Outside networks and addressing.



There are different ways that a NAT be configured on a network. These are:

- Static Nat: Maps an unregistered IP address to registered IP (globally unique) addresses on one-to-one basis.
- Dynamic NAT:Maps an unregistered IP address to a registered (globally unique) IP address from a group of registered (globally unique) IP addresses.
- Overloading: A special case of dynamic NAT that maps multiple unregistered IP addresses to a single registered (globally unique) IP address by using different port numbers. Dynamic NAT with overloading is also known also as **PAT (Port Address Translation)**.
- Overlapping: This occurs when your internal IP addresses belong to global IP address range that belong to another network

- Configuring NAT

When configuring NAT, NAT should be enabled on at least one inside and one outside interface.

Typical configuration commands on Cisco router are given below.

1. The command for enabling NAT on inside interface is:

R1(config-if)#ip nat inside

2. The command for enabling NAT on the outside interface is:

R1(config-if)#ip nat outside

Remember to enter into appropriate configuration modes before entering the commands. Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface.

VLAN and VTP Configuration and Troubleshooting:

When you are configuring VLANs and trunks on a switched network, the following types of configuration errors are most likely to be encountered:

1. Native VLAN mismatches
2. Trunk mode mismatches
3. VLANs and IP Subnets config issues
4. Allowed VLANs on trunks – Configuring a trunk route for allowed VLANs.

Things to remember in configuring VTP:

1. VTP is a Layer 2 messaging protocol. It carries configuration information throughout a single domain

2. VTP Modes are

Server : Create, modify, or delete VLANs (This is the deafult vtp mode on a switch)
Client : Can't create, change, or delete VLANs
Transparent : Used when a switch is not required to participate in VTP, but only pass the information to other switches

3. VTP domain is common to all switches participating in VTP

4. Pruning is a technique where in VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

5. Configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each time the VTP device undergoes a VLAN change, the config revision is incremented by one.

Typical VTP Configuration commands on a Cisco switch are given below:

SW1#vlan database
SW1(vlan)#vtp mode (Server/Client/Transparent)
SW1(vlan)#vtp domain <name>
SW1(vlan)#vtp password <password>
SW1(vlan)#vtp pruning